L'ensemble $\mathbb{Q}_p$ des nombres p-adiques

Julien Heyd

19 Janvier 2021

Sommaire

Introduction

- Construire de nouveaux corps contenant $\mathbb{Q}$.
- Deux manières : topologique et algébrique.
- Aboutissant aux mêmes corps.

Sommaire

Sommaire

Valuation p-adique

Pour $p \in \mathbb{P}$ un nombre premier.

Définition

(Valuation p-adique) Pour $a \in \mathbb{Q}\backslash\{0\}$,

$$a = p^m \frac{u}{v},$$

où $m \in \mathbb{Z}$ et u, v non divisible par p.
On définit alors $m =: ord_p(a)$ la valuation p-adique de a.
Pour $a = 0$, on pose $ord_p(a) = \infty$.

Valuation p-adique

Pour $p \in \mathbb{P}$ un nombre premier.

Définition

(Valuation p-adique) Pour $a \in \mathbb{Q}\backslash\{0\}$,

$$a = p^m \frac{u}{v},$$

où $m \in \mathbb{Z}$ et u, v non divisible par p.
On définit alors $m =: ord_p(a)$ la valuation p-adique de a.
Pour $a = 0$, on pose $ord_p(a) = \infty$.

Pour $a = \frac{u}{v} \in \mathbb{Q}$,

$$ord_p(a) = ord_p(u) - ord_p(v). \qquad (p \in \mathbb{P})$$

Valuation p-adique

Proposition

Pour $(a, b) \in \mathbb{Q}^2$,

1. $ord_p(ab) = ord_p(a) + ord_p(b)$
2. $\min\{ord_p(a), ord_p(b)\} \leqslant ord_p(a+b) \leqslant \max\{ord_p(a), ord_p(b)\}$

Valuation p-adique

Proposition

Pour $(a, b) \in \mathbb{Q}^2$,

1. $ord_p(ab) = ord_p(a) + ord_p(b)$
2. $\min\{ord_p(a), ord_p(b)\} \leqslant ord_p(a + b) \leqslant \max\{ord_p(a), ord_p(b)\}$

Preuve:

Valuation p-adique

Proposition

Pour $(a, b) \in \mathbb{Q}^2$,

1. $ord_p(ab) = ord_p(a) + ord_p(b)$
2. $\min\{ord_p(a), ord_p(b)\} \leqslant ord_p(a+b) \leqslant \max\{ord_p(a), ord_p(b)\}$

<u>Preuve</u>: Soient $a = p^m \frac{u_1}{v_1}$ et $b = p^n \frac{u_2}{v_2}$.

Valuation p-adique

Proposition

Pour $(a, b) \in \mathbb{Q}^2$,

1. $ord_p(ab) = ord_p(a) + ord_p(b)$
2. $\min\{ord_p(a), ord_p(b)\} \leqslant ord_p(a+b) \leqslant \max\{ord_p(a), ord_p(b)\}$

Preuve: Soient $a = p^m \frac{u_1}{v_1}$ et $b = p^n \frac{u_2}{v_2}$.
1) Par définition.

Valuation p-adique

Proposition

Pour $(a, b) \in \mathbb{Q}^2$,

1. $ord_p(ab) = ord_p(a) + ord_p(b)$
2. $\min\{ord_p(a), ord_p(b)\} \leqslant ord_p(a + b) \leqslant \max\{ord_p(a), ord_p(b)\}$

Preuve: Soient $a = p^m \frac{u_1}{v_1}$ et $b = p^n \frac{u_2}{v_2}$.
1) Par définition.
2)

Valuation p-adique

Proposition

Pour $(a, b) \in \mathbb{Q}^2$,

1. $ord_p(ab) = ord_p(a) + ord_p(b)$
2. $\min\{ord_p(a), ord_p(b)\} \leqslant ord_p(a+b) \leqslant \max\{ord_p(a), ord_p(b)\}$

Preuve: Soient $a = p^m \frac{u_1}{v_1}$ et $b = p^n \frac{u_2}{v_2}$.
1) Par définition.
2)

$$p^{\min\{m,n\}} U = a + b = p^{\max\{m,n\}} V,$$

Valuation p-adique

Proposition

Pour $(a, b) \in \mathbb{Q}^2$,

1. $ord_p(ab) = ord_p(a) + ord_p(b)$
2. $\min\{ord_p(a), ord_p(b)\} \leqslant ord_p(a+b) \leqslant \max\{ord_p(a), ord_p(b)\}$

Preuve: Soient $a = p^m \frac{u_1}{v_1}$ et $b = p^n \frac{u_2}{v_2}$.
1) Par définition.
2)

$$p^{\min\{m,n\}} U = a + b = p^{\max\{m,n\}} V,$$

avec $ord_p(U) \geqslant 0$ et $ord_p(V) \leqslant 0$.

Valuation p-adique

1. valuation p-adique : notion de proximité
2. Exemple : $p = 3$.

Valuation p-adique

1. valuation p-adique : notion de proximité
2. Exemple : $p = 3$.

$$a = 3^{ord_3(a)} u,$$

avec u non divisible par 3.

Valuation p-adique

1. valuation p-adique : notion de proximité
2. Exemple : $p = 3$.

$$a = 3^{ord_3(a)} u,$$

avec u non divisible par 3.

$*$ Si $a = 0$ dans $\mathbb{Z}/3^m\mathbb{Z}$

Valuation p-adique

1. valuation p-adique : notion de proximité
2. Exemple : $p = 3$.

$$a = 3^{ord_3(a)} u,$$

avec u non divisible par 3.
$*$ Si $a = 0$ dans $\mathbb{Z}/3^m\mathbb{Z}$ alors $a = 0$ dans $\mathbb{Z}/3^k\mathbb{Z}$ pour $0 \leqslant k \leqslant m$.

Valuation p-adique

1. valuation p-adique : notion de proximité
2. Exemple : $p = 3$.

$$a = 3^{ord_3(a)} u,$$

avec u non divisible par 3.
$*$ Si $a = 0$ dans $\mathbb{Z}/3^m\mathbb{Z}$ alors $a = 0$ dans $\mathbb{Z}/3^k\mathbb{Z}$ pour $0 \leqslant k \leqslant m$.
Conclusion: **"a est proche de 0 s'il est congru à $0 mod(3^m)$ pour m très grand."**

Valuation p-adique

1. valuation p-adique : notion de proximité
2. Exemple : $p = 3$.

$$a = 3^{ord_3(a)} u,$$

avec u non divisible par 3.
$*$ Si $a = 0$ dans $\mathbb{Z}/3^m\mathbb{Z}$ alors $a = 0$ dans $\mathbb{Z}/3^k\mathbb{Z}$ pour $0 \leqslant k \leqslant m$.
<u>Conclusion</u>: **"a est proche de 0 s'il est congru à $0 mod(3^m)$ pour m très grand."**

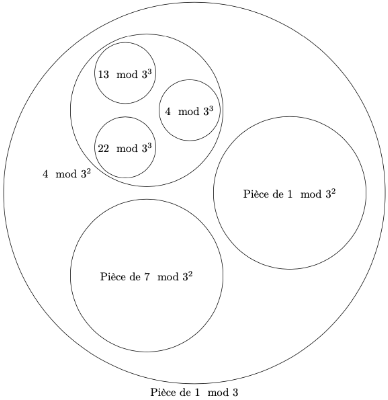

Figure 2.1 – Proximité selon la valuation 3-adique

Valuation p-adique

Définition (Convergence p-adique)

On dit qu'une suite $(x_n)_{n=0}^{\infty}$ d'éléments de $\mathbb{Q}$ converge p-adiquement vers $a \in \mathbb{Q}$ si :

$$\lim_{n \to +\infty} ord_p(x_n - a) = +\infty$$

Valuation p-adique

Définition (Convergence p-adique)

On dit qu'une suite $(x_n)_{n=0}^{\infty}$ d'éléments de $\mathbb{Q}$ converge p-adiquement vers $a \in \mathbb{Q}$ si :

$$\lim_{n \to +\infty} ord_p(x_n - a) = +\infty$$

Exemple: pour tout $n \geqslant 0$, on pose $x_n = x^n$ et $ord_p(x) \geqslant 1$.

