Propriété C_i des corps et conjecture de Kato-Kuzumaki

Hugo Vanneuville Laurent Vera
Sous la direction d'Olivier Wittenberg

13 novembre 2013

Table des matières

Introduction

Considérons un nombre premier p. Si n est un entier, intéressons-nous à la puissance maximale de p divisant n : la valuation p-adique de n. Si n est positif, sa décomposition en base p donne directement cette information.
On peut aussi définir la valuation p-adique sur les nombres rationnels. Pour l'étudier, on aimerait généraliser l'idée de décomposition en base p aux rationnels, on voudrait dire par exemple que :

$$\frac{1}{1-p} = \sum_{n=0}^{\infty} p^n.$$

Cette série ne peut avoir un sens que si p^n tend vers 0 lorsque n tend vers l'infini. Or, Hensel introduit le corps des nombres p-adiques $\mathbb{Q}_p$ dans lequel plus un nombre est divisible par une grande puissance de p, plus il est petit. Formellement, $\mathbb{Q}_p$ est l'ensemble des séries infinies :

$$\sum_{n=n_0}^{\infty} a_n p^n,$$

où $n_0 \in \mathbb{Z}$ et les a_n sont dans $\{0, ..., p-1\}$.
Le but de ce mémoire est d'étudier des équations polynomiales dans ce corps. Nous nous intéresserons plus particulièrement aux zéros de polynômes homogènes.
La théorie de Galois nous dit que de nombreuses réponses aux questions sur les zéros de polynômes se trouvent dans des extensions finies du corps initial. Nous allons donc, dans les deux premières parties, définir les nombres p-adiques et étudier les extensions finies du corps qu'ils forment. La troisième partie sera consacrée à la propriété C_i introduite par Artin et Lang : un corps K est dit C_i si, pour tous $n, d \in \mathbb{N}$ tels que $n > d^i$, tout polynôme homogène de degré d à n variables sur K admet un zéro non trivial. On verra que, contrairement à ce qu'avait conjecturé Artin, $\mathbb{Q}_p$ n'est pas C_2. Cependant, Kato et Kuzumaki conjecturent que, si $n > d^2$, tout polynôme homogène de degré d à n variables sur $\mathbb{Q}_p$ admet des zéros non triviaux dans des extensions de $\mathbb{Q}_p$ de degrés premiers entre eux. Ils le démontrent dans le cas d premier, la démonstration est présentée en quatrième partie.

1 Nombres p-adiques

1.1 Définition et propriétés de $\mathbb{Z}_p$

Nous allons définir $\mathbb{Q}_p$ comme corps de fractions d'un anneau intègre $\mathbb{Z}_p$. L'idée pour construire $\mathbb{Z}_p$ est la même que celle pour construire $\mathbb{Q}_p$: on veut que, formellement, les éléments de $\mathbb{Z}_p$ soient les séries infinies :

$$\sum_{n=0}^{\infty} a_n p^n,$$

où $0 \leqslant a_n \leqslant p-1$.

1.1.1 Définition de $\mathbb{Z}_p$

Pour tout $n \in \mathbb{N}^\star$, on considère $\mathbb{Z}/p^n\mathbb{Z}$ muni de sa structure d'anneau topologique (topologie discrète). On a alors, pour chaque couple (m,n) tel que $m \geqslant n$, des morphismes naturels $\varphi_{m,n} : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$, qui vérifient : $\varphi_{n,n} = \mathrm{Id}$ et pour tous $m \geqslant p \geqslant n$:

$$\varphi_{m,n} = \varphi_{p,n} \circ \varphi_{m,p}.$$

On munit $\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$ de sa structure naturelle d'anneau topologique produit. Cette topologie est métrisable, car produit dénombrable de topologies métrisables, et une suite $(x^k)_k$ converge vers x si et seulement si pour tout $N \in \mathbb{N}$, il existe k_0 tel que :

$$\forall k \geqslant k_0,\ \forall n \leqslant N,\ x_n^k = x_n.$$

Définition. *On note $\mathbb{Z}_p$ le sous-ensemble des éléments $x \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$ tels que, pour tous $m \geqslant n$, $x_n = \varphi_{m,n}(x_m)$. On dit que $\mathbb{Z}_p$ est la limite projective des $\mathbb{Z}/p^n\mathbb{Z}$, ce qu'on note :*

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

On appelle entiers p-adiques les éléments de $\mathbb{Z}_p$.

Les propriétés de morphismes continus des $\varphi_{m,n}$ entraînent que $\mathbb{Z}_p$ est un anneau topologique commutatif. L'anneau $\mathbb{Z}$ s'injecte dans $\mathbb{Z}_p$, via le morphisme d'anneaux :

$$x \mapsto (x \pmod{p^n})_n.$$

Les suites correspondant aux éléments x de $\mathbb{N}$ sont alors exactement les suites « constantes » à partir d'un certain rang (au sens où le représentant dans

$\{0, ..., p^n - 1\}$ du n-ième terme est constant à partir d'un certain rang, et égal à x).
Dans la suite, on confondra $\mathbb{Z}$ et son image dans $\mathbb{Z}_p$.
Les définitions entraînent que, pour tout $x \in \mathbb{Z}_p$:

$$p^n \mid x \Leftrightarrow \forall i \leqslant n, x_i = 0.$$

Si $x \in \mathbb{Z}_p$, on notera x_n le n-ème terme de x. On remarque que la projection de $\mathbb{Z}_p$ sur $\mathbb{Z}/p^n\mathbb{Z}$ a pour noyau $p^n\mathbb{Z}_p$, ce qui donne un isomorphisme de $\mathbb{Z}_p/p^n\mathbb{Z}_p$ sur $\mathbb{Z}/p^n\mathbb{Z}$, qui identifie x_n à $x \pmod{p^n}$.

1.1.2 Propriétés topologiques de $\mathbb{Z}_p$

On appelle topologie p-adique la topologie de $\mathbb{Z}_p$, induite par la topologie produit de $\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$ (qui est compact par le théorème de Tychonov). Ceci entraîne :

Proposition 1.1. *$\mathbb{Z}_p$ est compact.*

Démonstration. Il suffit de montrer que $\mathbb{Z}_p$ est fermé. Or, pour tous $m \geqslant n$, l'ensemble des suites x telles que $\varphi_{m,n}(x_m) = x_n$ est fermé, par définition de la topologie. Donc $\mathbb{Z}_p$ est fermé comme intersection de fermés. □

On métrise la topologie p-adique de la manière suivante : on commence par définir sur $\mathbb{Z}_p$ la valuation p-adique par :

$$v_p(x) = \sup\{n \in \mathbb{N};\ p^n \mid x\} = \sup\{n \in \mathbb{N};\ x_n = 0\}.$$

De manière générale, une valuation discrète v sur un anneau est une application à valeurs dans $G \cup \{\infty\}$ où G est un sous-groupe discret de $\mathbb{R}$ (donc de la forme $\alpha\mathbb{Z}$) vérifiant les trois propriétés suivantes :

1. $v(x) = \infty \Leftrightarrow x = 0$,
2. $v(xy) = v(x) + v(y)$,
3. $v(x + y) \geqslant \min\{v(x),\ v(y)\}$.

