Entiers p-adiques et corps p-adiques

1 Structure et topologie des entiers p-adiques

Exercice 1

1) Écrire les nombres $2/3$ et $-2/3$ sous la forme de nombres 5-adiques :

$$\sum_{n\geqslant 0} a_n \cdot 5^n$$

avec $a_n \in \{0,1,2,3,4\}$.

2) On considère un nombre p-adique :

$$x = \sum_{n\geqslant 0} a_n \cdot p^n \in \mathbb{Q}_p$$

avec $a_n \in \{0,1,2,...,p-1\}$. Montrer que $x \in \mathbb{Q}$ si, et seulement si, la suite $(a_n)_{n\geqslant 0}$ est périodique à partir d'un certain rang.

Exercice 2 Soit x un nombre rationnel. Déterminer pour quels nombre premiers p la suite $(x^n)_{n\geqslant 1}$ converge.

Exercice 3 Pour n et m deux entiers naturels non nuls tels que $n|m$, on note $\pi_{m,n}$ la projection naturelle $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. On pose :

$$\hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \{(x_n)_n \in \prod_n \mathbb{Z}/n\mathbb{Z} \mid \forall (n,m) \in (\mathbb{N}^*)^2, n|m \Rightarrow \pi_{m,n}(x_m) = x_n\}.$$

En notant $\mathscr{P}$ l'ensemble des nombres premiers, montrer que $\hat{\mathbb{Z}} \cong \prod_{p\in\mathscr{P}} \mathbb{Z}_p$.

Exercice 4 Soit p un nombre premier. Soient $a \in \mathbb{Q}_p$ et $r > 0$.

1) Montrer que la boule de centre a et de rayon r est ouverte et fermée. Quel est son bord ?
2) Quelle est la composante connexe de a dans $\mathbb{Q}_p$?

Exercice 5 Soit p un nombre premier. Soient a et b deux entiers naturels. Quelle est l'adhérence de l'ensemble $\Sigma_{a,b} := \{a + bn : n \geqslant 0\}$ dans $\mathbb{Z}_p$? A quelle condition sur (a,b) l'ensemble $\Sigma_{a,b}$ est-il dense dans $\mathbb{Z}_p$?

Exercice 6 Une **valeur absolue** sur un corps K est une application :

$$\|\cdot\| : K \to \mathbb{R}_{\geqslant 0}$$

telle que :

(i) $\forall x \in K,\ \|x\| = 0 \Leftrightarrow x = 0$.
(ii) $\forall x, y \in K,\ \|xy\| = \|x\|\,\|y\|$.
(iii) $\forall x, y \in K,\ \|x+y\| \leqslant \|x\| + \|y\|$.

Dans cet exercice, on étudie quelques propriétés générales des valeurs absolues.

1) On dit que $\|\cdot\|$ est **non archimédienne** si la suite $(\|n\|)_{n\geqslant 0}$ reste bornée. Montrer que $\|\cdot\|$ est non archimédienne si, et seulement si, elle vérifie l'inégalité triangulaire forte :

$$\forall x, y \in K,\ \|x+y\| \leqslant \max\{\|x\|, \|y\|\}.$$

2) On dit que deux valeurs absolues sont **équivalentes** si, et seulement si, elles induisent la même topologie sur K. Montrer que deux valeurs absolues $\|\cdot\|$ et $\|\cdot\|'$ sont équivalentes si, et seulement si, il existe $s > 0$ tel que $\|\cdot\|' = \|\cdot\|^s$.
3) Soient $\|\cdot\|_1, \ldots, \|\cdot\|_n$ des valeurs absolues sur K qui sont deux à deux non équivalentes. Montrer que, pour tout $\varepsilon > 0$ et tout $(x_1, \ldots, x_n) \in K^n$ il existe $x \in K$ tel que :

$$\forall i,\ \|x - x_i\|_i < \varepsilon.$$

Exercice 7 Dans cet exercice, on va trouver toutes les valeurs absolues sur $\mathbb{Q}$. Pour la terminologie utilisée, on pourra se référer à l'exercice précédent.

1) On suppose que $\|\cdot\|$ est non archimédienne, c'est-à-dire que la suite $(\|n\|)_{n\geqslant 0}$ reste bornée. Montrer qu'il existe un nombre premier p et un réel $c > 1$ tels que $\|x\| = c^{-v_p(x)}$ pour tout $x \in \mathbb{Q}$.
2) On suppose que $\|\cdot\|$ est archimédienne, c'est-à-dire que la suite $(\|n\|)_{n\geqslant 0}$ n'est pas bornée. Montrer qu'il existe un réel $s > 0$ tel que $\|x\| = |x|^s$ pour tout $x \in \mathbb{Q}$.

