Calendrier de l'Avent p-adique

J'utiliserai "🎀" dans les preuves lorsqu'un résultat est admis. J'essaierai de mettre des références pour combler ces manques d'ici le 25.
Dans tout ce document, p désignera un nombre premier.

❄ Définition 1 (Valeur absolue).

Soit $\mathbb{K}$ un corps.
On appelle *valeur absolue* sur $\mathbb{K}$ toute application $|\cdot| : \mathbb{K} \to \mathbb{R}^+$ vérifiant :

$$\begin{array}{ll} \text{(VA1)} & \forall x \in \mathbb{K}, |x| = 0 \Leftrightarrow x = 0 \\ \text{(VA2)} & \forall (x,y) \in \mathbb{K}^2, |xy| = |x||y| \\ \text{(VA3)} & \forall (x,y) \in \mathbb{K}^2, |x+y| \leq |x| + |y|. \end{array}$$

La valeur absolue est dite *ultramétrique* si de plus on a la condition :

$$\text{(VA3')} \quad \forall (x,y) \in \mathbb{K}^2, |x+y| \leq \max(|x|, |y|).$$

❄ Définition 2 (Valuation p-adique).

Soit $x \in \mathbb{Z}\backslash\{0\}$.
On définit l'entier naturel noté $v_p(x)$ suivant :

$$v_p(x) := \max\{m \in \mathbb{N},\ p^m | x\}.$$

On posera $v_p(0) = +\infty$.
Si $x = a/b \in \mathbb{Q}^*$, on définit de même dans $\mathbb{Z}$:

$$v_p(x) := v_p(a) - v_p(b).$$

Ce nombre ne dépend pas du représentant de x.

🎄 Fait du Jour 1.

L'application :

$$\begin{array}{rl} \mathbb{Q} \to & \mathbb{R}^+ \\ x \mapsto & \begin{cases} 0 \text{ si } x = 0 \\ p^{-v_p(x)} \text{ sinon} \end{cases} \end{array}$$

est une valeur absolue ultramétrique sur $\mathbb{Q}$, appelée *valeur absolue p-adique* et notée $|\cdot|_p$.

🎅 Démonstration

Assez claire.

🎁

Définition 3.

On définit sur $\mathbb{Q}$:

— La valeur absolue triviale[a] $|\cdot|_0 = \mathbb{1}_{\mathbb{Q}^*}$,

— La valeur absolue usuelle (ou infinie) $|\cdot|_\infty : x \mapsto \max\{x, -x\}$.

a. qu'on peut même définir sur tout corps

Fait du Jour 2.

Soit $|\cdot|$ une valeur absolue non triviale sur $\mathbb{Q}$. Alors on est dans l'un des cas (exclusifs) suivants :

(1) Il existe p premier et $b > 0$ tel que $|\cdot| = |\cdot|_p^b$,

(2) Il existe $\alpha \in]0, 1]$ tel que $|\cdot| = |\cdot|_\infty^\alpha$.

C'est le *théorème d'Ostrowski*[a].

a. avec un i

Démonstration

La disjonction de cas se fait selon s'il existe $n \in \mathbb{N}$ tel que $0 < |n| < 1$.
On n'étudie que la restriction à $\mathbb{N}$ de la valeur absolue car elle se prolonge de manière unique sur $\mathbb{Q}$ (en posant $|x| := |-x|$ si $x < 0$ est entier et $|\frac{a}{b}| = \frac{|a|}{|b|}$ si $a, b \in \mathbb{Z}\backslash\{0\}$).
On montre le lemme suivant :

S'il existe un nombre premier p tel que $|p| < 1$,

(i) Pour tout $b \in \mathbb{N}, |b| \leq 1$

(ii) Pour tout entier q premier avec $p, |q| = 1$.

(i) Soit $b \in \mathbb{N}$. Pour tout entier $k > 0$, on écrit $b^k = \sum_{i=0}^{h_k} b_{i,k} p^i$ (avec $0 \leq b_{i,k} < p$ et $b_{h_k,k} \neq 0$) en base p. Alors on obtient la majoration :

$$|b|^k = |b^k| \leq \sum_{i=0}^{h_k} |b_{i,k}||p|^i \leq (h_k + 1)M, \tag{†}$$

où $M = \max_{0 \leq l \leq p-1}(|l|)$. Or on a aussi

$$h_k \leq \frac{\ln(b^k)}{\ln(p)} < h_k + 1.$$

Posons $B := \frac{\ln(b)}{\ln(p)}$, de sorte que

$$|b| \leq M^{1/k}(Bk + 1)^{1/k},$$

d'où le résultat en passant à la limite en k.
(ii) Soit q premier avec p. Alors pour tout entier $n > 0$, p^n et q^n sont premiers entre eux, donc il existe u_n et v_n tels que :

$$u_n p^n + v_n q^n = 1.$$

Si on suppose que $|q| < 1$,

$$1 = |1| \leq |u_n p^n| + |v_n q^n| \overset{(i)}{\leq} |p|^n + |q|^n,$$

ce qui aboutit à une contradiction pour n assez grand.

(1) Supposons qu'il existe $n \in \mathbb{N}$ tel que $0 < |n| < 1$. Alors il existe un facteur premier p de n tel que $|p| < 1$. Alors en posant $b := -\frac{\ln(|p|)}{\ln(p)}$. Tout entier m s'écrit (de manière unique) $m = p^{v_p(m)} m'$, avec $p \nmid m'$. Donc $|m| = |p^{v_p(m)}||m'| = |p|^{v_p(m)} = |m|_p^b$.

(2) Supposons que pour tout entier $n, |n| \geq 1$. $|\cdot|$ est non triviale, donc il existe $a \in \mathbb{N}$ tel que $|a| > 1$. Posons $\alpha := \frac{\ln(|a|)}{\ln(a)}$. On a $0 < \alpha < 1$. En effet, avec l'inégalité triangulaire :

$$|a| \leq 1 + |a - 1| \leq \cdots \leq a.$$

On procède comme précédemment, avec cette fois-ci une majoration dans (†) par somme des termes d'une suite géométrique, ce qui nous donne en reprenant les notations, (avec p remplacé par a) :

$$|b| \leq M^{1/k} \left(\frac{|a|^{kB+1} - 1}{|a| - 1} \right)^{1/k},$$

d'où $|b| \leq |a|^B = b^\alpha$. Donc $\frac{\ln(|b|)}{\ln(b)} \leq \frac{\ln(|a|)}{\ln(a)} \leq \alpha$. En échangeant le rôle de a et b, si $|b| > 1$, alors $\frac{\ln(|b|)}{\ln(b)} = \alpha$.
Or tout entier $b > 1$ vérifie $|b| > 1$ (sinon, avec les calculs de (i), on aurait $|c| \leq 1$ pour tout entier c). Donc $|\cdot| = |\cdot|_\infty^\alpha$, ce qui assure le résultat.

Définition 4 (Nombres p-adiques).

On appelle *corps des nombres p-adiques*, et on note $\mathbb{Q}_p$, le complété de $\mathbb{Q}$ pour la valeur absolue $|\cdot|_p$.

Fait du Jour 3.

