Agrégation interne de mathématiques

Mathématiques générales 2023

3 septembre 2023

Vrai-Faux

(1) (a) Faux. Si $n > 1$, l'anneau $\mathbf{Z}/p^n\mathbf{Z}$ n'est pas réduit (l'image x de p dans $\mathbf{Z}/p^n\mathbf{Z}$ est non nulle mais $x^n = 0$) : l'anneau $\mathbf{Z}/p^n\mathbf{Z}$ n'est donc pas un corps dans ce cas. En revanche, c'est un corps lorsque $n = 1$.

Remarque. Le mieux est en fait de donner un exemple explicite : 2 est diviseur de zéro dans $\mathbf{Z}/4\mathbf{Z}$, qui n'est donc pas un corps.

(b) Faux. La classe $\overline{2}$ de 2 dans $\mathbf{Z}/7\mathbf{Z}$ vérifie $\overline{2}^3 = 1$: le sous-groupe de $(\mathbf{Z}/7\mathbf{Z})^\times$ engendré par $\overline{2}$ est d'ordre 3, il est donc strict (car $\#(\mathbf{Z}/7\mathbf{Z})^\times = 6$), donc $\overline{2}$ n'engendre pas $(\mathbf{Z}/7\mathbf{Z})^\times$.
(c) Vrai. On a $\#(\mathbf{Z}/9\mathbf{Z})^\times = \varphi(9) = 6$. Si $a \in \mathbf{Z}$, notons $\overline{a}$ son image dans $\mathbf{Z}/9\mathbf{Z}$. Comme $\mathsf{pgcd}(2, 9) = 1$, on a $\overline{2} \in (\mathbf{Z}/9\mathbf{Z})^\times$: d'après le théorème de Lagrange, l'ordre de $\overline{2}$ dans le groupe multiplicatif $(\mathbf{Z}/9\mathbf{Z})^\times$ divise 6. On a $\overline{2}^2 = \overline{4} \neq \overline{1}$, $\overline{2}^3 = -\overline{1} \neq \overline{1}$: cet ordre ne divise ni 2, ni 3, il vaut donc nécessairement 6, de sorte que $\overline{2}$ est un générateur de $(\mathbf{Z}/9\mathbf{Z})^\times$.
(d) Faux. Prenons $a = d = 5$ et $b = c = 0$. La matrice $M = \mathrm{diag}(5, 5) \in \mathsf{M}_2(\mathbf{Z})$ est inversible dans $\mathsf{M}_2(\mathbf{R})$ (on a $\det(M) = 25 \in \mathbf{R}^\times$), mais son image $\overline{M}$ dans $\mathsf{M}_2(\mathbf{Z}/5\mathbf{Z})$ est nulle, donc non inversible.
(e) Vrai. Si $x \in K \setminus \{0\}$, alors x est inversible dans K : on dispose de $x^{-1} \in K$. En supposant μ unitaire (ce qui semble implicite dans l'énoncé), on a $\mu(x)\mu(x^{-1}) = \mu(xx^{-1}) = \mu(1_K) = 1_L$, ce qui montre que $\mu(x) \neq 0$. Il en résulte que $\mathrm{Ker}(\mu) = \{0\}$, et donc que μ est injectif.

Remarque. On peut invoquer le fait que les seuls idéaux du corps K sont $\{0\}$ et K, mais la rédaction qui précède est préférable : elle est aussi efficace mais ne requiért aucun prérequis (en fait c'est l'argument qui sert à prouver l'énoncé sur les idéaux de K).

Exercice 1

(2) Supposons la famille $(x_1, \dots, x_{k+1})$ liée : il existe $\lambda_0, \dots, \lambda_{k+1} \in \mathbf{K}$ non tous nuls tels que $\sum_{i=1}^{k+1} \lambda_i x_i = 0$. Comme $(x_1, \dots, x_k)$ est libre, on a $\lambda_{k+1} \neq 0$: on peut écrire $x_{k+1} = -\sum_{i=1}^{k} \lambda_{k+1}^{-1}\lambda_i x_i$, ce qui montre que x_{k+1} est combinaison linéaire de $x_1, \dots, x_k$. Réciproquement, supposons que x_{k+1} soit combinaison linéaire de $x_1, \dots, x_k$: il existe $\lambda_1, \dots, \lambda_k \in \mathbf{K}$ tels que $x_{k+1} = \sum_{i=1}^{k} \lambda_i x_i$: en posant $\lambda_{k+1} = -1$, on a $\sum_{i=1}^{k+1} \lambda_i x_i = 0$: comme $\lambda_{k+1} \neq 0$, cela montre que la famille $(x_1, \dots, x_{k+1})$ est liée.

(3) On procède par récurrence sur $k \in \{1, \dots, n\}$. Un famille libre à un élément n'est autre que la donnée d'un vecteur non nul : il y a $\#E - 1 = \#\mathbf{K}^n - 1 = p^n - 1$ tels vecteurs. Supposons $k \in \{1, \dots, n-1\}$. D'après la question précédente, la donnée d'une famille libre $(x_1, \dots, x_{k+1})$ est équivalente à celle d'une famille libre $(x_1, \dots, x_k)$ (il y en a $(p^n - 1)(p^n - p) \cdots (p^n - p^{k-1})$ en vertu de l'hypothèse de récurrence) et d'un vecteur x_{k+1} qui n'est pas combinaison linéaire de $(x_1, \dots, x_k)$, *i.e.* qui n'appartient pas à $\mathrm{Vect}(x_1, \dots, x_k)$. Comme $\mathrm{Vect}(x_1, \dots, x_k) \simeq \mathbf{K}^k$ est de cardinal $\#\mathbf{K}^k = p^k$, il y a $\#E - p^k = p^n - p^k$ tels vecteurs. Finalement, il y a $(p^n - 1)(p^n - p) \cdots (p^n - p^{k-1})(p^n - p^k)$ telles familles.

(4) La donnée d'un élément de $\mathsf{M}_n(\mathbf{K})$ équivaut à celle celle de ses vecteurs colonnes (*i.e.* à de l'image de la base canonique par l'endomorphisme de $\mathbf{K}^n$ associé). L'élément appartient à $\mathsf{GL}_n(\mathbf{K})$ si et seulement si la famille des vecteurs colonnes est une base de $\mathbf{K}^n$. Il y a donc une bijection entre $\mathsf{GL}_n(\mathbf{K})$ et l'ensemble des bases de $\mathbf{K}^n$, ce qui montre que $\#\,\mathsf{GL}_n(\mathbf{K}) = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$.

Remarque. Le groupe $\mathsf{GL}_n(\mathbf{K})$ agit simplement transitivement sur l'ensemble des bases de $\mathbf{K}^n$ (étant donné deux bases de $\mathbf{K}^n$, il existe un unique élément de $\mathsf{GL}_n(\mathbf{K})$ qui envoie la première sur la deuxième). Le choix de n'importe quelle base (ci-dessus on a pris la base canonique) fournit une bijection de $\mathsf{GL}_n(\mathbf{K})$ sur l'ensemble des base de $\mathbf{K}^n$.

Exercice 2

(5) (a) On a $\varphi(1) = 1$. Supposons $i \in \mathbf{Z}_{>0}$. Les éléments $x \in \{1, \dots, p^i\}$ non premiers à p^i sont ceux divisibles par p, *i.e.* de la forme pk avec $k \in \{1, \dots, p^{i-1}\}$: il y en a p^{i-1}, d'où $\varphi(p^i) = p^i - p^{i-1}$.

On a $\mathscr{D}_{p^k} = \{p^i\}_{0 \leq i \leq k}$ donc $f(p^k) = \varphi(1) + \sum_{i=1}^{k} \varphi(p^i) = 1 + \sum_{i=1}^{k} \left(p^i - p^{i-1}\right) = p^k$ (somme télescopique).

(b) Si $d_1 \mid m_1$ et $d_2 \mid m_2$, alors $d_1 d_2 \mid m_1 m_2$, donc l'application P est bien définie. Comme $\mathsf{pgcd}(m_1, m_2) = 1$, il existe $r \in \mathbf{N}$, $p_1, \dots, p_r$ des entiers premiers deux à deux distincts, $a_1, \dots, a_r \in \mathbf{N}_{>0}$ et $s \in \{0, \dots, r\}$ tels que $m_1 = p_1^{a_1} \cdots p_s^{a_s}$ et $m_2 = p_{s+1}^{a_{s+1}} \cdots p_r^{a_r}$. Si $d \in \mathscr{D}_{m_1 m_2}$, il existe $\alpha_1, \dots, \alpha_r \in \mathbf{N}$ tels que $0 \leq \alpha_i \leq a_i$ pour tout $i \in \{1, \dots, r\}$ et $d = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Si $d_1 \in \mathscr{D}_{m_1}$ et $d_2 \in \mathscr{D}_{m_2}$ sont tels que $d_1 d_2 = d$, l'unicité de la factorisation en produit de nombres dans $\mathbf{Z} \setminus \{0\}$ implique qu'on a nécessairement $d_1 = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ et $d_2 = p_{s+1}^{\alpha_{s+1}} \cdots p_r^{\alpha_r}$. Cela montre que P est bijective.

Remarque. Autres approches.
• **Injectivité.** Si $(d_1, d_2), (d_1', d_2') \in \mathcal{D}_{m_1} \times \mathcal{D}_{m_2}$ sont tels que $P(d_1, d_2) = P(d_1', d_2')$, on a $d_1 \mid m_1$ et $d_2' \mid m_2$: comme $\mathsf{pgcd}(m_1, m_2) = 1$, on a *a fortiori* $\mathsf{pgcd}(d_1, d_2') = 1$. On a $d_1 \mid d_1 d_2 = d_1' d_2'$: le lemme de Gauss implique que $d_1 \mid d_1'$. Symétriquement, $d_1' \mid d_1$, et donc $d_1 = d_1'$. On a de même $d_2 = d_2'$, et P est injective.
• **Surjectivité.** Soit $m \in \mathcal{D}_{m_1 m_2}$. Posons $d_1 = \mathsf{pgcd}(m, m_1) \in \mathcal{D}_{m_1}$ et $d_2 = \frac{m}{d_1} \in \mathbf{N}_{>0}$: on a $\mathsf{pgcd}\left(d_2, \frac{m_1}{d}\right) = 1$. Comme $m \mid m_1 m_2$, on a $d_2 \mid \frac{m_1}{d_1} m_2$, d'où $d_2 \in \mathcal{D}_{m_2}$ en vertu du lemme de Gauss, ce qui montre que $m = d_1 d_2 = P(d_1, d_2)$.
On peut aussi raisonner par cardinalité. Reprenons les factorisations de m_1 et m_2 ci-dessus. Un entier $d \in \mathbf{N}_{>0}$ divise $m_1 m_2$ si et seulement si $d = p_1^{b_1} \cdots p_r^{b_r}$ avec $b_i \in \{0, \dots, a_i\}$ pour tout $i \in \{1, \dots, r\}$. Cela montre que $\#\mathcal{D}_{m_1 m_2} = \prod_{i=1}^{r} (1 + a_i)$. On a de même $\#\mathcal{D}_{m_1} = \prod_{i=1}^{s} (1 + a_i)$ et $\#\mathcal{D}_{m_2} = \prod_{i=s+1}^{r} (1 + a_i)$, ce qui montre que $\#\mathcal{D}_{m_1 m_2} = \#\mathcal{D}_{m_1} \#\mathcal{D}_{m_2}$, et conclut.

