III.7 Nombres p-adiques $\mathbb{Z}_p$, $\mathbb{Q}_p$ et $\mathbb{C}_p$

III.7.1 Introduction

On passe de l'ensemble des entiers $\mathbb{Z}$ (ou des décimaux $\mathbb{D}$) à l'ensemble des réels $\mathbb{R}$ en autorisant les nombres à avoir une infinité de chiffres (nuls ou non nuls) à droite de la virgule. Par exemple $\pi = 3,14159265358979\ldots$.

Il existe une autre façon de compléter $\mathbb{D}$ en un ensemble intéressant. Il s'agit d'autoriser les nombres à avoir une infinité de chiffres (nuls ou non nuls) à gauche de la virgule. Par exemple, $a = \ldots 11266421216213$ ou $b = \ldots 455323152,156$. Nous verrons plusieurs aspects (informels et formels) de ces nouveaux nombres

Le développement de cette idée de départ vient de Kurt Hensel [76], un mathématicien allemand (1861-1941) dans un article publié en 1897 (voir les références).

III.7.2 Définition informelle

Les nombres avec une infinité de chiffres à gauche et un nombre fini de chiffres à droite de la virgule en base p sont appelés nombres p-adiques, et leur ensemble est noté $\mathbb{Q}_p$.
Les nombres p-adiques qui n'ont aucun chiffre non nul à droite de la virgule sont appelés entiers p-adiques. Leur ensemble est noté $\mathbb{Z}_p$ et il est inclus dans $\mathbb{Q}_p$. On peut aussi noter que $\mathbb{Z} \subset \mathbb{Z}_p$ et, si p est premier, $\mathbb{Q} \subset \mathbb{Q}_p$.
Par exemple le nombre a de l'introduction est un entier p-adique alors que b est un nombre p-adique qui n'est pas entier.

Il s'avère qu'il y a une différence fondamentale entre ces nombres p-adiques et les nombres réels :
Les nombres p-adiques dépendent de la base de numération choisie.

Par exemple, en base 10 il existe des diviseurs de 0 ; pour éviter ce problème, dans la suite de ce document p sera un nombre premier (à une exception qui sera signalée.)

Il existe donc autant d'ensembles $\mathbb{Q}_p$ et $\mathbb{Z}_p$ qu'il existe de nombres premiers p, et ces $\mathbb{Q}_p$ et $\mathbb{Z}_p$ sont tous différents les uns des autres.

Par exemple, dans $\mathbb{Z}_7$, il existe une racine carrée de 2 qui est $\ldots 11266421216213$. En revanche, 2 n'a pas de racine carrée dans $\mathbb{Z}_2$.

III.7.3 Addition et multiplication

On calcule avec les nombres p-adiques comme avec les nombres décimaux, la présence d'une infinité de chiffres vers la gauche ne pose pas de problème particulier.

Exemple d'addition dans $\mathbb{Q}_7$:

$$\begin{array}{cccccccccccccc} & \ldots & 4 & 2 & 1 & 2 & 1 & 6 & 2 & 1 & 3 & & & \\ + & \ldots & 4 & 5 & 5 & 3 & 2 & 3 & 1 & 5 & 2 & , & 1 & 5 & 6 \\ \hline & \ldots & 2 & 0 & 6 & 5 & 4 & 2 & 3 & 6 & 5 & , & 1 & 5 & 6 \end{array}$$

(Attention à la retenue en base 7 !)

Un autre exemple intéressant, toujours en base 7 :

$$\begin{array}{cccccccccccc} & \ldots & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 \\ + & \ldots & & & & & & & & & 1 \\ \hline & \ldots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}$$

Autrement dit ... 666666666 = -1 (comme nombres 7-adiques).
Ceci se généralise et permet d'exprimer les nombres négatifs.