Exercice 8 Soit k un corps. Pour $x \in k[[T]]$ et $y \in k[[T]]$, on pose $v(x) = \max\{n \in \mathbb{N} / x \in (T^n)\}$ et $d(x, y) = e^{-v(x-y)}$.

1) Montrer que d définit une distance sur $k[[T]]$ et que $k[[T]]$ est alors complet pour cette distance. Quand $k[[T]]$ est-il compact ?
2) Montrer que $k[[T]]$ est un anneau principal dont les idéaux sont les (T^r) pour $r \geqslant 0$.

2 Equations sur les corps p-adiques

Exercice 9 Soit $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Q}_p[X]$. Montrer que les racines de f dans $\mathbb{Q}_p$ appartiennent à la boule fermée de centre 0 et de rayon $M := \max\{1, |a_0|_p, \ldots, |a_{n-1}|_p\}$.

Exercice 10 Soit p un nombre premier.

1) A l'aide du lemme de Hensel, calculer le groupe des racines de l'unité dans $\mathbb{Q}_p$.
2) En déduire que :

$$\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{F}_p^\times \times (1 + p\mathbb{Z}_p).$$

3) On suppose que p est impair et on considère les séries :

$$\log(1+z) = \sum_{n\geqslant 1} (-1)^{n+1} \frac{z^n}{n}, \quad \exp(z) = \sum_{n\geqslant 1} \frac{z^n}{n!}.$$

Montrer qu'elles induisent des isomorphismes réciproques entre $1+p\mathbb{Z}_p$ et $p\mathbb{Z}_p$, puis en déduire que :

$$\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{F}_p^\times \times \mathbb{Z}_p.$$

4) Que se passe-t'il quand $p = 2$?

Exercice 11 Soient l et p deux nombres premiers. On suppose que $\mathbb{Q}_p$ et $\mathbb{Q}_l$ sont isomorphes. En utilisant la question 1) de l'exercice précédent, montrer que $l = p$.

Exercice 12 Soit p un nombre premier.

1) Montrer que, pour tout $a \in \mathbb{Z}_p$, la suite $(a^{p^n})_{n\geqslant 0}$ converge. On note $\omega(a)$ sa limite.
2) Soit $\rho : \mathbb{Z}_p \to \mathbb{F}_p$. Montrer que $\omega : \mathbb{Z}_p \to \mathbb{Z}_p$ induit une application $\omega : \mathbb{F}_p \to \mathbb{Z}_p$ telle que $\rho \circ \omega$ est l'identité de $\mathbb{F}_p$ et $\omega|_{\mathbb{F}_p^\times} : \mathbb{F}_p^\times \to \mathbb{Z}_p^\times$ est un morphisme de groupes injectif. Quelle est l'image de ω ? L'application ω s'appelle le **relèvement de Teichmüller**.

Exercice 13 Soit p un nombre premier.

1) Soit $a \in \mathbb{Q}_p^\times$. On écrit $a = up^\alpha$ avec $u \in \mathbb{Z}_p^\times$ et $\alpha \in \mathbb{Z}$.
   a) Si p est impair, montrer que a est un carré dans $\mathbb{Q}_p$ si, et seulement si, α est pair et la réduction $[u]$ de u modulo p est un carré dans $\mathbb{F}_p$.
   b) Si $p = 2$, montrer que a est un carré dans $\mathbb{Q}_2$ si, et seulement si, α est pair et $u \equiv 1 \mod 8$.
2) Soient a et b dans $\mathbb{Q}_p^\times$. On définit le **symbole de Hilbert** de a et b de la manière suivante :

$$(a,b)_p := \begin{cases} 1 & \text{si l'équation } x^2 - ay^2 - bz^2 = 0 \text{ a des solutions non nulles dans } \mathbb{Q}_p, \\ -1 & \text{sinon.} \end{cases}$$

On cherche à prouver les formules suivantes :

$$(a,b)_p = \begin{cases} \left(\frac{\left[(-1)^{\alpha\beta} u^\beta v^\alpha\right]}{p}\right) & \text{si } p \text{ est impair} \\ (-1)^{\left[\frac{u-1}{2}\frac{v-1}{2} + \alpha\frac{v^2-1}{8} + \beta\frac{u^2-1}{8}\right]} & \text{sinon.} \end{cases} \tag{1}$$

où $a = p^\alpha u$ et $b = p^\beta v$ avec $\alpha, \beta \in \mathbb{Z}$ et $u, v \in \mathbb{Z}_p^\times$, et pour $t \in \mathbb{F}_p^\times$:

$$\left(\frac{t}{p}\right) := \begin{cases} 1 & \text{si } t \text{ est un carré dans } \mathbb{F}_p \\ -1 & \text{sinon} \end{cases}$$

est le **symbole de Legendre** de u modulo p.