Valuation p-adique

Définition (Convergence p-adique)

On dit qu'une suite $(x_n)_{n=0}^{\infty}$ d'éléments de $\mathbb{Q}$ converge p-adiquement vers $a \in \mathbb{Q}$ si :

$$\lim_{n \to +\infty} ord_p(x_n - a) = +\infty$$

Exemple: pour tout $n \geqslant 0$, on pose $x_n = x^n$ et $ord_p(x) \geqslant 1$.

$$ord_p\left(\sum_{k=0}^{n} x^k - \frac{1}{1-x}\right) = ord_p(x)(n+1)$$

Valuation p-adique

Définition (Convergence p-adique)

On dit qu'une suite $(x_n)_{n=0}^{\infty}$ d'éléments de $\mathbb{Q}$ converge p-adiquement vers $a \in \mathbb{Q}$ si :

$$\lim_{n \to +\infty} ord_p(x_n - a) = +\infty$$

Exemple: pour tout $n \geqslant 0$, on pose $x_n = x^n$ et $ord_p(x) \geqslant 1$.

$$ord_p(\sum_{k=0}^{n} x^k - \frac{1}{1-x}) = ord_p(x)(n+1)$$

fournit

$$\sum_{k=0}^{\infty} x^k = \frac{1}{1-x}.$$

Norme et distance p-adique

Définition (Valeur absolue p-adique)

Pour $a \in \mathbb{Q}$, on définit sa valeur absolue p-adique notée $|a_p$ par:

$$|a|_p = p^{-ord_p(a)}$$

Norme et distance p-adique

Définition (Valeur absolue p-adique)

Pour $a \in \mathbb{Q}$, on définit sa valeur absolue p-adique notée $|a_p$ par:

$$|a|_p = p^{-ord_p(a)}$$

Elle définit une norme sur $\mathbb{Q}$:

Norme et distance p-adique

Définition (Valeur absolue p-adique)

Pour $a \in \mathbb{Q}$, on définit sa valeur absolue p-adique notée $|a_p$ par:

$$|a|_p = p^{-ord_p(a)}$$

Elle définit une norme sur $\mathbb{Q}$: pour $a, b \in \mathbb{Q}$,

Norme et distance p-adique

Définition (Valeur absolue p-adique)

Pour $a \in \mathbb{Q}$, on définit sa valeur absolue p-adique notée $|a_p$ par:

$$|a|_p = p^{-ord_p(a)}$$

Elle définit une norme sur $\mathbb{Q}$: pour $a, b \in \mathbb{Q}$,

1. Séparation:

Norme et distance p-adique

Définition (Valeur absolue p-adique)

Pour $a \in \mathbb{Q}$, on définit sa valeur absolue p-adique notée $|a_p$ par:

$$|a|_p = p^{-ord_p(a)}$$

Elle définit une norme sur $\mathbb{Q}$: pour $a, b \in \mathbb{Q}$,

1. <u>Séparation</u>: $|a|_p = 0 \Longleftrightarrow a = 0$

Norme et distance p-adique

Définition (Valeur absolue p-adique)

Pour $a \in \mathbb{Q}$, on définit sa valeur absolue p-adique notée $|a_p$ par:

$$|a|_p = p^{-ord_p(a)}$$

Elle définit une norme sur $\mathbb{Q}$: pour $a, b \in \mathbb{Q}$,

1. Séparation: $|a|_p = 0 \iff a = 0$
2. Homogénéité sur $\mathbb{Q}$:

Norme et distance p-adique

Définition (Valeur absolue p-adique)

Pour $a \in \mathbb{Q}$, on définit sa valeur absolue p-adique notée $|a_p$ par:

$$|a|_p = p^{-ord_p(a)}$$

Elle définit une norme sur $\mathbb{Q}$: pour $a, b \in \mathbb{Q}$,

1. Séparation: $|a|_p = 0 \iff a = 0$
2. Homogénéité sur $\mathbb{Q}$: $|ab|_p = |a|_p|b|_p$

Norme et distance p-adique

Définition (Valeur absolue p-adique)

Pour $a \in \mathbb{Q}$, on définit sa valeur absolue p-adique notée $|a_p$ par:

$$|a|_p = p^{-ord_p(a)}$$

Elle définit une norme sur $\mathbb{Q}$: pour $a, b \in \mathbb{Q}$,

1. Séparation: $|a|_p = 0 \iff a = 0$
2. Homogénéité sur $\mathbb{Q}$: $|ab|_p = |a|_p|b|_p$
3. Inégalité triangulaire :

Norme et distance p-adique

Définition (Valeur absolue p-adique)

Pour $a \in \mathbb{Q}$, on définit sa valeur absolue p-adique notée $|a_p$ par:

$$|a|_p = p^{-ord_p(a)}$$

Elle définit une norme sur $\mathbb{Q}$: pour $a, b \in \mathbb{Q}$,

1. Séparation: $|a|_p = 0 \iff a = 0$
2. Homogénéité sur $\mathbb{Q}$: $|ab|_p = |a|_p|b|_p$
3. Inégalité triangulaire : grâce à

$$\min\{|a|_p, |b|_p\} \leqslant |a+b|_p \leqslant \max\{|a|_p, |b|_p\}$$

Norme et distance p-adique

Définition (Valeur absolue p-adique)

Pour $a \in \mathbb{Q}$, on définit sa valeur absolue p-adique notée $|a_p$ par:

$$|a|_p = p^{-ord_p(a)}$$

Elle définit une norme sur $\mathbb{Q}$: pour $a, b \in \mathbb{Q}$,

1. Séparation: $|a|_p = 0 \iff a = 0$
2. Homogénéité sur $\mathbb{Q}$: $|ab|_p = |a|_p|b|_p$
3. Inégalité triangulaire : grâce à

$$\min\{|a|_p, |b|_p\} \leqslant |a+b|_p \leqslant \max\{|a|_p, |b|_p\}$$

Notation : Valeur absolue p-adique = norme p-adique.

Norme et distance p-adique

Définition (Valeur absolue p-adique)

Pour $a \in \mathbb{Q}$, on définit sa valeur absolue p-adique notée $|a_p$ par:

$$|a|_p = p^{-ord_p(a)}$$

Elle définit une norme sur $\mathbb{Q}$: pour $a, b \in \mathbb{Q}$,

1. Séparation: $|a|_p = 0 \iff a = 0$
2. Homogénéité sur $\mathbb{Q}$: $|ab|_p = |a|_p|b|_p$
3. Inégalité triangulaire : grâce à

$$\min\{|a|_p, |b|_p\} \leqslant |a+b|_p \leqslant \max\{|a|_p, |b|_p\}$$

Notation : Valeur absolue p-adique = norme p-adique.
Ainsi, on peut réécrire :

Définition (Convergence p-adique)

On dit qu'une suite $(x_n)_{n=0}^{\infty}$ d'éléments de $\mathbb{Q}$ converge p-adiquement vers $a \in \mathbb{Q}$ si :

$$\lim_{n \to +\infty} |x_n - a|_p = 0$$

Norme et distance p-adique

$\mathbb{Q}$ est-il complet ?

Norme et distance p-adique

$\mathbb{Q}$ est-il complet ?

Proposition

$\mathbb{Q}$ munit de $|.|_p$ n'est pas complet.

Norme et distance p-adique

$\mathbb{Q}$ est-il complet ?

Proposition

$\mathbb{Q}$ munit de $|.|_p$ n'est pas complet.

Preuve : On va montrer que quelque soit la valeur absolue prise, $\mathbb{Q}$ est non complet, pour cela on va rappeler

Définition (Valeur absolue sur un corps K)

On appelle valeur absolue sur K toute application $|.|$ de K dans $\mathbb{R}_+$ qui vérifie :

1. Multiplicativité: $\forall (x,y) \in K^2$, $|xy| = |x||y|$.
2. Inégalité triangulaire: $\forall (x,y) \in K^2$, $|x+y| \leqslant |x| + |y|$.
3. Séparation: $\forall x \in K$, $|x| = 0 \Longleftrightarrow x = 0$.