76. Elle trouve son origine chez E. Kummer, un autre mathématicien allemand

Exemple de multiplication dans $\mathbb{Z}_7$:

$$\begin{array}{cccccccccc}
 & \ldots & 4 & 2 & 1 & 2 & 1 & 6 & 2 & 1 & 3 \\
\times & \ldots & 4 & 2 & 1 & 2 & 1 & 6 & 2 & 1 & 3 \\
\hline
 & \ldots & 5 & 6 & 3 & 6 & 5 & 4 & 6 & 4 & 2 \\
 & \ldots & 2 & 1 & 2 & 1 & 6 & 2 & 1 & 3 & \\
 & \ldots & 2 & 4 & 3 & 5 & 4 & 2 & 6 & & \\
 & \ldots & 6 & 4 & 2 & 6 & 1 & 4 & & & \\
 & \ldots & 1 & 6 & 2 & 1 & 3 & & & & \\
 & \ldots & 5 & 4 & 2 & 6 & & & & & \\
 & \ldots & 2 & 1 & 3 & & & & & & \\
 & \ldots & 2 & 6 & & & & & & & \\
 & \ldots & 5 & & & & & & & & \\
\hline
 & \ldots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2
\end{array}$$

Exemple de multiplication dans $\mathbb{Z}_{10}$ (10 qui n'est pas premier) :

$$\begin{array}{cccccccc}
 & \ldots & 0 & 1 & 0 & 1 & 1 & 2 \\
\times & \ldots & 1 & 4 & 0 & 6 & 2 & 5 \\
\hline
 & \ldots & 0 & 5 & 0 & 5 & 6 & 0 \\
 & \ldots & 2 & 0 & 2 & 2 & 4 & \\
 & \ldots & 0 & 6 & 7 & 2 & & \\
 & \ldots & 0 & 0 & 0 & & & \\
 & \ldots & 4 & 8 & & & & \\
 & \ldots & 2 & & & & & \\
\hline
 & \ldots & 0 & 0 & 0 & 0 & 0 & 0
\end{array}$$

III.7.4 Valuation et valeur absolue

La valuation $v_p(x)$ d'un nombre p-adique x non nul est le rang de son chiffre non nul le plus à droite. Exemples :

$$\begin{array}{rll}
 & v_7(\ldots 456321000) & = 3 \\
 & v_7(\ldots 1564231,0123) & = -4 \\
 & v_7(\ldots 13262123) & = 0 \\
\text{On convient que :} & v_p(0) & = +\infty
\end{array}$$

La valeur absolue $|x|_p$ d'un nombre p-adique x non nul est égale à $p^{-v_p(x)}$. Exemples :

$$\begin{array}{rlll}
 & |\ldots 456321000|_7 & = 7^{-3} = & \dfrac{1}{343} \\
 & |\ldots 1564231,0123|_7 & = 7^{4} = & 2401 \\
 & |\ldots 13262123|_7 & = 7^{0} = & 1 \\
\text{On convient que :} & |0|_p & = p^{-\infty} = & 0
\end{array}$$

Cette valeur absolue vérifie toutes les propriétés attendues :

$$|x|_p \geq 0$$

$$|x|_p = 0 \Leftrightarrow x = 0$$

$$|xy|_p = |x|_p |y|_p$$

$$|x+y|_p \leq |x|_p + |y|_p$$

Elle a en outre la propriété d'être *ultramétrique*, c'est-à-dire :

$$|x+y|_p \leq \max(|x|_p, |y|_p)$$

III.7.5 Définition formelle

Soit p un nombre premier. L'ensemble $\mathbb{Q}_p$ des nombres p-adiques est l'ensemble des nombres de la forme

$$x = \sum_{n \geq k} a_n p^n,$$

où $k \in \mathbb{Z}$ et les a_n sont des nombres entre 0 et $p-1$, en particulier $a_k \neq 0$.

L'ensemble $\mathbb{Z}_p$ des entiers [77] p-adiques est l'ensemble des nombres de la forme

$$x = \sum_{n \geq k} a_n p^n.$$

où $k \in \mathbb{N}$ et les a_n sont des nombres entre 0 et $p-1$, en particulier $a_k \neq 0$.

On peut retrouver facilement les inclusions : $\mathbb{Z} \subset \mathbb{Z}_p \subset \mathbb{Q}_p$ et (p est premier) $\mathbb{Q} \subset \mathbb{Q}_p$.

Les définitions précédentes permettent de définir une fonction appelée valuation p-adique : $v_p(x) = k$, et d'une valeur absolue p-adique $|x|_p = p^{-v_p(x)}$, et donc d'une distance p-adique : $d_p(x, y) = |x - y|_p$. Il va de soi que cette définition correspond exactement à la définition donnée dans la partie informelle, la distance définie ici est donc une distance ultramétrique (tous les points d'une boule en sont un centre, tous les triangles sont isocèles).

Pour cette distance, deux nombres sont d'autant plus proches que leur différence est divisible pas une puissance plus grande de p. Par exemple $d_3(1, 2) = |1|_3 = 1$, alors que $d_3(1, 244) = |243|_3 = |3^5|_3 = 3^{-5}$.