On remarque que si v est une valuation et x, y sont tels que $v(x) \neq v(y)$ alors $v(x + y) = \min\{v(x),\ v(y)\}$.
L'application v_p est bien une valuation discrète sur $\mathbb{Z}_p$. Cette valuation induit une distance sur $\mathbb{Z}_p$, définie par :

$$d_p(x, y) = \frac{1}{p^{v_p(x-y)}}.$$

Le facteur p^{-1} est choisi pour des raisons de normalisation. La distance d_p vérifie une inégalité plus forte que l'inégalité triangulaire :

$$d_p(x,y) \leqslant \max\{d_p(x,z),\ d_p(z,y)\},$$

avec égalité dès que $d_p(x,z) \neq d_p(z,y)$. On dit que la distance est *ultramétrique*, ou *non archimédienne*.
Puisque, pour $x \in \mathbb{Z}_p$ on a :

$$d_p(x,0) \leqslant \frac{1}{p^n} \Leftrightarrow x_1 = \ldots = x_n = 0,$$

il vient que d_p engendre la topologie p-adique (car les boules pour d_p forment une base de voisinages p-adiques de 0).

Proposition 1.2. *$\mathbb{Z}$ est dense dans $\mathbb{Z}_p$.*

Démonstration. Soit $x \in \mathbb{Z}_p$, on définit $u^k \in \mathbb{Z}$ comme l'unique entier de $\{0,\ldots,p^k-1\}$ tel que $x_k = u^k \pmod{p^k}$. On a alors :

$$\forall n \leqslant k,\ u_n^k = x_n.$$

Donc

$$d_p(x,u^k) \leqslant \frac{1}{p^k}.$$

D'où u^k converge vers x. □

Corollaire 1.3. *$\mathbb{Z}_p$ est le complété de $\mathbb{Z}$ pour la distance p-adique.*

Démonstration. $\mathbb{Z}_p$ est un compact métrique donc il est complet et $\mathbb{Z}$ s'y injecte de manière isométrique et dense pour la distance d_p. □

1.1.3 Propriétés algébriques de $\mathbb{Z}_p$

Proposition 1.4. *Les unités de $\mathbb{Z}_p$ sont les éléments de valuation nulle.*

Démonstration. Si $v_p(x) \geqslant 1$, alors $x \pmod{p} = 0$ et donc x n'est pas inversible. Si un terme de x, disons x_n, est non inversible dans $\mathbb{Z}/p^n\mathbb{Z}$, alors $x_1 = \varphi_{n,1}(x_n) = 0$ et donc $v_p(x) \geqslant 1$. □

On en déduit immédiatement que tout élément non nul de $\mathbb{Z}_p$ s'écrit de manière unique $p^n u$ avec u une unité de $\mathbb{Z}_p$. Remarquons que ceci donne l'intégrité de $\mathbb{Z}_p$. On peut également facilement décrire tous les idéaux de $\mathbb{Z}_p$:

Proposition 1.5. *Les idéaux non nuls de $\mathbb{Z}_p$ sont les $p^n\mathbb{Z}_p$.*

Démonstration. Soit I un idéal de $\mathbb{Z}_p$, non nul. La partie $v_p(I \setminus \{0\})$ de $\mathbb{N}$ est non vide et admet donc un minimum n atteint par $x = p^n u$ (où u unité). On a $p^n \in I$, donc $p^n\mathbb{Z}_p \subset I$ car I est un idéal.
Et si $y \in I$, $v_p(y) \geqslant n$ donc $y \in p^n\mathbb{Z}_p$. □

L'anneau $\mathbb{Z}_p$ est donc principal, de plus, il admet pour unique idéal maximal $p\mathbb{Z}_p$. C'est donc un anneau local.

Généralisons maintenons à $\mathbb{Z}_p$ le fait que tous les entiers naturels ont une écriture en base p de la forme $\sum_{n=0}^{k} a_n p^n$ où les entiers $a_n \in \{0, \ldots, p-1\}$ sont uniques.

Proposition 1.6 (Décomposition de Hensel)**.** *Tout entier p-adique x s'écrit de manière unique*

$$x = \sum_{n=0}^{\infty} a_n p^n,$$

avec $a_n \in \{0, \ldots, p-1\}$.

Démonstration. Remarquons tout d'abord que pour de telles séries on a :

$$v_p\left(\sum_{n=N}^{N+p} a_n p^n\right) \geqslant N,$$

donc la suite des sommes partielles est de Cauchy, donc converge dans $\mathbb{Z}_p$ par complétude.
Pour $m \in \mathbb{N}$, soit $(a_{n,m})_{0 \leqslant n \leqslant m-1} \in \{0, ..., p-1\}^m$ tel que

$$\sum_{n=0}^{m-1} a_{n,m} p^n$$

soit l'écriture en base p de l'unique représentant de x_m dans $\{0, ..., p^m - 1\}$. Par définition de $\mathbb{Z}_p$, $a_{n,m}$ ne dépend pas de m. On le note a_n. Or

$$\sum_{n=0}^{m-1} a_n p^n = x \pmod{p^m}.$$

Et donc :

$$x = \sum_{n=0}^{\infty} a_n p^n.$$

□

1.2 Nombres p-adiques

1.2.1 Définition de $\mathbb{Q}_p$

Définition. *$\mathbb{Q}_p$ est le corps des fractions de $\mathbb{Z}_p$. On appelle nombres p-adiques les éléments de $\mathbb{Q}_p$ et corps p-adique toute extension finie de $\mathbb{Q}_p$.*

On étend la valuation p-adique à $\mathbb{Q}_p$ en posant, pour $r = \frac{x}{y}$, $v_p(r) = v_p(x) - v_p(y)$, ce qui ne dépend pas du couple (x, y) de représentants de r. L'application v_p est bien une valuation discrète sur $\mathbb{Q}_p$. Vérifions l'inégalité ultramétrique :

$$\begin{aligned} v_p\left(\frac{x}{y} + \frac{x'}{y'}\right) &= v_p\left(\frac{xy' + x'y}{yy'}\right) \\ &= v_p(xy' + x'y) - v_p(yy') \\ &\geqslant \min\{v_p(x) + v_p(y'), v_p(x') + v_p(y)\} - v_p(y) - v_p(y') \\ &= \min\{v_p(x) - v_p(y), v_p(x') - v_p(y')\}. \end{aligned}$$

Ainsi, d_p s'étend en une distance sur $\mathbb{Q}_p$. On généralise aisément les propriétés suivantes montrées sur $\mathbb{Z}_p$:

Proposition 1.7. *1. Tout $r \in \mathbb{Q}_p$ non nul s'écrit de manière unique $p^n u$, avec $n \in \mathbb{Z}$ et u une unité de $\mathbb{Z}_p$.*

2. Tout $r \in \mathbb{Q}_p$ s'écrit de manière unique :

$$r = \sum_{n=n_0}^{\infty} a_n p^n,$$

avec $n_0 \in \mathbb{Z}$ et $a_n \in \{0, \ldots, p-1\}$. C'est la décomposition de Hensel de r.