Norme et distance p-adique

Il y a deux types :

Norme et distance p-adique

Il y a deux types :

Définition (Valeur absolue archimédienne et non-archimédienne)

On appelle valeur absolue sur K

1. non-archimédienne si pour tout $(x, y) \in K^2$, $|x + y| \leqslant \max\{|x|, |y|\}$.
2. archimédienne si pour tout $x \in K^*$ et $y \in K$, il existe $n \in \mathbb{N}$ tel que $|nx| > |y|$

Norme et distance p-adique

Proposition (Suite de Cauchy)

Pour $(x_n)_{n=0}^{\infty} \in K^{\mathbb{N}}$ avec K munit d'une valeur absolue non-archimédienne. $(x_n)_{n=0}^{\infty}$ est une suite de Cauchy si, et seulement si,

$$\lim_{n \to +\infty} |x_{n+1} - x_n| = 0.$$

Norme et distance p-adique

Proposition (Suite de Cauchy)

Pour $(x_n)_{n=0}^{\infty} \in K^{\mathbb{N}}$ avec K munit d'une valeur absolue non-archimédienne. $(x_n)_{n=0}^{\infty}$ est une suite de Cauchy si, et seulement si,

$$\lim_{n \to +\infty} |x_{n+1} - x_n| = 0.$$

<u>Preuve</u>:

Norme et distance p-adique

Proposition (Suite de Cauchy)

Pour $(x_n)_{n=0}^{\infty} \in K^{\mathbb{N}}$ avec K munit d'une valeur absolue non-archimédienne. $(x_n)_{n=0}^{\infty}$ est une suite de Cauchy si, et seulement si,

$$\lim_{n \to +\infty} |x_{n+1} - x_n| = 0.$$

Preuve:
(x_n) est une suite de Cauchy si :

$$\forall \epsilon > 0,\ \exists N \in \mathbb{N} \mid \forall (n,m) \in \mathbb{N}^2,\ m > n \geqslant N \Longrightarrow |x_n - x_m| \leqslant \epsilon$$

Norme et distance p-adique

Proposition (Suite de Cauchy)

Pour $(x_n)_{n=0}^{\infty} \in K^{\mathbb{N}}$ avec K munit d'une valeur absolue non-archimédienne. $(x_n)_{n=0}^{\infty}$ est une suite de Cauchy si, et seulement si,

$$\lim_{n \to +\infty} |x_{n+1} - x_n| = 0.$$

<u>Preuve</u>:
(x_n) est une suite de Cauchy si :

$$\forall \epsilon > 0,\ \exists N \in \mathbb{N} \mid \forall (n,m) \in \mathbb{N}^2,\ m > n \geqslant N \Longrightarrow |x_n - x_m| \leqslant \epsilon$$

- Qu'une suite de Cauchy vérifie $\lim_{n \to +\infty} |x_{n+1} - x_n| = 0$ suit immédiatement de la définition.

Norme et distance p-adique

Proposition (Suite de Cauchy)

Pour $(x_n)_{n=0}^{\infty} \in K^{\mathbb{N}}$ avec K munit d'une valeur absolue non-archimédienne. $(x_n)_{n=0}^{\infty}$ est une suite de Cauchy si, et seulement si,

$$\lim_{n \to +\infty} |x_{n+1} - x_n| = 0.$$

Preuve:
(x_n) est une suite de Cauchy si :

$$\forall \epsilon > 0,\ \exists N \in \mathbb{N} \mid \forall (n,m) \in \mathbb{N}^2,\ m > n \geqslant N \Longrightarrow |x_n - x_m| \leqslant \epsilon$$

- Qu'une suite de Cauchy vérifie $\lim_{n \to +\infty} |x_{n+1} - x_n| = 0$ suit immédiatement de la définition.
- Qu'une suite qui vérifie une telle propriété soit de Cauchy provient de l'inégalité ci-dessous:

Norme et distance p-adique

Proposition (Suite de Cauchy)

Pour $(x_n)_{n=0}^{\infty} \in K^{\mathbb{N}}$ avec K munit d'une valeur absolue non-archimédienne. $(x_n)_{n=0}^{\infty}$ est une suite de Cauchy si, et seulement si,

$$\lim_{n \to +\infty} |x_{n+1} - x_n| = 0.$$

Preuve:
(x_n) est une suite de Cauchy si :

$$\forall \epsilon > 0,\ \exists N \in \mathbb{N} \mid \forall (n, m) \in \mathbb{N}^2,\ m > n \geqslant N \Longrightarrow |x_n - x_m| \leqslant \epsilon$$

- Qu'une suite de Cauchy vérifie $\lim_{n \to +\infty} |x_{n+1} - x_n| = 0$ suit immédiatement de la définition.
- Qu'une suite qui vérifie une telle propriété soit de Cauchy provient de l'inégalité ci-dessous:

$$|x_m - x_n| = |x_m - x_{m-1} + \ldots + x_{n+1} - x_n| \leqslant \max\{|x_m - x_{m-1}|, \ldots, |x_{n+1} - x_n|\}$$

Preuve de la non complétude de $\mathbb{Q}$

Soit $|.|$ une valeur absolue sur $\mathbb{Q}$.

Preuve de la non complétude de $\mathbb{Q}$

Soit $|.|$ une valeur absolue sur $\mathbb{Q}$.
On invoque le théorème d'Ostrowski :

Preuve de la non complétude de $\mathbb{Q}$

Soit $|.|$ une valeur absolue sur $\mathbb{Q}$.
On invoque le théorème d'Ostrowski :

Théorème d'Ostrowski

Toute valeur absolue non triviale sur $\mathbb{Q}$ est équivalente à $|.|_p$ pour un entier premier p ou $p = \infty$ (la valeur absolue usuelle).

Preuve de la non complétude de $\mathbb{Q}$

Soit $|.|$ une valeur absolue sur $\mathbb{Q}$.
On invoque le théorème d'Ostrowski :

Théorème d'Ostrowski

Toute valeur absolue non triviale sur $\mathbb{Q}$ est équivalente à $|.|_p$ pour un entier premier p ou $p = \infty$ (la valeur absolue usuelle).

- Le cas $p = \infty$ est connu avec une suite $(x_n)_{n=0}^{\infty}$ définie par $x_{n+1} = \frac{1}{2}(x_n + \frac{2}{x_n})$
- p premier impair.

Preuve de la non complétude de $\mathbb{Q}$

Soit $|.|$ une valeur absolue sur $\mathbb{Q}$.
On invoque le théorème d'Ostrowski :

Théorème d'Ostrowski

Toute valeur absolue non triviale sur $\mathbb{Q}$ est équivalente à $|.|_p$ pour un entier premier p ou $p = \infty$ (la valeur absolue usuelle).

- Le cas $p = \infty$ est connu avec une suite $(x_n)_{n=0}^{\infty}$ définie par $x_{n+1} = \frac{1}{2}(x_n + \frac{2}{x_n})$
- p premier impair. On choisit $a \in \mathbb{Z}$ tel que:
  1. a n'est pas un carré dans $\mathbb{Q}$
  2. p ne divise pas a.
  3. a est un carré modulo p.

  a existe car on prend un $a = 1 mod(p)$.

Preuve de la non complétude de $\mathbb{Q}$

Soit $|.|$ une valeur absolue sur $\mathbb{Q}$.
On invoque le théorème d'Ostrowski :

Théorème d'Ostrowski

Toute valeur absolue non triviale sur $\mathbb{Q}$ est équivalente à $|.|_p$ pour un entier premier p ou $p = \infty$ (la valeur absolue usuelle).

- Le cas $p = \infty$ est connu avec une suite $(x_n)_{n=0}^{\infty}$ définie par $x_{n+1} = \frac{1}{2}(x_n + \frac{2}{x_n})$
- p premier impair. On choisit $a \in \mathbb{Z}$ tel que:
  1. a n'est pas un carré dans $\mathbb{Q}$
  2. p ne divise pas a.
  3. a est un carré modulo p.

  a existe car on prend un $a = 1 mod(p)$.
  En effet, la distance entre deux carrés successifs dans $\mathbb{Z}$ croit linéairement, alors il existe kp et $(k+1)p$ situé entre deux carrés successifs.