a) Pourquoi peut-on supposer que $(\alpha,\beta) \in \{(0,0),(0,1),(1,1)\}$?
b) En utilisant la question 1), montrer la formule (1) lorsque $(\alpha,\beta) = (0,1)$.
c) On suppose que $(\alpha,\beta) = (0,0)$.
   i) On suppose que p est impair. Montrer que l'équation $x^2 - [u]\,y^2 - [v]\,z^2 = 0$ admet des solutions non nulles dans $\mathbb{F}_p$. En déduire la formule (1) dans ce cas-là.
   ii) On suppose $p = 2$. Utiliser la question 1) pour établir la formule (1) dans ce cas.
d) On suppose que $(\alpha,\beta) = (1,1)$.
   i) Montrer que $(a,b)_p = (pu,-uv)_p$.
   ii) En déduire la formule (1) dans ce cas.

Exercice 14 Soient p un nombre premier et $a_1,\dots,a_5 \in \mathbb{Q}_p^\times$. On considère l'équation :

$$a_1x_1^2 + \cdots + a_5x_5^2 = 0. \tag{2}$$

On cherche à prouver que cette équation a nécessairement des solutions non nulles dans $\mathbb{Q}_p$.

1) Expliquer pourquoi on peut supposer que $v_p(a_i) \in \{0,1\}$ pour tout i. On fait cette hypothèse dans toute la suite de l'exercice.
2) Conclure dans le cas où p est impair. Pour cela, on rappelle que, d'après l'exercice précédent, si a et b sont des nombres p-adiques tels que $v_p(a) = v_p(b) = 0$, alors l'équation l'équation $x^2 - ay^2 - bz^2 = 0$ admet automatiquement des solutions p-adiques non nulles.
3) On suppose maintenant que $p = 2$.
   a) Expliquer pourquoi il suffit de trouver une solution primitive (c'est-à-dire avec $x_1,\dots,x_5$ non tous pairs) à l'équation (2) modulo 32.
   b) Conclure en utilisant un ordinateur ou une calculatrice.

Exercice 15 Montrer que 28 est un cube dans $\mathbb{Z}_3$.

Exercice 16 Existe-t'il $z \in \mathbb{Z}[i]/(51^{100})$ tel que $z^2 = 2$?

Exercice 17 Dans cet exercice, on s'intéresse à une variante du lemme de Hensel pour les systèmes d'équations.

1) Soit p un nombre premier. Soient $f_1,...,f_n$ des éléments de $\mathbb{Z}[X_1,...,X_m]$. Considérons le système d'équations (S) :

$$\begin{cases} f_1(x_1,...,x_m) &= 0 \\ f_2(x_1,...,x_m) &= 0 \\ & \dots \\ f_n(x_1,...,x_m) &= 0 \end{cases}$$

Soit $x \in (\mathbb{Z}/p\mathbb{Z})^m$ une solution de (S). On suppose que le rang de la matrice jacobienne $J(x) = \left(\frac{\partial f_i}{\partial x_j}(x)\right)_{i,j} \in \mathcal{M}_{n,m}(\mathbb{Z}/p\mathbb{Z})$ est égal à n. Montrer que le système (S) possède une unique solution dans $\mathbb{Z}_p$ qui relève x.

2) Trouver tous les nombres premiers p tels que l'équation $x^2 + 1 = 3y^2$ a des solutions dans $\mathbb{Z}_p$.

3) Combien de solutions possède le système d'équations :

$$\begin{cases} x^2 + 1 &= 3y^2 \\ x^3 + 3y^5 + y &= 2 \end{cases}$$

dans $\mathbb{Z}_5$?

Exercice 18

1) Soit $f \in \mathbb{Z}_p[X]$ un polynôme primitif. On suppose qu'il existe des polynômes $\overline{g}, \overline{h} \in \mathbb{F}_p[X]$ qui sont premiers entre eux et tels que la réduction $\overline{f}$ de f modulo p s'écrit $\overline{f} = \overline{g}\overline{h}$. Montrer qu'il existe $g, h \in \mathbb{Z}_p[X]$ deux polynômes relevant $\overline{g}$ et $\overline{h}$ respectivement tels que $\deg(g) = \deg(\overline{g})$ et $f = gh$.

2) Soit $f = a_0 + \cdots + a_n X^n \in \mathbb{Q}_p[X]$ un polynôme irréductible avec $a_0 a_n \neq 0$. Montrer que :

$$\max\{|a_0|_p, \ldots, |a_n|_p\} = \max\{|a_0|_p, |a_n|_p\}.$$