Démonstration. La deuxième propriété suit de la première et de la décomposition de Hensel dans $\mathbb{Z}_p$. Pour la première il suffit d'écrire :

$$r = \frac{x}{y} = \frac{p^{v_p(x)} u_1}{p^{v_p(y)} u_2} = p^n u,$$

où $n = v_p(x) - v_p(y) \in \mathbb{Z}$ et $u = u_1 u_2^{-1}$ est une unité de $\mathbb{Z}_p$. □

Corollaire 1.8. *$\mathbb{Z}_p$ est l'ensemble des éléments de $\mathbb{Q}_p$ de valuation positive.*

Démonstration. Si $x \in \mathbb{Q}_p$ est de valuation positive, il s'écrit $p^n u$ avec n positif et $u \in \mathbb{Z}_p$. Donc $x \in \mathbb{Z}_p$. □

1.2.2 Structure topologique de $\mathbb{Q}_p$

On peut en fait munir $\mathbb{Q}_p$ d'une *valeur absolue*, en posant $|x|_p = p^{-v_p(x)}$. De manière générale, une valeur absolue sur un corps K est une application $|.| : K \to \mathbb{R}_+$ telle que :

1. $|x| = 0 \Leftrightarrow x = 0$,
2. $|xy| = |x||y|$,
3. $|x + y| \leqslant |x| + |y|$.

On parle de valeur absolue *ultramétrique* lorsque $|x + y| \leqslant \max\{|x|, |y|\}$ (il y a alors égalité dès que $|x| \neq |y|$).
Une valuation discrète sur K induit une valeur absolue ultramétrique. En effet, si v est une valuation sur K et $0 < \lambda < 1$, alors $x \mapsto \lambda^{v(x)}$ est une valeur absolue ultramétrique.
L'application $|.|_p$ est donc une valeur absolue ultramétrique sur $\mathbb{Q}_p$. La décomposition des entiers en produits de facteurs premiers donne la formule :

$$\forall x \in \mathbb{Q}^\star,\ |x| \left(\prod_p |x|_p \right) = 1,$$

qui justifie le facteur de normalisation choisi.
La valeur absolue $|.|_p$ munit $\mathbb{Q}_p$ d'une structure de corps topologique, dont la topologie prolonge celle de $\mathbb{Z}_p$. La proposition 1.1 donne alors :

Proposition 1.9. *$\mathbb{Q}_p$ est localement compact.*

Démonstration. Il suffit de montrer que 0 admet une base de voisinages compacts. Or ce point admet pour base de voisinages fermés les $p^n\mathbb{Z}_p$, pour $n \in \mathbb{Z}$. En particulier, ces voisinages sont tous homéomorphes à $\mathbb{Z}_p$. On en déduit le résultat. □

Corollaire 1.10. *$\mathbb{Q}_p$ est complet. C'est le complété de $\mathbb{Q}$ pour la distance p-adique.*

Démonstration. Une suite de Cauchy de $\mathbb{Q}_p$ est bornée, donc converge par compacité des $p^n\mathbb{Z}_p$, $n \in \mathbb{Z}$.
Vérifions que $\mathbb{Q}$ est dense dans $\mathbb{Q}_p$. Si $x = \frac{a}{b} \in \mathbb{Q}_p$, on approche a et b par des suites (a_n) et (b_n) d'entiers. Par continuité des opérations, on a alors $\frac{a_n}{b_n} \underset{n\to+\infty}{\longrightarrow} x$. □

2 Corps p-adiques

Nous allons dans cette partie étudier les corps p-adiques qui sont, rappelons-le, les extensions finies de $\mathbb{Q}_p$. Il s'agit en particulier de se demander si l'on peut définir une valuation discrète sur ces corps qui prolonge la valuation p-adique.
Nous allons dans un premier temps regarder la structure étudiée sur $\mathbb{Z}_p$ et $\mathbb{Q}_p$ comme un cas particulier des anneaux de valuations discrètes et de leurs corps de fractions. Une telle structure sera aussi observée dans les corps p-adiques.

2.1 Anneaux de valuation discrète

Définition. *On dit d'un anneau commutatif A qu'il est de valuation discrète s'il est principal et local. On appellera uniformisante tout générateur de l'unique idéal maximal de A.*

Par exemple, $\mathbb{Z}_p$ est un anneau de valuation discrète et p est une uniformisante.
Cette terminologie est due à la propriété suivante :

Proposition 2.1. *Soient A un anneau de valuation discrète, $\mathfrak{m}$ son idéal maximal et π une uniformisante. On définit une valuation discrète sur A en posant :*

$$v(x) = \sup\{n \in \mathbb{N};\ x \in \mathfrak{m}^n\}.$$

Démonstration. $\mathfrak{m}$ est un idéal donc $v(x+y) \geqslant \min\{v(x), v(y)\}$.
On a clairement $v(xy) \geqslant v(x) + v(y)$. Notons $x = \pi^{v(x)}u$ et $y = \pi^{v(y)}v$, alors si on avait $\pi^{v(x)+v(y)+1} \mid xy$, on aurait $\pi \mid uv$ donc $\pi \mid u$ ou $\pi \mid v$ ce qui est absurde. Ainsi, $v(xy) = v(x) + v(y)$.
Pour la dernière propriété, il suffit de remarquer que :

$$\bigcap_{n=1}^{\infty} \mathfrak{m}^n = \{0\}.$$

En effet, si $x \in \mathfrak{m}^n \setminus \{0\}$ pour tout n, on peut écrire $x = \pi^n u_n$ avec $u_n \neq 0$, et par intégrité on a la relation de récurrence :

$$u_n = \pi u_{n+1}.$$

Comme π n'est pas inversible dans A, $u_{n+1} \notin Au_n$. Ainsi la suite d'idéaux $(u_n)_n$ est strictement croissante, ce qui contredit le fait que A est noethérien. □

Le corps des fractions d'un anneau de valuation discrète est alors naturellement muni d'une valuation discrète et donc d'une valeur absolue ultramétrique.
Réciproquement, on peut aussi définir les anneaux de valuation discrète via leur corps de fractions.

Définition. *Soit K un corps muni d'une valuation discrète. L'anneau de valuation de K, noté $\mathcal{O}_K$, est l'anneau des éléments de valuation positive (le fait que $\mathcal{O}_K$ soit un anneau résulte des propriétés d'une valuation). On note $\mathfrak{m}_K$ l'idéal de $\mathcal{O}_K$ des éléments de valuation strictement positive.*

Proposition 2.2. *$\mathcal{O}_K$ est un anneau de valuation discrète d'idéal maximal $\mathfrak{m}_K$. Ses unités sont les éléments de valuation nulle et K est son corps de fractions.*

Démonstration. Si I est un idéal non nul, soit α un élément de I de valuation strictement positive minimale (ce qui existe puisque la valuation est discrète). On a $\alpha\mathcal{O}_K \subset I$, et réciproquement, si $x \in I$, alors $v(x\alpha^{-1}) \geqslant 0$, donc $x\alpha^{-1} \in \mathcal{O}_K$. Ainsi :

$$I = \alpha\mathcal{O}_K = \{x;\ v(x) \geqslant v(\alpha)\}.$$

Ceci montre que $\mathcal{O}_K$ est principal, et que ses idéaux sont les $\mathfrak{m}_K^n$, il est donc de plus local. □

Par exemple, si K est un corps, on définit une valuation discrète sur $K((X))$ par :

$$v\left(\sum_{n=n_0}^{\infty} a_n X^n\right) = \min\{n;\ a_n \neq 0\}.$$

Donc $K[[X]]$ est un anneau de valuation discrète, d'idéal maximal (X).

Définition. *On appelle corps résiduel de K le corps $\mathcal{O}_K/\mathfrak{m}_K$.*

Par exemple, le corps résiduel de $\mathbb{Q}_p$ est $\mathbb{F}_p$, et celui de $K((X))$ est K.