Preuve de la non complétude de $\mathbb{Q}$

Soit $|.|$ une valeur absolue sur $\mathbb{Q}$.
On invoque le théorème d'Ostrowski :

Théorème d'Ostrowski

Toute valeur absolue non triviale sur $\mathbb{Q}$ est équivalente à $|.|_p$ pour un entier premier p ou $p = \infty$ (la valeur absolue usuelle).

- Le cas $p = \infty$ est connu avec une suite $(x_n)_{n=0}^{\infty}$ définie par $x_{n+1} = \frac{1}{2}(x_n + \frac{2}{x_n})$
- p premier impair. On choisit $a \in \mathbb{Z}$ tel que:
  1. a n'est pas un carré dans $\mathbb{Q}$
  2. p ne divise pas a.
  3. a est un carré modulo p.

  a existe car on prend un $a = 1 mod(p)$.
  En effet, la distance entre deux carrés successifs dans $\mathbb{Z}$ croit linéairement, alors il existe kp et $(k+1)p$ situé entre deux carrés successifs.
  Alors $a = 1 + kp$ convient.

Preuve de la non complétude de $\mathbb{Q}$

Construction d'une suite de Cauchy $(x_n)_{n=0}^{\infty} \in \mathbb{Z}^{\mathbb{N}}$ qui ne converge pas dans $\mathbb{Q}$ pour $|.|_p$.

Preuve de la non complétude de $\mathbb{Q}$

Construction d'une suite de Cauchy $(x_n)_{n=0}^{\infty} \in \mathbb{Z}^{\mathbb{N}}$ qui ne converge pas dans $\mathbb{Q}$ pour $|.|_p$.
On va construire pour cela :

- x_0 tel que $x_0^2 \equiv a \ mod(p)$
- $x_1 \equiv x_0 \ mod(p)$
- $x_1^2 \equiv a \ mod(p^2)$.

Preuve de la non complétude de $\mathbb{Q}$

Construction d'une suite de Cauchy $(x_n)_{n=0}^{\infty} \in \mathbb{Z}^{\mathbb{N}}$ qui ne converge pas dans $\mathbb{Q}$ pour $|.|_p$.
On va construire pour cela :

- x_0 tel que $x_0^2 \equiv a \ mod(p)$
- $x_1 \equiv x_0 \ mod(p)$
- $x_1^2 \equiv a \ mod(p^2)$.

<u>En effet</u>, On sait déjà par le 3 ième point qu'il existe x_0 tel que $x_0^2 \equiv a \ mod(p)$ et notons b_0 le plus petit entier positif tel que $x_0 \equiv b_0 \mod p$.
On cherche x_1 sous la forme $x_1 = b_0 + b_1 p$ avec $b_1 \in \mathbb{Z}$.

Preuve de la non complétude de $\mathbb{Q}$

Construction d'une suite de Cauchy $(x_n)_{n=0}^{\infty} \in \mathbb{Z}^{\mathbb{N}}$ qui ne converge pas dans $\mathbb{Q}$ pour $|.|_p$.

On va construire pour cela :

- x_0 tel que $x_0^2 \equiv a \; mod(p)$
- $x_1 \equiv x_0 \; mod(p)$
- $x_1^2 \equiv a \; mod(p^2)$.

<u>En effet</u>, On sait déjà par le 3 ième point qu'il existe x_0 tel que $x_0^2 \equiv a \; mod(p)$ et notons b_0 le plus petit entier positif tel que $x_0 \equiv b_0 \mod p$.

On cherche x_1 sous la forme $x_1 = b_0 + b_1 p$ avec $b_1 \in \mathbb{Z}$.

Calculons x_1^2:

$$x_1^2 \equiv b_0^2 + 2 b_0 b_1 p \mod p^2$$

Preuve de la non complétude de $\mathbb{Q}$

Construction d'une suite de Cauchy $(x_n)_{n=0}^{\infty} \in \mathbb{Z}^{\mathbb{N}}$ qui ne converge pas dans $\mathbb{Q}$ pour $|.|_p$.
On va construire pour cela :

- x_0 tel que $x_0^2 \equiv a \ mod(p)$
- $x_1 \equiv x_0 \ mod(p)$
- $x_1^2 \equiv a \ mod(p^2)$.

En effet, On sait déjà par le 3 ième point qu'il existe x_0 tel que $x_0^2 \equiv a \ mod(p)$ et notons b_0 le plus petit entier positif tel que $x_0 \equiv b_0 \mod p$.
On cherche x_1 sous la forme $x_1 = b_0 + b_1 p$ avec $b_1 \in \mathbb{Z}$.
Calculons x_1^2:

$$x_1^2 \equiv b_0^2 + 2b_0 b_1 p \mod p^2$$

On veut que $x_1^2 \equiv a \mod p^2$ i.e. $b_0^2 + 2b_0 b_1 p \equiv a \mod p^2$.

Preuve de la non complétude de $\mathbb{Q}$

Construction d'une suite de Cauchy $(x_n)_{n=0}^{\infty} \in \mathbb{Z}^{\mathbb{N}}$ qui ne converge pas dans $\mathbb{Q}$ pour $|.|_p$.
On va construire pour cela :

- x_0 tel que $x_0^2 \equiv a \; mod(p)$
- $x_1 \equiv x_0 \; mod(p)$
- $x_1^2 \equiv a \; mod(p^2)$.

<u>En effet</u>, On sait déjà par le 3 ième point qu'il existe x_0 tel que $x_0^2 \equiv a \; mod(p)$ et notons b_0 le plus petit entier positif tel que $x_0 \equiv b_0 \mod p$.
On cherche x_1 sous la forme $x_1 = b_0 + b_1 p$ avec $b_1 \in \mathbb{Z}$.
Calculons x_1^2:

$$x_1^2 \equiv b_0^2 + 2b_0 b_1 p \mod p^2$$

On veut que $x_1^2 \equiv a \mod p^2$ i.e. $b_0^2 + 2b_0 b_1 p \equiv a \mod p^2$.
b_0^2 et a étant congru au même nombre, il existe un $k \in \mathbb{Z}$ tel que $b_0^2 = a - kp$.

Preuve de la non complétude de $\mathbb{Q}$

Construction d'une suite de Cauchy $(x_n)_{n=0}^{\infty} \in \mathbb{Z}^{\mathbb{N}}$ qui ne converge pas dans $\mathbb{Q}$ pour $|.|_p$.
On va construire pour cela :

- x_0 tel que $x_0^2 \equiv a \ mod(p)$
- $x_1 \equiv x_0 \ mod(p)$
- $x_1^2 \equiv a \ mod(p^2)$.

<u>En effet</u>, On sait déjà par le 3 ième point qu'il existe x_0 tel que $x_0^2 \equiv a \ mod(p)$ et notons b_0 le plus petit entier positif tel que $x_0 \equiv b_0 \mod p$.
On cherche x_1 sous la forme $x_1 = b_0 + b_1 p$ avec $b_1 \in \mathbb{Z}$.
Calculons x_1^2:

$$x_1^2 \equiv b_0^2 + 2b_0 b_1 p \mod p^2$$

On veut que $x_1^2 \equiv a \mod p^2$ i.e. $b_0^2 + 2b_0 b_1 p \equiv a \mod p^2$.
b_0^2 et a étant congru au même nombre, il existe un $k \in \mathbb{Z}$ tel que $b_0^2 = a - kp$.
Ainsi:

$$a \equiv b_0^2 + 2b_0 b_1 p \equiv a + p(2b_0 b_1 - k) \mod p^2$$

$$\iff p(2b_0 b_1 - k) \equiv 0 \mod p^2 \iff 2b_0 b_1 - k \equiv 0 \mod p$$

Et b_0 n'étant pas un multiple de p, il suffit de prendre b_1 tel que $b_1 \equiv k(2b_0)^{-1} \mod p$.

Preuve de la non complétude de $\mathbb{Q}$

Construction d'une suite de Cauchy $(x_n)_{n=0}^{\infty} \in \mathbb{Z}^{\mathbb{N}}$ qui ne converge pas dans $\mathbb{Q}$ pour $|.|_p$.
On va construire pour cela :

- x_0 tel que $x_0^2 \equiv a \ mod(p)$
- $x_1 \equiv x_0 \ mod(p)$
- $x_1^2 \equiv a \ mod(p^2)$.