Pour tout $x \in \mathbb{Q}$,

$$|x|_\infty \prod_{p \text{ premier}} |x|_p = |x|_0.$$

C'est la *formule du produit*.

Démonstration

Pour 0, la formule est claire. Si $x \neq 0$ est un entier, on écrit sa décomposition en produit de premiers :

$$x = \prod_{p \text{ premier}} p^{v_p(x)}$$

qui assure le résultat en mettant les termes du même côté, et on étend la formule aux rationnels.

Définition 5 (Entiers p-adiques).

On appelle *anneau des entiers p-adiques* l'ensemble $\mathbb{Z}_p := \{x \in \mathbb{Q}_p, |x|_p \leq 1\}$.

Fait du Jour 4.

$(\mathbb{Z}_p, +, \times, |\cdot|_p)$ est un sous anneau topologique intègre et complet de $\mathbb{Q}_p$.

Démonstration

Tout est clair dans les propriétés de sous-anneau (on notera pour la stabilité par $+$ que l'on utilise le caractère ultramétrique de la valeur absolue sur $\mathbb{Z}_p$, par restriction de celle sur $\mathbb{Q}_p$). Si $|xy|_p = 0, |x|_p|y|_p = 0$, donc $|x|_p = 0$ ou $|y|_p = 0$ par intégrité de $\mathbb{Q}$, d'où $x = 0$ ou $y = 0$. $\mathbb{Z}_p$ est fermé dans un complet, donc est complet.

Fait du Jour 5.

(*i*) Les éléments inversibles de $\mathbb{Z}_p$ sont exactement $\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p, |x|_p = 1\}$.

(*ii*) $\mathbb{Z}_p$ est un anneau principal, et ses idéaux non nuls sont de la forme $p^k\mathbb{Z}_p, k \in \mathbb{N}$.

(*iii*) $\mathbb{Z}_p$ est un anneau local, d'unique idéal maximal $p\mathbb{Z}_p$.

Démonstration

(*i*) Soit $x \in \mathbb{Z}_p$ tel que $|x|_p = 1$. Alors $1 = |1|_p = |xx^{-1}|_p = |x|_p|x^{-1}|_p = |x|_p^{-1}$, donc $x^{-1} \in \mathbb{Z}_p$, donc $x \in \mathbb{Z}_p^\times$. Réciproquement, si $x \in \mathbb{Z}_p^\times$, $|x|_p^{-1} \leq 1, |x|_p \leq 1$ et $|x|_p^{-1}|x|_p = 1$ implique $|x|_p = 1$.

(*ii*) Remarquons déjà que l'image de $\mathbb{Q}_p$ par $|\cdot|_p$ est exactement l'ensemble $\{p^k, k \in \mathbb{Z}\}$: cela découle de la densité de $\mathbb{Q}$ dans $\mathbb{Q}_p$ et de la continuité de $|\cdot|_p$.
Soit I un idéal non nul de $\mathbb{Z}_p$. Alors l'ensemble $\{|x|_p, x \in I\}$ est inclus dans $\{p^{-k}, k \in \mathbb{N}\}$. Donc il existe $x_* \in I$ et $k_* \in \mathbb{N}$ tel que $|x_*|_p = p^{-k_*} = \max\{|x|_p, x \in I\}$. Montrons que $I = p^{k_*}\mathbb{Z}_p$.
Soit $x \in I$. On écrit $|x|_p = p^{-k}$ et $x' = xp^{-k_*}$. Alors $|x'|_p = p^{k_*-k} \leq 1$ car $k_* \leq k$ par définition. Donc $x = p^{k_*}x' \in p^{k_*}\mathbb{Z}_p$.
Réciproquement, notons $x = p^{-k_*}x_*$. Alors $|x|_p = 1$, donc x est inversible dans $\mathbb{Z}_p$, d'où $p^{k_*}\mathbb{Z}_p = x_*x^{-1}\mathbb{Z}_p = x_*\mathbb{Z}_p \subset I$.

(*iii*) $p\mathbb{Z}_p = \mathbb{Z}_p \setminus \mathbb{Z}_p^\times$ est idéal maximal de $\mathbb{Z}_p$, ce qui assure le dernier point.

Fait du Jour 6.

Soit $x \in \mathbb{Z}_p$.

Il existe une unique suite $(b_n)_{n\geq 0} \in [\![0, p-1]\!]^{\mathbb{N}}$ telle que $\sum_{n\geq 0} b_n p^n$ converge vers x.
Cette série est appelée *développement de Hensel* de x.

Démonstration

Il suffit de montrer qu'il existe une unique suite $(a_n)_{n\geq 0} \in \prod_{n\geq 0}[\![0, p^n - 1]\!]$, avec $a_n = a_{n-1} \pmod{p^{n-1}}$ pour $n \geq 2$, qui converge vers x. Il suffira d'écrire chaque a_n en base p pour obtenir les coefficients b_n (la condition de congruence garantit son existence et unicité).

Soit $n \geq 1$. Montrons l'existence d'un unique $a_n \in [\![0, p^n - 1]\!]$ tel que $|x - a_n|_p \leq p^{-n}$.
Déjà, $\mathbb{Q}$ étant dense dans $\mathbb{Q}_p$, il existe $a/b \in \mathbb{Q}$ tel que $\left|x - \frac{a}{b}\right|_p \leq p^{-n}$. Or $\left|\frac{a}{b}\right|_p \leq \max\{|x|_p, \left|x - \frac{a}{b}\right|_p\} \leq 1$, donc $p \nmid b$, donc il existe un entier $0 \leq b' \leq p^n - 1$ tel que $bb' = 1 \pmod{p^n}$. Alors on calcule $\left|\frac{a}{b} - ab'\right|_p \leq p^{-n}$, et si on note a_n le représentant de ab' dans $[\![0, p^n - 1]\!]$ modulo p^n, on a $|x - a_n|_p \leq p^{-n}$.
Pour l'unicité de a_n, l'inégalité $|a_n - a'_n|_p \leq p^{-n}$ pour un autre candidat a'_n permet de conclure.

Remarque .

En fait, l'anneau $\mathbb{Z}_p$ est isomorphe en tant qu'anneau topologique, à l'ensemble $[\![0, p-1]\!]^{\mathbb{N}}$ (donc des séries telles que décrites au dessus), muni des bonnes opérations, à savoir l'addition et la multiplication "avec retenues" (comme dans $\mathbb{Z}$, mais avec une infinité de termes à gauche), et de la valeur absolue définie comme p^{-N} où N est le plus petit entier pour laquelle $b_N \neq 0$. Pour les détails (calculatoires certes, mais c'est un des avantages de cette définition équivalente), voir [[Gir24], II - 2.].

Définition 6 (Système projectif).

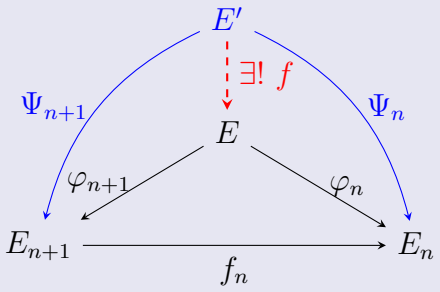
Soit $\mathscr{C}$ une catégorie.
On appelle *système projectif* de $\mathscr{C}$ toute famille $(E_n, f_n)_{n\in\mathbb{N}}$, avec E_n un objet de $\mathscr{C}$ et $f_n : E_{n+1} \to E_n$ un morphisme, pour tout $n \in \mathbb{N}$.

