Intermède : nombres p-adiques

1. Définition de l'anneau $\mathbb{Z}_p$ des entiers p-adiques

Soit p un nombre premier. On considère les anneaux $\mathbb{Z}/p^n$, $n \geq 0$, et les homomorphisme d'anneaux canoniques $\rho_{m,n} : \mathbb{Z}/p^m \to \mathbb{Z}/p^n$, $m \geq n \geq 0$.

Définition 1.1. *On note $\mathbb{Z}_p$ le sous-anneau de l'anneau $\prod_{n\geq 1} \mathbb{Z}/p^n$ constitué des éléments $(x_1, x_2, \ldots, x_n, \ldots)$ vérifiant $\rho_{m,n}(x_m) = x_n$ pour $m \geq n \geq 1$, ou ce qui revient au même $\rho_{n+1,n}(x_{n+1}) = x_n$ pour $n \geq 1$. L'anneau $\mathbb{Z}_p$ s'appelle l'anneau des entiers p-adiques. On note $\varepsilon_n : \mathbb{Z}_p \to \mathbb{Z}/p^n$ l'homomorphisme d'anneaux induit par la projection $\prod_{n\geq 1} \mathbb{Z}/p^n \to \mathbb{Z}/p^n$.*

Remarque 1.2. Soit $\mathcal{A}$ la catégorie dont les objets sont les anneaux (commutatifs unitaires) et dont les morphismes sont les homomorphismes d'anneaux. Pour tout anneau A l'application (ensembliste)

$$\mathrm{Hom}_{\mathcal{A}}(A, \mathbb{Z}_p) \to \prod_{n\geq 1} \mathrm{Hom}_{\mathcal{A}}(A, \mathbb{Z}/p^n) \qquad , \qquad f \mapsto (\varepsilon_n \circ f)_{n\geq 1}$$

induit une bijection de l'ensemble $\mathrm{Hom}_{\mathcal{A}}(A, \mathbb{Z}_p)$ sur le sous-ensemble du produit $\prod_{n\geq 1} \mathrm{Hom}_{\mathcal{A}}(A, \mathbb{Z}/p^n)$ constitué des éléments $(f_n)_{n\geq 1}$ vérifiant

$$f_n = \rho_{n+1,n} \circ f_{n+1}$$

pour tout $n \geq 1$.

Exercice 1.3. On note $\eta : \mathbb{Z} \to \mathbb{Z}_p$ l'homomorphisme unité (l'unique homomorphisme envoyant $1_{\mathbb{Z}}$ sur $1_{\mathbb{Z}_p}$). Montrer que η est injectif.

La question 3.5 de l'exercice ci-après montre en particulier qu'il existe des éléments de $\mathbb{Z}_p$ qui ne sont pas dans l'image de η (au moins pour $p > 2$) ; pour des exemples beaucoup plus prosaïques et une représentation très concrète des éléments de $\mathbb{Z}_p$ voir 4.10.

Exercice 1.4. Soit p un nombre premier.

1) Soient x et y deux entiers relatifs ; soit $n \geq 1$ un entier naturel.

1.1) Montrer que l'on a l'implication

$$x \equiv y \pmod{p^n} \;\Rightarrow\; x^p \equiv y^p \pmod{p^{n+1}} \qquad .$$

1.2) Montrer que l'on a l'implication

$$x \equiv y \pmod{p} \;\Rightarrow\; x^{p^{n-1}} \equiv y^{p^{n-1}} \pmod{p^n} \qquad .$$

2) Soit x un entier relatif. Montrer que l'on a la congruence

$$x^{p^{n+1}} \;\equiv\; x^{p^n} \pmod{p^n} \qquad .$$

[Indication. Observer que l'on a $x^p \equiv x \pmod{p}$.]

3) On note $\rho_n : \mathbb{Z} \to \mathbb{Z}/p^n$ l'homomorphisme canonique.

3.1) Montrer que l'application

$$\mathbb{Z} \to \prod_{n\geq 1} \mathbb{Z}/p^n \qquad , \qquad x \mapsto (\rho_1(x), \rho_2(x^p), \ldots, \rho_n(x^{p^{n-1}}), \ldots)$$

induit une application $\mathbb{Z}/p \to \mathbb{Z}_p$.

On note τ cette application.

3.2) Vérifier que l'application composée $\varepsilon_1 \circ \tau$ est l'identité de $\mathbb{Z}/p$ (τ s'appelle le *relèvement de Teichmüller*).

3.3) Vérifier que l'on a $\tau(0) = 0$ et $\tau(1) = 1$.

3.4) Vérifier que l'on a $\tau(xy) = \tau(x)\tau(y)$ pour tous x et y dans $\mathbb{Z}/p$ (observer par contre que l'on n'a pas en général $\tau(x + y) = \tau(x) + \tau(y)$).

3.5) Vérifier enfin que l'on a $(\tau(x))^p = \tau(x)$ pour tout x dans $\mathbb{Z}/p$.

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

Proposition 2.1. *Pout tout entier $n \geq 1$, la suite de groupes abéliens*

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\varepsilon_n} \mathbb{Z}/p^n \longrightarrow 0$$

est exacte.

Démonstration. Conséquence des énoncés 2.2 et 2.3 ci-après dont la vérification est laissée au lecteur.

Soient m et n deux entiers avec $0 \leq m \leq n$; la multiplication par p^{n-m}, vue comme un endomorphisme du groupe abélien $\mathbb{Z}$, induit un homomorphisme injectif de groupes abéliens, $\mathbb{Z}/p^m \to \mathbb{Z}/p^n$, que l'on note $\iota_{m,n}$.