(c) Observons que si $d_1 \in \mathscr{D}_{m_1}$ et $d_2 \in \mathscr{D}_{m_2}$, on a $\mathsf{pgcd}(d_1, d_2) = 1$ (parce que $\mathsf{pgcd}(m_1, m_2) = 1$), ce qui implique que $\varphi(d_1 d_2) = \varphi(d_1)\varphi(d_2)$ comme rappelé dans le préambule de l'énoncé (cela résulte du théorème des restes chinois). D'après la question précédente, on a donc

$$\begin{aligned} f(m_1 m_2) = \sum_{(d_1, d_2) \in \mathscr{D}_{m_1} \times \mathscr{D}_{m_2}} \varphi(d_1 d_2) &= \sum_{d_1 \in \mathscr{D}_{m_1}} \sum_{d_2 \in \mathscr{D}_{m_2}} \varphi(d_1)\varphi(d_2) \\ &= \Big(\sum_{d_1 \in \mathscr{D}_{m_1}} \varphi(d_1) \Big) \Big(\sum_{d_2 \in \mathscr{D}_{m_2}} \varphi(d_2) \Big) = f(m_1) f(m_2). \end{aligned}$$

(d) Écrivons $n = p_1^{k_1} \cdots p_r^{k_r}$ avec $r \in \mathbf{N}$, $p_1, \dots, p_r$ premiers deux à deux distincts et $k_1, \dots, k_r \in \mathbf{N}$. D'après la question (5) (a), on a $f(p_i^{k_i}) = p_i^{k_i}$ pour tout $i \in \{1, \dots, r\}$: comme $p_1^{k_1}, \dots, p_r^{k_r}$ sont deux à deux premiers entre eux, la question précédente implique que $f(n) = f\left(p_1^{k_1}\right) \cdots f\left(p_r^{k_r}\right) = p_1^{k_1} \cdots p_r^{k_r} = n$.

(6) (a) Si $x \in \mathbf{K}^\times$, le théorème de Lagrange implique que l'ordre de x dans le groupe $\mathbf{K}^\times$ divise $\#\mathbf{K}^\times = c$. Cela montre que $\mathbf{K}^\times = \bigsqcup_{d \in \mathscr{D}_c} \Omega_d$, où Ω_d désigne l'ensemble des éléments d'ordre d dans $\mathbf{K}^\times$. La réunion étant disjointe, on a donc $c = \#\mathbf{K}^\times = \sum_{d \in \mathscr{D}_c} \#\Omega_d = \sum_{d \in \mathscr{D}_c} N(d)$.

(b) (i) Si $h \in H$, il existe $k \in \mathbf{Z}$ tel que $h = x^k$, donc $h^d = x^{kd} = 1$. Cela montre que les éléments de H sont tous des racines du polynôme $X^d - 1$. Dans le corps $\mathbf{K}$, ce dernier a au plus d racines : comme $\#H = d$ (par définition de l'ordre), cela montre que $X^d - 1$ est scindé dans $\mathbf{K}[X]$ et que ses racines, simples, sont précisément les éléments de H. Si $y \in \mathbf{K}^\times$ est d'ordre d, alors $y^d = 1$, donc y est racine du polynôme $X^d - 1$, de sorte que $y \in H$ en vertu de ce qui prècède.
(ii) Si $d \in \mathscr{D}_c$ est tel que $N(d) \neq 0$, alors $\mathbf{K}^\times$ contient un élément x d'ordre d. D'après la question précédente, tous les éléments d'ordre d appartiennent à $H = \langle x \rangle \simeq \mathbf{Z}/d\mathbf{Z}$. Comme le groupe H a $\varphi(d)$ générateurs (*i.e.* éléments d'ordre d), cela montre que $N(d) = \varphi(d)$ dans ce cas. Finalement, on a montré que $N(d) \in \{0, \varphi(d)\}$, en particulier $N(d) \leq \varphi(d)$.
(c) D'après les questions (5) et (6) (a), on a $0 = f(c) - c = \sum_{d \in \mathscr{D}_c} (\varphi(d) - N(d))$, et $\varphi(d) - N(d) \in \mathbf{N}$ pour tout $d \in \mathscr{D}_c$ en vertu de la question précédente. Une somme d'entiers naturels est nulle si et seulement si chacun des entiers est nul : cela montre que $N(d) = \varphi(d)$ pour tout $d \in \mathscr{D}_c$. En particulier, on a $N(c) = \varphi(c) > 0$: le groupe $\mathbf{K}^\times$ contient un élément d'ordre c. Comme il est d'ordre c, il est cyclique.

Problème
I. Valuation et valeur absolue p-adiques

I.A. Définition de la valuation

(7) On a $|n| < 2^n \leq p^{|n|}$: cela montre que l'ensemble $\{i \in \mathbf{N}\,;\, p^i \mid n\}$ est majoré. Il est non vide (il contient 0) : il a donc un plus grand élément k. On a alors $p^k \mid n$ et $p^{k+1} \nmid n$.

(8) Par définition, on peut écrire $a = p^{v_p(a)}a'$ et $b = p^{v_p(b)}b'$ avec $a', b' \in \mathbf{Z}\setminus\{0\}$ non divisibles par p, *i.e.* premiers à p. On a $ab = p^{v_p(a)+v_p(b)}a'b'$: comme $a'b'$ est premier à p, cela implique que $v_p(ab) = v_p(a)+v_p(b)$.

(9) On a $ad = bc$, donc $v_p(a)+v_p(d) = v_p(b)+v_p(c)$ (*cf* question précédente), soit $v_p(a)-v_p(b) = v_p(c)-v_p(d)$.

(10) Écrivons $r = \frac{a}{b}$ et $s = \frac{c}{d}$ avec a, b, c, d des entiers relatifs non nuls. On a $rs = \frac{ac}{bd}$, donc

$$v_p(rs) = v_p(ac) - v_p(bd) = (v_p(a) + v_p(c)) - (v_p(b) + v_p(d)) = v_p(a) - v_p(b) + v_p(c) - v_p(d) = v_p(r) + v_p(s)$$

en vertu de de la question (8).

(11) Soit $d \in \mathbf{N}_{>0}$ tel que $dr, ds \in \mathbf{Z}$ un dénominateur commun. On peut écrire $dr = p^{v_p(dr)}a$ et $ds = p^{v_p(ds)}b$ avec a, b entiers non divisibles par p. Quitte à échanger r et s, on peut supposer que $v_p(r) \leq v_p(s)$, d'où $v_p(dr) = v_p(r) + v_p(d) \leq v_p(s) + v_p(d) = v_p(ds)$. On a alors

$$d(r-s) = p^{v_p(dr)}a - p^{v_p(ds)}b = p^{v_p(dr)}\big(a - p^{v_p(ds)-v_p(dr)}b\big)$$

ce qui implique que $v_p(dr) \leq v_p(d(r-s))$ *i.e.* $v_p(r) = v_p(dr) - v_p(d) \leq v_p(d(r-s)) - v_p(d) = v_p(r-s)$.

(12) Si $u \in \mathbf{Z}\cup\{+\infty\}$, on a $u + \infty = +\infty$ et $u \leq +\infty$.
• Soient $r, s \in \mathbf{Q}$. Si $rs \neq 0$, la question (10) montre que $v_p(rs) = v_p(r) + v_p(s)$. Si $s = 0$, on a $rs = 0$, donc $v_p(rs) = v_p(0) = +\infty$ et $v_p(r) + v_p(s) = v_p(r) + \infty = +\infty$, de sorte que $v_p(rs) = v_p(r) + v_p(s)$. De façon symétrique, l'égalité est aussi valable si $r = 0$.
• Soient $r, s \in \mathbf{Q}$. Si $r = s$, on a $v_p(r-s) = v_p(0) = +\infty \geq \min\{v_p(r), v_p(s)\}$. Si $s = 0$, on a $v_p(r-s) = v_p(r)$ et $\min\{v_p(r), v_p(s)\} = \min\{v_p(r), +\infty\} = v_p(r)$: on a bien $v_p(r-s) \geq \min\{v_p(r), v_p(s)\}$ dans ce cas. Il en est de même si $s = 0$. Le cas où r, s et $r-s$ son non nuls est couvert par la question (11).

I.B. Étude de $v_p(n!)$

(13) On a $E_k = \{p^k m\}_{\substack{m\in\mathbf{N}_{>0}\\ p^k m\leq n}} = \{p^k m\}_{m\in\{1,2,\ldots,\lfloor n/p^k\rfloor\}}$. Cela montre que $\#E_k = \left\lfloor \frac{n}{p^k} \right\rfloor$.

(14) On a $i \in E_k \Leftrightarrow k \leq v_p(i) \Leftrightarrow k \in \{1, \ldots, v_p(i)\}$ (si on se restreint aux entiers k non nuls, ce qui n'est pas complètement clair dans l'énoncé, mais est plus commode pour la suite), d'où $\#\{k \in \mathbf{N}_{>0}\,;\, i \in E_k\} = v_p(i)$. Il en résulte que

$$v_p(n!) = \sum_{i=1}^{n} v_p(i) = \sum_{i=1}^{n} \#\{k \in \mathbf{N}_{>0}\,;\, i \in E_k\} = \sum_{i=1}^{n}\sum_{k=1}^{\infty} \mathbf{1}_{i\in E_k} = \sum_{k=1}^{\infty} \#E_k = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Remarque. La somme qui précède n'a qu'un nombre fini de termes non nuls, parce que $\lfloor \frac{n}{p^k} \rfloor = 0$ dès que $n < p^k$, *i.e.* dès que $k > \frac{\ln(n)}{\ln(p)}$.

(15) D'après la question précédente, on a $v_2(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{2^k} \right\rfloor$ et $v_5(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{5^k} \right\rfloor$, d'où $v_2(n!) \geq v_5(n!)$ pour tout $n \in \mathbf{N}_{>0}$. Il en résulte que le nombre de zéros à la fin de l'écriture décimale de $n!$ est égal à $v_5(n!)$. Ici $v_5(100!) = \sum_{k=1}^{\infty} \left\lfloor \frac{100}{5^k} \right\rfloor = \frac{100}{5} + \frac{100}{25} = 24$: il y a donc 24 zéros à la fin de l'écriture décimale de 100!.

(16) On a $\left\lfloor \frac{n}{p^k} \right\rfloor \leq \frac{n}{p^k}$ pour tout $k \in \mathbf{N}_{>0}$, donc $v_p(n!) \leq n\sum_{k=1}^{\infty} \frac{1}{p^k} = n\frac{1/p}{1-1/p} = \frac{n}{p-1}$ (somme d'une série géométrique).

Remarque. On peut être un peu plus précis on a $v_p(n!) = \frac{n-s_p(n)}{p-1}$, où $s_p(n)$ est la somme des chiffres de l'écriture de n en base p (ce qui montre qu'en fait, on a toujours $v_p(n!) \leq \frac{n-1}{p-1}$). En effet, écrivons $n = \sum_{i=0}^{\infty} a_i p^i$ avec $a_i \in \{0, \ldots, p-1\}$ pour tout $i \in \mathbf{N}$ et $a_i = 0$ pour $i \gg 0$. On a $\frac{n}{p^k} = \frac{a_0}{p^k} + \cdots + \frac{a_k-1}{p} + \sum_{i\geq k} a_i p^{i-k}$. Comme $0 \leq \frac{a_0}{p^k} + \cdots + \frac{a_k-1}{p} \leq \sum_{i=0}^{k-1} \frac{p-1}{p^i} = 1 - \frac{1}{p^k} < 1$, on a donc $\left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{i\geq k} a_i p^{i-k}$. D'après ce qui précède, cela implique que $v_p(n!) = \sum_{k=1}^{\infty}\sum_{i\geq k} a_i p^{i-k} = \sum_{i=0}^{\infty}\sum_{k=1}^{i} a_i p^{i-k} = \sum_{i=0}^{\infty} a_i \frac{p^i-1}{p-1} = \frac{n-s_p(n)}{p-1}$. On montre cette formule dans le cas particulier où $p = 2$ dans la partie suivante.

