

Analyse non-archimédien II

I - L'expansion p-adique:

Théorème 1: Tout $a \in \mathbb{Q}_p$ admet un unique développement sous la forme:

$$a = \sum_{n=n_0}^{\infty} d_n p^n \quad \dots (*)$$

où $0 \leq d_n \leq p-1$ et $n_0 \in \mathbb{Z}$.

Si $d_{n_0} \neq 0$, alors $v_p(a) = n_0$.

Remarque 1: 1) On remarque que dans (*), il y a une infinité de chiffres avant la virgule et un nombre fini de chiffres après la virgule c.-à-d.

$$a = \dots d_n \dots d_2 d_1 d_0 \cdot d_{-1} d_{-2} \dots d_{n_0}$$

la virgule.

Cette écriture est la forme ~~canonique~~ **canonique** de a dans $\mathbb{Q}_p$ (ou l'expansion p-adique de a dans $\mathbb{Q}_p$).

2) Dans $\mathbb{R}$, il n'y a pas d'unicité par exemple on a

$$1,000 \dots = 0,999 \dots \quad \text{(Exercice 1)}$$

Définition (des entiers p-adiques)

On dit que $a \in \mathbb{Q}_p$ est un entier p-adique si son expansion p-adique ne contient que des puissances positives ou nulles, on le note $\mathbb{Z}_p$ c.-à-d.

$$\mathbb{Z}_p = \{ a \in \mathbb{Q}_p ; a = \sum_{n=0}^{\infty} d_n p^n, \text{ où } 0 \leq d_n \leq p-1 \}$$

Remarque 2: On a $\mathbb{Z}_p = \{a \in \mathbb{Q}_p; |a|_p \leq 1\}$, car

C) Si $a \in \mathbb{Z}_p$, alors $a = \sum_{n=0}^{\infty} d_n p^n$, ne contient que des puissances positives. D'où $v_p(a) \geq 0$, donc $p^{-v_p(a)} \leq 1 = p^0$; i.e.; $|a|_p \leq 1$.

D) Si $a \in \mathbb{Q}_p$ tq $|a|_p \leq 1$, alors $p^{-v_p(a)} \leq 1$. Donc $v_p(a) \geq 0$, d'où l'expansion de a ne contient que des puissances positives, alors $a \in \mathbb{Z}_p$.

Théorème 2: $\mathbb{Z}_p$ est compacte.

II - Opérations arithmétiques sur $\mathbb{Q}_p$:

1. L'addition:

Si $a = \sum_{n=n_0}^{\infty} a_n p^n$ et $b = \sum_{n=m_0}^{\infty} b_n p^n$, on a

$$a+b = \sum_{n=l_0}^{\infty} (a_n + b_n) p^n \quad (**)$$

où $l_0 = \min(n_0, m_0)$.

L'écriture $(**)$ n'est pas la forme canonique. Pour avoir la forme canonique on applique la méthode Classique.

Exemples:

a) $p=5$;

$$\begin{array}{r} a = \quad \overset{1}{2} \overset{1}{3} \overset{1}{2} 1 0 0 4 \\ + b = \quad 1 1 \cancel{8} 4 0 1 \\ \hline a+b = \quad 4 0 1 0 0 3 0 4 \end{array}$$

e) $1 = p^0 + 0p^1 + \dots + 0p^5 + \dots = \dots 0001_0$; $\forall p$ -Premier.

3) Soit $a = -1 = \dots a_2 a_1 a_0$, où $0 \leq a_i \leq p-1$
 on a: $1 + a = 0 \Rightarrow a = -1$;

et on a: $1 + a = 0 \Leftrightarrow$

$$\begin{array}{r} 1 = \dots 00001. \\ + \\ a = \dots a_4 a_3 a_2 a_1 a_0. \\ \hline 1+a = \dots 00000. \end{array}$$

donc; $1 + a_0 \equiv 0 [p] \Rightarrow a_0 = p-1$

et $1 + a_1 \equiv 0 [p] \Rightarrow a_1 = p-1$

de même :

$$a_n = p-1, \quad \forall p, \forall n,$$

d'où $-1 = \dots (p-1)(p-1)(p-1).$
 $= \sum_{i=0}^{\infty} (p-1) p^i, \quad \forall p \text{ première.}$

Exercice 2: Calculer 3-5 dans $\mathbb{Z}_5$.

Remarque:

1. Si $0 \in \mathbb{N}$; on a $a = \sum_{i=0}^{N_0} a_i p^i$ (dans $\mathbb{Q}_p$)

2. Si $a \in \mathbb{Z}^-$; $a = \sum_{i=0}^{\infty} a_i p^i$ (exemple (-1) dans $\mathbb{Q}_p$)

3. Si $a \in \mathbb{Q}_p$ et $a \notin \mathbb{Z}_p$; on a
 $a = \sum_{i=-m}^{\infty} a_i p^i$ où $m \in \mathbb{N}$.

2. La multiplication:

Si $a, b \in \mathbb{Q}_p$ tq $a = \sum_{n=N_0}^{\infty} a_n p^n$ et $b = \sum_{n=N_0}^{\infty} b_n p^n$

alors on a: $a \cdot b = \sum_{n=N_0+N_0}^{\infty} u_n p^n \dots (xxx)$

où

$$u_{m_0+m_0} = a_{m_0} b_{m_0}$$

$$U_{n_0+m_0+1} = a_{n_0} \cdot b_{m_0+1} + a_{n_0+1} \cdot b_{m_0}$$

$$U_{n_0+m_0+2} = a_{n_0} \cdot b_{m_0+2} + a_{n_0+1} \cdot b_{m_0+1} + a_{n_0+2} \cdot b_{m_0}$$

⋮

L'écriture $(***)$ n'est pas nécessairement la forme canonique.
Pour avoir la forme canonique, on fait comme dans le cas decimal.