Proposition 2.2. *Soient m et n deux entiers avec $m \geq n \geq 0$.*

(a) *La suite de groupes abéliens*

$$0 \longrightarrow \mathbb{Z}/p^{m-n} \xrightarrow{\iota_{m-n,m}} \mathbb{Z}/p^m \xrightarrow{\rho_{m,n}} \mathbb{Z}/p^n \longrightarrow 0$$

est exacte.

(b) *L'homorphisme composé*

$$\mathbb{Z}/p^n \xrightarrow{\iota_{n,m}} \mathbb{Z}/p^m \xrightarrow{\rho_{m,n}} \mathbb{Z}/p^n$$

coïncide avec la multiplication par p^{m-n}.

Proposition 2.3. *Pour tous entiers n, k et l, avec $n \geq 0$ et $l \geq k \geq 0$, le diagramme de groupes abéliens*

$$\begin{array}{ccc} \mathbb{Z}/p^l & \xrightarrow{\iota_{l,n+l}} & \mathbb{Z}/p^{n+l} \\ {\scriptstyle \rho_{l,k}}\downarrow & & \downarrow{\scriptstyle \rho_{n+l,n+k}} \\ \mathbb{Z}/p^k & \xrightarrow{\iota_{k,n+k}} & \mathbb{Z}/p^{n+k} \end{array}$$

est commutatif.

Démonstration de 2.1 à l'aide de 2.2 et 2.3. Soit $x := (x_1, x_2, \ldots, x_n, \ldots)$ un élément de $\mathbb{Z}_p \subset \prod_{n\geq 1} \mathbb{Z}/p^n$. Si x_n est nul alors on a $\rho_{n+k,n}(x_{n+k}) = 0$ pour tout entier $k \geq 0$. D'après 2.2 (a), il existe un élément y_k de $\mathbb{Z}/p^k$, uniquement déterminé, avec $\iota_{k,n+k}(y_k) = x_{n+k}$. D'après 2.3, l'élément $y := (y_1, y_2, \ldots, y_k, \ldots, \ldots)$ de $\prod_{n\geq 1} \mathbb{Z}/p^n$ appartient à $\mathbb{Z}_p$. D'après 2.2 (b), on a $p^n y = x$. Il reste à montrer que la multiplication par p^n de $\mathbb{Z}_p$ dans $\mathbb{Z}_p$ est injective. Soit y un élément de $\mathbb{Z}_p$; toujours d'après 2.2 (b), on a $\varepsilon_{k+n}(p^n y) = \iota_{k,n+k}(\varepsilon_k(y))$ pour tout entier $k \geq 1$, comme les homomorphismes $\iota_{k,k+n}$ sont injectifs, $p^n y = 0$ implique $\varepsilon_k(y) = 0$ pour tout $k \geq 1$, c'est-à-dire $y = 0$. □

Scholie 2.4. *L'homomorphisme d'anneaux $\varepsilon_n : \mathbb{Z}_p \to \mathbb{Z}/p^n$ induit un isomorphisme d'anneaux $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n$.*

[On observe que le diagramme

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\eta} & \mathbb{Z}_p \\ & {\scriptstyle \rho_n}\searrow \quad \swarrow{\scriptstyle \varepsilon_n} & \\ & \mathbb{Z}/p^n & \end{array}$$

est commutatif ; cette observation et le scholie ci-dessus montrent qu'il ne serait pas déraisonnable de remplacer la notation ε_n par ρ_n.]

Proposition 2.5. *Soit x un élément de $\mathbb{Z}_p$ Les deux propriétés suivantes sont équivalentes :*
(i) x est inversible ;
(ii) $\varepsilon_1(x)$ est inversible (ou ce qui revient au même non nul).

Démonstration. Conséquence de la proposition suivante dont la démonstration est laissée au lecteur.

Proposition 2.6. *Soit x un élément de $\mathbb{Z}/p^n$. Les deux propriétés suivantes sont équivalentes :*
(i) x est inversible ;
(ii) $\rho_{n,1}(x)$ est inversible (ou ce qui revient au même non nul).

Démonstration de 2.5 à l'aide de 2.6. Soit $x := (x_1, x_2, \ldots, x_n, \ldots)$ un élément de $\prod_{n\geq 1} \mathbb{Z}/p^n$. Si x appartient à $\mathbb{Z}_p$ et si x_1 est inversible alors x possède un inverse, disons y, dans l'anneau $\prod_{n\geq 1} \mathbb{Z}/p^n$, d'après 2.6. On achève en constatant que y appartient aussi à $\mathbb{Z}_p$. □

Proposition-Définition 2.7. *Tout élément x de $\mathbb{Z}_p - \{0\}$ s'écrit de façon unique*

$$x \;=\; p^n u$$

avec $n \in \mathbb{N}$ et $u \in \mathbb{Z}_p^\times$. L'entier n s'appelle la valuation p-adique *de x et se note* $\mathrm{v}_p(x)$.

Démonstration. Soit x un élément de $\mathbb{Z}_p - \{0\}$. Soit $\mathrm{D}(x)$ le sous-ensemble de $\mathbb{N}$ constitué des entiers k tels que p^k divise x dans $\mathbb{Z}_p$; $\mathrm{D}(x)$ possède les deux propriétés suivantes :

– 0 appartient à $\mathrm{D}(x)$;

– $\mathrm{D}(x)$ est majoré.

La première est évidente, la seconde résulte de l'implication $k \in \mathrm{D}(x) \Rightarrow \varepsilon_l(x) = 0$ pour $l \leq k$.