I.C. Une caractérisation des puissances de 2

(17) Soit $k = \sum_{i=0}^{\infty} a_i 2^i$ l'écriture de k en base 2 (on a $a_i = 0$ pour $i \gg 0$, de sorte que la somme est finie). Posons $i_0 = \inf\{i \in \mathbf{N}\,;\, a_i = 0\}$. On a donc $k = 1+2+\cdots+2^{i_0-1}+\sum_{i>i_0} a_i 2^i = 2^{i_0}-1+\sum_{i>i_0} a_i 2^i$, d'où $s(k) = i_0 + \sum_{i>i_0} a_i$ et $k+1 = 2^{i_0} + \sum_{i>i_0} a_i 2^i$. Cela implique que $v_2(k+1) = i_0$, et que $s(k+1) = 1 + \sum_{i>i_0} a_i = 1 + s(k) - i_0$, de sorte que $v_2(k+1) = i_0 = s(k) - s(k+1) + 1$.

(18) D'après la question précédente, on a

$$\begin{aligned} v_2(n!) &= \sum_{k=2}^{n} v_2(k) = \sum_{k=2}^{n} (s(k-1) - s(k) + 1) \\ &= \sum_{k=1}^{n-1} s(k) - \sum_{k=2}^{n} s(k) + n - 1 = s(1) - s(n) + n - 1 = n - s(n). \end{aligned}$$

(19) On a $\binom{n}{k} = \frac{n!}{k!(n-k)!}$, donc

$$v_2\big(\tbinom{n}{k}\big) = v_2(n!) - v_2(k!) - v_2((n-k)!) = (n - s(n)) - (k - s(k)) - (n - k - s(n-k)) = s(k) + s(n-k) - s(n)$$

en vertu de la question précédente. Si n est une puissance de 2, on a $s(n) = 1$. Supposons $1 \leq k < n$: on a $k, n-k \in \mathbf{N}_{>0}$, donc $s(k) \geq 1$ et $s(n-k) \geq 1$, ce qui prouve que $v_2\big(\binom{n}{k}\big) \geq 1$, et donc que $\binom{n}{k}$ est un entier pair.

(20) Posons $r = v_2(n)$: on peut écrire $n = 2^r + \sum_{i>r} a_i 2^i$ avec $a_i \in \{0,1\}$ pour tout $i > r$ et $a_i = 0$ si $i \gg 0$. Posons $k = 2^r$: on a $s(n-k) = s(n) - 1$. Comme $s(k) = 1$, cela implique que

$$v_2\big(\tbinom{n}{k}\big) = v_2(n!) - v_2(k!) - v_2((n-k)!) = (n - s(n)) - (k - s(k)) - (n - k - s(n-k)) = s(k) + s(n-k) - s(n) = 0$$

i.e. que $\binom{n}{k}$ est impair. D'après l'hypothèse, cela implique que $k \notin \{1, \ldots, n-1\}$. Comme $k \in \{1, \ldots, n\}$, on a nécessairement $n = k = 2^r$ et n est une puissance de 2.

I.D. Valeur absolue p-adique

(21) Posons $\frac{1}{p^{+\infty}} = 0$: on a $|x|_p = \frac{1}{p^{v_p(x)}}$ pour *tout* $x \in \mathbf{Q}$. On a $v_p(xy) = v_p(x) + v_p(y)$ d'après la question (12), d'où $|xy|_p = \frac{1}{p^{v_p(xy)}} = \frac{1}{p^{v_p(x)+v_p(y)}} = |x|_p \, |y|_p$. De même, on a $v_p(x-y) \geq \min\{v_p(x), v_p(y)\}$, donc

$$|x-y|_p = \tfrac{1}{p^{v_p(x-y)}} \leq \tfrac{1}{p^{\min\{v_p(x), v_p(y)\}}} = \max\big\{\tfrac{1}{p^{v_p(x)}}, \tfrac{1}{p^{v_p(y)}}\big\} = \max\{|x|_p, |y|_p\}.$$

Cela implique que $|x+y|_p \leq \max\{|x|_p, |-y|_p\} = \max\{|x|_p, |y|_p\} \leq |x|_p + |y|_p$ vu que $|-y|_p = |y|_p$ car $v_p(-y) = v_p(y)$ (parce que $v_p(-1) = 0$).

Remarque. Il est utile d'invoquer la question (12) et pas les précédentes, pour pouvoir inclure sans vérifications supplémentaires le cas où $xy = 0$.

(22) On a $d_p(x,z) = |x-z|_p = |x-y+y-z|_p \leq \max\{|x-y|_p, |y-z|_p\} = \max\{d_p(x,y), d_p(y,z)\}$. Cela implique en particulier que $d_p(x,z) \leq d_p(x,y) + d_p(y,z)$ (inégalité triangulaire). Pour montrer que d_p est une distance, il suffit d'observer que $d_p(x,y) = 0 \Rightarrow |x-y|_p = 0 \Rightarrow v_p(x-y) = +\infty \Rightarrow x = y$ (séparation), et que $d_p(x,y) = d_p(y,x)$ parce que $|x-y|_p = |-1|_p \, |y-x|_p = |y-x|_p$ (symétrie) parce que $|-1|_p = 0$.

(23) On a $|p^n|_p = \frac{1}{p^n} \xrightarrow[n\to\infty]{} 0$, ce qui montre que $\lim_{n\to\infty} p^n = 0$ dans l'espace métrique $(\mathbf{Q}, d_p)$.

II. Les entiers p-adiques

II.A. Définition de $\mathbf{Z}_p$

(24) Si $(a_n)_{n\geq 0} \in \mathbf{Z}_p$, on a bien sûr $a_{n+1} \equiv a_n \mod p^{n+1}$ par définition. Réciproquement, soit $(a_n)_{n\geq 0}$ une suite d'entiers tels que $a_n \in \{0, \ldots, p^{n+1}-1\}$ et $a_{n+1} \equiv a_n \mod p^{n+1}$ pour tout $n \in \mathbf{N}$. Soit $n \in \mathbf{N}$. Montrons par récurrence sur $m \geq n$ que $a_m \equiv a_n \mod p^{n+1}$. C'est trivial si $m = n$: supposons $m > n$. Par hypothèse, on a $a_m \equiv a_{m-1} \mod p^m$, donc $a_m \equiv a_{m-1} \mod p^{n+1}$ vu que $m \geq n+1$. Par hypothèse

de récurrence, on a en outre $a_{m-1} \equiv a_n \mod p^{n+1}$: par transitivité, on a donc $a_m \equiv a_n \mod p^{n+1}$, ce qui conclut.

(25) Par hypothèse, il existe $q \in \mathbf{Z}$ tel que $a_{n+1} = qp^{n+1} + a_n$. Comme $a_n \in \{0, \dots, p^{n+1} - 1\}$, cette écriture n'est autre que la division euclidienne de a_{n+1} par p^{n+1}. Par ailleurs, on a aussi $a_{n+1} = u_{n+1}p^{n+1} + \sum_{i=0}^{n} u_i p^i$, et $0 \leq \sum_{i=0}^{n} u_i p^i \leq \sum_{i=0}^{n} (p-1)p^i = p^{n+1} - 1$. Par unicité de la division euclidienne, on a nécessairement $q = u_{n+1}$ et $a_n = \sum_{i=0}^{n} u_i p^i$.

(26) Si un tel k existe, on a $a_n = 0$ (parce que $v_p(a_n) = +\infty$) pour tout $n < k$, et $a_n \neq 0$ (parce que $v_p(a_n) < +\infty$) pour tout $n \geq k$. On a donc nécessairement $k = \min\{n \in \mathbf{N}\,;\, a_n \neq 0\}$, ce qui prouve l'unicité. Montrons l'existence. Vu ce qui précède, posons $k = \min\{n \in \mathbf{N}\,;\, a_n \neq 0\}$; c'est un entier bien défini parce que la suite $(a_n)_{n\geq 0}$ n'est pas nulle par hypothèse. Si $n < k$, on a $a_n = 0$ donc $v_p(a_n) = +\infty$. Par définition, on a $a_k \in p^k\,\mathbf{Z} \cap \{1, \dots, p^{k+1} - 1\}$, ce qui implique $a_k = u_k p^k$ avec $u_k \in \{1, \dots, p-1\}$, d'où $v_p(a_k) = k$. Si $n > k$, on a $a_n \equiv a_k \mod p^{k+1}$: il existe $m \in \mathbf{Z}$ tel que $a_n = a_k + p^{k+1}m = p^k(u_k + pm)$. Comme $p \nmid u_k$, on a $p \nmid a_k + pm$, et donc $v_p(a_n) = k$.

(27) Soit $n \in \mathbf{N}$. Par définition de la division euclidienne, on a $a_n \in \{0, \dots, p^{n+1} - 1\}$. Par ailleurs, on a $p^{n+1} \mid x - a_n$ et $p^{n+2} \mid x - a_{n+1}$, d'où $p^{n+1} \mid x - a_{n+1}$. Cela implique que $p^{n+1} \mid (x - a_n) - (x - a_{n+1}) = a_{n+1} - a_n$, soit encore $a_{n+1} \equiv a_n \mod p^{n+1}$. D'après la question (24), la suite $(a_n)_{n\geq 0}$ définit un élément de $\mathbf{Z}_p$.

(28) • Comme $7 < p^{n+1}$ pour tout $n \geq 1$, on a $\theta(7) = (2, 7, 7, \dots)$.
• On a $-7 = 3 - 10$ et $-7 = 5^{n+1} - 7 - 5^{n+1}$ avec $0 < 5^{n+1} - 7 < 5^{n+1}$ lorsque $n > 0$, ce qui montre que $\theta(-7) = (3, 18, 118, \dots, 5^{n+1} - 7, \dots)$.

(29) Soient $x.y \in \mathbf{Z}$ tels que $\theta(x) = \theta(y) = (a_n)_{n\geq 0}$. On a alors $p^{n+1} \mid x - a_n$ et $p^{n+1} \mid y - a_n$ et donc $p^{n+1} \mid x - y$, soit encore $n < v_p(x - y)$ pour tout $n \in \mathbf{N}$. Cela implique que $v_p(x - y) = +\infty$, *i.e.* que $x - y = 0$, soit encore $x = y$.

(30) • On a $0 < \alpha_n = \frac{p^{n+1}-1}{p-1} \leq p^{p+1} - 1$. Par ailleurs, $\alpha_{n+1} - \alpha_n = p^{n+1}$, donc $\alpha_{n+1} \equiv \alpha_n \mod p^{n+1}$: d'après la question (24), $\alpha \in \mathbf{Z}_p$.
• Supposons qu'il existe $x \in \mathbf{Z}$ tel que $(\alpha_n)_{n\geq 0} = \theta(x)$. Si $x \geq 0$, on a $\alpha_n = x$ dès que $x < p^{n+1}$, *i.e.* dès que $n > \frac{\ln(x)}{\ln(p)}$: cela implique que la suite $(\alpha_n)_{n\geq 0}$ est stationnaire à partir d'un certain rang, ce qui n'est pas. On a donc nécessairement $x < 0$. Écrivons $x = p^{n+1} + x - p^{n+1}$: on a $0 \leq p^{n+1} + x < p^{n+1}$ dès que $-x \geq p^{n+1}$ *i.e.* dès que $n > \frac{\ln(-x)}{\ln(p)}$, ce qui implique que $\alpha_n = p^{n+1} + x$ pour $n \gg 0$. On a de même $\alpha_{n+1} = p^{n+2} + x$ et donc $\alpha_{n+1} - \alpha_n = p^{n+2} - p^{n+1}$ pour $n \gg 0$. Comme $\alpha_{n+1} - \alpha_n = p^{n+1}$, cela implique que $p^{n+1} = p^{n+2} - p^{n+1}$, *i.e.* $p^{n+2} = 2p^{n+1}$ pour $n \gg 0$, et donc $p = 2$.
Si $p \neq 2$, on arrive à une contradiction, qui montre qu'un tel x n'existe pas. Si $p = 2$ par contre, on a $\alpha_n = 2^{n+1} - 1$, ce qui montre que $\alpha = \theta(-1)$ et donc un tel x existe dans ce cas (il y a donc une petite erreur dans l'énoncé, qui oublie la cas $p = 2$).