On remarque que, sur tout corps muni d'une valuation discrète K, il existe une topologie naturelle qui fait de K un corps topologique en posant pour base de voisinage en 0 les idéaux de $\mathcal{O}_K$. C'est la topologie engendrée par la valeur absolue correspondant à la valuation. Dans toute la suite, si l'on parle d'un corps muni d'une valuation discrète, on le considérera muni de cette topologie.

2.2 Valuation sur les corps p-adiques

2.2.1 Extension de la valuation p-adique

Le but de ce paragraphe est de prouver que si K est un corps p-adique alors il existe une unique valuation sur K qui prolonge la valuation p-adique.

Lemme 2.3. *Soient K un corps muni d'une valeur absolue $|.|$ localement compact et E un K-espace vectoriel de dimension finie. Toutes les normes sur E sont équivalentes, où N_1 et N_2 sont dites équivalentes si :*

$$\exists C, D > 0,\ CN_1 \leqslant N_2 \leqslant DN_2,$$

ce qui revient à dire que N_1 et N_2 engendrent la même topologie.

Démonstration. Soit $(e_1, ..., e_n)$ une base de E. On définit $\|(x_1, ..., x_n)\|_\infty = \max\{|x_1|, ..., |x_n|\}$. Mais alors, $(E, \|.\|_\infty)$ est localement compact.
En particulier, il existe $\varepsilon > 0$ tel que $S(0, \varepsilon)$ soit compacte et donc, par continuité de la multiplication par un scalaire, $S(0, 1)$ est compacte.
Soit N une norme sur E. Si $x, y \in E$, alors :

$$N(x - y) = N\left(\sum_{i=1}^{n}(x_i - y_i)e_i\right) \leqslant \|x - y\|_\infty \sum_{i=1}^{n} N(e_i).$$

Et donc, $N : (E, \|.\|_\infty) \to \mathbb{R}$ est lipschitzienne donc continue. Enfin, $N_{|S(0,1)}$ est continue sur un compact donc atteint ses bornes. On en déduit le résultat. □

Théorème 2.4. *Soient K un corps p-adique et n la dimension de K sur $\mathbb{Q}_p$. Il existe une unique valuation discrète v qui étend v_p sur K. De plus, l'image de v est un sous-groupe discret de $\mathbb{R}$ de la forme $\frac{1}{e}\mathbb{Z}$, avec $e \mid n$.*

Démonstration. Montrons l'unicité. On remarque que, si v étend v_p à K, alors $x \mapsto p^{-v(x)}$ étend $|.|_p$ à K. Or le lemme 2.3 donne l'unicité à équivalence près pour l'extension de la valeur absolue $|.|_p$ à K. En effet, si $\|.\|_1$ et $\|.\|_2$ sont deux valeurs absolues qui étendent $|.|_p$ à K telles qu'il existe $x \in \mathbb{K}$ tel que $\|x\|_1 \neq \|x\|_2$, alors en regardant x^n, on remarque que $\|.\|_1$ et $\|.\|_2$ ne peuvent pas être équivalentes.
Montrons maintenant l'existence. Soit $N_{K/\mathbb{Q}_p}$ la norme de K sur $\mathbb{Q}_p$. On note $n = [K : \mathbb{Q}_p]$. Pour $x \in K$, définissons :

$$v(x) = \frac{1}{n} v_p\left(N_{K/\mathbb{Q}_p}(x)\right).$$

Déjà, la restriction de v à $\mathbb{Q}_p$ est bien v_p. De plus, v est à valeurs dans $\frac{1}{n}\mathbb{Z} \cup \{\infty\}$ et $v(x) = \infty \Leftrightarrow x = 0$. On a aussi $v(xy) = v(x) + v(y)$. Reste donc

à montrer que si $x, y \in K, v_p(x+y) \geqslant \min\{v_p(x),\ v_p(y)\}$.
Pour cela, il suffit de montrer que si $x \in K$ est tel que $v(x) \geqslant 0$ alors $v(x+1) \geqslant 0$. En remarquant que :

$$\frac{1}{n} v_p\left(N_{K/\mathbb{Q}_p}(x)\right) = \frac{1}{[\mathbb{Q}_p(x) : \mathbb{Q}_p]} v_p\left(N_{\mathbb{Q}_p(x)/\mathbb{Q}_p}(x)\right),$$

on se ramène au cas où $K = \mathbb{Q}_p(x)$.
Regardons la valeur absolue p-adique. Il suffit de montrer que $|N_{K/\mathbb{Q}_p}(1+x)|_p \leqslant 1$.
Soit A la matrice de la multiplication par x dans la base $(1, x, ..., x^{n-1})$. Notons, sur $\mathcal{M}_n(\mathbb{Q}_p)$, $\|.\|$ la norme infinie par rapport à la valeur absolue p-adique. Montrons que $\sup\{\|A^i\|; i \in \mathbb{N}\} < \infty$. Supposons le contraire. Pour tout $j \in \mathbb{N}^*$, soit $i_j \in \mathbb{N}$ tel que $\|A^{i_j}\| > j$.
Soit α_j un coefficient de A^{i_j} de valeur absolue maximale. On note :

$$B_j = \frac{A^{i_j}}{\alpha_j}.$$

En particulier, pour tout j, $\|B_j\| = 1$. Par compacité, on peut donc considérer $(B_{j_k})_k$ qui converge vers une matrice B telle que $\|B\| = 1$. Or $|\det(A)|_p \leqslant 1$, donc :

$$|\det(B_j)|_p < \frac{|\det(A^{i_j})|_p}{j^n} \leqslant \frac{1}{j^n}.$$

Et donc $\det(B) = 0$, et il existe $y \in K$ non nul tel que $B(y) = 0$.
Nous allons montrer que, pour tout i, $B(x^i y) = 0$. Or $\|B\| = 1$ et $(y, xy, ..., x^{n-1}y)$ est une base de K sur $\mathbb{Q}_p$, on aura alors la contradiction attendue.
A étant la matrice de multiplication par x, on a :

$$\begin{aligned} B(x^i y) &= \lim_{k\to\infty} B_{j_k}(x^i y) \\ &= x^i \lim_{k\to\infty} B_{j_k}(y) \\ &= 0. \end{aligned}$$

On peut ainsi considérer $M > 0$ qui majore $\{\|A^i\|; i \in \mathbb{N}\}$. En regardant la formule polynomiale du déterminant, en développant $(I+A)^l$ avec le binôme de Newton, et en utilisant le fait que $|.|_p$ est non archimédienne, on remarque que :

$$\begin{aligned} |N_{K/\mathbb{Q}_p}(1+x)|_p^l &= |\det\left((I+A)^l\right)|_p \\ &\leqslant \|(I+A)^l\|^n \\ &\leqslant \left(\max\left\|\binom{l}{i} A^i\right\|\right)^n \\ &\leqslant M^n. \end{aligned}$$

Cela étant vrai pour tout l, on en déduit le résultat. Le corps K est donc muni d'une valuation discrète.
L' image de v est donc un sous-groupe de $\frac{1}{n}\mathbb{Z}$ de la forme $v(\pi)\mathbb{Z}$, où π désigne une uniformisante. On a $p = \pi^e u$ où u est une unité de $\mathcal{O}_K$, et $e \in \mathbb{N}^*$, et donc, en passant aux valuations, $1 = v(\pi)e$. □

Cela donne aussi l'existence et l'unicité à équivalence près du prolongement de la valeur absolue p-adique sur tout corps p-adique.
On a le corrolaire suivant :

Corollaire 2.5. *Soient K un corps p-adique, v la valuation sur K qui étend la valuation p-adique et L une extension finie de K. Il existe une unique valuation sur L qui étende v et elle est définie par :*

$$x \mapsto \frac{1}{[L:K]} v\left(N_{L/K}(x)\right).$$

Pour ce qui est de la topologie naturelle sur les corps p-adiques :

Proposition 2.6. *Soit K un corps p-adique, soit π est une uniformisante de K. On a :*
$(\pi^n \mathcal{O}_K)_{n\in\mathbb{Z}}$ est une base de voisinages compacts de 0.