On pose $n = \sup \mathrm{D}(x)$. Par définition x s'écrit $p^n u$ avec $u \in \mathbb{Z}_p$; cette écriture est unique puisque la multiplication par p^n est injective (Proposition 2.1). On a $\varepsilon_1(u) \neq 0$ car $n+1$ n'appartient pas à $\mathrm{D}(x)$, si bien que u est inversible dans $\mathbb{Z}_p$ (Proposition 2.5). □

Corollaire 2.8. *L'anneau $\mathbb{Z}_p$ est intègre.*

Démonstration. Soient x et x' deux éléments non nuls de $\mathbb{Z}_p$. D'après 2.7 on a $x = p^n u$ et $x' = p^{n'} u'$ avec $n \in \mathbb{N}$, $n' \in \mathbb{N}$, $u \in \mathbb{Z}_p^\times$, $u' \in \mathbb{Z}_p^\times$. Le produit uu' appartient à $\mathbb{Z}_p^\times$ et est donc en particulier non nul ; le produit $xx' = p^{n+n'} uu'$ est non nul puisque la multiplication par $p^{n+n'}$ est injective (Proposition 2.1). □

Corollaire 2.9. *Soit I un idéal non nul de l'anneau $\mathbb{Z}_p$. Alors il existe un entier $n \geq 0$, uniquement déterminé, tel que l'on a $I = p^n \mathbb{Z}_p$.*

Démonstration. Soit I un idéal non nul de $\mathbb{Z}_p$. Le sous-ensemble non vide $\mathrm{v}_p(I - \{0\})$ de $\mathbb{N}$ possède un plus petit élément que l'on note n. Soit x_0 un élément de $I - \{0\}$ avec $\mathrm{v}_p(x_0) = n$. D'après 2.7, on a $x_0 = p^n u$ avec $u \in \mathbb{Z}_p^\times$; puisque l'on a $p^n = u^{-1} x_0$, p^n appartient à I et l'on a $p^n \mathbb{Z}_p \subset I$. Toujours d'après 2.7, tout élément de $I - \{0\}$ est divisible par p^n si bien que l'on a $I \subset p^n \mathbb{Z}_p$. □

Les énoncés 2.8 et 2.9 impliquent le suivant :

Scholie 2.10. *L'anneau $\mathbb{Z}_p$ est principal.*

Exercice 2.11. Soit M un groupe abélien, en d'autres termes un $\mathbb{Z}$-module.

Montrer que les conditions suivantes sont équivalentes :
(i) L'ensemble sous-jacent à M est fini de cardinal une puissance de p.
(ii) En tant que $\mathbb{Z}$-module, M est de type fini et annulé par une puissance de p.
(iii) Il existe un entier naturel n tel que M possède une structure de $\mathbb{Z}/p^n$-module, uniquement déterminée en fonction de M et n, pour laquelle M est de type fini, et qui induit sa structure de $\mathbb{Z}$-module *via* l'homomorphisme d'anneaux $\rho_n : \mathbb{Z} \to \mathbb{Z}/p^n$.
(iv) Il existe une structure de $\mathbb{Z}_p$-module sur M, uniquement déterminée en fonction de M, qui induit sa structure de $\mathbb{Z}$-module *via* l'homomorphisme d'anneaux $\eta : \mathbb{Z} \to \mathbb{Z}_p$, pour laquelle M est un $\mathbb{Z}_p$-module de type fini de torsion.

Montrer que si ces conditions sont satisfaites, alors il existe une suite finie d'entiers $n_1 \geq n_2 \geq \ldots \geq n_r > 0$, uniquement déterminée en fonction de M, telle que l'on a un isomorphisme de $\mathbb{Z}$-module ou de $\mathbb{Z}_p$-modules :

$$M \;\approx\; \mathbb{Z}/p^{n_1} \oplus \mathbb{Z}/p^{n_2} \oplus \ldots \oplus \mathbb{Z}/p^{n_r} \qquad .$$

Remarque 2.12. Tout élément x de $\mathbb{Z}-\{0\}$ s'écrit de façon unique $x = p^n u$ avec n dans $\mathbb{N}$ et u dans $\mathbb{Z}-\{0\}$ non divisible par p. L'entier n s'appelle la valuation p-adique de x et se note $\mathrm{v}_p(x)$. Les propositions 2.5 et 2.7 montrent que le diagramme

$$\begin{array}{ccc} \mathbb{Z}-\{0\} & \xrightarrow{\quad\eta\quad} & \mathbb{Z}_p-\{0\} \\ & {\scriptstyle \mathrm{v}_p}\searrow \quad \swarrow{\scriptstyle \mathrm{v}_p} & \\ & \mathbb{N} & \end{array}$$

est commutatif, en d'autres termes que l'application $\mathrm{v}_p : \mathbb{Z}_p - \{0\} \to \mathbb{N}$ prolonge l'application $\mathrm{v}_p : \mathbb{Z} - \{0\} \to \mathbb{N}$.

Conventions. On note $\overline{\mathbb{N}}$ la réunion disjointe $\mathbb{N} \coprod \{+\infty\}$ ($+\infty$ est ici juste un symbole). L'addition $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ se prolonge à $\overline{\mathbb{N}}$ en convenant que l'on a $n + (+\infty) = +\infty$ pour tout n dans $\overline{\mathbb{N}}$. De même on prolonge la relation d'ordre de $\overline{\mathbb{N}}$ en convenant que l'on a $n \leq (+\infty)$ pour tout n dans $\overline{\mathbb{N}}$. On prolonge l'application $\mathrm{v}_p : \mathbb{Z}_p - \{0\} \to \mathbb{N}$ en une application $\mathrm{v}_p : \mathbb{Z}_p \to \overline{\mathbb{N}}$ en posant $\mathrm{v}_p(0) = +\infty$.