Remarque. En anticipant un peu, on a un autre argument : $\mathbf{Z}_p$ est un anneau et θ un morphisme d'anneaux injectif. Comme $(p-1)\alpha_n = p^{n+1} - 1$, on a $(p-1)\alpha = -1$: si un tel x existe, on a $(p-1)x + 1 \in \mathrm{Ker}(\theta)$, d'où $(p-1)x + 1 = 0$, *i.e.* $x = -\frac{1}{p-1}$. C'est un entier si et seulement si $p = 2$, et il vaut alors -1 : on retrouve ce qui précède.

(31) Si $x = 0$, on a $v_p(x) = +\infty = \tilde{v}_p(0) = \tilde{v}_p(\theta(0))$. Supposons désormais $n \neq 0$: la suite $(a_n)_{n\geq 0} = \theta(x)$ n'est pas nulle. Posons $k = v_p(x)$: on a $p^k \mid x$, donc $a_n = 0$ si $n < k$. Par ailleurs, on a $x \equiv a_k \mod p^{p+1}$: comme $p^k \mid x$ et $p^{k+1} \nmid x$, on a $p^k \mid a_k$ et $p^{k+1} \nmid a_k$, d'où $v_p(a_k) = k$. Si $n > k$, on a $a_n \equiv a_k \mod p^{n+1}$, donc $p^k \mid a_n$ et $p^{k+1} \nmid a_n$, soit $v_p(a_n) = k$. Cela signifie précisément que $\tilde{v}_p(\theta(x)) = k = v_p(x)$.

II.B. Structure d'anneau

(32) Soit $n \in \mathbf{N}$. Par définition de la division euclidienne, on a bien sûr $c_n \in \{0, \dots, p^{n+1} - 1\}$. Par ailleurs, on a $p^{n+1} \mid a_{n+1} - a_n$ et $p^{n+1} \mid b_{n+1} - b_n$, d'où $p^{n+1} \mid (a_{n+1} + b_{n+1}) - (a_n + b_n)$. Comme $p^{n+1} \mid a_n + b_n - c_n$ et $p^{n+2} \mid a_{n+1} + b_{n+1} - c_{n+1}$ (de sorte que $p^{n+1} \mid a_{n+1} + b_{n+1} - c_{n+1}$), on en déduit que $p^{n+1} \mid c_{n+1} - c_n$, soit encore $c_{n+1} \equiv c_n \mod p^{n+1}$. D'après la question (24), cela implique que $(c_n)_{n\geq 0} \in \mathbf{Z}_p$.

(33) • L'élément $\theta(0) \in \mathbf{Z}_p$ est la suite nulle. C'est l'élément neutre pour la loi $+$.

• Si $a = 0$, alors $b = 0$ vérifie $a + b = 0$: supposons désormais que $a \neq 0$. On dispose de $k = \tilde{v}_p(a)$: on a $p^k \mid a_n$ pour tout $n \in \mathbf{N}$. On définit $b = (b_n)_{n\geq 0}$ par $b_n = \begin{cases} 0 & \text{si } n < k \\ p^{n+1} - a_n & \text{si } n \geq k \end{cases}$. Par construction, on a $b_n \in \{0, \dots, p^{n+1} - 1\}$ pour tout $n \in \mathbf{N}$. Par ailleurs, on a $p^k \mid b_n$ pour tout $n \in \mathbf{N}$ (c'est évident si $n < k$, et résulte du fait que $p^k \mid a_n$ et $b_n = p^{n+1} - a_n$ si $n \geq k$. Soit $n \in \mathbf{N}$. On a bien sûr $b_{n+1} \equiv b_n \mod p^{n+1}$ si $n + 1 \leq k$ puis que $p^k \mid b_n$ et $p^k \mid b_{n+1}$. Supposons $k > n$. Il existe $m \in \mathbf{Z}$ tel que $a_{n+1} = a_n + p^{n+1}m$: on a $b_{n+1} = p^{n+2} - a_{n+1} = p^{n+2} - a_n - p^{n+1}m = b_n + p^{n+1}(p - m - 1)$, de sorte que $b_{n+1} \equiv b_n \mod p^{n+1}$. Cela montre que $b \in \mathbf{Z}_p$. Comme $p^{n+1} \mid a_n + b_n$ pour tout $n \in \mathbf{N}$, on a $a + b = 0$.
• La loi + est une loi de composition interne sur $\mathbf{Z}_p$. Elle est commutative et associative en vertu de la commutativité et de l'associativité de l'addition dans $\mathbf{Z}/p^{n+1}\mathbf{Z}$ pour tout $n \in \mathbf{N}$. D'après ce qui précède, elle admet un élément neutre, et tout élément admet un inverse. Cela signifie que $(\mathbf{Z}_p, +)$ est un groupe abélien.

(34) Notons $1 \in \mathbf{Z}^{\mathbf{N}}$ la suite constante égale à 1. Elle définit trivialement un élément de $\mathbf{Z}_p$. Par ailleurs, la définition de la loi . implique que c'est un élément neutre pour la multiplication.

(35) Soit $a = (a_n)_{n\in\mathbf{N}} \in \mathbf{Z}_p$ telle que $(\exists b \in \mathbf{Z}_p \setminus \{0\})\, ab = 0$. Écrivons $b = (b_n)_{n\in\mathbf{N}}$: pour tout $n \in \mathbf{N}$, on a $p^{n+1} \mid a_n b_n$, *i.e.* $n + 1 \leq v_p(a_n) + v_p(b_n)$. Posons $k = \tilde{v}_p(b)$: pour tout $n \geq k$, on a $v_p(b_n) = k$, et donc $n + 1 - k \leq v_p(a_n)$, *i.e.* $p^{n+1-k} \mid a_n$. Comme $a_n \equiv a_{n-k} \mod p^{n-k+1}$, cela implique que $p^{n-k+1} \mid a_{n-k}$ pour tout $n \geq k$, de sorte que $p^{n+1} \mid a_n$ pour tout $n \in \mathbf{N}$. Comme $a_n \in \{0, \dots, p^{n+1} - 1\}$, cela implique que $a_n = 0$ pour tout $n \in \mathbf{N}$, *i.e.* $a = 0$. Cela montre que $(\mathbf{Z}_p, +, .)$ est un anneau intègre.

(36) • Si $n \geq v_p(a)+v_p(b)$, on a $n \geq v_p(a)$, donc $v_p(a_n) = v_p(a)$, et de même $v_p(b_n) = v_p(b)$. Cela implique que $v_p(a_n b_n) = v_p(a_n)+v_p(b_n) = v_p(a)+v_p(b)$: comme $v_p(a)+v_p(b) < n+1$, le reste d_n de la division euclidienne de $a_n b_n$ par p^{n+1} vérifie encore $v_p(d_n) = v_p(a) + v_p(b)$. Comme c'est vrai pour tout $n \geq v_p(a) + v_p(b)$, cela montre que $v_p(ab) = v_p(a) + v_p(b)$.
• Posons $m := \min\{v_p(a), v_p(b)\}$. Par définition, on a $v_p(a_n) \geq v_p(a) \geq m$ pour tout $n \in \mathbf{N}$. On a de même $v_p(b_n) \geq m$ pour tout $n \in \mathbf{N}$. Il en résulte que $v_p(a_n - b_n) \geq \min\{v_p(a_n), v_p(b)\} \geq m$ pour tout $n \in \mathbf{N}$. Cela implique que $v_p(a - b) \geq m$.

(37) Soient $x, y \in \mathbf{Z}$: l'élément $\theta(x + y)_n$ (resp. $\theta(x)_n$, resp. $\theta(y)_n$) est le reste de la division euclidienne de $x+y$ (resp. x, resp. y) par p^{n+1} : cela implique que $\theta(x+y)_n \equiv x+y \mod p^{n+1}$ (resp. $\theta(x)_n \equiv x \mod p^{n+1}$, resp. $\theta(y)_n \equiv y \mod p^{n+1}$), de sorte que $\theta(x+y)_n \equiv \theta(x)_n+\theta(y)_n \mod p^{n+1}$, puis que le reste de la division euclidienne de $\theta(x)_n+\theta(y)_n$ par p^{n+1} est $\theta(x+y)_n$, ce qui signifie précisément que $\theta(x+y) = \theta(x)+\theta(y)$ dans $\mathbf{Z}_p$. On montre de la même manière que $\theta(xy) = \theta(x)\theta(y)$, ce qui prouve que $\theta\colon \mathbf{Z} \to \mathbf{Z}_p$ est un morphisme d'anneaux. On a vu dans la question (29) qu'il est injectif.

Remarque. De fait, θ est l'unique morphisme unitaire $\mathbf{Z} \to \mathbf{Z}_p$.

(38) Si a est inversible, il existe $b = (b_n)_{n\geq 0}$ tel que $ab = 1$. Cela implique que pour tout $n \in \mathbf{N}$, on a $a_n b_n \equiv 1 \mod p^{n+1}$. Pour $n = 0$, cela signifie que $a_0 b_0 \equiv 1 \mod p$, ce qui implique que $a_0 \neq 0$. Réciproquement, supposons $a_0 \neq 0$: on a $a_0 \in \{1, \dots, p - 1\}$. Comme $a_n \equiv a_0 \mod p$ pour tout $n \in \mathbf{N}$, cela montre que $v_p(a) = 0$, *i.e.* que a_n est inversible modulo p^{n+1} pour tout $n \in \mathbf{N}$: soit $b_n \in \{1, \dots, p^{n+1} - 1\}$ l'inverse de a_n modulo p^{n+1}. En termes savants, b_n est l'unique représentant dans $\{0, \dots, p^{n+1} - 1\}$ de l'inverse de la classe de a_n dans $\mathbf{Z}/p^{n+1}\mathbf{Z}$. Par définition, on a $b_n \in \{0, \dots, p^{n+1} - 1\}$ et $a_n b_n \equiv 1 \mod p^{n+1}$ pour tout $n \in \mathbf{N}$. Si $n \in \mathbf{N}$, on a $p^{n+1} \mid a_n b_n$ et $p^{n+2} \mid a_{n+1} b_{n+1}$. Comme $p^{n+1} \mid a_{n+1} - a_n$, on a aussi $p^{n+1} \mid a_n b_{n+1}$, ce qui montre que $p^{n+1} \mid a_n(b_{n+1} b_n)$. On a $v_p(a_n) = 0$: l'entier a_n est premier à p. D'après le lemme de Gauss, on a donc $p^{n+1} \mid b_{n+1} - b_n$, soit encore $b_{n+1} \equiv b_n \mod p^{n+1}$. D'après la question (24), cela montre que $b \in \mathbf{Z}_p$. Les congruences $a_n b_n \equiv 1 \mod p^{n+1}$ pour tout $n \in \mathbf{N}$ montrent alors que $ab = 1$, et donc que a est inversible dans l'anneau $(\mathbf{Z}_p, +, .)$.