<u>En effet</u>, On sait déjà par le 3 ième point qu'il existe x_0 tel que $x_0^2 \equiv a \ mod(p)$ et notons b_0 le plus petit entier positif tel que $x_0 \equiv b_0 \mod p$.
On cherche x_1 sous la forme $x_1 = b_0 + b_1 p$ avec $b_1 \in \mathbb{Z}$.
Calculons x_1^2:

$$x_1^2 \equiv b_0^2 + 2b_0 b_1 p \mod p^2$$

On veut que $x_1^2 \equiv a \mod p^2$ i.e. $b_0^2 + 2b_0 b_1 p \equiv a \mod p^2$.
b_0^2 et a étant congru au même nombre, il existe un $k \in \mathbb{Z}$ tel que $b_0^2 = a - kp$.
Ainsi:

$$a \equiv b_0^2 + 2b_0 b_1 p \equiv a + p(2b_0 b_1 - k) \mod p^2$$

$$\iff p(2b_0 b_1 - k) \equiv 0 \mod p^2 \iff 2b_0 b_1 - k \equiv 0 \mod p$$

Et b_0 n'étant pas un multiple de p, il suffit de prendre b_1 tel que $b_1 \equiv k(2b_0)^{-1} \mod p$.
Ce qui prouve l'existence de x_1.

Preuve de la non complétude de $\mathbb{Q}$

Par itération,

Preuve de la non complétude de $\mathbb{Q}$

Par itération, on peut construire $(x_n)_{n=0}^{\infty}$ telle que

$$x_n \equiv x_{n-1} \mod (p^n) \text{ et } x_n^2 \equiv a \mod (p^{n+1})$$

Preuve de la non complétude de $\mathbb{Q}$

Par itération, on peut construire $(x_n)_{n=0}^{\infty}$ telle que

$$x_n \equiv x_{n-1} \mod (p^n) \text{ et } x_n^2 \equiv a \mod (p^{n+1})$$

De plus la suite est de Cauchy par :

$$\forall n \in \mathbb{N},\ |x_{n+1} - x_n|_p = |\lambda p^{n+1}|_p \leqslant p^{-(n+1)} \to 0$$

Preuve de la non complétude de $\mathbb{Q}$

Par itération, on peut construire $(x_n)_{n=0}^{\infty}$ telle que

$$x_n \equiv x_{n-1} \mod (p^n) \text{ et } x_n^2 \equiv a \mod (p^{n+1})$$

De plus la suite est de Cauchy par :

$$\forall n \in \mathbb{N},\ |x_{n+1} - x_n|_p = |\lambda p^{n+1}|_p \leqslant p^{-(n+1)} \to 0$$

et on a :

$$\forall n \in \mathbb{N},\ |x_n^2 - a|_p = |\mu p^{n+1}|_p \leqslant p^{-(n+1)} \to 0$$

Preuve de la non complétude de $\mathbb{Q}$

Par itération, on peut construire $(x_n)_{n=0}^{\infty}$ telle que

$$x_n \equiv x_{n-1} \mod (p^n) \text{ et } x_n^2 \equiv a \mod (p^{n+1})$$

De plus la suite est de Cauchy par :

$$\forall n \in \mathbb{N},\ |x_{n+1} - x_n|_p = |\lambda p^{n+1}|_p \leqslant p^{-(n+1)} \to 0$$

et on a :

$$\forall n \in \mathbb{N},\ |x_n^2 - a|_p = |\mu p^{n+1}|_p \leqslant p^{-(n+1)} \to 0$$

Donc par continuité de la racine carré, $(x_n)_{n=0}^{\infty}$ admet une limite non rationnel.

Preuve de la non complétude de $\mathbb{Q}$

Par itération, on peut construire $(x_n)_{n=0}^{\infty}$ telle que

$$x_n \equiv x_{n-1} \mod (p^n) \text{ et } x_n^2 \equiv a \mod (p^{n+1})$$

De plus la suite est de Cauchy par :

$$\forall n \in \mathbb{N},\ |x_{n+1} - x_n|_p = |\lambda p^{n+1}|_p \leqslant p^{-(n+1)} \to 0$$

et on a :

$$\forall n \in \mathbb{N},\ |x_n^2 - a|_p = |\mu p^{n+1}|_p \leqslant p^{-(n+1)} \to 0$$

Donc par continuité de la racine carré, $(x_n)_{n=0}^{\infty}$ admet une limite non rationnel. Donc $\mathbb{Q}$ est non complet.

- Pour $p = 2$, on procède de même avec le choix d'un $a \in \mathbb{Z}$ tel que:
  1. a n'est pas un cube dans $\mathbb{Q}$
  2. a impair.
  3. a est un cube modulo 2.

  et d'une suite de Cauchy $(x_n)_{n=0}^{\infty} \in \mathbb{Z}^{\mathbb{N}}$ non convergente dans $\mathbb{Q}$ vérifiant :

$$x_n \equiv x_{n-1} \mod (2^n) \text{ et } x_n^3 \equiv a \mod (2^{n+1})$$

Sommaire

Complétion p-adique de $\mathbb{Q}$

Soit $\mathcal{C}_p$ l'ensemble des suites de Cauchy sur $(\mathbb{Q}, |\cdot|_p)$.

Complétion p-adique de $\mathbb{Q}$

Soit $\mathcal{C}_p$ l'ensemble des suites de Cauchy sur $(\mathbb{Q}, |\cdot|_p)$.

$$\mathcal{C}_p := \{(x_n)_{n=0}^{\infty} \in \mathbb{Q}^{\mathbb{N}} \mid \forall \epsilon \in \mathbb{Q}_+^*,\ \exists N_\epsilon > 0 \mid \forall (n, m) \in \mathbb{N}^2,\ n, m \geqslant N_\epsilon \implies |x_n - x_m|_p < \epsilon\}$$

Complétion p-adique de $\mathbb{Q}$

Soit $\mathcal{C}_p$ l'ensemble des suites de Cauchy sur $(\mathbb{Q}, |\cdot|_p)$.

$$\mathcal{C}_p := \{(x_n)_{n=0}^{\infty} \in \mathbb{Q}^{\mathbb{N}} \mid \forall \epsilon \in \mathbb{Q}_+^*,\ \exists N_\epsilon > 0 \mid \forall (n,m) \in \mathbb{N}^2,\ n, m \geqslant N_\epsilon \Longrightarrow |x_n - x_m|_p < \epsilon\}$$

Propriété

$\mathcal{C}_p$ est munit d'une structure d'anneau commutatif.

Complétion p-adique de $\mathbb{Q}$

Soit $\mathcal{C}_p$ l'ensemble des suites de Cauchy sur $(\mathbb{Q}, |\cdot|_p)$.

$$\mathcal{C}_p := \{(x_n)_{n=0}^{\infty} \in \mathbb{Q}^{\mathbb{N}} \mid \forall \epsilon \in \mathbb{Q}_+^*, \ \exists N_\epsilon > 0 \mid \forall (n,m) \in \mathbb{N}^2, \ n, m \geqslant N_\epsilon \Longrightarrow |x_n - x_m|_p < \epsilon\}$$

Propriété

$\mathcal{C}_p$ est munit d'une structure d'anneau commutatif.

En effet, on le voit comme sous-anneau de $(\mathbb{Q}^{\mathbb{N}}, +, \cdot)$.

Complétion p-adique de $\mathbb{Q}$

On veut un espace où les suites de Cauchy à valeurs dans $\mathbb{Q}^{\mathbb{N}}$ convergent.

Complétion p-adique de $\mathbb{Q}$

On veut un espace où les suites de Cauchy à valeurs dans $\mathbb{Q}^{\mathbb{N}}$ convergent.
On définit alors $\sim$:

$$(x_n) \sim (y_n) \Longleftrightarrow \lim_{n \to +\infty} |y_n - x_n|_p = 0.$$

Complétion p-adique de $\mathbb{Q}$

On veut un espace où les suites de Cauchy à valeurs dans $\mathbb{Q}^{\mathbb{N}}$ convergent.
On définit alors $\sim$:

$$(x_n) \sim (y_n) \Longleftrightarrow \lim_{n \to +\infty} |y_n - x_n|_p = 0.$$

Propriété

$\sim$ est une relation d'équivalence sur $\mathcal{C}_p$.