Démonstration. Par continuité de la multiplication, il suffit de montrer qu'un des $\pi^n\mathcal{O}_K$ est compact. Or, par le lemme 2.3, toutes les normes sur le $\mathbb{Q}_p$-espace vectoriel K sont équivalentes. De plus, la norme infinie relative à une quelconque base de K donne la compacité locale. Donc K muni de la topologie issue de la valuation p-adique est localement compact. Par ailleurs, les $\pi^n\mathcal{O}_K$ étant fermés (regarder une valeur absolue sur K) et formant une base de voisinages de 0, ils sont compacts à partir d'un certain rang. □

2.2.2 Corps résiduels des corps p-adiques

On vient de voir que les corps p-adiques sont munis d'une unique valuation discrète qui étend celle de $\mathbb{Q}_p$. On peut donc étudier leurs corps résiduels.

Proposition 2.7. *Soit K un corps p-adique de dimension n sur $\mathbb{Q}_p$. Le corps résiduel de K est une extension finie de $\mathbb{F}_p$, de degré $f \leqslant n$.*

Démonstration. Déjà,

$$\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p \hookrightarrow \mathcal{O}_K/\mathfrak{m}_K$$

est bien définie car $\mathbb{Z}_p \subset \mathcal{O}_K$ et $p\mathbb{Z}_p \subset \mathfrak{m}_K$.

Montrons que $\mathcal{O}_K/\mathfrak{m}_K$ est une extension finie de $\mathbb{F}_p$ de degré inférieur ou égal à n.
Considérons $a_1, \ldots, a_{n+1} \in \mathcal{O}_K$ et montrons que $(a_1 \pmod{\mathfrak{m}_K}, \ldots, a_{n+1} \pmod{\mathfrak{m}_K})$ est liée sur $\mathbb{F}_p$.
Déjà, $a_1, ..., a_{n+1}$ sont liés sur $\mathbb{Q}_p$. On écrit :

$$\sum_{i=1}^{n+1} a_i b_i = 0, \quad b_i \in \mathbb{Q}_p,$$

avec les b_i non tous nuls.
En multipliant par p^{-k} où k est la plus petite valuation des b_i et en passant dans $\mathcal{O}_K/\mathfrak{m}_K$, on remarque que les $a_i \pmod{\mathfrak{m}_K}$ sont liés sur $\mathbb{F}_p$. □

On veut maintenant démontrer une relation entre les dimensions des extensions des corps résiduels et des corps p-adiques. Pour trouver une telle relation, on regarde une base de l'extension des corps résiduels, qu'on va essayer de remonter en une base de l'extension initiale.
Soient K un corps p-adique de dimension n sur $\mathbb{Q}_p$ et v la valuation sur K qui étend v_p. Dans toute la suite de cette partie, on note π une uniformisante de v, et $e = \frac{1}{v(\pi)}$.

Lemme 2.8. *Soit $(y_i)_{1\leqslant i\leqslant f} \in \mathcal{O}_K^f$ tel que $(\overline{y_i})_{1\leqslant i\leqslant f}$ soit une base de $\mathcal{O}_K/\mathfrak{m}_K$ sur $\mathbb{F}_p$. Il existe $(\lambda_{i,j})_{1\leqslant i\leqslant f;\, 0\leqslant j\leqslant e-1}$ des entiers p-adiques tels que :*

$$x - p^{\lfloor v(x)\rfloor}\left(\sum_{j=0}^{e-1}\left(\sum_{i=1}^{f}\lambda_{i,j}y_i\right)\pi^j\right)$$

soit de valuation supérieure à $\lfloor v(x)\rfloor + 1$.

Démonstration. Si $x = 0$ on a le résultat.
Sinon, montrons par récurrence sur $k \leqslant e-1$ qu'il existe $(\lambda_{i,j})_{1\leqslant i\leqslant f;\, 0\leqslant j\leqslant k}$ tel que

$$x - p^{\lfloor v(x)\rfloor}\left(\sum_{j=0}^{k}\left(\sum_{i=1}^{f}\lambda_{i,j}y_i\right)\pi^j\right)$$

soit de valuation supérieure ou égale à $\lfloor v(x)\rfloor + \frac{k+1}{e}$.
La valuation de $p^{-\lfloor v(x)\rfloor}x$ est positive, il existe donc $(\lambda_{i,0})_{1\leqslant i\leqslant f} \in \mathbb{Z}_p^f$ tel que :

$$p^{-\lfloor v(x)\rfloor}x - \sum_{i=1}^{k}\lambda_{i,0}y_i$$

soit de valuation supérieure ou égale à $\frac{1}{e}$.
Si le résultat est vrai jusqu'à k, on remarque que :

$$p^{-\lfloor v(x)\rfloor}\pi^{-(k+1)}\left(x - p^{\lfloor v(x)\rfloor}\sum_{j=0}^{k}\left(\sum_{i=1}^{f}\lambda_{i,j}y_i\right)\pi^j\right)$$

est de valuation positive. On peut donc définir $(\lambda_{i,k+1})_{1\leqslant i\leqslant f}$ comme dans le cas $j = 0$. □

Théorème 2.9. *On a la relation $n = ef$.*

Démonstration. Montrons que si $(y_i)_{1\leqslant i\leqslant f} \in \mathcal{O}_K^f$ est tel que $(\overline{y_i})_{1\leqslant i\leqslant f}$ est une base de $\mathcal{O}_K/\mathfrak{m}_K$ sur $\mathbb{F}_p$, alors $(\pi^j y_i)_{1\leqslant i\leqslant f;\, 0\leqslant j\leqslant e-1}$ est une base de K sur $\mathbb{Q}_p$.
La famille est libre : soient $\lambda_{i,j} \in \mathbb{Q}_p$ tels que :

$$\sum_{\substack{1\leqslant i\leqslant f\\ 0\leqslant j\leqslant e-1}} \lambda_{i,j}y_i\pi^j = 0.$$

Supposons par l'absurde qu'il existe i tel que :

$$\sum_{j=0}^{e-1}\lambda_{i,j}\pi^j \neq 0.$$

Mais alors, on peut définir

$$v_1 = e\min\left\{v\left(\sum_{j=0}^{e-1}\lambda_{i,j}\pi^j\right); 1\leqslant i\leqslant f\right\}.$$