Définition 7 (Limite projective).

Soit $(E_n, f_n)_{n\in\mathbb{N}}$ un système projectif de $\mathscr{C}$.
On appelle *limite projective* de ce système tout objet E de $\mathscr{C}$ muni de morphismes $(\varphi_n : E \to E_n)_{n\in\mathbb{N}}$ vérifiant :

i) Pour tout $n \in \mathbb{N}$, $\varphi_n = f_n \circ \varphi_{n+1}$

ii) (Propriété universelle) Si $(E', (\psi_n)_{n\in\mathbb{N}})$ vérifie $\psi_n = f_n \circ \psi_{n+1}$ pour tout $n \in \mathbb{N}$, alors il existe un unique morphisme $f : E' \to E$ tel que : $\forall n \in \mathbb{N}$, $\psi_n = \varphi_n \circ f$.



Remarque .

Si elle existe, la limite projective est unique à isomorphisme près. On note alors avec les précédentes notations $(E, \varphi_n)_{n\in\mathbb{N}} = \varprojlim (E_n, f_n)_{n\in\mathbb{N}}$, ou encore $E = \varprojlim E_n$ si le contexte est clair.

Fait du Jour 7.

$\mathbb{Z}_p \simeq \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ (dans la catégorie des anneaux topologiques).

Démonstration

On se contentera de montrer le résultat dans la catégorie des ensembles (sachant que l'on a pas défini les opérations "avec retenues" pour la structure algébrique, et que l'on a pas assez développé la structure topologique non plus, mais c'est bien fait par exemple dans [[Gir24], III-3.] ou [[Rob00], 1.4.7]). Pour tout entier $n \geq 1$, on définit

$$\varphi_n : \begin{array}{ccc} \mathbb{Z}_p & \longrightarrow & \mathbb{Z}/p^n\mathbb{Z} \\ \sum_{k\geq 0} a_k p^k & \longmapsto & \sum_{k=0}^{n-1} a_k p^k \end{array} \quad \text{et} \quad f_n : \begin{array}{ccc} \mathbb{Z}/p^{n+1}\mathbb{Z} & \longrightarrow & \mathbb{Z}/p^n\mathbb{Z} \\ \sum_{k=0}^{n} a_k p^k & \longmapsto & \sum_{k=0}^{n-1} a_k p^k \end{array},$$

qui sont bien compatibles.
Il suffit maintenant de vérifier la propriété universelle. Soit un autre candidat $(X, (\psi_n)_{n\in\mathbb{N}})$. Soit $x \in X$. On définit les coefficients $a_n(x)$ par récurrence, en posant $a_0(x) = \psi_1(x)$ et pour tout $n \geq 1, a_n(x) = \frac{1}{p^n}(\psi_{n+1}(x) - \sum_{k=0}^{n-1} a_k(x)p^k)$, de sorte à ce que l'on ait bien $\psi_{n+1}(x) = \sum_{k=0}^{n} a_k(x)p^k = \varphi_{n+1}(f(x))$ si l'on pose $f(x) = \sum_{k\geq 0} a_k(x)p^k$. Ceci donne l'existence et l'unicité de $f : X \to \mathbb{Z}_p$ qui fait commuter le diagramme.

Remarque .

Nous avons alors à disposition 3 définitions équivalentes de $\mathbb{Z}_p$ (la première topologique, la deuxième calculatoire, la troisième algébrique), bénéficiant chacune de ses avantages et inconvénients.
On pourra explorer les références [Rob00], [Ami75] ou [Gou20] (notamment les premiers paragraphes) pour s'en convaincre.

Fait du Jour 8.

$\mathbb{Q}_p = \mathrm{Frac}(\mathbb{Z}_p)$

Démonstration

Si $x \in \mathbb{Q}_p$. On pose $x' = |x|_p x$, et comme au dessus, $x' \in \mathbb{Z}_p$, donc $x \in \frac{1}{p^{-v_p(x)}}\mathbb{Z}_p \subset \mathrm{Frac}(\mathbb{Z}_p)$. L'autre inclusion est claire car $\mathrm{Frac}(\mathbb{Z}_p)$ est le plus petit corps contenant $\mathbb{Z}_p$.

Remarque .

Avec les deux derniers faits, on peut alors écrire uniquement tout élément x de $\mathbb{Q}_p$ comme la somme d'une série $\sum_{n\geq N} b_n p^n$, avec $b_n \in [\![0, p-1]\!]$ et $N \in \mathbb{Z}$, donc comme un développement en base p avec une infinité de termes avant la virgule, et un nombre fini avant, à l'inverse du développement en base p pour les nombres réels.
Une deuxième différence est l'unicité d'un tel développement qui n'est plus vérifiée dans le cas réel (on se souvient par exemple que $0,222\cdots = 1$ en base 3).

Fait du Jour 9.

Soit $x = \sum_{n\geq N} b_n p^n \in \mathbb{Q}_p$.
Alors x est rationnel si, et seulement si la suite $(b_n)_{n\geq N}$ est périodique à partir d'un certain rang.

Démonstration

Nécessité : Il existe un entier $k \geq 1$ et $n_* \in \mathbb{Z}$ tels que pour tout $n \geq N, a_{n+k} = a_n$. On a : $x = \sum_{n=N}^{n_*-1} b_n p^n + \sum_{n=n_*}^{\infty} b_n p^n$, et

$$\sum_{n=n_*}^{\infty} b_n p^n = \sum_{n=0}^{k-1} b_{n_*+n} p n_* + n + \sum_{n=0}^{k-1} b_{n_*+n+k} p^{n_*+n+k} + \cdots = \sum_{n=0}^{k-1}\sum_{j=0}^{\infty} \overbrace{b_{n_*+n+kj}}^{=b_{n_*+n}} p^{n_*+n+kj} =$$
$$\sum_{n=0}^{k-1} b_{n_*+n} p^{n_*+n} \sum_{j=0}^{\infty} p^{kj} = \sum_{n=0}^{k-1} b_{n_*+n} p^{n_*+n} \frac{1}{1-p^k} \in \mathbb{Q},$$

la dernière égalité en reconnaissant une somme géométrique car $|p^k|_p < 1$ (oui oui). Donc $x \in \mathbb{Q}$.
Suffisance : Si $x = 0$, le résultat est assez clair. Sinon, il existe des entiers r, a, b tels que $p \nmid b$ et $x = p^r \frac{a}{b}$.
$p \nmid b$ donc $\langle p \rangle = \mathbb{Z}/b\mathbb{Z}$, donc il existe s tel que $p^s = 1 \pmod b$, d'où $\frac{a}{b} = \frac{a'}{p^s-1}$ pour un entier a'.
Si $a' > 0$, en posant $k = v_p(a') + 1$, on a $0 < a' < p^k$. De plus, sachant que p^k et $p^s - 1$ sont premiers entre eux, le théorème de Bézout nous donne l'existence de deux entiers α, β vérifiant :

$$a' = \beta(p^s - 1) - \alpha p^k, \ 0 \leq \alpha \leq p^s - 2, \ 0 < \beta \leq p^k - 1.$$

On peut donc écrire ces entiers en base p :

$$\alpha = \sum_{j=0}^{s-1} \alpha p^j, \ \beta = \sum_{j=0}^{k-1} \beta_j p^j.$$

Donc :

$$\frac{a}{b} = \beta + \frac{\alpha p^k}{1-p^s} = \sum_{j=0}^{k-1} \beta_j p^j + \left(\sum_{j=0}^{s-1} \alpha p^l\right)\left(\sum_{i=0}^{\infty} p^{is+k}\right),$$

donc le développement est bien périodique à partir d'un certain rang, et il en est de même pour celui de x.
Enfin, si $a' < 0$, on écrit $a' = (-1) \times (-a')$, et en se rappelant que $-1 = \sum_{j=0}^{\infty}(p-1)p^j$, on retrouve un développement périodique pour x.