Cette valeur absolue munit l'ensemble des nombres p-adiques d'une topologie. Il faut prendre garde qu'elle est différente de celle de $\mathbb{R}$. Le sens du « grand » et du « petit » peut être inversé :

Dans $\mathbb{R}$, la suite $u_n = p^{-n}$, c'est-à-dire des nombres qui s'écrivent $0,1$; $0,01$; $0,001$; $0,0001$; ... en base p tend vers 0 (u_n devient de plus en plus petit).
Dans $\mathbb{Q}_p$, la suite $u_n = p^{-n}$ n'est pas convergente (u_n devient de plus en plus grand).

Dans $\mathbb{R}$, la suite $u_n = p^n$, c'est-à-dire des nombres qui s'écrivent 1 ; 10 ; 100 ; 1000 ; ... en base p n'est pas convergente (u_n devient de plus en plus grand).
Dans $\mathbb{Q}_p$, la suite $u_n = p^n$, tend vers 0 (u_n devient de plus en plus petit).

III.7.6 Propriétés algébriques et analytiques

L'ensemble $\mathbb{Z}_p$ est un anneau intègre. Les entiers p-adiques qui n'ont pas d'inverse dans $\mathbb{Z}_p$ sont les éléments de l'idéal $p\mathbb{Z}_p$ (du point de vue informel, c'est exactement ceux dont le premier chiffre à gauche de la virgule est 0). Cet ensemble des non inversibles est un idéal de $\mathbb{Z}_p$ et c'est même son seul idéal maximal : on dit que $\mathbb{Z}_p$ est un anneau local.

L'ensemble $\mathbb{Q}_p$ est un corps. Muni de sa topologie, il est complet. Il a donc beaucoup de points communs avec $\mathbb{R}$ (en fait, en un certain sens que l'on ne détaillera pas, on peut considérer $\mathbb{R}$ comme l'ensemble des nombres ∞-adiques).
On peut définir sur $\mathbb{Q}_p$ une fonction exponentielle, à l'aide d'une série entière :

$$\exp_p(x) = \sum \frac{x^n}{n!}.$$

On peut définir de même les fonctions transcendantes usuelles : logarithme p-adique, fonctions trigonométriques p-adiques...

On dispose sur $\mathbb{Q}_p$ des notions de limite, de dérivée, de primitive, d'équations différentielles... Bref c'est un corps où on peut faire de l'analyse.

Le corps $\mathbb{Q}_p$ n'est pas algébriquement clos : les exemples ci-dessous utilisent un petit résultat sur les polynômes [78] et le Lemme de Hensel (cf. infra),

Dans $\mathbb{Q}_2$, le polynôme $X^2 + X + 1 = 0$ n'a pas de racine.
Dans $\mathbb{Q}_p$, il existe $k \in [1, p[$ tel que le polynôme $X^2 - k = 0$ [79] n'ait pas de racine.

77. Un simple argument diagonal permet de montrer que $\mathbb{Z}_p$ n'est pas dénombrable
78. On peut vérifier facilement que les polynômes utilisés ont une racine dans $\mathbb{Q}_p$ si et seulement si ses solutions sont dans Z_p
79. Si $n > 2$ et $0 < i < p$, alors $i^2 \equiv (p-i)^2$ $[p]$, il est donc possible de trouver un k qui ne soit pas carré modulo p

III.7.7 Quelques théorèmes intéressants

Lemme de Hensel : soit $\varphi \in \mathbb{Z}_p[X]$ et soit $a \in \mathbb{Z}_p$ tel que $\varphi(a) \equiv 0\ [p]$ et $\varphi'(a) \not\equiv 0\ [p]$, alors il existe un unique entier p-adique α tel que $(\varphi(\alpha) = 0) \wedge (a \equiv \alpha\ [p])$.

Remarque : la démonstration du lemme de Hensel (pas très compliquée) est constructive, elle repose sur la construction d'une suite de Cauchy donc convergente dans $\mathbb{Z}_p$, dont la limite est la valeur cherchée.

Théorème d'Ostrowski : Toute valeur absolue $|\cdot|$ sur $\mathbb{Q}$ est équivalente à l'un des cas suivants :

- La valeur absolue triviale $|\cdot|_0$ définie par $|0|_0 = 0 \wedge \forall x(x \neq 0 \Rightarrow |x|_0 = 1)$.
- La valeur absolue euclidienne $|\cdot|_\infty$ (c'est-à-dire la valeur absolue usuelle sur $\mathbb{Q}$).
- La valeur absolue p-adique $|\cdot|_p$ pour un certain p premier.