On a :

$$\sum_{i=1}^{f}\left(\sum_{j=0}^{e-1}\pi^{j-v_1}\lambda_{i,j}\right)y_i = 0.$$

Or $(\overline{y_i})$ est libre, donc en passant dans $\mathcal{O}_K/\mathfrak{m}_K$, on a pour tout i :

$$\overline{\sum_{j=0}^{e-1}\pi^{j-v_1}\lambda_{i,j}} = 0,$$

contredisant la définition de v_1.
Reste donc à montrer que $(\pi^j)_{0\leqslant j\leqslant e-1}$ est libre sur $\mathbb{Q}_p$. Soient $\lambda_j \in \mathbb{Q}_p$ tels que :

$$\sum_{j=0}^{e-1}\lambda_j\pi^j = 0.$$

Si les λ_j sont non tous nuls, on peut définir $v_2 = \min\{(\lambda_j \pi^j)\,; 0 \leqslant j \leqslant e-1\}$.
Or :

$$v\left(\lambda_j \pi^j\right) \in \mathbb{Z} + \frac{j}{e} \cup \{\infty\},$$

et l'intersection de ces ensembles, pour $j = 0, ..., e-1$ est $\{\infty\}$, donc v_2 est uniquement atteint et

$$v_2 = v\left(\sum_{j=0}^{e-1} \lambda_j \pi^j\right),$$

ce qui est la contradiction attendue.
Utilisons le lemme 2.8 pour montrer que la famille considérée est génératrice.
Soit $x \in K$, on définit $(\lambda_{i,j,n})_{1 \leqslant i \leqslant f;\, 0 \leqslant j \leqslant e-1;\, n \in \mathbb{N}}$ des entiers p-adiques et $(x_n)_{n \in \mathbb{N}}$ par récurrence comme suit :
On pose $x_0 = x$, et $(\lambda_{i,j,0})_{1 \leqslant i \leqslant f;\, 0 \leqslant j \leqslant e-1}$ tels que :

$$x - p^{\lfloor v(x) \rfloor} \left(\sum_{j=0}^{e-1} \left(\sum_{i=1}^{f} \lambda_{i,j,0} y_i\right) \pi^j\right)$$

soit de valuation supérieure à $\lfloor v(x) \rfloor + 1$.
Puis on pose :

$$x_{n+1} = x_n - p^{\lfloor v(x) \rfloor + n} \left(\sum_{j=0}^{e-1} \left(\sum_{i=1}^{f} \lambda_{i,j,n} y_i\right) \pi^j\right)$$

et $(\lambda_{i,j,n+1})_{1 \leqslant i \leqslant f;\, 0 \leqslant j \leqslant e-1}$ tels que :

$$x_{n+1} - p^{\lfloor v(x) \rfloor + n + 1} \left(\sum_{j=0}^{e-1} \left(\sum_{i=1}^{f} \lambda_{i,j,n+1} y_i\right) \pi^j\right)$$

soit de valuation supérieure à $\lfloor v(x) \rfloor + n + 2$.
Mais alors,

$$\sum_{i,j} \left(\sum_{n \in \mathbb{N}} \lambda_{i,j,n} p^{\lfloor v(x) \rfloor + n}\right) y_i \pi^j = x.$$

Ceci conclut la démonstration. □

3 Propriété C_i des corps

Le but de ce mémoire est d'étudier les zéros de polynômes homogènes. Avant cela, regardons des équations plus simples dans $\mathbb{Q}_p$.
On peut déjà remarquer que les éléments de $\mathbb{Q}_p$ qui sont des puissances n-èmes sont tous de valuation divisible par n.
On peut remarquer que $\mathbb{Q}_2$ n'admet pas de racine de -1. En effet, $\mathbb{Z}/4\mathbb{Z}$ n'en admet pas, donc $\mathbb{Z}_2$ non plus par sa définition et donc $\mathbb{Q}_2$ n'admet pas de racine de -1.

3.1 Lemme de Hensel

On aimerait maintenant avoir une méthode permettant de relever dans $\mathbb{Z}_p$ des zéros qu'un polynôme admet dans $\mathbb{F}_p$. Le lemme de Hensel en fournit une. On verra que la démonstration est analogue à la méthode de Newton.

Théorème 3.1 (Lemme de Hensel)**.** *Soient* $P = \sum_{n=0}^{d} c_n X^n \in \mathbb{Z}_p[X]$ *et* $\alpha \in \mathbb{Z}_p$ *tel que* $P(\alpha) = 0 \pmod p$ *mais* $P'(\alpha) \neq 0 \pmod p$*. Il existe* $a \in \mathbb{Z}_p$ *tel que* $P(a) = 0$ *et* $\alpha = a \pmod p$*.*

Démonstration. Montrons par récurrence l'existence d'une suite $(a_n)_{n\geq 1}$ d'entiers telle que :
$\forall n \in \mathbb{N}^\star, 0 \leqslant a_n < p^n$, $P(a_n) = 0 \pmod{p^n}$, $P'(a_n) \neq 0 \pmod p$ et $a_{n+1} = a_n \pmod{p^n}$.
On choisit a_1 l'unique entier de $\{0, .., p-1\}$ tel que $a_1 = a \pmod p$. Supposons construits les n premiers termes de la suite. Par analogie avec la méthode de Newton, on choisit a_{n+1} l'unique entier de $\{0, ..., p^{n+1} - 1\}$ tel que :

$$a_{n+1} = a_n - \frac{P(a_n)}{P'(a_n)} \pmod{p^{n+1}}.$$

On a immédiatement $a_{n+1} = a_n \pmod{p^n}$ et $P'(a_{n+1}) \pmod p = P'(a_n) \pmod p \neq 0$. Vérifions que $P(a_{n+1}) = 0 \pmod{p^{n+1}}$. Toutes les égalités suivantes sont écrites modulo p^{n+1} :

$$\begin{aligned}
P(a_{n+1}) &= P\left(a_n - \frac{P(a_n)}{P'(a_n)}\right) \\
&= \sum_{k=0}^{d} c_k \left(a_n - \frac{P(a_n)}{P'(a_n)}\right)^k \\
&= c_0 + \sum_{k=1}^{d} c_k \sum_{j=0}^{k} \binom{k}{j} (-1)^j \frac{P(a_n)^j}{P'(a_n)^j} a_n^{k-j} \\
&= c_0 + \sum_{k=1}^{d} c_k \left(a_n^k - k a_n^{k-1} \frac{P(a_n)}{P'(a_n)}\right) \\
&= P(a_n) - \left(\sum_{k=1}^{d} k c_k a_n^{k-1}\right) \frac{P(a_n)}{P'(a_n)} \\
&= 0.
\end{aligned}$$

De plus, $(a_n)_{n\geqslant 1}$ converge dans $\mathbb{Z}_p$ vers $a = (a_n \pmod{p^n})_{n\geq 1}$ car :

$$\forall n \in \mathbb{N}^\star,\ \forall k \geq n,\ a_k = a_n \pmod{p^n}.$$

Et on a alors que $a = a_n \pmod{p^n}$. De plus, pour tout $n \in \mathbb{N}^\star$:

$$\begin{aligned}
P(a) \pmod{p^n} &= P(a_n) \pmod{p^n} \\
&= 0.
\end{aligned}$$

Ainsi, $P(a) = 0$. □

De ce lemme, on peut déduire que, contrairement à $\mathbb{Q}_2$, $\mathbb{Q}_5$ admet une racine de -1. En effet, dans $\mathbb{F}_5$, $3^2 = -1$ et $2 \times 3 \neq 0$ donc on peut relever 3 en une racine de -1.