Fait du Jour 10.

Soient p et q deux nombres premiers.

1) Si $\mathbb{Z}_p$ et $\mathbb{Z}_q$ sont isomorphes en tant qu'anneaux, alors $p = q$.
2) Si $\mathbb{Z}_p$ et $\mathbb{Z}_q$ sont isomorphes en tant que groupes topologiques, alors $p = q$.

Démonstration

1) Notons $\varphi : \mathbb{Z}_p \xrightarrow{\sim} \mathbb{Z}_q$ un tel isomorphisme d'anneaux. On note $\pi : \mathbb{Z}_q \twoheadrightarrow \mathbb{Z}_q/q\mathbb{Z}_q$ la projection canonique. Alors on a $\mathrm{Ker}(\pi \circ \varphi) = \varphi^{-1}\mathrm{Ker}(\pi) = \varphi^{-1}(q\mathbb{Z}_q) = p\mathbb{Z}_p$ (un idéal maximal est envoyé sur un autre idéal maximal). Par passage au quotient, on obtient un isomorphisme $\overline{\varphi} : \mathbb{Z}_p/p\mathbb{Z}_p \xrightarrow{\sim} \mathbb{Z}_q/q\mathbb{Z}_q$. Or la projection :

$$\begin{array}{rccc} p_n : & \mathbb{Z}_p & \longrightarrow & \mathbb{Z}/p^n\mathbb{Z} \\ & \sum_{k\geq 0} a_k p^k & \longmapsto & \sum_{k=0}^{n-1} a_k p^k \end{array}$$

nous donne par passage au quotient un isomorphisme $\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$, donc en particulier on a par cardinalité via $\overline{\varphi}, p = q$.

2) Notons $\psi : \mathbb{Z}_p \xrightarrow{\sim} \mathbb{Z}_q$ un tel isomorphisme de groupes topologiques. Par ce qui est écrit avant, $[\mathbb{Z}_p : p\mathbb{Z}_p] = p$, donc on a aussi $[\mathbb{Z}_q : \psi(p\mathbb{Z}_p)]$. Montrons que $\mathbb{Z}_q/\psi(p\mathbb{Z}_p)$ est cyclique (on aura alors le résultat sachant que p et q sont premiers entre eux).
$p\mathbb{Z}_p$ est ouvert, donc il en est de même de $\psi(p\mathbb{Z}_p)$. Comme $(q^k\mathbb{Z}_q)_{k\geq 0}$ est une base de voisinages ouverts de 0 dans $\mathbb{Z}_q$, il existe un entier k_* tel que $q^{k_*}\mathbb{Z}_q \subset \psi(p\mathbb{Z}_p)$ en est un sous groupe. Donc on a un morphisme surjectif $s : \mathbb{Z}_q/q^{k_*}\mathbb{Z}_q \simeq \mathbb{Z}/q^{k_*}\mathbb{Z} \twoheadrightarrow \mathbb{Z}_q/\psi(p\mathbb{Z}_p)$ (le premier isomorphisme vient de la remarque dans 1)). En passant au quotient, sachant qu'un sous groupe de $\mathbb{Z}/q^{k_*}\mathbb{Z}$ est de la forme $\mathbb{Z}/q^j\mathbb{Z}$, on a : $\mathbb{Z}_q/\psi(p\mathbb{Z}_p) \simeq \mathbb{Z}/p^{k_*+j}\mathbb{Z}$, ce qui conclut.

Définition 8.

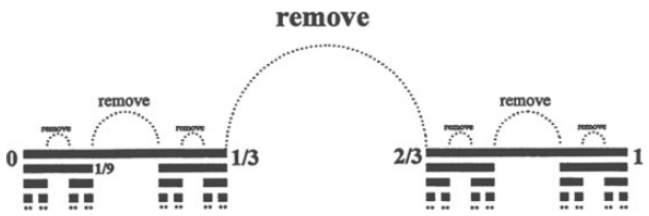
On appelle *p-ième ensemble de Cantor*, et on note C_p, le sous ensemble de $[0,1]$ des nombres n'ayant que des nombres pairs dans leur développement en base $2p-1$, *ie*

$$C_p = \left\{ \sum_{k=1}^{\infty} \frac{2a_k}{(2p-1)^k}, 0 \leq a_k \leq p-1 \right\}.$$

On le munit de la topologie euclidienne induite.

Remarque .

On peut voir les ensembles de Cantor comme le résultat d'un processus itératif dans lequel, $[0,1]$ est découpé en $2p-1$ morceaux de même longueur, et desquels on ne garde que les numéros pairs, puis on réitère sur chaque morceau restant et ainsi de suite.
Ci-dessous une illustration de C_2, tiré de [Rob00], p.8.



The Cantor set

Fait du Jour 11.

$\mathbb{Z}_p$ est homéomorphe à C_2.
En particulier, tous les $\mathbb{Z}_p$ sont homéomorphes.

Démonstration

En fait, il est facile de montrer que tout $\mathbb{Z}_p$ est homéomorphes à C_p par l'application :

$$\begin{array}{rccc} \chi_p : & \mathbb{Z}_p & \longrightarrow & C_p \\ & \sum_{n=0}^{\infty} a_n p^n & \longmapsto & \sum_{n=0}^{\infty} \frac{2a_n}{(2p-1)^{n+1}} \end{array} .$$

Ensuite, un théorème de Brouwer (dont on trouvera une démonstration par exemple dans [Fra11]) nous affirme que tout espace est homéomorphe à C_2 si, et seulement s'il est non vide, métrisable, compact, totalement discontinu (*ie* chaque singleton est une composante connexe) et parfait (*ie* aucun singleton n'est ouvert).
Il suffit de montrer que tout C_p vérifie ces propriétés. Il est non vide, métrique (induite par celle sur $[0,1]$), compact (car fermé borné).
Si deux points $a < b$ de C_p ont coefficients respectifs (dans l'écriture comme dans la définition) (a_n) et (b_n), alors en notant $N = \min\{k \in \mathbb{N}, a_k \neq b_k\}$ et $c_n = a_n$ si $n \neq N$, $c_N = (a_N + b_N)/2$, le nombre c ainsi défini vérifie $a < c < b$ et $c \notin C_p$, donc $a \in [0,c] \cap C_p$ et $b \in [c,1] \cap C_p$, qui sont deux fermés, ce qui assure la totale discontinuité. Enfin, on se convainc facilement que

tout point a de C_p est limite d'une suite d'élément de $C_p \setminus \{a\}$, donc que l'espace est parfait. On aurait aussi pu prouver ces résultats directement sur $\mathbb{Z}_p$, mais peut être une représentation linéaire aide à comprendre les propriétés.