Avec ces conventions, on a l'énoncé suivant :

Proposition 2.13. *Soient x et y deux éléments de $\mathbb{Z}_p$. On a :*

$$\mathrm{v}_p(xy) \;=\; \mathrm{v}_p(x) + \mathrm{v}_p(y) \qquad , \qquad \mathrm{v}_p(x+y) \;\geq\; \inf(\mathrm{v}_p(x), \mathrm{v}_p(y)) \qquad .$$

3. Le corps $\mathbb{Q}_p$ des nombres p-adiques

On a vu dans le paragraphe précédent que l'anneau $\mathbb{Z}_p$ est intègre.

Rappel. Soit A un anneau (commutatif unitaire) intègre ; la définition formelle de son corps des fractions est la même *mutatis mutandis* que celle de $\mathbb{Q}$ à partir de $\mathbb{Z}$. L'anneau A s'identifie à un sous-anneau de son corps des fractions.

Définition 3.1. *On note $\mathbb{Q}_p$ le corps des fractions de $\mathbb{Z}_p$; $\mathbb{Q}_p$ s'appelle le corps des nombres p-adiques.*

La vérification de l'affirmation contenue dans l'énoncé ci-dessous est laissée au lecteur.

Proposition-Définition 3.2. *Tout élément x de $\mathbb{Q}_p - \{0\}$ s'écrit de façon unique*

$$x \;=\; p^n u$$

avec $n \in \mathbb{Z}$ et $u \in \mathbb{Z}_p^\times$. L'entier n s'appelle la valuation p-adique *de x et se note $\mathrm{v}_p(x)$.*

Observations.
– Par définition, l'application $\mathrm{v}_p : \mathbb{Q}_p - \{0\} \to \mathbb{Z}$ prolonge l'application $\mathrm{v}_p : \mathbb{Z}_p - \{0\} \to \mathbb{N}$.
– L'homomorphisme d'anneaux "unité" $\mathbb{Z} \to \mathbb{Z}_p$ (qui est injectif, Excercice 1.3) induit un homomorphisme de corps $\mathbb{Q} \to \mathbb{Q}_p$ (forcément injectif). En d'autres termes, le corps $\mathbb{Q}_p$ est de caractéristique zéro. En d'autres termes encore, $\mathbb{Z}$ et $\mathbb{Q}$ s'identifient respectivement à un sous-anneau de $\mathbb{Q}_p$ et à un sous-corps de $\mathbb{Q}_p$. On constate que $\mathbb{Z}$ l'intersection, dans $\mathbb{Q}_p$, de $\mathbb{Q}$ et $\mathbb{Z}_p$ (le lecteur aura à coeur de vérifier cette affirmation).

4. Topologie de $\mathbb{Q}_p$

Définition 4.1. *Soit K un corps. Une* valeur absolue *sur K est une application $x \mapsto |x|$ de K dans $\mathbb{R}$ vérifiant les axiomes suivants :*

– $|x| \geq 0$ *pour tout x et* $|x| = 0 \iff x = 0$,

– $|xy| = |x||y|$ *pour tout x et tout y ,*

– $|x + y| \leq |x| + |y|$ *pour tout x et tout y .*

Si l'axiome suivant (qui implique le précédent) :

– $|x + y| \leq \sup(|x|, |y|)$ *pour tout x et tout y*

est vérifié on dit que la valeur absolue est non archimédienne.

La vérification de l'affirmation contenue dans l'énoncé ci-dessous est laissée au lecteur.

Définition-Proposition 4.2. *Soit x un élément de $\mathbb{Q}_p$; on pose*

$$|x|_p \;=\; \begin{cases} 0 & \text{pour } x = 0, \\ p^{-\mathrm{v}_p(x)} & \text{pour } x \neq 0. \end{cases}$$

L'application $x \mapsto |x|_p$ est une valeur absolue non archimédienne sur le corps $\mathbb{Q}_p$ que l'on appelle la valeur absolue p-adique.

Exercice 4.3. Soit x un élément de $\mathbb{Q}$. On note $|x|_\infty$ la valeur absolu de x vu comme un élément de $\mathbb{R}$: $|x|_\infty = \sup(x, -x)$. On note V la réunion disjointe de l'ensemble $\{2, 3, 5, 7, \ldots\}$ des nombres premiers et du symbole ∞. Vérifier que le sous-ensemble de V constitué des v avec $|x|_v \neq 1$, disons V_x, est fini et que l'on a l'égalité

$$\prod_{v \in \mathrm{V}} |x|_v \;=\; 1$$

(le premier membre étant défini comme le produit fini indexé par V_x).

Soit K un corps muni d'une valeur absolue $|\ |$; on note $\mathrm{d} : K \times K \to \mathbb{R}$ l'application $(x, y) \mapsto |y - x|$. L'application d ainsi définie est une distance sur K qui en fait un espace métrique (et *a fortiori* un espace topologique). L'addition et la multiplication de K sont des applications continues de $K \times K$ dans K ; $K - \{0\}$ est un ouvert de K et l'application $x \mapsto x^{-1}$ de $K - \{0\}$ dans $K - \{0\}$ est continue.

Dans le cas de $\mathbb{Q}_p$ et de la valeur absolue p-adique, qui est non archimédienne, l'inégalité triangulaire $\mathrm{d}(x, z) \leq \mathrm{d}(x, y) + \mathrm{d}(y, z)$ est impliquée par l'inégalité *ultratriangulaire* $\mathrm{d}(x, z) \leq \sup(\mathrm{d}(x, y), \mathrm{d}(y, z))$ (l'espace métrique $\mathbb{Q}_p$ est dit *ultramétrique*).