(39) • Supposons qu'il existe $b = (b_n)_{n\geq 0} \in \mathbf{Z}_p$ tel que $a = \theta(p^k)b$ dans $\mathbf{Z}_p$. Cela signifie que pour tout $n \in \mathbf{N}$, a_n est le reste de la division euclidienne de $p^k b_n$ par p^{n+1}. Cela implique que $a_n = 0$ pour tout $n < k$, et donc que $v_p(a) \geq k$.
• Réciproquement, supposons que $v_p(a) \geq k$. Pour tout $n \in \mathbf{N}$, on a $p^k \mid a_n$. Pour $n \in \mathbf{N}$, il existe $b_n \in \{0, \dots, p^{n+1} - 1\}$ unique tel que $a_{n+k} = p^k b_n$. Comme $a_{n+k+1} \equiv a_{n+k} \mod p^{n+k+1}$, soit encore $p^k b_{n+1} \equiv p^k b_n \mod p^{n+k+1}$, on a $b_{n+1} \equiv b_n \mod p^{n+1}$ en divisant par p^k. On a donc $b := (b_n)_{n\geq 0} \in \mathbf{Z}_p$. Par construction, on a $a = \theta(p^k)b$.

Remarque. Vu l'identification entre $\mathbf{Z}$ et son image $\theta(\mathbf{Z}) \subset \mathbf{Z}_p$, on pourrait aussi bien écrire $a = p^k b$ dans ce qui précède.

(40) Soit $I \subset \mathbf{Z}_p$ un idéal non nul. Posons $k = \min\{v_p(a)\}_{a \in I \setminus \{0\}}$. Il existe $a \in I \setminus \{0\}$ tel que $v_p(a) = k$. D'après la question précédente, il existe $b \in \mathbf{Z}_p$ tel que $a = \theta(p^k)b$. On a $k = v_p(a) = v_p(\theta(p^k)) + v_p(b)$ en vertu de la question (36) : comme $v_p(\theta(p^k)) = k$ en vertu de la question (31), on a $v_p(b) = 0$, soit $b_0 \neq 0$. D'après la question (38), cela implique que $b \in \mathbf{Z}_p^\times$: il en résulte que $p^k = b^{-1}a \in I$, de sorte que $p^k\,\mathbf{Z}_p \subset I$. Par ailleurs, si $a \in I \setminus \{0\}$, on a $v_p(a) \geq k$: d'après la question précédente, on a $p^k \mid a$ dans $\mathbf{Z}_p$, *i.e.* $a \in p^k\,\mathbf{Z}_p$. Cela montre que $I \subset p^k\,\mathbf{Z}_p$, et finalement que $I = p^k\,\mathbf{Z}_p$.
Finalement, les idéaux de $\mathbf{Z}_p$ sont $\{0\}$ et les $p^k\,\mathbf{Z}_p$ pour $k \in \mathbf{N}$. Cela montre en particulier que $\mathbf{Z}_p$ est principal.

(41) • Soient $a, b, c, d \in \mathbf{Z}$ avec $bd \neq 0$, tels que $(a,b)\mathcal{R}(c,d)$: on a $ad = bc$. Comme θ est un morphisme d'anneaux, on a $\theta(a)\theta(d) = \theta(b)\theta(c)$, *i.e.* $(\theta(a), \theta(b))\mathcal{R}(\theta(c), \theta(d))$, ce qui montre que $\Theta\big(\frac{a}{b}\big) := \overline{(\theta(a), \theta(b))}$ ne dépend que de la classe $\frac{a}{b}$ de (a,b) modulo $\mathcal{R}$, et donc que l'application Θ est bien définie.
• Le fait que Θ soit un morphisme de corps résulte du fait que θ est un morphisme d'anneaux. Si $a, b, c, d \in \mathbf{Z}$ avec $bd \neq 0$, on a $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, donc

$$\begin{aligned}\Theta\big(\tfrac{a}{b} + \tfrac{c}{d}\big) = \Theta\big(\tfrac{ad+bc}{bd}\big) &= \overline{(\theta(ad+bc), \theta(bd))} = \overline{(\theta(a)\theta(d) + \theta(b)\theta(c), \theta(b)\theta(d))} \\ &= \overline{(\theta(a), \theta(b))} + \overline{(\theta(c), \theta(d))} = \Theta\big(\frac{a}{b}\big) + \Theta\big(\tfrac{c}{d}\big).\end{aligned}$$

On montre de même que $\Theta\big(\frac{a}{b}.\frac{c}{d}\big) = \Theta\big(\frac{a}{b}\big)\Theta\big(\frac{c}{d}\big)$ (c'est plus simple). Cela montre que Θ est un morphisme d'anneaux. Il est unitaire parce que $\Theta(1) = \overline{(\theta(1), \theta(1))} = 1$.
• Tout morphisme de corps est injectif (un corps n'a pas beaucoup d'idéaux) : le morphisme Θ ne fait pas exception.

(42) Par hypothèse, on a $ad = bc$, donc $v_p(a) + v_p(d) = v_p(b) + v_p(c)$ en vertu de la question (36), ce qui montre que $v_p(a) - v_p(b) = v_p(c) - v_p(d)$.

(43) Si $x \in \mathbf{Z}_p$, on a $x = \frac{x}{1}$, donc $v_p(x) = \tilde{v}_p(x) - \tilde{v}_p(1) = \tilde{v}_p(x)$: cela montre que v_p prolonge $\tilde{v}_p$. Comme $\tilde{v}_p$ est à valeurs dans $\mathbf{N} \cup \{+\infty\}$, cela implique aussi que $v_p(x) \geq 0$.
Réciproquement, soit $x \in \mathbf{Q}_p$ tel que $v_p(x) \geq 0$. Si $x = 0$, on a bien sûr $x \in \mathbf{Z}_p$: supposons $x \neq 0$. Écrivons $x = \frac{a}{b}$ avec $(a,b) \in E$. Comme $x \neq 0$, on a $a \neq 0$. On peut écrire $a = p^{v_p(a)}a'$ et $b = p^{v_p(b)}b'$ avec $a', b' \in \mathbf{Z}_p$ tels que $v_p(a') = v_p(b') = 0$, *i.e.* $a', b' \in \mathbf{Z}_p^\times$. On a alors $\frac{a}{b} = p^{v_p(a) - v_p(b)}\frac{a'}{b'}$. Comme $v_p(x) = v_p(a) - v_p(b) \in \mathbf{N}$ et $\frac{a'}{b'} in\, \mathbf{Z}_p^\times$, on a $\frac{a}{b} \in \mathbf{Z}_p$, et donc $x \in \mathbf{Z}_p$.

II.C. Topologie dans $\mathbf{Q}_p$

(44) Par définition, comme $k \geq n+1$, on a $a_k \equiv a_n \mod p^{n+1}$, *i.e.* $v_p(a_k - a_n) \geq n+1$. Cela implique que $v_p(a - \theta(a_n)) \geq n+1$, soit encore $|a - \theta(a_n)|_p \leq \frac{1}{p^{n+1}}$, de sorte que $\lim\limits_{n\to\infty} |a - \theta(a_n)|_p = 0$, *i.e.* $\lim\limits_{n\to\infty} \theta(a_n) = a$ dans l'espace métrique $(\mathbf{Z}_p, |.|_p)$.

(45) Soit $a = (a_n)_{n\geq 0} \in \mathbf{Z}_p$. On a vu dans la question précédente que $\lim\limits_{n\to\infty} \theta(a_n) = a$. Comme $a_n \in \mathbf{N}$ pour tout $n \in \mathbf{N}$, cela implique en particulier que $\theta(\mathbf{N})$ est dense dans $(\mathbf{Z}_p, |.|_p)$: c'est *a fortiori* le cas de $\theta(\mathbf{Z})$.

(46) Supposons que $v_p(a) \geq l$: on a $a_{l-1} = 0$, *i.e.* $\sum\limits_{i=0}^{l-1} u_i p^i = 0$. Par unicité de l'écriture d'un entier en base p, cela montre que $u_0 = u_1 = \cdots = u_{l-1} = 0$.
Réciproquement, supposons que $u_0 = u_1 = \cdots = u_{l-1} = 0$. On a $u_n = 0$ si $n < l$ et $v_p(u_n) \geq l$ si $n \geq 0$. Cela implique que $v_p(a) \geq l$.

(47) (a) Soit $i \in \mathbf{N}$. Comme $(a^{(k)})_{k\geq 0}$ est de Cauchy, il existe $N \in \mathbf{N}$ tel que $k, l \geq N \Rightarrow v_p\big(a^{(k)} - a^{(l)}\big) \geq i+1$. Si $k, l \geq N$, on a donc $a_i^{(k)} = a_i^{(l)}$. Par unicité de l'écriture en base p, cela implique que $u_i^{(k)} = u_i^{(l)}$ dès que $k, l \geq N$, ce qui montre que la suite $(u_i^{(k)})_{k\geq 0}$ est stationnaire.

(47) (b) Pour $i \in \mathbf{N}$, posons $u_i = \lim\limits_{k\to\infty} a_i^{(k)}$ (cela a un sens en vertu de la question précédente). Comme $u_i^{(k)} \in \{0, \ldots, p-1\}$ pour tout $k \in \mathbf{N}$, on a $u_i \in \{0, \ldots, p-1\}$ pour tout $i \in \mathbf{N}$. Pour $n \in \mathbf{N}$, on pose alors $a_n = \sum\limits_{i=0}^{n} u_i p^i \in \{0, \ldots, p^{n+1} - 1\}$. La suite $a = (a_n)_{n\in\mathbf{N}}$ définit un élément de $\mathbf{Z}_p$.
Si $m \in \mathbf{N}$, il existe $N \in \mathbf{N}$ tel que $k, l \geq N \Rightarrow v_p\big(a^{(k)} - a^{(l)}\big) \geq m+1$. Quitte à augmenter N, on peut en outre supposer que $l \geq N \Rightarrow a_m^{(l)} = a_m$: comme $v_p\big(a^{(l)} - a_m^{(l)}\big) \geq m+1$ et $v_p(a_m - a) \geq m+1$, on a donc

$l \geq N \Rightarrow v_p\big(a^{(l)} - a\big) \geq m+1$. Il en résulte que $k \geq N \Rightarrow v_p\big(a^{(k)} - a\big) \geq m+1$. Comme c'est vrai pour tout $m \in \mathbf{N}$, on a $\lim\limits_{k\to\infty} d_p\big(a^{(k)}, a\big) = 0$, ce qui signifie que $\lim\limits_{k\to\infty} a^{(k)} = a$: la suite $\big(a^{(k)}\big)_{k\geq 0}$ converge dans $\mathbf{Z}_p$.

Remarque. Une suite de Cauchy est bornée : si $(a^{(k)})_{k\geq 0}$ est une suite de Cauchy dans $\mathbf{Q}_p$, il existe $r \in \mathbf{N}$ tel que $\big|a^{(k)}\big|_p \leq p^r$ soit encore $a^{(k)} \in p^{-r}\,\mathbf{Z}_p$ pour tout $k \in \mathbf{N}$. La suite $(p^r a^{(k)})_{k\geq 0}$ est à valeurs dans $\mathbf{Z}_p$ et est de Cauchy : d'après la question qu'on vient de traiter, elle converge. Si $\alpha \in \mathbf{Z}_p$ désigne sa limite, on a $\lim\limits_{k\to\infty} a^{(k)} = p^{-r}\alpha \in \mathbf{Q}_p$. Cela montre la suite $(a^{(k)})_{k\geq 0}$ converge dans $\mathbf{Q}_p$, qui est donc complet.