Remarque .

Il existe d'autres représentations des $\mathbb{Z}_p$ plus "naturelle" avec p. On en trouvera (avec de belles illustrations !) dans [Rob00], §1.2.

Fait du Jour 12.

i) Tout triangle de $\mathbb{Q}_p$ est isocèle,

ii) Tout point d'une boule de $\mathbb{Q}_p$ en est son centre,

iii) Deux boules de $\mathbb{Q}_p$ sont ou bien disjointes, ou bien comparables,

iv) Toute boule ouverte de $\mathbb{Q}_p$ est fermée, et réciproquement.

Démonstration

On aura besoin d'un résultat préliminaire : si $(x, y, z) \in \mathbb{Q}_p^3$ sont tels que $d(x, y) \neq d(y, z)$, alors $d(x, z) = \max(d(x, y), d(y, z))$. En effet, on peut supposer $d(x, y) < d(y, z)$, et alors :

$$d(x, z) \leq \max(d(x, y), d(y, z)) = d(y, z) \text{ et } d(y, z) \leq \max(d(y, x), d(x, z)) = d(x, z),$$

donc $d(x, z) = d(y, z) = \max(d(x, y), d(y, z))$.

i) Clair d'après ce qui vient d'être montré.

ii) Soient $x \in \mathbb{Q}_p$ et $r > 0$. On note $\mathbb{B}(x, r) := \{y \in \mathbb{Q}_p, d(x, y) < r\}$ la boule ouverte de centre x et de rayon r. Soient $y, z \in \mathbb{B}(x, r)$. Alors :

$$d(y, z) \leq \max(d(y, x), d(x, z)) < r,$$

donc $\mathbb{B}(x, r) \subseteq \mathbb{B}(y, r)$ et l'autre inclusion est semblable, donc y est bien un centre de $\mathbb{B}(x, r)$.

iii) Soient $x, y \in \mathbb{Q}_p$ et $r, r' > 0$ tels que $\mathbb{B}(x, r) \cap \mathbb{B}(y, r') \neq 0$. Alors il existe un point commun z aux deux boules. D'après *ii)*, c'est un centre de chacune d'elles, donc l'une est incluse dans l'autre (en fonction de si $r > r'$ ou $r \leq r'$).

iv) Soit $\mathbb{B}$ une boule ouverte de rayon r. Alors $\mathbb{B}^c = \bigcup_{x \in \mathbb{B}^c} \mathbb{B}(x, r)$ d'après *iii)*, donc $\mathbb{B}^c$ est ouvert, donc $\mathbb{B}$ est fermée.

Remarque .

Ces propriétés sont vraies dans tout corps ultramétrique.

Fait du Jour 13.

i) $\mathbb{Z}_p$ est compact,

ii) $\mathbb{Q}_p$ est localement compact,

iii) Si V est un $\mathbb{Q}_p$-espace vectoriel normé, alors V est localement borné si, et seulement si, V est de dimension finie (sur $\mathbb{Q}_p$).

Démonstration

i) C_2 est compact, donc par un fait précédent, $\mathbb{Z}_p$ l'est.

ii) Une boule fermée centrée en un point est homéomorphe à $\mathbb{Z}_p$.

iii) Si V est de dimension finie n, il est isomorphe à $\mathbb{Q}_p^n$, et cet isomorphisme est un homéomorphisme, donc V est localement borné. Réciproquement, soit K un voisinage compact de 0. Notons que $V = \bigcup_{x\in V}(x + pK)$, et comme K est compact, il existe $a_1, \dots, a_m$ tels que $K \subset \bigcup_{i=1}^m (a_i + pK)$. Notons $L = \mathrm{Vect}(a_1, \dots, a_m)$. C'est un sous espace vectoriel de V, donc est fermé, et le quotient V/L est séparé. L'image A de K dans ce quotient est toujours un voisinage compact de 0, et $A \subset pA$, d'où pour tout entier $n, p^{-n}A \subset A$. On a donc les inclusions $A \subset V/L \subset \bigcup_{n\in\mathbb{N}} p^{-n}A \subset A$ (car $|p^{-n}|_p \to \infty$), donc V/L est compact, donc $V/L = 0$ et $V = L$ est de dimension finie.

Fait du Jour 14.

1) Notons $\overline{\mathbb{Q}}_p$ la clotûre algébrique de $\mathbb{Q}_p$. Alors il existe une unique valeur absolue sur $\overline{\mathbb{Q}}_p$ qui prolonge celle de $\mathbb{Q}_p$.
2) La complétion $\mathbb{C}_p$ de $\overline{\mathbb{Q}}_p$ pour cette valeur absolue est algébriquement close.

Démonstration

1) Montrons d'abord que la valeur absolue se prolonge de manière unique à toute extension algébrique finie de $\mathbb{Q}_p$:

   Soit $\mathbb{L}$ une extension finie de $\mathbb{Q}_p$, de degré $d = [\mathbb{L}, \mathbb{Q}_p]$. Alors il existe une unique valeur absolue $|\cdot|$ sur $\mathbb{L}$ telle que $|\cdot| = |\cdot|_p$ sur $\mathbb{Q}_p$. De plus,

   $$\forall a \in \mathbb{L}, |a| = |N_{\mathbb{L}/\mathbb{Q}_p}(a)|_p^{1/d},$$

   où $N_{\mathbb{L}/\mathbb{Q}_p}(a)$ est la norme de a dans l'extension $\mathbb{L}/\mathbb{Q}_p$, c'est à dire le déterminant de l'endomorphisme de $\mathbb{L}$ (vu comme $\mathbb{Q}_p$-espace vectoriel) $\varphi_a : x \mapsto ax$.

   Vérifions que la formule ci-dessus définit bien une valeur absolue.

   (VA1) $|0| = |N_{\mathbb{L}/\mathbb{Q}_p}(0)|_p^{1/d} = 0$,

   (VA2) Soient $a, b \in \mathbb{L}$. On a (en écrivant simplement la définition) $\varphi_{ab} = \varphi_a \circ \varphi_b$ et le déterminant est un morphisme, donc $|ab| = |N_{\mathbb{L}/\mathbb{Q}_p}(ab)|_p^{1/d} = |N_{\mathbb{L}/\mathbb{Q}_p}(a)N_{\mathbb{L}/\mathbb{Q}_p}(b)|_p^{1/d} = |a||b|$,

(VA3) Soit $a \in \mathbb{L}$. Quitte à utiliser la multiplicativité, il suffit de montrer que si $|1+a| \leq \max(1,|a|)$, autrement dit, si $|a| \leq 1$, alors $|1+a| \leq 1$.
Soit $f(X) = X^r + \cdots + a_0$ le polynôme minimal de a sur $\mathbb{Q}_p$. On peut montrer 🎀 avec un peu l'algèbre linéaire que $N_{\mathbb{L}/\mathbb{Q}_p}(a) = ((-1)^r a_0)^{d/r}$. Donc, sachant $|N_{\mathbb{L}/\mathbb{Q}_p}(a)|_p \leq 1, |a_0|_p \leq 1$, donc $a_0 \in \mathbb{Z}_p$. Or f est irréductible et unitaire, donc on peut montrer 🎀 que $f \in \mathbb{Z}_p[X]$. Or le polynôme minimal de $1+a$ est $f(X-1)$, donc $N_{\mathbb{L}/\mathbb{Q}_p}(1+a) = ((-1)^r f(-1))^{d/r} \in \mathbb{Z}_p$, ce qui assure $|1+a| \leq 1$ et le résultat.