3.2 Corps C_i

On s'intéresse ici aux polynômes homogèmes à plusieurs variables. Chacun possède $(0, ..., 0)$ comme zéro trivial. Le but est de trouver un zéro non trivial.
Avant de commencer à étudier ces polynômes, faisons une remarque de vocabulaire. Si E est un K-espace vectoriel de dimension finie n, une *forme homogène* sur E est une application $f : E \to K$ telle que, si $(e_1, ..., e_n)$ est une base de E, alors $(x_1, ..., x_n) \mapsto f(x_1 e_1 + ... + x_n e_n)$ est un polynôme homogène en les x_i. Cette propriété ne dépend pas du choix de la base.

Définition. *Un corps K est dit C_i si, pour tous $n, d \in \mathbb{N}$ tels que $n > d^i$, tout polynôme homogène de degré d en n variables sur K admet un zéro non trivial.*

On peut remarquer qu'être C_0 équivaut à être algébriquement clos. En effet, si un corps K n'est pas algébriquement clos, alors il existe une extension stricte finie L de K. Notons $n = [L : K]$ et $(e_1, ..., e_n)$ une base de L sur K. En pensant à la norme on définit :

$$f(X_1, ..., X_n) = \det\left(X_1 m_{e_1} + ... + X_n m_{e_n}\right),$$

où les m_{e_i} sont les multiplications par e_i.
Le polynôme f est homogène à $n > 1$ variables. Pour tout $(x_1, ..., x_n) \in K^n$, $f(x_1, ..., x_n) = N_{L/K}(x_1 e_1 + ... + x_n e_n)$ et donc f n'a aucun zéro non trivial.

Proposition 3.2 (Chevalley)**.** *Les corps finis sont C_1.*

Démonstration. Soient q une puissance d'un nombre premier p, $n > d \geqslant 1$ et f un polynôme homogène sur $\mathbb{F}_q$ en n variables de degré d. Remarquons que :

$$\sum_{(x_1,...,x_n)\in\mathbb{F}_q^n} f(x_1, ..., x_n)^{q-1} = 0. \tag{1}$$

En effet, en écrivant f comme somme de ses monômes, on voit que pour avoir (1), il suffit de montrer que pour tous $r_1, ..., r_n$ tels que $r_1 + ... + r_n = d(q-1)$, on a :

$$A := \sum_{(x_1,...,x_n)\in\mathbb{F}_q^n} x_1^{r_1} ... x_n^{r_n} = 0.$$

Or :

$$A = \prod_{i=1}^{n} \sum_{x_i\in\mathbb{F}_q} x_i^{r_i}.$$

De plus, comme $n > d$, il existe i tel que $0 \leqslant r_i \leqslant q - 2$.
Si $r_i = 0$ alors $A = 0$, sinon on a :

$$\sum_{x_i\in\mathbb{F}_q} x_i^{r_i} = \sum_{j=1}^{q-1} y^{r_i},$$

où y est un générateur du groupe cyclique $\mathbb{F}_q^*$. Et donc :

$$\sum_{x_i\in\mathbb{F}_q} x_i^{r_i} = \frac{1 - y^{r_i(q-1)}}{1 - y^{r_i}} = 0.$$

D'où $A = 0$.
On peut alors prouver la proposition. En effet, pour tout $y \in \mathbb{F}_q^*, y^{q-1} = 1$ et donc (1) permet de dire que p divise le nombre de zéros de f. Or f admet $(0, ..., 0)$ comme zéro, donc f admet un zéro non trivial. □

Qu'en est-il de $\mathbb{Q}_p$? Il n'est clairement pas C_0 car p n'admet pas de racine dans $\mathbb{Q}_p$. Et même :

Proposition 3.3. *$\mathbb{Q}_p$ n'est pas C_1.*

Démonstration. Supposons d'abord $p = 2$ et regardons la forme $x^2 + y^2 + z^2$. Supposons qu'elle admette un zéro non trivial (x_0, y_0, z_0). Quitte à multiplier par une puissance de 2, et à permuter les variables, on peut supposer que $x_0, y_0, z_0 \in \mathbb{Z}_2$ et x_0 de valuation nulle. En passant modulo 2, on remarque qu'un seul des (y_0, z_0) est de valuation nulle, l'autre étant divisible par 2. Mais alors, en réduisant modulo 4, on obtient $2 = 0 \pmod 4$ (écrire la décomposition de Hensel), ce qui est absurde.
Supposons maintenant $p \neq 2$. Il existe alors exactement $\frac{p+1}{2} < p$ carrés dans $\mathbb{F}_p$. Soit $a \in \{1, ..., p-1\}$ un représentant d'un élément de $\mathbb{F}_p$ qui n'est pas un carré. Regardons l'équation :

$$x^2 + py^2 = az^2.$$

Supposons par l'absurde qu'elle admette une solution non triviale (x_0, y_0, z_0). Pour tout $n \in \mathbb{Z}$, $p^n(x_0, y_0, z_0)$ en étant aussi une, on peut supposer que x_0, y_0, z_0 sont de valuation positive et que l'un d'entre eux est de valuation nulle.
On remarque que si x_0 ou z_0 est de valuation nulle, alors ils le sont tous les deux. De plus, si y_0 est de valuation nulle et x_0 et z_0 ne le sont pas, alors la valuation de py_0^2 est strictement plus petite que celle de $x_0^2 - az_0^2$. Donc x_0 et z_0 sont forcément tous les deux de valuation nulle.
On passe modulo p :

$$x_0^2 = az_0^2 \pmod p,$$

et même :

$$\left(\frac{x_0}{z_0}\right)^2 = a \pmod p,$$

qui est la contradiction attendue. □

La décomposition de Hensel donne une similitude formelle entre $\mathbb{F}_p((X))$ et les nombres p-adiques. En tant que corps munis d'une valuation discrète, ils ont des structures analogues, à la fois par la définition de la valuation et par le fait qu'ils ont le même corps résiduel. Or, Serge Lang prouve que si K un

corps fini, $K((X))$ est C_2.
Emil Artin a émis la conjecture suivante : soit p un nombre premier, $\mathbb{Q}_p$ est C_2. On verra cependant qu'elle est fausse.

3.3 $\mathbb{Q}_p$ et la propriété C_2

3.3.1 Cas des degrés 2 et 3

On s'attend d'autant plus à ce que la conjecture d'Artin soit vraie qu'elle est vérifiée pour les degrés 2 et 3 (Hasse [9] pour le degré 2, Lewis [10] pour le degré 3). On ne démontrera ici que le cas du degré 2 avec $p \neq 2$ à l'aide du lemme de Hensel :

Proposition 3.4. *Soit p un nombre premier différent de 2. Tout polynôme homogène de degré 2 à 5 variables et à coefficients dans $\mathbb{Q}_p$ admet un zéro non trivial dans $\mathbb{Q}_p$.*

Démonstration. Déjà, par réduction des formes quadratiques, on peut se ramener à la résolution d'une équation du type :