Exemple : dans $\mathbb{Q}_7$ on a

$$\begin{array}{r} a = \dots\dots\dots 263. \\ \times b = \dots\dots\dots 154. \\ \hline \dots\dots\dots 445. \\ \dots\dots\dots 041. \\ \dots\dots\dots 263. \\ \hline a \times b = \dots\dots\dots 455. \end{array}$$

3 - La division :

Soit $a, b \in \mathbb{Q}_p$ tq $b \neq 0$

$$\frac{a}{b} = ?$$

On peut supposer sans perte de généralité que $b \in \mathbb{Z}_p$, i.e.

$$\begin{array}{l} \text{et } b = \dots\dots\dots b_2 b_1 b_0; b_0 \neq 0 \\ a = \dots\dots\dots a_2 a_1 a_0 \dots a_{-1} \dots a_{-m} \end{array}$$

$$\text{donc } \frac{a}{b} = ? \dots\dots\dots a_2 a_1 a_0 \dots a_{-1} \dots a_{-m} \overline{) b_2 b_1 b_0} \dots\dots\dots C_{-m}$$

$$\text{où } C_m \in \{0, 1, \dots, p-1\} \text{ et } C_{-m} \times b_0 \equiv a_{-m} [p].$$

Exemple; on calcule $\frac{24}{17}$ dans φ_3 .

③na: $24 = 2 \times 3 + 2 \times 3^0 = \dots 000220.$

$$17 = 2 + 2 \times 3 + 1 \times 3^2 = \dots 000122.$$

$2 + 2 \times 5 + 1 \times 5 = -000122.$

$\begin{array}{r} -00220 \\ -00000 \\ \hline 000220 \\ -000122 \\ \hline 000100 \\ -00000 \\ \hline 000100 \\ -00000 \\ \hline 000100 \\ -00000 \\ \hline 000100 \\ -00000 \\ \hline 000100 \\ -00000 \\ \hline 000100 \end{array}$

$-00\overset{1}{5}\overset{1}{5}22.$

$201010.$

donc $\frac{24}{17} = \dots 201010.$

Résultats :

1) Si $b = \dots b_2 b_1 b_0 \cdot \in \mathbb{Z}_p$ et $b_0 \neq 0$, alors $\frac{1}{b} \in \mathbb{Z}_p$
(i.e. l'inverse de cet entier p-adique est un entier p-adique)

2) L'inverse de $p = \frac{1}{p}$ n'est pas un entier p -adique, car

$$\forall a \in \mathbb{Z}_p, \text{ où } a = \sum_{n=0}^{\infty} a_n p^n; \text{ on a}$$

$$p \cdot a = p \cdot \left(\sum_{n=0}^{\infty} a_n p^n \right) = a_0 p + a_1 p^2 + \dots \neq 1 = 1 \cdot p^0 + 0 \cdot p^1 + 0 \cdot p^2 + \dots$$

(Il est clair que $\frac{1}{p} = p^{-1} = \dots 0000.1 \in \mathbb{Z}_p$).

3) Si $b = \frac{b_1 b_2 \dots b_p}{b_0} \in \mathbb{Q}_p$ et $b_0 \neq 0$, alors l'inverse de b (i.e. $\frac{1}{b}$) n'est pas un entier p -adique car.

$$\forall a \in \mathbb{Z}_p, \exists n \text{ s.t. } a = \sum_{n=0}^{\infty} a_n p^n; \exists n \text{ s.t. } a$$

$$a \cdot b = \left(\sum_{n=0}^{\infty} a_n p^n \right) \cdot \left(\sum_{n=1}^{\infty} b_n p^n \right) = \sum_{n=1}^{\infty} c_n p^n \neq 1.$$

Théorème 1: Si $a = \dots a_n a_{n+1} a_{n+2} \dots \in \mathbb{Z}_p$, alors on a.

(a possède son inverse dans $\mathbb{Z}_p$) $\Leftrightarrow$ ($a_0 \neq 0$).

* **N.B** l'inverse existe toujours dans $\mathbb{Q}_p$ si $a \neq 0$.

Notation:

$\mathbb{Z}_p^*$ est l'ensemble des entiers p -adiques inversibles dans $\mathbb{Z}_p$.

Remarque: à partir de Théorème précédente on a

$$\mathbb{Z}_p^* = \left\{ a = \sum_{n=0}^{\infty} a_n p^n ; a_0 \neq 0 \right\}.$$

Conséquence: Si $x \in \mathbb{Q}_p$ et $|x|_p = p^{-n}$, alors x s'écrit sous la forme $x = p^n \cdot u$ où $u \in \mathbb{Z}_p^*$, car

$$\begin{aligned} |x|_p = p^{-n} &\Rightarrow v_p(x) = n \\ &\Rightarrow x = a_n p^n + a_{n+1} p^{n+1} + \dots ; a_n \neq 0 \\ &= p^n \cdot (a_n + a_{n+1} p + \dots) \\ &= p^n \cdot u ; \text{ où } u \in \mathbb{Z}_p^*. \end{aligned}$$

Exercice 03: a) Calculer dans $\mathbb{Q}_7$

1) $30 \cdot 2 - 56 \cdot 4 = ?$

2) $263 \cdot x - 154 \cdot = ?$

3) $421 \div 153 \cdot = ?$

b) calculer $\frac{1}{2}$ dans $\mathbb{Q}_5$.

Exercice 04: Si $a = \dots a_n a_{n+1} a_{n+2} \dots \in \mathbb{Z}_p$;
calculer $(-a)$.