Complétion p-adique de $\mathbb{Q}$

On veut un espace où les suites de Cauchy à valeurs dans $\mathbb{Q}^{\mathbb{N}}$ convergent.
On définit alors $\sim$:

$$(x_n) \sim (y_n) \iff \lim_{n \to +\infty} |y_n - x_n|_p = 0.$$

Propriété

$\sim$ est une relation d'équivalence sur $\mathcal{C}_p$.

Définition

Soit $\mathcal{N} := \{(x_n)_{n=0}^{\infty} \in \mathbb{Q}^{\mathbb{N}} \mid \lim_{n \to +\infty} x_n = 0\}$.

Complétion p-adique de $\mathbb{Q}$

On veut un espace où les suites de Cauchy à valeurs dans $\mathbb{Q}^{\mathbb{N}}$ convergent.
On définit alors $\sim$:

$$(x_n) \sim (y_n) \iff \lim_{n \to +\infty} |y_n - x_n|_p = 0.$$

Propriété

$\sim$ est une relation d'équivalence sur $\mathcal{C}_p$.

Définition

Soit $\mathcal{N} := \{(x_n)_{n=0}^{\infty} \in \mathbb{Q}^{\mathbb{N}} \mid \lim_{n \to +\infty} x_n = 0\}$.

Propriété

$\mathcal{N}$ est un idéal maximal de $\mathcal{C}_p$.

Complétion p-adique de $\mathbb{Q}$

On veut un espace où les suites de Cauchy à valeurs dans $\mathbb{Q}^{\mathbb{N}}$ convergent.
On définit alors $\sim$:

$$(x_n) \sim (y_n) \Longleftrightarrow \lim_{n\to+\infty} |y_n - x_n|_p = 0.$$

Propriété

$\sim$ est une relation d'équivalence sur $\mathcal{C}_p$.

Définition

Soit $\mathcal{N} := \{(x_n)_{n=0}^{\infty} \in \mathbb{Q}^{\mathbb{N}} \mid \lim_{n\to+\infty} x_n = 0\}$.

Propriété

$\mathcal{N}$ est un idéal maximal de $\mathcal{C}_p$.

Définition

On définit l'ensemble des nombres p-adique par

$$\mathbb{Q}_p := \mathcal{C}_p/\mathcal{N} = \mathcal{C}_p/\sim .$$

Complétion p-adique de $\mathbb{Q}$

Théorème

Pour $p \in \mathbb{P} \cup \{\infty\}$, $\mathbb{Q}_p$ est un corps commutatif contenant $\mathbb{Q}$.

Complétion p-adique de $\mathbb{Q}$

Théorème

Pour $p \in \mathbb{P} \cup \{\infty\}$, $\mathbb{Q}_p$ est un corps commutatif contenant $\mathbb{Q}$.

Preuve:

Complétion p-adique de $\mathbb{Q}$

Théorème

Pour $p \in \mathbb{P} \cup \{\infty\}$, $\mathbb{Q}_p$ est un corps commutatif contenant $\mathbb{Q}$.

Preuve: L'idéal $\mathcal{N}$ étant maximal et $\mathcal{C}_p$ étant un anneau commutatif, par quotient,

Complétion p-adique de $\mathbb{Q}$

Théorème

Pour $p \in \mathbb{P} \cup \{\infty\}$, $\mathbb{Q}_p$ est un corps commutatif contenant $\mathbb{Q}$.

Preuve: L'idéal $\mathcal{N}$ étant maximal et $\mathcal{C}_p$ étant un anneau commutatif, par quotient, il suit que $\mathbb{Q}_p$ est un corps commutatif.

Complétion p-adique de $\mathbb{Q}$

Théorème

Pour $p \in \mathbb{P} \cup \{\infty\}$, $\mathbb{Q}_p$ est un corps commutatif contenant $\mathbb{Q}$.

Preuve: L'idéal $\mathcal{N}$ étant maximal et $\mathcal{C}_p$ étant un anneau commutatif, par quotient, il suit que $\mathbb{Q}_p$ est un corps commutatif.
Ensuite, on va montrer que $\mathbb{Q}_p$ contient un sous-corps s'identifiant à $\mathbb{Q}$

Complétion p-adique de $\mathbb{Q}$

Théorème

Pour $p \in \mathbb{P} \cup \{\infty\}$, $\mathbb{Q}_p$ est un corps commutatif contenant $\mathbb{Q}$.

Preuve: L'idéal $\mathcal{N}$ étant maximal et $\mathcal{C}_p$ étant un anneau commutatif, par quotient, il suit que $\mathbb{Q}_p$ est un corps commutatif.
Ensuite, on va montrer que $\mathbb{Q}_p$ contient un sous-corps s'identifiant à $\mathbb{Q}$: considérons alors l'application

$$i : q \in \mathbb{Q} \mapsto \overline{(q)}_{n=0}^{\infty} \in \mathbb{Q}_p.$$

Cette application est trivialement injective, donc bijective sur son image, de plus, par définition des lois $+$ et $\cdot$ sur $\mathbb{Q}_p$,

Complétion p-adique de $\mathbb{Q}$

Théorème

Pour $p \in \mathbb{P} \cup \{\infty\}$, $\mathbb{Q}_p$ est un corps commutatif contenant $\mathbb{Q}$.

Preuve: L'idéal $\mathcal{N}$ étant maximal et $\mathcal{C}_p$ étant un anneau commutatif, par quotient, il suit que $\mathbb{Q}_p$ est un corps commutatif.
Ensuite, on va montrer que $\mathbb{Q}_p$ contient un sous-corps s'identifiant à $\mathbb{Q}$: considérons alors l'application

$$i : q \in \mathbb{Q} \mapsto \overline{(q)}_{n=0}^{\infty} \in \mathbb{Q}_p.$$

Cette application est trivialement injective, donc bijective sur son image, de plus, par définition des lois $+$ et $\cdot$ sur $\mathbb{Q}_p$, c'est aussi un homomorphisme d'anneaux,

Complétion p-adique de $\mathbb{Q}$

Théorème

Pour $p \in \mathbb{P} \cup \{\infty\}$, $\mathbb{Q}_p$ est un corps commutatif contenant $\mathbb{Q}$.

Preuve: L'idéal $\mathcal{N}$ étant maximal et $\mathcal{C}_p$ étant un anneau commutatif, par quotient, il suit que $\mathbb{Q}_p$ est un corps commutatif.
Ensuite, on va montrer que $\mathbb{Q}_p$ contient un sous-corps s'identifiant à $\mathbb{Q}$: considérons alors l'application

$$i : q \in \mathbb{Q} \mapsto \overline{(q)}_{n=0}^{\infty} \in \mathbb{Q}_p.$$

Cette application est trivialement injective, donc bijective sur son image, de plus, par définition des lois $+$ et $\cdot$ sur $\mathbb{Q}_p$, c'est aussi un homomorphisme d'anneaux, et $\mathbb{Q}$ est donc isomorphe à $\mathrm{Im}\, i = \{$les classes des suites constantes$\}$, qui est donc un sous-corps de $\mathbb{Q}_p$.

Complétion p-adique de $\mathbb{Q}$

Remarque

Pour $q \in \mathbb{Q}$, on note $q := \overline{(q)}_{n=0}^{\infty} \in \mathbb{Q}_p$.

Complétion p-adique de $\mathbb{Q}$

Remarque

Pour $q \in \mathbb{Q}$, on note $q := \overline{(q)}_{n=0}^{\infty} \in \mathbb{Q}_p$.

Remarque

On a $\mathbb{Q}_\infty := \mathbb{R}$.
Ainsi pour la suite, on va seulement étudier les $\mathbb{Q}_p$ pour $p \in \mathbb{P}$.

Construction de l'espace métrique $\mathbb{Q}_p$ et propriétés topologiques

Soit $p \in \mathbb{P}$.

Construction de l'espace métrique $\mathbb{Q}_p$ et propriétés topologiques

Soit $p \in \mathbb{P}$.