(48) • Suppons que la suite $(S_n)_{n\geq 0}$ converge dans $\mathbf{Q}_p$: notons S sa limite. Si $k \in \mathbf{N}_{>0}$, on a alors $x_k = S_k - S_{k-1}$, donc $\lim\limits_{k\to\infty} x_k = S - S = 0$, soit encore $\lim\limits_{k\to\infty} |x_k|_p = 0$.
• Réciproquement, supposons que $\lim\limits_{k\to\infty} |x_k|_p = 0$. Soit $\varepsilon \in \mathbf{R}_{>0}$: il existe $N \in \mathbf{N}$ tel que $k \geq N \Rightarrow |x_k|_p < \varepsilon$. Si $l \geq k \geq N$, on a

$$|S_l - S_k|_p = \left|\sum_{i=k+1}^{l} x_i\right|_p \leq \max_{k<i\leq l} |x_i|_p < \varepsilon$$

en vertu de la question (21) (l'inégalité ultramétrique, démontrée pour les rationnels, est encore valable sur $\mathbf{Q}_p$: elle résulte de la question (36)). Cela montre que la suite $(S_n)_{n\geq 0}$ est de Cauchy dans $\mathbf{Q}_p$. D'après la question précédente, elle converge.

III. Termes nuls d'une suite récurrente linéaire

(49) La relation $u_{n+1} = a_0 u_n + a_1 u_{n+1} + \cdots + a_{d-1} u_{n+d-1}$ se traduit par l'égalité $U_{n+1} = AU_n$ avec

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ a_0 & a_1 & \cdots & \cdots & a_{d-1} \end{pmatrix} \in \mathsf{M}_d(\mathbf{Z})$$

(matrice compagnon du polynôme $P(X) = X^d - a_{d-1}X^{d-1} - \cdots - a_0$). Une récurrence immédiate implique alors que $U_n = A^n U_0$ pour tout $n \in \mathbf{N}$. Posons $X = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$: on a $u_n = X^T U_n = X^T A^n U_0$ pour tout $n \in \mathbf{N}$.

(50) En développant par rapport à la première colonne, on a $\det(A) = (-1)^{d+1} a_0$: comme $a_0 \neq 0$, on a $A \in \mathsf{GL}_d(\mathbf{Q})$.

Remarque. L'énoncé est un peu vague : il ne précise pas inversible dans quel anneau. En particulier, si $a_0 \notin \{\pm 1\}$, la matrice A n'est pas inversible dans $\mathsf{M}_d(\mathbf{Z})$.

(51) Soit p un nombre premier ne divisant pas a_0 (il en existe vu qu'il y a une infinité de nombres premiers mais seulement un nombre fini qui divisent a_0). En notant avec une barre l'image d'un entier dans $\mathbf{Z}/p\,\mathbf{Z}$, on a $\det(\overline{A}) = \overline{\det(A)} = \overline{a_0}$ (parce que la surjection canonique $\mathbf{Z} \to \mathbf{Z}/p\,\mathbf{Z}$ est un morphisme d'anneaux) : comme $p \nmid a_0$, on a $\overline{a_0} \in \mathbf{Z}/p\,\mathbf{Z}\setminus\{0\}$, *i.e.* $\det(\overline{A}) \in (\mathbf{Z}/p\,\mathbf{Z})^\times$ (rappelons que comme p est premier, l'anneau $\mathbf{Z}/p\,\mathbf{Z}$ est un corps donc $(\mathbf{Z}/p\,\mathbf{Z})^\times = \mathbf{Z}/p\,\mathbf{Z}\setminus\{0\}$), ce qui montre que $\overline{A} \in \mathsf{GL}_d(\mathbf{Z}/p\,\mathbf{Z})$.

(52) Le groupe $\mathsf{GL}_g(\mathbf{Z}/p\,\mathbf{Z})$ est fini. D'après la question (4), il est d'ordre $k = (p^d-1)(p^d-p)\cdots(p^d-p^{d-1})$. D'après le théorème de Lagrange, on a $\overline{A}^k = \overline{\mathrm{I}}_d$, ce qui signifie que $A^k \equiv \mathrm{I}_d \mod p\,\mathsf{M}_d(\mathbf{Z})$, soit encore qu'il existe $B \in \mathsf{M}_d(\mathbf{Z})$ telle que $A^k = \mathrm{I}_d + pB$.

(53) Manifestement, l'énoncé ne dit pas ce qu'il veut : il semble demander de prouver que la suite $\big(p^j \frac{f_j(n)}{j!}\big)_{j\geq 0}$ définit un élément de $\mathbf{Z}_p$ (vu comme ensemble des suites d'entiers vérifiant certaines propriétés données au début de la partie II-A, ce qui est rigoureusement faux en général : les rationnels $p^j \frac{f_j(n)}{j!}$ ne sont pas entiers en général, et même quand ils le sont, il n'on aucune raison de vérifier les encadrements et congruences définnissant $\mathbf{Z}_p$. Vu la suite, la vraie question est : montrer que la suite $\big(p^j \frac{f_j(n)}{j!}\big)_{j\geq 0}$ est à valeurs dans $\mathbf{Z}_p$. A fond, il s'agit de montrer que pour tout $j \in \mathbf{N}$ et tout $x \in \mathbf{Z}$ (ici on l'applique à $x = f_j(n)$), on a $p^j \frac{x}{j!} \in \mathbf{Z}_p$. Comme $\mathbf{Z}_p$ est un anneau, il suffit de montrer que $\frac{p^j}{j!} \in \mathbf{Z}_p$ pour tout $j \in \mathbf{N}$. On a déjà $p^j, j! \in \mathbf{Z}_p$ et $j! \neq 0$, donc $\frac{p^j}{j!} \in \mathbf{Q}_p = \mathrm{Frac}(\mathbf{Z}_p)$. Par ailleurs, on a $v_p(p^j) = j$ et $v_p(j!) \leq \frac{j}{p-1}$ (en vertu de la question (16)), donc $v_p\big(\frac{p^j}{j!}\big) = v_p(p^j) - v_p(j!) \geq j - \frac{j}{p-1} = \frac{p-2}{p-1} j \geq 0$: la question (43) montre alors que $\frac{p^j}{j!} \in \mathbf{Z}_p$, ce qui achève la preuve.

(54) • D'après la question (48), la série $S(n)$ converge dans $\mathbf{Q}_p$ si et seulement si son terme général tend vers 0. En reprenant le calcul de la question précédente, on a

$$v_p\big(p^j \tfrac{f_j(n)}{j!}\big) = j - v_p(j!) + v_p(f_j(n)) \geq \tfrac{p-2}{p-1} j.$$

Comme $p > 2$ par hypothèse, on a $\lim\limits_{j\to\infty} v_p\big(p^j \tfrac{f_j(n)}{j!}\big) = +\infty$, *i.e.* que $\lim\limits_{j\to\infty} p^j \tfrac{f_j(n)}{j!} = 0$, et permet de conclure à la convergence de la série $S(n)$ dans $\mathbf{Q}_p$. Comme chacun des termes de la série appartient à $\mathbf{Z}_p$ (*cf* question précédente) et comme $\mathbf{Z}_p$ est complet donc fermé dans $\mathbf{Q}_p$ (*cf* question (47)), la série converge en fait dans $\mathbf{Z}_p$.

Remarque. Le point admis avant la question (55) est faux dans cette généralité. Supposons $p \neq 2$... Fixons une partie quelconque $A \subset \mathbf{Z}$ et posons $f_j = \mathbf{1}_A$ (la fonction caractéristique de A) pour tout $j \in \mathbf{N}$. On dispose de $S(n) = \sum\limits_{j=0}^{\infty} p^j \tfrac{f_j(n)}{j!}$ pour tout $n \in \mathbf{Z}$. Par construction, on a $S(n) = 0$ dès que $n \in \mathbf{Z}\setminus A$ (tous les termes de la somme sont nuls). Si $n \in A$, on a $S(n) = \sum\limits_{j=0}^{\infty} \tfrac{p^j}{j!} = 1 + \sum\limits_{j=1}^{\infty} \tfrac{p^j}{j!}$. Le calcul fait plus haut montre que $\tfrac{p^j}{j!} \in p\,\mathbf{Z}_p$ lorsque $j > 0$: on a donc $S(n) \equiv 1 \mod p\,\mathbf{Z}_p$, en particulier $S(n) \neq 0$ quand $n \in A$. En choisissant A non vide de complémentaire infini dans $\mathbf{N}$ (par exemple A l'ensemble des entiers pairs), on obtient un contre-exemple).
Cela dit, et c'est sans doute ce que le rédacteur avait en tête, le résultat annoncé est valide lorsque les fonctions f_j sont *polynômiales* : l'application S est alors une série entière à coefficents dans $\mathbf{Z}_p$, et cela résulte de la théorie des polygônes de Newton (*cf* chapitre IV paragraphe 4 de Koblitz, *p*-adic numbers, *p*-adic analysis, and zeta-functions, Springer, Graduate text in Mathematics **58**).

(55) Avec les notations de la question (49), on a $u_{kn+r} = X^T A^{kn+r} U_0 = X^T (\mathrm{I}_d + pB)^n A^r U_0$. Comme I_d et B commutent, on a $(\mathrm{I}_d + pB)^n = \sum\limits_{j=0}^{n} \binom{n}{j} p^j B^j = \sum\limits_{j=0}^{n} \tfrac{p^j}{j!} n(n-1)\cdots(n-j+1)$ (binôme de Newton). Si $j \in \mathbf{N}$ et $n \in \mathbf{Z}$, posons $f_j(n) = n(n-1)\cdots(n-j+1) X^T B^j A^r U_0$. Cela définit une application polynomiale sur $\mathbf{Z}$ à valeurs dans $\mathbf{Z}$. Observons par ailleurs que si $j > n$, on a $n(n-1)\cdots(n-j+1) = 0$, *i.e.* $f_j(n) = 0$. Cela montre donc que $u_{kn+r}(n) = \sum\limits_{j=0}^{n} p^j \tfrac{f_j(n)}{j!} = \sum\limits_{j=0}^{\infty} p^j \tfrac{f_j(n)}{j!}$. D'après le point admis (et dont l'usage est licite vu que les fonctions f_j sont polynomiales), si l'ensemble $Z_r(u)$ est infini, alors il est égal à n en entier.

IV. Exponentielle p-adique et applications

IV.A. Définition de l'exponentielle

(56) D'après la question (16), on a $v_p(n!) \leq \tfrac{n}{p-1}$ pour tout $n \in \mathbf{N}$. Si $x \in \mathbf{Q}_p$, on a

$$v_p\big(\tfrac{x^n}{n!}\big) = n v_p(x) - v_p(n!) \geq n v_p(x) - \tfrac{n}{p-1} = n\big(v_p(x) - \tfrac{1}{p-1}\big).$$

Si $v_p(x) > \tfrac{1}{p-1}$, on a donc $\lim\limits_{n\to\infty} v_p\big(\tfrac{x^n}{n!}\big) = +\infty$, soit encore $\lim\limits_{n\to\infty} \tfrac{x^n}{n!} = 0$ dans $\mathbf{Q}_p$. D'après la question (48), la série $e_p(x)$ converge dans $\mathbf{Q}_p$.

Remarque. • Le calcul qui précède montre en fait un peu plus. Si $v_p(x) > \tfrac{1}{p-1}$, alors $\tfrac{x^n}{n!} \in \mathbf{Z}_p$ pour tout $n \in \mathbf{N}$, ce qui montre qu'en fait, la série $e_p(x)$ converge dans $\mathbf{Z}_p$.
• Dans tout l'énoncé, on ne travaille qu'avec des éléments de $\mathbf{Q}_p$, sur lequel la valuation p-adiques est à valeurs dans $\mathbf{Z}\cup\{\infty\}$: le rationnel $\tfrac{1}{p-1}$ est un peu déroutant de prime abord. Il s'explique parce qu'on peut étendre la définition de l'exponentielle à des extensions de $\mathbf{Q}_p$ (par exemple une clôture algébrique de $\mathbf{Q}_p$ voire le complété d'icelle) sur lesquelles la valuation p-adique se prolonge, mais n'est plus à valeurs entières, mais rationnelles. La borne $\tfrac{1}{p-1}$ subsiste dans ce contexte plus général.