Exercice 4.4. Vérifier que le sous-ensemble $\mathbb{Z}_p$ de l'espace métrique $\mathbb{Q}_p$ est la boule fermée de centre 0 et de rayon 1.

Exercice 4.5. On munit l'ensemble $\mathbb{Z}_p$ de la topologie induite par la valeur absolue p-adique et l'ensemble $\mathbb{Z}/p^n$ de sa topologie discrète. Montrer l'application $\varepsilon_n : \mathbb{Z}_p \to \mathbb{Z}/p^n$ est continue.

Théorème 4.6. *Muni de la métrique induite par la valeur absolue p-adique, $\mathbb{Z}_p$ est complet.*

Démonstration. Soit $x : \mathbb{N} \to \mathbb{Z}_p$ une suite de Cauchy pour cette métrique. Soit $n \geq 1$ un entier ; par définition d'une suite de Cauchy, il existe un entier $C_n \geq 0$ tel que l'on a $|x(l) - x(k)|_p \leq p^{-n}$ pour $k \geq C_n, l \geq C_n$. Par définition de la valeur absolue p-adique l'inégalité $|x(l) - x(k)|_p \leq p^{-n}$ équivaut à $\varepsilon_n(x(k)) = \varepsilon_n(x(l))$; on a donc $\varepsilon_n(x(k)) = \varepsilon_n(x(C_n))$ pour $k \geq C_n$. On pose $L_n = \varepsilon_n(x_{C_n})$; on constate que l'élément $L := (L_1, L_2, \ldots, L_n, \ldots)$ de $\prod_{n \geq 1} \mathbb{Z}/p^n$ appartient à $\mathbb{Z}_p$ et que l'on a $|x(k) - L|_p \leq p^{-n}$ pour $k \geq C_n$. Cette dernière inégalité montre que la suite x converge vers L. □

Corollaire 4.7. *Muni de la métrique induite par la valeur absolue p-adique, $\mathbb{Q}_p$ est complet.*

Démonstration. Soit $x : \mathbb{N} \to \mathbb{Q}_p$ une suite de Cauchy pour cette métrique. L'inégalité triangulaire montre que la suite $\mathbb{N} \to \mathbb{R}$, $k \mapsto |x(k)|_p$ est aussi une suite de Cauchy ; elle est donc en particulier majorée : il existe un entier $n \geq 0$ tel que l'on a $|x(k)|_p \leq p^n$ pour tout k dans $\mathbb{N}$, c'est-à-dire que $p^n x(k)$ appartient à $\mathbb{Z}_p$ pour tout k dans $\mathbb{N}$. Ceci montre que 4.6 implique 4.7. □

Exercice 4.8. Montrer que $\mathbb{Z}$ est dense dans $\mathbb{Z}_p$ et que $\mathbb{Q}$ est dense dans $\mathbb{Q}_p$.

Commentaires

Si l'on munit $\mathbb{R}$ de la métrique induite par la valeur absolue $|\ |_\infty$ (notation de 4.3), alors $\mathbb{R}$ est complet et $\mathbb{Q}$ est dense dans $\mathbb{R}$. Ces deux propriétés font que $\mathbb{R}$ est le complété de $\mathbb{Q}$ muni de la métrique induite par la valeur absolue $|\ |_\infty$ (c'est d'ailleurs une façon de définir $\mathbb{R}$!). Pareillement 4.7 et 4.8 font que l'espace métrique $\mathbb{Q}_p$ est le complété de $\mathbb{Q}$ muni de la métrique induite par la valeur absolue $|\ |_p$.

Soit $|\ |$ une valeur absolue sur $\mathbb{Q}$. On peut montrer qu'il existe un élément v de $\{\infty, 2, 3, 5, 7, \ldots\}$ (notation de 4.3) et une constante réelle $c > 0$, avec $c \leq 1$ pour $v = \infty$, uniquement déterminés, telle que l'on a $|x| = (|x|_v)^c$ pour tout x dans $\mathbb{Q}$ (Théorème d'Ostrowski, le lecteur est encouragé à consulter l'article Wikipédia sur ce théorème, version française et anglaise). Il en résulte que le complété de $\mathbb{Q}$ pour la métrique induite par la valeur absolue $|\ |$ coïncide avec $\mathbb{Q}_v$ (avec la convention $\mathbb{Q}_\infty = \mathbb{R}$).

Exercice 4.9. Montrer que l'espace métrique $\mathbb{Z}_p$ est compact.

[Indication. Utiliser le critère de Bolzano-Weierstrass dont on rappelle l'énoncé ci-après.

Soit E un espace métrique. Les deux conditions suivantes sont équivalentes :
(i) E est compact ;
(ii) toute suite à valeurs dans E admet une sous-suite convergente.]

L'espace métrique $\mathbb{Q}_p$ est-il compact ?

[Pour trancher la question, considérer par exemple la fonction continue $\mathbb{Q}_p \to \mathbb{R}$, $x \mapsto |x|_p$ (au fait pourquoi cette fonction est-elle continue ?).]

Exercice 4.10 (séries de nombres p-adiques)**.** Soit $u : \mathbb{N} \to \mathbb{Q}_p$ une suite de nombres p-adiques. Sans surprise, on dit que la série u est convergente si la suite $n \mapsto \sum_{k=0}^{n} u(k)$ est convergente ; dans ce cas la limite de cette dernière suite s'appelle la somme de la série et se note $\sum_{k=0}^{+\infty} u(k)$.

1) Soit $u : \mathbb{N} \to \mathbb{Q}_p$ une suite de nombres p-adiques. Montrer que les deux conditions suivantes sont équivalentes :
(i) La série u est convergente.
(ii) La suite u converge vers 0.