Pour l'unicité, si une autre valeur absolue $|\cdot|'$ sur $\mathbb{L}$ vérifie la même propriété, alors on peut montrer 🎀, car l'on est en dimension finie, qu'elle est équivalente à $|\cdot|$, donc qu'elle en est une puissance 🎀. En évaluant sur un élément de $\mathbb{Q}_p$ de norme distincte de 0 et 1, on trouve qu'elles sont en fait égales.

Montrons ensuite que la valeur de $|x|$ pour $x \in \overline{\mathbb{Q}}_p$ ne dépend pas de l'extension (finie) $\mathbb{L}$ dans laquelle l'on consière x, par exemple que :

$$|N_{\mathbb{L}/\mathbb{Q}_p}(x)|^{1/[\mathbb{L}:\mathbb{Q}_p]} = |N_{\mathbb{Q}_p(x)/\mathbb{Q}_p}(x)|^{1/[\mathbb{Q}_p(x):\mathbb{Q}_p]},$$

pour toute extension finie $\mathbb{L}$, ce qui est vrai d'après le théorème de la base téléscopique et la formule $N_{\mathbb{L}/\mathbb{Q}_p}(x) = ((-1)^{[\mathbb{Q}_p(x):\mathbb{Q}_p]} f(0))^{[\mathbb{L}:\mathbb{Q}_p]/[\mathbb{Q}_p(x):\mathbb{Q}_p]}$ pour f le polynôme minimal de x sur $\mathbb{L}$.

2) Soit $f = X^n + \sum_{i=0}^{n-1} a_i X^i$ un polynôme à coefficients dans $\mathbb{C}_p$. Or, $\overline{\mathbb{Q}}_p$ est dense dans $\mathbb{C}_p$, donc pour tout entier $0 \leq i \leq n-1$, il existe des coefficients $(a_{i,j})_{j\geq 0}$ de $\overline{\mathbb{Q}}_p$ tels que pour tout indice i et tout entier j assez grand, $|a_{i,j} - a_i| < \min(|a_i|, \frac{1}{j})$. Par inégalité ultramétrique, on a déjà $|a_{i,j}| = |a_i|$. Nous noterons pour tout entier j,

$$f_j = X^n + \sum_{i=0}^{n-1} a_{i,j} X^i.$$

Ces polynômes sont à coefficients dans $\overline{\mathbb{Q}}_p$, donc il existe une racine x_j à f_j dans $\overline{\mathbb{Q}}_p$ pour tout j. On voudrait trouver, à partir de la suite x_j et d'une *potentielle limite*, une racine à f dans $\mathbb{C}_p$.
Regardons d'abord le contrôle qu'impose les coefficients de f sur les x_j.
Notons que de $f_j(x_j) = 0$, on a l'inégalité

$$|x_j^n| = \left|\sum_{i=0}^{n-1} a_{i,j} x_j^i\right| \leq \max_{0\leq i\leq n-1} |a_{i,j}||x_j^i| = \max_{0\leq i\leq n-1} |a_i||x_j|^i.$$

Pour tout entier j, notons i_j un indice qui réalise ce maximum. Alors $|x_j| \leq |a_{i_j}|^{\frac{1}{n-i_j}}$, donc en notant $C := \max_{0\leq i\leq n-1} |a_i|^{\frac{1}{n-i}}$, on a

$$|x_j| \leq C.$$

Ensuite, on peut regarder la « taille » de la valeur que prend f en la suite x_j :

$$|f(x_j)| = |f(x_j) - f_j(x_j)| = \left|\sum_{i=0}^{n-1}(a_i - a_{i,j})x_j^i\right| \leq \max_{0\leq i\leq n-1}|a_i - a_{i,j}||x_j|^i \leq$$
$$\max_{0\leq i\leq n-1}|a_i - a_{i,j}|\max(1, C^{n-1}) \leq \frac{\max(1, C^{n-1})}{j}$$

par construction des $a_{i,j}$. Ainsi, la suite $(f(x_j))_{j\geq 0}$ converge vers 0.
Enfin, notons $(\alpha_i)_{1\leq i\leq n}$ les racines de f dans un corps de décomposition $\mathbb{C}_p \subset \mathbb{L}$. Alors l'égalité au dessus se réécrie :

$$\lim_{j\to\infty}\prod_{i=1}^{n}(x_j - \alpha_i) = 0.$$

Donc il existe un indice k tel que la suite $(x_j - \alpha_k)_{j\geq 0}$ admette une sous suite d'extractrice φ qui converge vers 0. En particulier, $(x_{\varphi(j)})_{j\geq 0}$ est de Cauchy dans $\mathbb{C}_p$ donc converge dans $\mathbb{C}_p$ par complétude, vers α_k, qui est une racine de f, ce qui achève la démonstration.
On trouvera les détails dans l'annexe A de [Jun25].

Remarque .

Là aussi, le résultat est vrai pour tout corps ultramétrique (avec la même démonstration). J'ai d'ailleurs "copié" la preuve du cas général, peut être est-il possible de faire plus simple dans le cas particulier de $\mathbb{Q}_p$.

Définition 9.

On appelle *corps des nombres complexes p-adiques*, et on note $\mathbb{C}_p$, la complétion de la clotûre algébrique de $\mathbb{Q}_p$. Nous noterons encore $|\cdot|_p$ la valeur absolue sur ce corps.

Fait du Jour 15.

Soit $(a_n)_{n\geq 0}$ une suite d'éléments de $\mathbb{C}_p$ ou $\mathbb{Q}_p$ [a].
Alors la série $\sum_{n\geq 0} a_n$ est convergente si, et seulement si, $(a_n)_{n\geq 0}$ converge vers 0.

a. ou tout corps ultramétrique complet

Démonstration

En fait, nous allons montrer que dans nos hypothèses, une suite $(u_n)_{n\geq 0}$ est de Cauchy si, et seulement si $|u_{n+1} - u_n|_p \to 0$, le lien suite-série (et la complétude) nous donnera le résultat. Le sens direct est clair. Réciproquement, soit $\varepsilon > 0$. Il existe $N \in \mathbb{N}$ tel que pour tout entier et $n > N$, $|u_n - u_{n+1}|_p < \varepsilon$. Soient m et n des entiers tels que $m > n > N$. Alors :

$$|u_m - u_n|_p \leq \max(|u_m - u_{m+1}|_p, |u_{m+1} - u_n|_p) \leq \cdots \leq \max_{n\leq k\leq m-1}(|u_k - u_{k+1}|_p) \leq \varepsilon.$$

Donc $(u_n)_{n\in\mathbb{N}}$ est de Cauchy.