(57) Soit $N \in \mathbf{N}$. Si $n \in \{0,\dots,N\}$, on a $\tfrac{(x+y)^n}{n!} = \tfrac{1}{n!}\sum\limits_{i=0}^{n} \binom{n}{i} x^i y^{n-i} = \sum\limits_{i=0}^{n} \tfrac{x^i}{i!}\tfrac{y^{n-i}}{(n-i)!} = \sum\limits_{\substack{i,j\in\mathbf{N}\\ i+j=n}} \tfrac{x^i}{i!}\tfrac{y^j}{j!}$, donc

$$\Big(\sum_{i=0}^{N} \tfrac{x^i}{i!}\Big)\Big(\sum_{j=0}^{N} \tfrac{y^j}{j!}\Big) - \sum_{n=0}^{N} \tfrac{(x+y)^n}{n!} = \sum_{0\leq i,j\leq N} \tfrac{x^i}{i!}\tfrac{y^j}{j!} - \sum_{\substack{0\leq i,j\leq n\\ i+j\leq N}} \tfrac{x^i}{i!}\tfrac{y^j}{j!} = \sum_{\substack{0\leq i,j\leq n\\ i+j>N}} \tfrac{x^i}{i!}\tfrac{y^j}{j!}.$$

Suppsons $v_p(x), v_p(y) > \tfrac{1}{p-1}$: si $i, j \in \mathbf{N}$, on a

$$v_p\big(\tfrac{x^i}{i!}\tfrac{y^j}{j!}\big) = i v_p(x) - v_p(i!) + j v_p(y) - v_p(j!) \geq i\big(v_p(x) - \tfrac{1}{p-1}\big) + j\big(v_p(y) - \tfrac{1}{p-1}\big) \geq (i+j)\mu$$

où $\mu = \min\{v_p(x), v_p(y)\} - \frac{1}{p-1} \in \mathbf{R}_{>0}$. On a donc $v_p\Big(\sum\limits_{\substack{0\leq i,j\leq n\\ i+j>N}} \frac{x^i}{i!}\frac{y^j}{j!}\Big) \geq \sup\limits_{\substack{0\leq i,j\leq n\\ i+j>N}} v_p\big(\frac{x^i}{i!}\frac{y^j}{j!}\big) \geq N\mu$ (inégalité ultramétrique), de sorte que $\left|\Big(\sum\limits_{i=0}^{N}\frac{x^i}{i!}\Big)\Big(\sum\limits_{j=0}^{N}\frac{y^j}{j!}\Big) - \sum\limits_{n=0}^{N}\frac{(x+y)^n}{n!}\right|_p \leq \frac{1}{p^{N\mu}}$ pour tout $N \in \mathbf{N}$, ce qui implique

$$\lim_{N\to\infty}\left[\Big(\sum_{i=0}^{N}\frac{x^i}{i!}\Big)\Big(\sum_{j=0}^{N}\frac{y^j}{j!}\Big) - \sum_{n=0}^{N}\frac{(x+y)^n}{n!}\right] = 0,$$

soit encore $e_p(x)e_p(y) - e_p(x+y) = 0$, ce qu'on voulait.

(58) On a $v_p\big((-1)^{n+1}\frac{t^n}{n}\big) = nv_p(t) - v_p(n)$. Comme $p^{v_p(n)} \mid n$, on a $p^{v_p(n)} \leq n$, donc $v_p(n) \leq \frac{\ln(n)}{\ln(p)}$, ce qui implique que $v_p\big((-1)^{n+1}\frac{t^n}{n}\big) \geq nv_p(t) - \frac{\ln(n)}{\ln(p)}$. L'hypothèse $|t|_p < 1$ signifie que $v_p(t) > 0$, ce qui implique que $\lim\limits_{n\to\infty}\big(nv_p(t) - \frac{\ln(n)}{\ln(p)}\big) = +\infty$, soit encore $\lim\limits_{n\to\infty}(-1)^{n+1}\frac{t^n}{n} = 0$ dans $\mathbf{Q}_p$: la question (48) implique la convergence de la série $l_p(1+t)$.

IV.B. Inversibles de $\mathbf{Z}/p^n\mathbf{Z}$

(59) Un entier x a une image dans $\mathbf{Z}/p^n\mathbf{Z}$ inversible si et seulement s'il est premier à p^n *i.e.* à p. Cela implique que son image n'est pas inversible si et seulement si $p \mid x$. Il en résulte que $(\mathbf{Z}/p^n\mathbf{Z})\setminus(\mathbf{Z}/p^n\mathbf{Z})^\times = p\,\mathbf{Z}/p^n\mathbf{Z}$. On a $\#\,\mathbf{Z}/p^n\mathbf{Z} = p^n$ et $\#p\,\mathbf{Z}/p^n\mathbf{Z} = p^{n-1}$: cela montre que $\varphi(p^n) = \#(\mathbf{Z}/p^n\mathbf{Z})^\times = p^n - p^{n-1} = p^{n-1}(p-1)$.

(60) Notons $f\colon \mathbf{Z}/p^n\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$ la surjection canonique (c'est la réduction modulo p). C'est un morphisme d'anneaux. Il induit un morphisme de groupes multiplicatifs $\pi\colon (\mathbf{Z}/p^n\mathbf{Z})^\times \to (\mathbf{Z}/p\mathbf{Z})^\times$ (introduit dans la question suivante). Il suffit alors d'observer que H n'est autre que le noyau de π : c'est donc un sous-groupe de $(\mathbf{Z}/p^n\mathbf{Z})^\times$.

Remarque. On a $\#(\mathbf{Z}/p^n\mathbf{Z})^\times = \#\operatorname{Im}(\pi)\#\operatorname{Ker}(\pi)$. Comme $\#(\mathbf{Z}/p^n\mathbf{Z})^\times = p^{n-1}(p-1)$ en vertu de la question (59) et $\#\operatorname{Ker}(\pi) = \#H = p^{n-1}$, on en déduit que $\#\operatorname{Im}(\pi) = p-1 = \#(\mathbf{Z}/p\,\mathbf{Z})^\times$, ce qui prouve que π est surjectif (ce que l'on peut démontrer directement en relevant les éléments de $(\mathbf{Z}/p\,\mathbf{Z})^\times$ dans $\mathbf{Z}\setminus p\,\mathbf{Z}$ puis en réduisant modulo p^n).

(61) (a) Comme p est premier, le quotient $\mathbf{K} = \mathbf{Z}/p\mathbf{Z}$ est un corps. Il est fini (de cardianl p) : d'après la question (6), son groupe multiplicatif $\mathbf{K}^\times = (\mathbf{Z}/p\,\mathbf{Z})^\times$ est cyclique. Soit α un générateur de $(\mathbf{Z}/p\,\mathbf{Z})^\times$. Choisissons un relèvement $\widehat{\alpha}$ de α dans $(\mathbf{Z}/p^n\mathbf{Z})^\times$, *i.e.* tel que $\pi(\widehat{\alpha}) = \alpha$ (c'est possible vu queπ est surjectif). Soit m l'ordre de $\widehat{\alpha}$ dans $(\mathbf{Z}/p^n\mathbf{Z})^\times$. On a $\widehat{\alpha}^m = \overline{1}$ donc $\alpha^m = \pi\big(\widehat{\alpha}^m\big) = \pi(\overline{1}) = \widetilde{1}$, ce qui montre que $p-1 \mid m$. D'après le théorème de Lagrange, on a en outre $m \mid \#(\mathbf{Z}/p^n\mathbf{Z})^\times = p^{n-1}(p-1)$. Cela montre que $m = p^r(p-1)$ avec $r \in \{0,\dots,n-1\}$. Choisissons un entier $a \in \mathbf{Z}$ tel que $\overline{a} = \widehat{\alpha}^{p^r} \in (\mathbf{Z}/p^n\mathbf{Z})^\times$. Par construction, $\overline{a}$ est d'ordre $p-1$. Par ailleurs, on a $\pi(\overline{a}) = \pi\big(\widehat{\alpha}^{p^r}\big) = \alpha^{p^r} = \alpha$ vu que $\alpha^p = \alpha$ (car $\alpha^{p-1} = \widetilde{1}$), si bien que $\widetilde{a} = \alpha$ engendre $(\mathbf{Z}/p\,\mathbf{Z})^\times$.

(61) (b) Comme $\overline{a}$ et $\widetilde{a}$ sont d'ordre $p-1$ dans $(\mathbf{Z}/p^n\mathbf{Z})^\times$ et $(\mathbf{Z}/p\,\mathbf{Z})^\times$ respectivement, les applications $\mathbf{Z} \to (\mathbf{Z}/p^n\mathbf{Z})^\times$ et $\mathbf{Z} \to (\mathbf{Z}/p\,\mathbf{Z})^\times$ définies par $k \mapsto \overline{a}^k$ et $k \mapsto \widetilde{a}^k$ respectivement se factorisent à travers des morphismes $f\colon \mathbf{Z}/(p-1)\,\mathbf{Z} \to (\mathbf{Z}/p^n\mathbf{Z})^\times$ et $g\colon \mathbf{Z}/(p-1)\,\mathbf{Z} \to (\mathbf{Z}/p\,\mathbf{Z})^\times$. Comme $\widetilde{a}$ engendre $(\mathbf{Z}/p\,\mathbf{Z})^\times$, le morphisme g est un isomorphisme par cardinalité. On peut donc définir le morphisme de groupes composé $\varphi = f \circ g^{-1}\colon (\mathbf{Z}/p\,\mathbf{Z})^\times \to (\mathbf{Z}/p^n\mathbf{Z})^\times$. Par ailleurs, on a $\pi(\overline{a}) = \widetilde{a}$, donc $\pi \circ f = g$, ce qui implique que $\pi \circ \varphi = \pi \circ f \circ g^{-1} = \mathsf{Id}_{(\mathbf{Z}/p\,\mathbf{Z})^\times}$.

Remarque. Il y a une coquille dans l'énoncé : on obtient l'identité de $(\mathbf{Z}/p\,\mathbf{Z})^\times$ et non de $(\mathbf{Z}/p^n\mathbf{Z})^\times$.

(61) (c) Notons $i\colon H \to (\mathbf{Z}/p^n\mathbf{Z})^\times$ le morphisme d'inclusion. On dispose donc de l'application

$$\begin{aligned}\psi\colon H \times (\mathbf{Z}/p\,\mathbf{Z})^\times &\to (\mathbf{Z}/p^n\mathbf{Z})^\times\\ (h,x) &\mapsto h\varphi(x)\end{aligned}$$

C'est un morphisme de groupes (le membre de gauche étant muni de la structure de groupe produit) parce que $(\mathbf{Z}/p^n\mathbf{Z})^\times$ est abélien. Soit $(h,x) \in \operatorname{Ker}(\psi)$: on a $h\varphi(x) = \overline{1}$: en appliquant π, on a $\widetilde{1} = \pi(h)\pi(\varphi(x)) = x$ vu que $h \in H = \operatorname{Ker}(\pi)$ et $\pi \circ \varphi = \mathsf{Id}_{(\mathbf{Z}/p\,\mathbf{Z})^\times}$. Comme φ est un morphisme de groupes, on a $\varphi(x) = \varphi(\widetilde{1}) = \overline{1}$, et donc $h = h\varphi(x) = \overline{1}$. Cela montre que $\operatorname{Ker}(\psi) = \{(\overline{1},\widetilde{1})\}$, et donc que ψ est injectif. Comme $\#H = p^{n-1}$ et $\#(\mathbf{Z}/p\,\mathbf{Z})^\times = p-1$, on a $\#\big(H \times (\mathbf{Z}/p\,\mathbf{Z})^\times\big) = pn - 1(p-1) = \#(\mathbf{Z}/p^n\mathbf{Z})^\times$ (*cf* question (59)) : par cardinalité, ψ est un isomorphisme.