2) Soit x un élément de $\mathbb{Z}_p$. Montrer qu'il existe une suite

$$c : \mathbb{N} \to \{0, 1, \ldots, p-1\} \qquad ,$$

uniquement déterminée en fonction de x, telle que l'on a

$$x \;=\; \sum_{n=0}^{+\infty} c(n)\, p^n \qquad .$$

L'écriture ci-dessus s'appelle le *développement p-adique* de x.

Expliciter les développements p-adiques de $(1-p)^{-1}$ et -1.

Montrer que l'application $x \mapsto c$ est une bijection de l'ensemble $\mathbb{Z}_p$ sur l'ensemble $\{0, 1, \ldots, p-1\}^{\mathbb{N}}$. L'ensemble $\mathbb{Z}_p$ est-il dénombrable ?

3) Soit x un élément de $\mathbb{Q}_p$. Montrer qu'il existe une application

$$c : \mathbb{Z} \to \{0, 1, \ldots, p-1\} \qquad ,$$

uniquement déterminée en fonction de x, telle que l'ensemble des n avec $c(n) \neq 0$ est minoré, et telle que l'on a

$$x \;=\; \sum_{n=-\infty}^{+\infty} c(n)\, p^n$$

(le lecteur aura à coeur d'expliciter la signification du second membre).

Il est clair que x appartient à $\mathbb{Z}_p$ si et seulement si l'on a $c(n) = 0$ pour $n < 0$; évidemment, l'écriture ci-dessus s'appelle encore le *développement p-adique* de x.

Montrer que les deux conditions suivantes sont équivalentes :
(i) x appartient à $\mathbb{Q}$;
(ii) l'application c est périodique "à partir d'un certain rang", en clair il existe un entier n_0 et un entier $\nu > 0$ tels que l'on a $c(n+\nu) = c(n)$ pour $n \geq n_0$.

5. Relèvement dans $\mathbb{Z}_p$ de certaines solutions modulo p d'équations polynômiales

Ce titre énigmatique fait référence à l'énoncé suivant :

Théorème 5.1. *Soit P un polynôme de $\mathbb{Z}_p[X]$. Soit ξ un élément de $\mathbb{Z}/p$ vérifiant $(\varepsilon_1 P)(\xi) = 0$ et $(\varepsilon_1 P')(\xi) \neq 0$ (en d'autres termes soit ξ une racine simple dans $\mathbb{Z}/p$ du polynôme $\varepsilon_1 P$ de $\mathbb{Z}/p[X]$). Alors il existe un élément x de $\mathbb{Z}_p$, uniquement déterminé, vérifiant $\varepsilon_1(x) = \xi$ et $P(x) = 0$.*

On va donner deux démonstrations de ce théorème. La première, purement algébrique, utilise essentiellement la définition 1.1. La seconde utilise la structure d'espace métrique de $\mathbb{Z}_p$ introduite au paragraphe 4 et le théorème de point fixe concernant les applications contractantes d'un espace métrique complet dans lui-même.

Il sera commode, pour ces deux démonstrations, de disposer de l'énoncé suivant, concernant la définition même du dérivé formel d'un polynôme.

Proposition 5.2. *Soient A un anneau (commutatif unitaire) et P un polynôme de $A[X]$. Alors il existe un polynôme R_P de $A[X,Y]$ (uniquement déterminé en fonction de P) tel que l'on a*

$$P(Y) - P(X) \;=\; P'(X)\,(Y-X) + \mathrm{R}_P(X,Y)\,(Y-X)^2 \qquad .$$

Démonstration. Il est clair qu'il suffit de traiter le cas $P = X^n$ avec $n \in \mathbb{N}$. Les cas $n = 0$ et $n = 1$ sont triviaux. Pour $n \geq 2$, la formule du binôme donne

$$\begin{aligned} Y^n - X^n \;&=\; (X + (Y-X))^n - X^n \;= \\ &(nX^{n-1})\,(Y-X) + \left(\sum_{k=2}^{n} \binom{n}{k} X^{n-k} Y^k\right)(Y-X)^2 \qquad . \qquad \square \end{aligned}$$

Exercice 5.3. Montrer que l'identité de la proposition 5.2 implique la partie unicité du théorème 5.1, en clair que si x et y sont deux éléments de $\mathbb{Z}_p$ avec $\varepsilon_1(x) = \xi$, $P(x) = 0$, $\varepsilon_1(y) = \xi$ et $P(y) = 0$ alors on a $x = y$.

[Ne pas oublier que l'on a l'hypothèse $(\varepsilon_1 P')(\xi) \neq 0$.]

Première démonstration du théorème 5.1. Le lecteur vérifiera que le théorème 5.1 est une conséquence immédiate de l'énoncé ci-dessous.

Lemme 5.4. *Soit $n \geq 1$ un entier ; soit P un polynôme $(\mathbb{Z}/p^{n+1})[X]$. Soit x un élément de $\mathbb{Z}/p^n$ vérifiant $(\rho_{n+1,n}P)(x) = 0$ et $(\rho_{n+1,1}P')(\rho_{n,1}(x)) \neq 0$. Alors il existe un élément y de $\mathbb{Z}/p^{n+1}$, uniquement déterminé, vérifiant $\rho_{n+1,n}(y) = x$ et $P(y) = 0$.*

Démonstration. La rédation ci-après de la démonstration de ce lemme est un peu pédante ; le lecteur est encouragé à la démystifier !