Fait du Jour 16.

$\mathbb{C}$ et $\mathbb{C}_p$ sont isomorphes (en tant que corps).

Démonstration

Voir [Rob00], III.3.5.

Fait du Jour 17.

Soit $P \in \mathbb{Z}_p[X]$. Soit $x_* \in \mathbb{Z}_p$ tel que $P(x_*) = 0 \pmod{p^n}$ et $k := -\log_p(|P'(x_*)|_p) < n/2$.
Alors il existe un unique $x \in \mathbb{Z}_p$ tel que $P(x) = 0, x = x_* \pmod{p^{n-k}}$ et $|P'(x)|_p = |P'(x_*)|_p$.
C'est le *lemme de Hensel*.

Remarque .

Le cas $n = 1$ est déjà très intéressant, c'est celui qu'on retrouve le plus dans la littérature.

Démonstration

Existence : Nous construisons une suite dans l'idée de l'algorithme de Newton, qui approximera de mieux en mieux la solution.
Commençons par préciser cet algorithme de Newton : dans les conditions de l'énoncé, si on note $\hat{x} = x_* - \frac{P(x_*)}{P'(x_*)}$, alors :

1) $P(\hat{x}) = 0 \pmod{p^{n+1}}$
2) $\hat{x} = x_* \pmod{p^{n-k}}$
3) $|P'(\hat{x})|_p = |P'(x_*)|_p$.

Ce sont des vérifications, en utilisant notamment un développement de Taylor (voir [Rob00], I.6.4 pour les détails).
La suite définie par $x_0 = x_*$ et $x_{j+1} = \hat{x_j}$ est donc une suite de Cauchy d'éléments de $\mathbb{Z}_p$, qui converge vers une racine de P, avec les conditions requises.
Unicité : Si $y \in \mathbb{Z}_p$ vérifie les mêmes conditions, on a $x = y \pmod{p^{n-k}}$, donc avec $n > 2k, x = y \pmod{p^{k+1}}$ (†).
En développant avec la formule de Taylor :

$$P(x) = P(y) + P'(y)(x-y) + (x-y)^2 A, A \in \mathbb{Z}_p$$

Or x et y sont deux racines, donc $(x-y)(P'(y) + (x-y)A) = 0$. De plus, $|P'(y)|_p = p^{-k}$ et $|(x-y)A|_p \geq p^{-k-1}$ via (†), donc $(P'(y) + (x-y)A) \neq 0$, d'où $x = y$.

Définition 10 (Valuation).

Soient $\mathbb{K}$ une extension finie de $\mathbb{Q}_p$ de degré n et $\alpha \in \mathbb{K}$.
On appelle *valuation* de α le nombre $v_p(\alpha) := -\log_p(|\alpha|) = -\frac{1}{n}\log_p(|N_{\mathbb{K}/\mathbb{Q}_p}(\alpha)|_p)$.

Définition 11.

Soit $\mathbb{K}$ une extension finie de $\mathbb{Q}_p$ de degré n.
On appelle *indice de ramification* de $\mathbb{K}$ sur $\mathbb{Q}_p$ l'entier e vérifiant : $v_p(\mathbb{K}) = \frac{1}{e}\mathbb{Z}$.
Si $e = 1$, on dit que l'extension est *sans ramification*. Si $e = n$, on dit que l'extension est *totalement ramifiée*.

Remarque .

Cette définition est bien valide, car $v_p(\mathbb{K})$ est un sous groupe additif de $\frac{1}{n}\mathbb{Z}$, donc de la forme décrite.

Définition 12.

Soit $\mathbb{K}$ une extension finie de $\mathbb{Q}_p$ de degré n.
On appelle *anneau des entiers de* $\mathbb{K}$ et on note $\mathscr{O}_\mathbb{K}$ l'anneau $\{x \in \mathbb{K}, |x|_p \leq 1\}$, et *corps résiduel de* $\mathbb{K}$ le quotient $k_\mathbb{K} = \mathscr{O}_\mathbb{K}/\mathfrak{m}_\mathbb{K}$, où $\mathfrak{m}_\mathbb{K} = \{x \in \mathbb{K}, |x|_p < 1\}$.

Remarque .

On vérifiera que $\mathfrak{m}_\mathbb{K}$ est bien idéal maximal (c'est même le seul) de $\mathscr{O}_\mathbb{K}$.
On peut aussi vérifier que $k_\mathbb{K}$ est une extension finie de $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. En effet, $\mathscr{O}_\mathbb{K} \cap \mathbb{Z}_p = p\mathbb{Z}_p$, donc $\mathbb{F}_p \simeq \mathbb{Z}_p/p\mathbb{Z}_p \subset k_\mathbb{K}$. De plus, si $a_1, \dots, a_{n+1} \in k_\mathbb{K}$, il existe $b_1, \dots, b_{n+1} \in \mathbb{Q}_p$ non tous nuls tels que $(\dagger) : a_1b_1 + \cdots + a_{n+1}b_{n+1} = 0$ (car le degré de l'extension est exactement n). Il existe alors $m \in \mathbb{Z}$ tel que pour tout i, $p^m b_i \in \mathbb{Z}_p$ et pour au moins un $j, p^m b_j \notin p\mathbb{Z}_p$. En projetant $(\dagger)$ dans $k_\mathbb{K}$ (donc les b_i dans $\mathbb{F}_p$), on trouve une relation de liaison entre les $\overline{a_i}$, non triviale car $\overline{p^m b_j} \neq 0$, d'où $[k_\mathbb{K} : \mathbb{F}_p] \leq n = [\mathbb{K} : \mathbb{Q}_p]$.

Fait du Jour 18.

Soit $\mathbb{K}$ une extension finie de $\mathbb{Q}_p$ de degré n. On note $f = [k_\mathbb{K} : \mathbb{F}_p]$ et e l'indice de ramification de $\mathbb{K}$ dans $\mathbb{Q}_p$.
Alors $n = ef$.

Démonstration

Voir [Rob00], p.99.

Définition 13.

On appelle polynôme d'Eisenstein tout polynôme $X^r + a_{r-1}X^{r-1} + \cdots + a_0$ à coefficients dans $\mathbb{Z}_p$, avec $p|a_i$ pour tout i, et $p^2 \nmid a_0$.

Fait du Jour 19.

— Soit $\mathbb{K}$ une extension finie de $\mathbb{Q}_p$ de degré n, de degré de ramification e. Si $\mathbb{K}$ est totalement ramifié, et $\pi \in \mathbb{K}$ vérifie $v_p(\pi) = \frac{1}{e}$, alors π est racine d'un polynôme d'Eisenstein de degré

e. Réciproquement, si α est une racine d'un tel polynôme, alors $\mathbb{Q}_p(\alpha)$ est totalement ramifiée de degré e.