(62) D'après le calcul fait dans la question (59), on a $v_p\big(\frac{x^n}{n!}\big) \geq n\big(v_p(x) - \frac{1}{p-1}\big)$. Comme p est impair, on a $\frac{1}{p-1} < 1$: si $n > 0$, on a donc $v_p\big(\frac{x^n}{n!}\big) > 0$, *i.e.* $v_p\big(\frac{x^n}{n!}\big) \geq 1$ vu que v_p est à valeurs entières. Cela implique que $\frac{x^n}{n!} \in p\,\mathbf{Z}_p$ pour tout $n > 0$. Comme $p\,\mathbf{Z}_p$ est fermé dans $\mathbf{Q}_p$ (parce que $\mathbf{Z}_p$ est complet, *cf* question (47)), la série convergente $\sum_{n=1}^{\infty} \frac{x^n}{n!}$ appartient à $p\,\mathbf{Z}_p$. Il en résulte que $e_p(x) \in 1 + p\,\mathbf{Z}_p \subset \mathbf{Z}_p$.

(63) Supposons $n > 0$. D'après la question précédente, l'application e_p induit une application $p\,\mathbf{Z}_p \to \mathbf{Z}_p$: on dispose bien du composé $\pi_n \circ e_p \colon p\,\mathbf{Z}_p \to \mathbf{Z}/p^n\,\mathbf{Z}$. On a vu en fait que $e_p(p\,\mathbf{Z}_p) \subset 1 + p\,\mathbf{Z}_p$. Par ailleurs, on a $1 + p\,\mathbf{Z}_p \subset \mathbf{Z}_p^\times$ en vertu de la question (39), et l'application induite $p\,\mathbf{Z}_p \to \mathbf{Z}_p^\times$ (encore notée e_p) est un morphisme de groupes de $(p\,\mathbf{Z}_p, +)$ vers $(\mathbf{Z}_p^\times, .)$ (*cf* question (57)). Enfin, le morphisme d'anneaux π_n induit un morphisme de groupes multiplicatifs $\pi_n \colon \mathbf{Z}_p^\times \to (\mathbf{Z}/p^n\,\mathbf{Z})^\times$. Le composé $\pi_n \circ e_p$ fournit donc en fait un morphisme de groupes de $(p\,\mathbf{Z}_p, +)$ vers $((\mathbf{Z}/p^n\,\mathbf{Z})^\times, .)$. Notons-le ε_n. Si $k, n \in \mathbf{N}_{>0}$, on a comme plus haut $v_p\big(\frac{p^{nk}}{k!}\big) = nk - v_p(k!) \geq nk - \frac{k}{p-1} \geq \big(n - \frac{1}{2}\big)k$ (parce que $p \geq 3$ par hypothèse). Si $k \geq 2$, on a donc $v_p\big(\frac{p^{kn}}{n!}\big) \geq 2n - 1 \geq n$. On a en outre $v_p\big(\frac{p^{nk}}{k!}\big) = n$ lorsque $k = 1$. Comme dans la question précédente, cela implique que $e_p(p^n) - 1 = \sum_{k=1}^{\infty} \frac{p^{nk}}{k!} \in p^n\,\mathbf{Z}_p$, si bien que $\pi_n(e_n(p^n)) = \overline{1}$, *i.e.* $p^n \in \mathrm{Ker}(\varepsilon_n)$. Cela signifie précisément que $\varepsilon_n(x) = (\pi_n \circ e_p)(x)$ ne dépend que de la classe de x modulo p^n, *i.e.* que de l'image X de x dans $p\,\mathbf{Z}_p/p^n\,\mathbf{Z}_p \simeq p\,\mathbf{Z}/p^n\,\mathbf{Z}$ (notons que le morphisme surjectif $\pi_n \colon \mathbf{Z}/p^n\,\mathbf{Z}$ se factorise en un isomorphisme $\mathbf{Z}_p/p^n\,\mathbf{Z}_p \xrightarrow{\sim} \mathbf{Z}/p^n\,\mathbf{Z}$, parce que $\mathrm{Ker}(\pi_n) = p^n\,\mathbf{Z}_p$).

(64) D'après la question précédente, le morphisme $\varepsilon_n \colon p\,\mathbf{Z}_p \to (\mathbf{Z}/p^n\,\mathbf{Z})^\times$ se factorise en un morphisme de groupes $\widetilde{\varepsilon}_n \colon p\,\mathbf{Z}_p/p^n\,\mathbf{Z}_p \to (\mathbf{Z}/p^n\,\mathbf{Z})^\times$. Comme on l'a vu dans la question (62), le morphisme e_p envoie $p\,\mathbf{Z}_p$ dans $1 + p\,\mathbf{Z}_p$: le morphisme $\widetilde{\varepsilon}_n$ est à valeurs dans $H = \overline{1} + p\,\mathbf{Z}/p^n\,\mathbf{Z}$.
Si $t \in p\,\mathbf{Z}_p$, on a $|t|_p < 1$: on dispose de $l_p(1+t) \in \mathbf{Q}_p$. Si $n \in \mathbf{N}_{>0}$, on a

$$v_p\big((-1)^{n+1}\tfrac{t^n}{n}\big) \geq nv_p(t) - \tfrac{\ln(n)}{\ln(p)} \geq n - \tfrac{\ln(n)}{\ln(p)} = 1 + \tfrac{(n-1)\ln(p) - \ln(n)}{\ln(p)} = 1 + \tfrac{\lambda(n)}{\ln(p)}$$

où $\lambda \colon [1, +\infty[\to \mathbf{R}$ est donnée par $\lambda(x) = (x-1)\ln(p) - \ln(x)$. Étudions la fonction λ : on a $\lambda(1) = 0$, et $\lambda'(x) = \ln(p) - \frac{1}{x} \geq \ln(p) - 1 > 0$ (parce que $p \geq 3$) ; la fonction λ est donc strictement croissante, d'où positive sur $[1, +\infty[$. Il en résulte que $v_p\big((-1)^{n+1}\frac{t^n}{n}\big) \geq 1$ pour tout $n > 0$, ce qui implique que $l_p(1+t) \in p\,\mathbf{Z}_p$. D'après le point admis après la question (58), on a en outre $e_p(l_p(1+t)) = 1+t$: le morphisme $e_p \colon p\,\mathbf{Z}_p \to 1 + p\,\mathbf{Z}_p$ est donc surjectif. Il en est donc de même de $\widetilde{\varepsilon}_n \colon p\,\mathbf{Z}_p/p^n\,\mathbf{Z}_p \to 1 + p\,\mathbf{Z}/p^n\,\mathbf{Z}$. Comme on l'a vu ci-dessus, le morphisme d'anneaux π_n induit un isomorphisme de groupes $\mathbf{Z}_p/p^n\,\mathbf{Z}_p \xrightarrow{\sim} \mathbf{Z}/p^n\,\mathbf{Z}$: on a donc un isomorphisme de groupes $p\,\mathbf{Z}/p^n\,\mathbf{Z} \xrightarrow{\sim} p\,\mathbf{Z}_p/p^n\,\mathbf{Z}_p$. Composé avec $\widetilde{\varepsilon}_n$, cela fournit un morphisme de groupes surjectif

$$p\,\mathbf{Z}/p^n\,\mathbf{Z} \to 1 + p\,\mathbf{Z}/p^n\,\mathbf{Z}$$

qui est nécessairement un isomorphisme par cardinalité (la source et le but sont d'ordre p^{n-1}).

(65) Ici $p = 5$ et $n = 3$. Un générateur de $(5\,\mathbf{Z}/125\,\mathbf{Z}, +)$ est $\overline{5}$: d'après la question précédente, son image par l'isomorphisme $\widetilde{\varepsilon}_3 \colon 5\,\mathbf{Z}/125\,\mathbf{Z} \to 1 + 5\,\mathbf{Z}/125\,\mathbf{Z}$ est un générateur de $(1 + 5\,\mathbf{Z}/125\,\mathbf{Z}, .)$. Comme on l'a vu plus haut, on a $v_5\big(\frac{5^k}{k!}\big) \geq k\big(1 - \frac{1}{4}\big) = \frac{3k}{4}$, de sorte que $k \geq 4 \Rightarrow v_5\big(\frac{5^k}{k!}\big) \geq 3$. On a aussi $v_5\big(\frac{5^3}{3!}\big) = 3$: cela montre que $e_5(5) \equiv \sum_{k=0}^{2} \frac{5^k}{k!} \mod 125\,\mathbf{Z}_5$. On a $2 \times 3 \equiv 1 \mod 5$, d'où $2 \times 3 \times 25 \equiv 25 \mod 125$, de sorte que $\frac{25}{2} \equiv 75 \mod 125\,\mathbf{Z}_5$. Finalement, $e_5(5) \equiv 1 + 5 + 75 \mod 125\,\mathbf{Z}_5$, et donc $\widetilde{\varepsilon}_5(\overline{5}) = \overline{81}$ est un générateur de $(1 + 5\,\mathbf{Z}/125\,\mathbf{Z}, .)$.

Remarque. On peut montrer de façon plus élémentaire (par récurrence sur n) que si p est premier impair, alors la classe de $1 + p$ est un générateur de $(1 + p\,\mathbf{Z}/p^n\,\mathbf{Z}, .)$, donc ici $\overline{6}$ est aussi un générateur de $(1 + 5\,\mathbf{Z}/125\,\mathbf{Z}, .)$.

(66) D'après la question (64) (resp. la question (4)), le groupe $(1 + p\,\mathbf{Z}/p^n\,\mathbf{Z}, .)$ (resp. $((\mathbf{Z}/p\,\mathbf{Z})^\times, .)$) est cyclique, donc isomorphe à $(\mathbf{Z}/p^{n-1}\,\mathbf{Z}, +)$ (resp. $(\mathbf{Z}/(p-1)\,\mathbf{Z}, +)$). Par ailleurs, il existe un isomorphisme $(\mathbf{Z}/p^n\,\mathbf{Z})^\times \xrightarrow{\sim} (1 + p\,\mathbf{Z}/p^n\,\mathbf{Z}) \times (\mathbf{Z}/p\,\mathbf{Z})^\times$ en vertu de la question (61) : on en déduit qu'il existe un isomorphisme

$$(\mathbf{Z}/p^n\,\mathbf{Z})^\times \xrightarrow{\sim} (\mathbf{Z}/p^{n-1}\,\mathbf{Z}) \times (\mathbf{Z}/(p-1)\,\mathbf{Z})$$

(le groupe de départ étant multiplicatif, celui de droite additif). Comme $\mathsf{pgcd}(p^{n-1}, p-1) = 1$, le théorème des restes chinois implique que le morphisme naturel $\mathbf{Z}/p^{n-1}(p-1)\,\mathbf{Z} \to (\mathbf{Z}/p^{n-1}\,\mathbf{Z}) \times (\mathbf{Z}/(p-1)\,\mathbf{Z})$ est un isomorphisme de groupes additifs. on en déduit un isomorphisme de $((\mathbf{Z}/p^n\,\mathbf{Z})^\times, .)$ sur $(\mathbf{Z}/p^{n-1}(p-1)\,\mathbf{Z}, +)$, ce qui prouve que $((\mathbf{Z}/p^n\,\mathbf{Z})^\times, .)$ est cyclique.