Soit R l'ensemble des "relèvements" de x dans $\mathbb{Z}/p^{n+1}$: $R = \rho_{n+1,n}^{-1}(x)$. L'ensemble R est non vide et possède une structure canonique de droite affine sur le corps $\mathbb{Z}/p$, en clair, l'application

$$\mathbb{Z}/p \times R \to R \qquad , \qquad (\alpha, r) \mapsto r + \iota_{1,n+1}(\alpha)$$

(on rappelle, voir la démonstration de 2.1, que la notation $\iota_{1,n+1}$ désigne l'homomorphisme injectif de groupes abéliens, de $\mathbb{Z}/p$ dans $\mathbb{Z}/p^{n+1}$, induit par la multiplication par p^n) définit une action libre et transitive du groupe $\mathbb{Z}/p$ sur R. L'hypothèse $(\rho_{n+1,n}P)(x) = 0$ implique $\rho_{n+1,n}(P(r)) = 0$ pour tout r dans R ; il existe donc un élément ϕ de $\mathbb{Z}/p$, uniquement déterminé en fonction de r, tel que l'on a $P(r) = \iota_{1,n+1}(\phi)$. On note $f : R \to \mathbb{Z}/p$ l'application $r \mapsto \phi$; f est une application affine dont l'application linéaire sous-jacente $\widetilde{f} : \mathbb{Z}/p \to \mathbb{Z}/p$ est un isomorphisme.

Décodons. On pose $\delta = (\rho_{n+1,1}P')(\rho_{n,1}(x))$, par hypothèse δ est un élément de $(\mathbb{Z}/p)^\times$; on observera que l'on a aussi $\delta = (\rho_{n+1,1}P')(\rho_{n+1,1}(r))$ pour tout r dans R. Soient r_0 et r_1 deux éléments de R ; en prenant $A = \mathbb{Z}/p^{n+1}$ dans 5.2 et en spécialisant les indéterminées X et Y respectivement en r_0 et r_1, on constate que l'on a

$$f(r_1) - f(r_0) \;=\; \delta(r_1 - r_0)$$

(observer que l'on a $(r_1 - r_0)^2 = 0$).

Le point y de R dont l'énoncé 5.4 affirme l'existence et l'unicité est l'unique solution de l'équation $f(y) = 0$: $y = r - \iota_{1,n+1}(\delta^{-1}f(r))$ pour un choix arbitraire de r dans R (théorie de l'équation du premier degré !). □

Seconde démonstration du théorème 5.1.

On pose $B = \varepsilon_1^{-1}(\xi)$; B est un fermé non vide de $\mathbb{Z}_p$ (Exercice 4.5). En fait B est une boule fermée de $\mathbb{Z}_p$ (ce qui justifie la notation) : soient c un point de B et x un point de $\mathbb{Z}_p$, l'égalité $\varepsilon_1(x) = \xi$ équivaut à l'inégalité $|x - c|_p \leq p^{-1}$.

Soit δ un élément de $\mathbb{Z}_p$ avec $\varepsilon_1(\delta) = (\varepsilon_1 P')(\xi)$; δ appartient donc à $\mathbb{Z}_p^\times$ (Proposition 2.5). Soit y un élément de B, alors $y - \delta^{-1}P(y)$ appartient aussi à B puisque l'on a $\varepsilon_1(P(y)) = (\varepsilon_1 P)(\varepsilon_1(y)) = (\varepsilon_1 P)(\xi) = 0$. On note $f : B \to B$, l'application $y \mapsto y - \delta^{-1}P(y)$. La proposition 5.2 implique que l'on a l'inégalité

$$(*) \qquad |f(z) - f(y)|_p \ \leq \ p^{-1}\,|z - y|_p$$

pour tous y et z dans B. Détaillons. L'identité de 5.2 montre que l'on a $f(z) - f(y) = a(y,z)(z - y)$ avec $a(y,z) = 1 - \delta^{-1}P'(y) + \mathrm{R}_P(y,z)(z - y)$. On constate que l'on a $\varepsilon_1(a(y,z)) = 0$ soit encore $|a(y,z)|_p \leq p^{-1}$.

On achève en invoquant le théorème de point fixe concernant les applications contractantes d'un espace métrique complet dans lui-même. Le sous-espace B, muni de la métrique induite par celle de $\mathbb{Z}_p$, est complet puisqu'il est fermé dans $\mathbb{Z}_p$ qui est complet (Théorème 4.6). L'inégalité $(*)$ ci-dessus dit que l'application $f : B \to B$ est contractante, elle possède donc un unique point fixe que l'on note x. Or pour tout point y de B, l'égalité $f(y) = y$ équivaut à l'égalité $P(y) = 0$. □

Exercice 5.5. Que donne le théorème 5.1 si l'on prend pour P le polynôme $X^p - X$? Plus précisément, que donne dans ce cas la seconde démonstration du théorème 5.1, si l'on prend $\delta = -1$? Faire le lien avec l'exercice 1.4.

Exercice 5.6. Vérifier que l'on peut remplacer, dans la seconde démonstration du théorème 5.1, l'application $B \to B$, $y \mapsto y - \delta^{-1}P(y)$ par l'application

$$B \to B \qquad , \qquad y \mapsto y - \frac{P(y)}{P'(y)}$$

(*méthode de Newton*).

Exercice 5.7. Soit $p > 2$ un nombre premier.

1) Soit d un élément de $\mathbb{Z}_p^\times$, montrer que les conditions suivantes sont équivalentes :
(i) $\varepsilon_1(d)$ est un carré dans $(\mathbb{Z}/p)^\times$;
(ii) d est un carré dans $\mathbb{Z}_p^\times$;
(iii) d est un carré dans $\mathbb{Q}_p^\times$.

[Pour l'implication (i)⇒(ii), utiliser le théorème 5.1 avec $P = X^2 - d$.]