— Soit un entier $f > 0$. Il existe une unique extension non ramifiée $\mathbb{K}_f^{\text{unram}}$ de degré f de $\mathbb{Q}_p$, obtenue en adjoingnant une racine primitive $(p^f - 1)$-ième de l'unité. De plus, si $\mathbb{K}$ est une extension de $\mathbb{Q}_p$ de degré n, d'indice de ramification e et de degré résiduel f, alors il existe π racine d'un polynôme d'Eisenstein à coefficients dans $\mathbb{K}_f^{\text{unram}}$, tel que $\mathbb{K} = \mathbb{K}_f^{\text{unram}}(\pi)$.

Démonstration

Voir [Rob00], II.3, III.1.

Définition 14 (Séries exponentielle et logarithmique p-adiques).

— On appelle *série exponentielle p-adique* la série formelle $\exp_p(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!} \in \mathbb{Q}_p[[X]]$.

— On appelle *série logarithmique p-adique* la série formelle $\log_p(1+X) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} X^n \in \mathbb{Q}_p[[X]]$.

Fait du Jour 20.

Le rayon de convergence de $\exp_p$ est $p^{\frac{-1}{p-1}}$ et celui de $\log_p$ est 1. De plus, ce sont des isomorphismes réciproques l'un de l'autre entre le disque ouvert [a] $D(0, p^{\frac{-1}{p-1}})$ (multiplicativement) et $D(0,1)$ (additivement).

a. on notera qu'en ultramétrique, les disques sont tous ouverts et fermés à la fois, nous parlons donc bien ici de $D(0,r) = \{x \in \mathbb{C}_p, |x|_p < r\}$.

Démonstration

On rappelle la formule d'Hadamard : le rayon de convergence d'une série entière $\sum_{k\geq 0} a_k X^k$ est $\rho = \frac{1}{\limsup |a_k|_p^{1/k}}$.
On peut en déduire facilement le rayon de convergence de $\log_p$, et pour $\exp_p$, on applique la formule de Legendre : $v_p(n!) = \sum_{k=0}^{\infty} \lfloor \frac{n}{p^k} \rfloor$ (c'est une somme finie).
Ensuite, on peut calculer formellement que $\exp_p \circ \log_p(1+X) = 1+X$ et $\log_p \circ \exp_p(X) = X$.
Ce qui est plus délicat à montrer est que $\exp_p$ est bien à valeurs dans $D(0,1)$ et $\log_p$ dans $D(0, p^{\frac{-1}{p-1}})$ (par des calculs de valuation p-adique principalement).
On trouvera les détails par exemple dans [[Kob77], p.80].

Fait du Jour 21.

— Si $p > 2$, il existe exactement 3 extensions quadratiques (non isomorphes) de $\mathbb{Q}_p$: $\mathbb{Q}_p(\sqrt{p}), \mathbb{Q}_p(\sqrt{u})$ et $\mathbb{Q}_p(\sqrt{pu})$, où u n'est pas un carré modulo p.

— Si $p = 2$, il en existe 7 : $\mathbb{Q}_p(\sqrt{-1}), \mathbb{Q}_p(\sqrt{\pm 5}), \mathbb{Q}_p(\sqrt{\pm 2})$ et $\mathbb{Q}_p(\sqrt{\pm 10})$.

Démonstration

Voir [Deb67], ou [[Lee], p.6].

Fait du Jour 22.

Il existe une unique extension de $\log_p$ à $\mathbb{C}_p^\times$ vérifiant $\log_p(xy) = \log_p(x) + \log_p(y)$ pour tout $x, y \in \mathbb{C}_p^\times$, et $\log_p(p) = 0$.
C'est un résultat dû à *Iwasawa*.

Démonstration

Voir [Mar67b], ou [[Mur02], Théorème 4.7].

Fait du Jour 23.

Soit $(a_k)_{k\geq 0} \in \mathbb{Z}_p^{\mathbb{N}}$ une suite d'entiers p-adiques bornée. Supposons que pour tout entier $m \in \mathbb{N}$, il existe $N_m \in \mathbb{N}$ tel que :

$$\forall (k, k') \in \mathbb{N}^2, (k = k' \pmod{p^{N_m}}) \Rightarrow (a_k = a_{k'} \pmod{p^m}).$$

Alors il existe une fonction continue $f : \mathbb{Z}_p \to \mathbb{Z}_p$ telle que, pour tout $k \in \mathbb{N}$, $f(k) = a_k$.
C'est un début de la *théorie d'interpolation p-adique*.

Démonstration

Voir [Mur02], Theorème 5.0.

Fait du Jour 24.

L'identité est le seul automorphisme de corps de $\mathbb{Q}_p$.

Démonstration

Voir [Rob00], p.53.

Fait du Jour 25.

Joyeux Noël !

Démonstration

Clair si vous fêtez Noël bien entouré.e, sinon, je vous souhaite quand même une bonne journée !

Remarque (Remerciements).

Je remercie mon camarade de Rennes qui se reconnaîtra l'idée du calendrier de l'Avent (il avait fait l'année dernière la même chose version $\mathrm{GL}_n(\mathbb{K})$), et aux quelques personnes qui ont lu et relu le document !

Remarque .

Il reste beaucoup de choses à dire sur les p-adiques, et je n'ai quasiment rien dit sur leurs applications, alors qu'ils sont fondamentaux dans beaucoup de branches de géométrie algébrique/arithmétique modernes (par exemple dans le principe local/global dont le théorème de Hasse-Minkowski donne une idée convaincante), et pourraient aussi permettre la démonstration de la conjecture de Riemann dans le cadre du programme de Langlands (ou un truc comme ça, j'y comprends rien).

Remarque .

Enfin, merci d'avoir participer à ce projet ! Il reste ouvert à modifications et améliorations, j'essaierai de le mettre accessible en ligne, avec un moyen de me contacter.

p-adiquement.

Références

[Ami75] Y. Amice. *Les nombres p-adiques*. Presses universitaires de France, 1975.

[Deb67] G. Debord. *La société du spectacle*. folio essais, 1967.

[Des] B. Deschamps. « Groupes profinis et théorie de Galois ». In : (). url : https://perso.univ-lemans.fr/~bdesch/profinis.pdf.

[Fra11] M. Francis. « Two Topological Uniqueness Theorems for Spaces of Real Numbers ». In : *Arxiv* (2011). url : https://arxiv.org/pdf/1210.1008.

[Gir24] M. Girodon. « Les nombres p-adiques et les groupes profinis ». Université de Strasbourg, 2024.

[Gou20] F. Q. Gouvêa. *p-adic Numbers, an introduction*. Springer, 2020.

[Jun25] D. Junger. « Critères de rationalité de séries formelles : applications à l'arithmétique et à la géométrie algébrique ». Université de Strasbourg, 2025.

[Kob77] N. Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*. Springer, 1977.

[Lee] S. Lee. « Some facts about p-adic numbers ». In : (). url : https://seewoo5.github.io/math-notes/number-theory/p-adic_numbers/padicprop.pdf.

[Mar67a] K. Marx. *Le Capital volume 1*. folio essais, 1867.

[Mar67b] K. Marx. *Le Capital volume 2*. folio essais, 1867.

[Mar67c] K. Marx. *Le Capital volume 3*. folio essais, 1867.

[Mur02] M. R. Murty. *Introduction to p-adic Analytic Number Theory*. American Mathematical Society, 2002.

[Rob00] A. M. Robert. *A Course in p-adic Analysis*. Springer, 2000.