Proposition-Définition (Norme p-adique sur $\mathbb{Q}_p$)

Pour un nombre p-adique a, soit $(a_n)_{n=0}^{\infty}$ un représentant de a, on définit alors la norme p-adique de a, toujours notée $|a|_p$, par:

$$|a|_p = \lim_{n \to +\infty} |a_n|_p$$

Construction de l'espace métrique $\mathbb{Q}_p$ et propriétés topologiques

Soit $p \in \mathbb{P}$.

Proposition-Définition (Norme p-adique sur $\mathbb{Q}_p$)

Pour un nombre p-adique a, soit $(a_n)_{n=0}^{\infty}$ un représentant de a, on définit alors la norme p-adique de a, toujours notée $|a|_p$, par:

$$|a|_p = \lim_{n \to +\infty} |a_n|_p$$

Preuve: En effet, elle vérifie les axiomes : **séparation**, **inégalité triangulaire** et **homogénéité** puisque ils sont vrais sur $\mathbb{Q}$.

Construction de l'espace métrique $\mathbb{Q}_p$ et propriétés topologiques

Attention !: Est-ce que $|\cdot|_p : \mathbb{Q}_p \to \mathbb{R}_+$?

Construction de l'espace métrique $\mathbb{Q}_p$ et propriétés topologiques

Attention !: Est-ce que $|\cdot|_p : \mathbb{Q}_p \to \mathbb{R}_+$?
Ce qui se justifie par :

Proposition

Soit $(x_n)_{n=0}^{\infty} \in \mathcal{C}_p \backslash \mathcal{N}$, la suite $(|x_n|_p)_{n=0}^{\infty}$ est constante à partir d'un certain rang.

Construction de l'espace métrique $\mathbb{Q}_p$ et propriétés topologiques

Attention !: Est-ce que $|\cdot|_p : \mathbb{Q}_p \to \mathbb{R}_+$?
Ce qui se justifie par :

Proposition

Soit $(x_n)_{n=0}^{\infty} \in \mathcal{C}_p \backslash \mathcal{N}$, la suite $(|x_n|_p)_{n=0}^{\infty}$ est constante à partir d'un certain rang.

Ainsi,

Définition

(Valuation p-adique sur $\mathbb{Q}_p$)
La valuation p-adique $ord_p(a)$ d'un nombre $a \in \mathbb{Q}_p$ est l'unique entier $m \in \mathbb{Z} \cup \{\infty\}$ tel que:

$$|a|_p = p^{-m}$$

Construction de l'espace métrique $\mathbb{Q}_p$ et propriétés topologiques

Lemme

$(\mathbb{Q}, |.|_p)$ est dense dans $(\mathbb{Q}_p, |.|_p)$.

Construction de l'espace métrique $\mathbb{Q}_p$ et propriétés topologiques

Lemme

$(\mathbb{Q}, |.|_p)$ est dense dans $(\mathbb{Q}_p, |.|_p)$.

Lemme

$(\mathbb{Q}_p, |.|_p)$ est complet.

Curiosités topologiques de $\mathbb{Q}_p$

Proposition

Soit $(a_n)_{n=0}^{\infty}$ une suite de $\mathbb{Q}_p$.
Alors, la série $\sum a_n$ converge dans $\mathbb{Q}_p$ si et seulement si la suite $(a_n)_{n\in\mathbb{N}}$ tend p-adiquement vers 0.

Curiosités topologiques de $\mathbb{Q}_p$

Proposition

Soit $(a_n)_{n=0}^{\infty}$ une suite de $\mathbb{Q}_p$.
Alors, la série $\sum a_n$ converge dans $\mathbb{Q}_p$ si et seulement si la suite $(a_n)_{n\in\mathbb{N}}$ tend p-adiquement vers 0.

Proposition

Toute boule ouverte dans $\mathbb{Q}_p$ est aussi fermée.

Curiosités topologiques de $\mathbb{Q}_p$

Proposition

Soit $(a_n)_{n=0}^{\infty}$ une suite de $\mathbb{Q}_p$.
Alors, la série $\sum a_n$ converge dans $\mathbb{Q}_p$ si et seulement si la suite $(a_n)_{n\in\mathbb{N}}$ tend p-adiquement vers 0.

Proposition

Toute boule ouverte dans $\mathbb{Q}_p$ est aussi fermée.

Proposition

Tout point d'une boule de $\mathbb{Q}_p$ en est un centre.

Curiosités topologiques de $\mathbb{Q}_p$

Proposition

Il y a un nombre dénombrable de boules ouvertes sur $\mathbb{Q}_p$.

Curiosités topologiques de $\mathbb{Q}_p$

Proposition

Il y a un nombre dénombrable de boules ouvertes sur $\mathbb{Q}_p$.

Proposition

Deux boules de $\mathbb{Q}_p$ sont d'intersection non vide <u>si et seulement si</u> l'une est incluse dans l'autre.

Sommaire

L'anneau $\mathbb{Z}_p$ des entiers p-adiques

Supposons que $\mathbb{Q}_p$ est déjà construit.

L'anneau $\mathbb{Z}_p$ des entiers p-adiques

Supposons que $\mathbb{Q}_p$ est déjà construit.
On va décrire $\mathbb{Q}_p$ à l'aide de

Proposition-Définition

L'ensemble $\mathbb{Z}_p$ des entiers p-adiques est donné par

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid ord_p(x) \geqslant 0\} = \{x \in \mathbb{Q}_p \mid |x|_p \leqslant 1\} = \overline{B}(0,1)$$

est un anneau commutatif intègre lorsqu'il est muni des mêmes lois que $\mathbb{Q}_p$.

L'anneau $\mathbb{Z}_p$ des entiers p-adiques

Supposons que $\mathbb{Q}_p$ est déjà construit.
On va décrire $\mathbb{Q}_p$ à l'aide de

Proposition-Définition

L'ensemble $\mathbb{Z}_p$ des entiers p-adiques est donné par

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid ord_p(x) \geqslant 0\} = \{x \in \mathbb{Q}_p \mid |x|_p \leqslant 1\} = \overline{B}(0,1)$$

est un anneau commutatif intègre lorsqu'il est muni des mêmes lois que $\mathbb{Q}_p$.

On va voir le lien entre $\mathbb{Q}_p$ et $\mathbb{Z}_p$.

L'anneau $\mathbb{Z}_p$ des entiers p-adiques

Supposons que $\mathbb{Q}_p$ est déjà construit.
On va décrire $\mathbb{Q}_p$ à l'aide de

Proposition-Définition

L'ensemble $\mathbb{Z}_p$ des entiers p-adiques est donné par

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid ord_p(x) \geqslant 0\} = \{x \in \mathbb{Q}_p \mid |x|_p \leqslant 1\} = \overline{B}(0,1)$$

est un anneau commutatif intègre lorsqu'il est muni des mêmes lois que $\mathbb{Q}_p$.

On va voir le lien entre $\mathbb{Q}_p$ et $\mathbb{Z}_p$.
Dans la partie suivante, on va décrire algébriquement $\mathbb{Z}_p$.

L'anneau $\mathbb{Z}_p$ des entiers p-adiques

Supposons que $\mathbb{Q}_p$ est déjà construit.
On va décrire $\mathbb{Q}_p$ à l'aide de

Proposition-Définition

L'ensemble $\mathbb{Z}_p$ des entiers p-adiques est donné par

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid ord_p(x) \geqslant 0\} = \{x \in \mathbb{Q}_p \mid |x|_p \leqslant 1\} = \overline{B}(0,1)$$

est un anneau commutatif intègre lorsqu'il est muni des mêmes lois que $\mathbb{Q}_p$.

On va voir le lien entre $\mathbb{Q}_p$ et $\mathbb{Z}_p$.
Dans la partie suivante, on va décrire algébriquement $\mathbb{Z}_p$.
Ainsi, on obtiendra une construction algébrique de $\mathbb{Q}_p$.

L'anneau $\mathbb{Z}_p$ des entiers p-adiques

Supposons que $\mathbb{Q}_p$ est déjà construit.
On va décrire $\mathbb{Q}_p$ à l'aide de

Proposition-Définition

L'ensemble $\mathbb{Z}_p$ des entiers p-adiques est donné par

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid ord_p(x) \geqslant 0\} = \{x \in \mathbb{Q}_p \mid |x|_p \leqslant 1\} = \overline{B}(0,1)$$

est un anneau commutatif intègre lorsqu'il est muni des mêmes lois que $\mathbb{Q}_p$.