2) On note $(\mathbb{Z}/p)^{\times 2}$ (resp. $\mathbb{Z}_p^{\times 2}$, resp. $\mathbb{Q}_p^{\times 2}$) le sous-groupe de $(\mathbb{Z}/p)^\times$ (resp. $\mathbb{Z}_p^\times$, resp. $\mathbb{Q}_p^\times$) constitué des carrés.

2.1) Montrer que le groupe quotient $(\mathbb{Z}/p)^\times/(\mathbb{Z}/p)^{\times 2}$ est cyclique d'ordre 2.

2.2) Montrer que l'homomorphisme d'anneaux $\varepsilon_1 : \mathbb{Z}_p \to \mathbb{Z}/p$ induit un isomorphisme de groupes

$$\mathbb{Z}_p^\times/\mathbb{Z}_p^{\times 2} \to (\mathbb{Z}/p)^\times/(\mathbb{Z}/p)^{\times 2} \qquad .$$

2.3) Expliciter un isomorphisme de groupes

$$\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \to \mathbb{Z}/2 \times ((\mathbb{Z}/p)^\times/(\mathbb{Z}/p)^{\times 2}) \qquad .$$

Exercice 5.8. Dans cet exercice on prend $p = 2$.

1) Soit d un élément de $\mathbb{Z}_2^\times$, montrer que les conditions suivantes sont équivalentes :
(i) on a $\varepsilon_3(d) = 1$;
(ii) il existe un élément r de $\mathbb{Z}_2$ avec $\varepsilon_2(r) = 1$ et $r^2 = d$;
(iii) d est un carré dans $\mathbb{Z}_2^\times$;
(iv) d est un carré dans $\mathbb{Q}_p^\times$.

[Pour l'implication (i)⇒(ii), utiliser le théorème 5.1 avec $P = 2X^2 + X - \frac{d-1}{8}$.]

Montrer que si la condition (i) est vérifiée alors l'élément r de la condition (ii) est uniquement déterminé en fonction de d.

2) On note $\mathbb{Z}_2^{\times 2}$ (resp. $\mathbb{Q}_2^{\times 2}$) le sous-groupe de $\mathbb{Z}_2^\times$ (resp. $\mathbb{Q}_2^\times$) constitué des carrés.

2.1) Montrer que le groupe $(\mathbb{Z}/8)^\times$ est isomorphe à $\mathbb{Z}/2 \times \mathbb{Z}/2$ et plus précisément que $\{-1, 5\}$ est une base de $(\mathbb{Z}/8)^\times$ vu comme un $\mathbb{Z}/2$-espace vectoriel.

2.2) Montrer que l'homomorphisme d'anneaux $\varepsilon_3 : \mathbb{Z}_2 \to \mathbb{Z}/8$ induit un isomorphisme de groupes

$$\mathbb{Z}_2^\times/\mathbb{Z}_2^{\times 2} \to (\mathbb{Z}/8)^\times \qquad .$$

2.3) Expliciter un isomorphisme de groupes

$$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2} \to \mathbb{Z}/2 \times (\mathbb{Z}/8)^\times \qquad .$$

Expliciter une base de $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$, vu comme un $\mathbb{Z}/2$-espace vectoriel.

Exercice 5.9. Soit S un ensemble fini non vide de nombres premiers impairs. Soient $d > 0$ et $a > 0$ deux nombres entiers, avec $d \not\equiv 0 \pmod p$ et $a^2 \equiv d \pmod p$ pour tout p dans S.
On considère la fraction rationnelle de $\mathbb{Q}(X)$ suivante

$$f(X) \;=\; \frac{1}{2}(X + \frac{d}{X}) \qquad .$$

On note enfin $x : \mathbb{N} \to \mathbb{Q}$ la suite de rationnels strictement positifs définie par $x(0) = a$ et $x(n) = f(x(n-1))$ pour $n \geq 1$.

(L'exercice est une illustration de la méthode de Newton, voir Exercice 5.6, car l'on a

$$f(X) \;=\; X - \frac{P(X)}{P'(X)}$$

pour $P = X^2 - d$.)

1) Soit p un nombre premier dans S. Montrer qu'il existe un élément r_p de $\mathbb{Z}_p$, uniquement déterminé, vérifiant $r_p \equiv a \pmod{p\mathbb{Z}_p}$ et $r_p^2 = d$.
[Utiliser le théorème 5.1.]

2) Montrer que la suite x converge dans $\mathbb{R}$ vers $\sqrt{d}$ et plus précisément qu'il existe un nombre réel $C > 0$ tel que l'on a l'inégalité

$$|\, x(n) - \sqrt{d}\,|_\infty \;\leq\; C \left(\frac{|\, a - \sqrt{d}\,|_\infty}{a + \sqrt{d}} \right)^{2^n}$$

pour tout n dans $\mathbb{N}$.

3) Soit p un nombre premier dans S. Montrer que la suite x converge dans $\mathbb{Q}_p$ vers r_p et plus précisément que l'on a l'égalité et l'inégalité suivantes

$$|x(n) - r_p|_p \;=\; \left(|a - r_p|_p\right)^{2^n} \;\leq\; p^{-2^n}$$

pour tout n dans $\mathbb{N}$.

[Indication pour les questions 2 et 3. Soit K un corps de caractéristique différente de 2. Considérer la fraction rationnelle de $K(X,Y)$ suivante

$$\mathrm{F}(X,Y) \;=\; \frac{1}{2}(X + \frac{Y^2}{X})$$

et observer que l'on a l'identité

$$\frac{\mathrm{F}(X,Y) - Y}{\mathrm{F}(X,Y) + Y} \;=\; \left(\frac{X - Y}{X + Y}\right)^2 \qquad . \qquad]$$