Théorème de Hasse-Minkowski : Une forme quadratique possède une racine non nulle dans $\mathbb{Q}$ si et seulement si elle admet une racine non nulle dans $\mathbb{R}$ et dans chacun des $\mathbb{Q}_p$ pour tous p nombres premiers (Principe Local-Global).

A noter qu'il existe des contre-exemples pour les degrés supérieurs, en particulier, le contre-exemple de Selmer $3x^3 + 4y^3 + 5z^3 = 0$ qui possède des racines dans $\mathbb{R}$ (trivial) et dans chacun des $\mathbb{Q}_p$, mais pas dans $\mathbb{Q}$.

Formule du produit En notant $\mathbb{P}$ l'ensemble des nombres premiers : $\forall n \in \mathbb{N} \left(\prod_{p \in \mathbb{P}} |n|_p \right) \cdot |n|_\infty = 1$.

III.7.8 Les nombres complexes p-adiques

Comme $\mathbb{Q}_p$ n'est pas algébriquement clos, on peut s'intéresser à sa clôture algébrique $\overline{\mathbb{Q}}_p$. Malheureusement ce corps n'est plus complet.
En revanche, le complété de la clôture algébrique de $\mathbb{Q}_p$ est à la fois complet et algébriquement clos. C'est le corps des nombres complexes p-adiques, noté $\mathbb{C}_p$ du fait de sa ressemblance avec $\mathbb{C}$.

Quelques propriétés :

- $\mathbb{C}$ et $\mathbb{C}_p$ sont isomorphes en tant que corps (la théorie des corps algébriquement clos est $\aleph_1$-catégorique).
- Par contre, il n'y a pas d'isomorphisme unique entre les deux, ni même d'isomorphisme canonique, et encore moins d'isomorphisme explicite.
- $\mathbb{C}$ et $\mathbb{C}_p$ ont des topologies complètement différentes.

III.7.9 Synonymes, Isomorphismes, Exemples

Les nombres p-adiques ont été introduits dans certains collèges français par l'association MATh en JEANS, sous le terme de *brenoms*. Une illustration du fait qu'on peut faire d'excellentes mathématiques dès le collège...

On peut donner deux constructions alternatives à la définition formelle, ci-dessus :

L'ensemble des entiers p-adiques $\mathbb{Z}_p$ est la limite projective des $\mathbb{Z}/p^n\mathbb{Z}$:

$$\mathbb{Z}_p = \lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z}$$

Le lecteur qui n'est pas familier avec cette notion peut la comprendre de la façon suivante : pour tout n, la troncation aux n chiffres les plus à droite est un morphisme de $\mathbb{Z}_p$ dans $\mathbb{Z}/p^n\mathbb{Z}$. L'ensemble $\mathbb{Z}_p$ est donc en quelque sorte l'ensemble $\mathbb{Z}/p^n\mathbb{Z}$ où « on a fait tendre n vers l'infini ».
Une fois $\mathbb{Z}_p$ construit, $\mathbb{Q}_p$ s'obtient de la même façon qu'on obtient $\mathbb{Q}$ à partir de $\mathbb{Z}$ (son corps des fractions).

Seconde construction :

Tout nombre entier relatif α, peut s'écrire comme un produit de nombres premiers : $\alpha = \pm \prod_{k=1}^{n} p_k^{\alpha_k}$ où p_k est le $k^{\text{ième}}$ nombre premier ; pour tout nombre premier p, on peut donc écrire $\alpha = p^n \cdot q$ où q est un entier relatif premier avec p.

La valuation p-adique est alors définie par $v_p(\alpha) = n$ et la valeur absolue p-adique par $|\alpha|_p = p^{-v_p(n)} = p^{-n}$ (ce qui permet de construire une distance p-adique, c'est-à-dire une (nouvelle) topologie, sur $\mathbb{Z}$).