On va voir le lien entre $\mathbb{Q}_p$ et $\mathbb{Z}_p$.
Dans la partie suivante, on va décrire algébriquement $\mathbb{Z}_p$.
Ainsi, on obtiendra une construction algébrique de $\mathbb{Q}_p$.

L'anneau $\mathbb{Z}_p$ des entiers p-adiques

Proposition

$$\mathbb{Q}_p = \bigcup_{m \in \mathbb{Z}} p^m \mathbb{Z}_p.$$

L'anneau $\mathbb{Z}_p$ des entiers p-adiques

Proposition

$$\mathbb{Q}_p = \bigcup_{m \in \mathbb{Z}} p^m \mathbb{Z}_p.$$

Lemme

$$Frac(\mathbb{Z}_p) \simeq \mathbb{Q}_p.$$

Où

$$\left\{ \begin{array}{lcl} Frac(\mathbb{Z}_p) & \longrightarrow & \mathbb{Q}_p \\ \frac{a}{b} & \longmapsto & \frac{a}{b} \end{array} \right. .$$

Construction de $\mathbb{Z}_p$

Proposition-Définition

On définit

$$\mathbb{Z}_{(p)} := \{\frac{a}{b} \mid a, b \in \mathbb{Z}, p \nmid b\}$$

un sous-anneau de $\mathbb{Q}$ et de $\mathbb{Z}_p^{top}$.

Construction de $\mathbb{Z}_p$

Proposition-Définition

On définit

$$\mathbb{Z}_{(p)} := \{\frac{a}{b} \mid a, b \in \mathbb{Z}, p \nmid b\}$$

un sous-anneau de $\mathbb{Q}$ et de $\mathbb{Z}_p^{top}$.

Proposition

Pour tout entier $m \geqslant 0$,

$$\mathbb{Z}/p^m\mathbb{Z} \simeq \mathbb{Z}_{(p)}/p^m\mathbb{Z}_{(p)} \simeq \mathbb{Z}_p^{top}/p^m\mathbb{Z}_p^{top}$$

Construction de $\mathbb{Z}_p$

Grâce à

Définition (Limite inverse)

Soient $\{X_n\}_{n=1}^{\infty}$ une suite d'ensembles, et $\{f_n : X_{n+1} \to X_n\}_{n=1}^{\infty}$ une suite d'applications

$$\dots \xrightarrow{f_4} X_4 \xrightarrow{f_3} X_3 \xrightarrow{f_2} X_2 \xrightarrow{f_1} X_1$$

On appelle limite inverse de la suite $\{X_n\}_{n=1}^{\infty}$ et on note $\varprojlim_n X_n$ le sous-ensemble de $\prod_{n=1}^{\infty} X_n$ donné par:

$$\varprojlim_n X_n = \{(a_n)_{n=1}^{\infty} \in \prod_{n=1}^{\infty} X_n \mid \forall n \geqslant 1, f_n(a_{n+1}) = a_n\}$$

Construction de $\mathbb{Z}_p$

Grâce à

Définition (Limite inverse)

Soient $\{X_n\}_{n=1}^{\infty}$ une suite d'ensembles, et $\{f_n : X_{n+1} \to X_n\}_{n=1}^{\infty}$ une suite d'applications

$$\dots \xrightarrow{f_4} X_4 \xrightarrow{f_3} X_3 \xrightarrow{f_2} X_2 \xrightarrow{f_1} X_1$$

On appelle limite inverse de la suite $\{X_n\}_{n=1}^{\infty}$ et on note $\varprojlim_n X_n$ le sous-ensemble de $\prod_{n=1}^{\infty} X_n$ donné par:

$$\varprojlim_n X_n = \{(a_n)_{n=1}^{\infty} \in \prod_{n=1}^{\infty} X_n \mid \forall n \geqslant 1, f_n(a_{n+1}) = a_n\}$$

Ainsi

Proposition

$$\mathbb{Z}_p^{top} = \mathbb{Z}_p \simeq \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} =: \mathbb{Z}_p^{alg}$$

Construction de $\mathbb{Z}_p$

Ainsi

Théorème

$$\mathbb{Q}_p^{top} \simeq \mathbb{Q}_p^{alg}.$$

Expansion p-adique

Théorème

Soit $x \in \mathbb{Q}_p$. Alors x admet une écriture de la forme:

$$x = \sum_{n=m}^{\infty} c_n p^n, \ c_n \in \{0, 1, \ldots, p-1\} \text{ et } m \in \mathbb{Z}$$

De plus cette écriture est unique que l'on note $x = (\ldots c_{m+1} c_m)_p$.

Exemples:

$* \ 1 = 1 \times p^0 = \ldots 001_p =: 1_2$

Expansion p-adique

Théorème

Soit $x \in \mathbb{Q}_p$. Alors x admet une écriture de la forme:

$$x = \sum_{n=m}^{\infty} c_n p^n, \; c_n \in \{0, 1, \ldots, p-1\} \text{ et } m \in \mathbb{Z}$$

De plus cette écriture est unique que l'on note $x = (\ldots c_{m+1} c_m)_p$.

Exemples:

$*$ $1 = 1 \times p^0 = \ldots 001_p =: 1_2$

$*$ $p = 1 \times p + 0 \times p^0 =: 10_p$

Expansion p-adique

Théorème

Soit $x \in \mathbb{Q}_p$. Alors x admet une écriture de la forme:

$$x = \sum_{n=m}^{\infty} c_n p^n, \ \ c_n \in \{0, 1, \ldots, p-1\} \text{ et } m \in \mathbb{Z}$$

De plus cette écriture est unique que l'on note $x = (\ldots c_{m+1} c_m)_p$.

Exemples:

$*$ $1 = 1 \times p^0 = \ldots 001_p =: 1_2$
$*$ $p = 1 \times p + 0 \times p^0 =: 10_p$
$*$ $-1_2 = \ldots 111_2$

Expansion p-adique

Théorème

Soit $x \in \mathbb{Q}_p$. Alors x admet une écriture de la forme:

$$x = \sum_{n=m}^{\infty} c_n p^n, \;\; c_n \in \{0, 1, \dots, p-1\} \text{ et } m \in \mathbb{Z}$$

De plus cette écriture est unique que l'on note $x = (\dots c_{m+1} c_m)_p$.

<u>Exemples</u>:

$* \; 1 = 1 \times p^0 = \dots 001_p =: 1_2$
$* \; p = 1 \times p + 0 \times p^0 =: 10_p$
$* \; -1_2 = \dots 111_2$ car $\dots 111_2 + 1_2 = \dots 000_2 =: 0_2$

Expansion p-adique

Théorème

Soit $x \in \mathbb{Q}_p$. Alors x admet une écriture de la forme:

$$x = \sum_{n=m}^{\infty} c_n p^n, \; c_n \in \{0, 1, \ldots, p-1\} \text{ et } m \in \mathbb{Z}$$

De plus cette écriture est unique que l'on note $x = (\ldots c_{m+1} c_m)_p$.

Exemples:

$*$ $1 = 1 \times p^0 = \ldots 001_p =: 1_2$
$*$ $p = 1 \times p + 0 \times p^0 =: 10_p$
$*$ $-1_2 = \ldots 111_2$ car $\ldots 111_2 + 1_2 = \ldots 000_2 =: 0_2$

Avec ce théorème, on peut compter dans $\mathbb{Q}_p$.

Bibliographie

- Number Theory 1, Fermat's Dreams ; Kazuya Kato, Nobushige Kurokawa, Takeshi Saito. Éditions de l'American Mathematical Society.
- p-adique Numbers, An introduction ; Fernando Q. Gouvêa. Éditions Springer-Verlag Berlin Heidelberg GmbH.
- Géométrie Algébrique. Une introduction ; Daniel Perrin. Éditions EDP Sciences.
- Topological properties of $\mathbb{Z}_p$ and $\mathbb{Q}_p$ and Euclidean models; Samuel Trautwein, Esther Röder, Giorgio Barozzi ; https://www2.math.ethz.ch/education/bachelor/seminars/hs2011/p-adic/report5.pdf