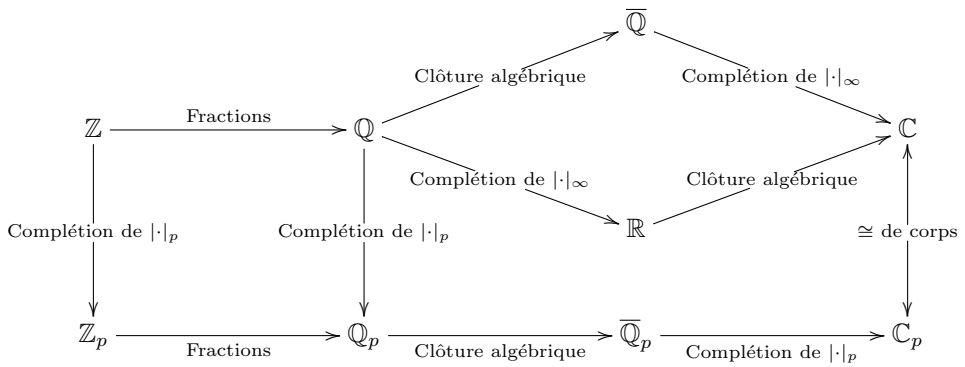
Avec cette valeur absolue, $\mathbb{Z}$ n'est pas complet, par exemple la suite $u_n = 1 + p^2 + \cdots + p^{2n}$ est bien de Cauchy, mais elle n'est pas convergente (elle converge vers $\dfrac{1}{1-p^2} \notin \mathbb{Z}$). On pose $\mathbb{Z}_p =$ le complété de $\mathbb{Z}$ pour la distance p-adique. On peut alors envisager le corps des fractions de $\mathbb{Z}_p$, noté $\mathbb{Q}_p$. La valuation p-adique se prolonge naturellement à ce corps de fractions :

Soit $\alpha \in \mathbb{Z}_p$, $\beta \in \mathbb{Z}_p$ alors on pose $v_p\left(\dfrac{\alpha}{\beta}\right) = v_p(\alpha) - v_p(\beta)$ ce qui permet de définir la valeur absolue et la distance p-adique sur $\mathbb{Q}_p$ qui est complet pour la topologie associée.

Remarque : on aurait pu partir de $\mathbb{Q}$ en munissant cet ensemble d'une distance p-adique (définie comme ci-dessus, mais avec α et β dans $\mathbb{Z}$), puis en complétant cet ensemble pour cette distance, le résultat eut été le même : $\mathbb{Q}_p$, qui est donc au choix :

1. Le complété de $\mathbb{Q}$ pour la valeur absolue p-adique (de même que $\mathbb{R}$ est le complété de $\mathbb{Q}$ pour la valeur absolue usuelle).
2. Le corps des fractions du complété de $\mathbb{Z}$ pour la valeur absolue p-adique (de même que $\mathbb{Q}$ est le corps des fractions de $\mathbb{Z}$).

Pour résumer :



III.7.10 Utilisation en physique

Si les nombres p-adiques semblent aussi naturels que les nombres réels dans le paysage mathématique, il n'en est pas de même en physique, où ils sont pratiquement absents. Quelques tentatives ont été faites pour construire une physique p-adique, mais relèvent pour l'instant, au moins en partie, d'un jeu de l'esprit.

Les nombres p-adiques sont utilisés en cryptographie, et pour la mise au point de « Code Correcteurs d'Erreurs ».

Topological Geometrodynamics (TGD) : une théorie physique en essor depuis les années 80.

On pourra aussi consulter *p-Adic Mathematical Physics*, ci-dessous.

III.7.11 Références

1. K. Hensel, *Über eine neue Begründung der Theorie der algebraischen Zahlen*, Jahresbericht der Deutschen Mathematiker, Volume 6, pages 83 - 88, 1897.
2. Irem de Limoges, *Nombres p-adiques*, Stage « Arithmétique », Limoges, 2009.
3. V. Lefèvre, *Thème de recherche N° 2 : les BRENOMS*, 1994.
4. *Site : Maths en jeans*, il y a plusieurs sujets sur les brenoms (niveau $6^{\text{ième}}$ à 2^{nde}).
5. L. Merel, *Nombres algébriques et nombres p-adiques* , Université Pierre et Marie Curie, Université Denis Diderot, cours préparatoire aux études doctorales, 2003-2004.
6. B. Dragovich, A. Yu. Khrennikov, S. V. Kozyrev, I. V. Volovich, *p-Adic Mathematical Physics* , Institute of Physics Belgrade Serbie, Växjö University Suède, Steklov Mathematical Institute Moscou Russie, 2009.
7. M. Pitkanen, *Topological Geometrodynamics (TGD): an Overall View* , Finland, 2009.