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 + a_5x_5^2 = 0,$$

où $a_1, ..., a_5 \in \mathbb{Q}_p$.
Si l'un des a_i est nul, on a un zéro non trivial. Sinon, quitte à faire un changement de variable du type $(y_1, ..., y_5) = (p^{n_1}x_1, ..., p^{n_5}x_5)$, où $n_1, ..., n_5 \in \mathbb{Z}$, on se ramène à $a_1, ..., a_5$ de valuation 0 ou 1. Mais alors, quitte à diviser l'équation par p et à permuter les indices, on peut supposer que a_1, a_2, a_3 sont de valuation nulle.
Cherchons une solution telle que $x_4 = x_5 = 0$. Il suffit donc de savoir résoudre dans $\mathbb{Z}_p$ l'équation :

$$ax^2 + by^2 + cz^2 = 0,$$

où a, b, c sont de valuation nulle.
Les corps finis étant C_1, on trouve $x_0, y_0, z_0 \in \mathbb{Z}_p$ (avec, par exemple, $x_0 \neq 0 \pmod p$) solution modulo p de l'équation. On peut même supposer $x_0 = 1$. Il suffit alors de résoudre dans $\mathbb{Z}_p$ l'équation :

$$a + by^2 + cz^2 = 0,$$

connaissant une solution modulo p $(y_0, z_0) \in \mathbb{Z}_p^2$. Comme a est de valuation nulle, on peut supposer que y_0 ou z_0 aussi, disons y_0.
On veut pour cela utiliser le lemme de Hensel, et donc se ramener à une seule variable. L'idée géométrique est de couper la conique définie par l'équation

ci-dessus par une droite passant par $(y_0, z_0) \pmod p$. Si de plus elle coupe la conique en un point distinct de $(y_0, z_0) \pmod p$, c'est-à-dire qu'elle est non tangente à la conique, on obtiendra un polynôme de degré 2 à racines simples auquel on pourra alors appliquer le lemme de Hensel.
Comme y_0 et b sont non nuls modulo p, on peut trouver $\tau \in \mathbb{Z}_p$ tel que :

$$by_0\tau \neq -cz_0 \pmod p.$$

En posant $y = \tau z + \rho$, où $\rho = y_0 - \tau z_0$, on remarque qu'il suffit de résoudre l'équation :

$$(c + b\tau^2)z^2 + 2b\rho\tau z + a + b\rho^2 = 0,$$

sachant que z_0 en est une solution modulo p. Or la dérivée de ce polynôme évaluée en z_0 est :

$$2(c + b\tau^2)z_0 + 2b\rho\tau = 2(cz_0 + by_0\tau)$$

elle est donc bien non nulle modulo p, par définition de τ et car $p \neq 2$. Le lemme de Hensel permet de conclure. □

La propriété C_2 n'est cependant pas vraie pour tous les degrés, comme nous allons le voir dans le prochain paragraphe.

3.3.2 Un contre-exemple à la conjecture d'Artin

En 1966, Guy Terjanian a donné un contre-exemple à la conjecture d'Artin en montrant :

Proposition 3.5 (Terjanian)**.** $\mathbb{Q}_2$ *n'est pas* C_2.

Démonstration. Terjanian construit un polynôme homogène de degré 4 en 18 variables sur $\mathbb{Z}_2$. On aura le résultat en montrant qu'il n'admet pas de zéro non trivial.
On pose :

$$g(X, Y, Z) = X^2YZ + Y^2ZX + Z^2XY + X^2Y^2 + X^2Z^2 + Y^2Z^2 - X^4 - Y^4 - Z^4$$

et :

$$f(X_1, ..., X_9) = g(X_1, X_2, X_3) + g(X_4, X_5, X_6) + g(X_7, X_8, X_9).$$

Montrons que :

$$\forall (x_1, ..., x_9) \in \mathbb{Z}_2^9, (f(x_1, ..., x_9) = 0 \pmod 4) \Rightarrow 2 \mid x_1, ..., x_9. \qquad (2)$$

On pourra conclure car alors si on pose $h = f(X_1, ..., X_9) + 4f(X_{10}, ..., X_{18})$ on a :

$$\begin{aligned} \forall x_1, ..., x_{18} \in \mathbb{Z}_2,\ h(x_1, ..., x_{18}) = 0 &\Rightarrow f(x_1, ..., x_9) = 0 \pmod 4 \\ &\Rightarrow 2 \mid x_1, ..., x_9 \\ &\Rightarrow f(x_1, ..., x_9) = 0 \pmod{16} \\ &\Rightarrow f(x_{10}, ..., x_{18}) = 0 \pmod 4. \end{aligned}$$

Ainsi,

$$\forall x_1, ..., x_{18} \in \mathbb{Z}_2,\ h(x_1, ..., x_{18}) = 0 \Rightarrow 2 \mid x_1, ..., x_{18}.$$

Or, si $(x_1, ..., x_{18}) \in \mathbb{Q}_2^{18}$ est un zéro non trivial de h, on regarde $n = \min\{m \in \mathbb{N};\ \forall i,\ 2^m \mid x_i\}$. Mais alors, $\frac{1}{2^n}(x_1, ..., x_{18}) \in \mathbb{Z}_2^{18}$ est un zéro de h tel que 2 ne divise pas tout x_i.
Reste à montrer (2).

On remarque que la classe de congruence modulo 4 de $g(x, y, z)$ ne dépend que de la classe de congruence modulo 2 de x,y et z :
Montrons par exemple que $g(x + 2, y, z) = g(x, y, z) \pmod 4$, les autres cas se montrant de la même façon. On a :

$$\begin{aligned} g(x+2, y, z) &= (x+2)^2yz + y^2z(x+2) + z^2(x+2)y \\ &\quad +(x+2)^2y^2 + (x+2)^2z^2 + y^2z^2 \\ &\quad -(x+2)^4 - y^4 - z^4 \pmod 4 \\ &= g(x, y, z) + 2y^2z + 2z^2y \pmod 4. \end{aligned}$$

Or, pour tous y, z, $y^2z + z^2y = 0 \pmod 2$.

Par ailleurs, $g(x, y, z) = 0 \pmod 4$ si et seulement si $2 \mid x, y, z$. De plus, si 2 ne divise pas à la fois x, y et z alors $g(x, y, z) = 3 \pmod 4$.
En effet, si $2 \mid x, y, z$ alors $g(x, y, z) = 0 \pmod{16}$ et si (par symétrie), 2 ne divise pas x, alors il suffit d'étudier les cas suivants :

1. $x = 1 \pmod 4, y = 0 \pmod 4, z = 0 \pmod 4$. Dans ce cas, $g(x, y, z) = -1 = 3 \pmod 4$.
2. $x = 1 \pmod 4, y = 1 \pmod 4, z = 0 \pmod 4$. Dans ce cas, $g(x, y, z) = 1 - 1 - 1 = 3 \pmod 4$.
3. $x = 1 \pmod 4, y = 1 \pmod 4, z = 1 \pmod 4$. Dans ce cas, $g(x, y, z) = 6 - 3 = 3 \pmod 4$.

On a alors (2) car ni 3 ni 6 ni 9 ne sont congrus à 0 modulo 4. □

Il a même été démontré que les corps p-adiques ne sont C_i pour aucun i (Arkhipov–Karatsuba [8], Alemu [7]).

3.4 Propriété C_i^0

Définition. *Soient K un corps et f un polynôme homogène à coefficients dans K. On note $\mathcal{N}(f)$ le sous-groupe de $\mathbb{Z}$ engendré par les degrés des extensions dans lesquelles on trouve des zéros non triviaux de f.*
Le corps K sera dit C_i^0 si pour tout polynôme homogène f de degré d en n variables, tels que $d^i < n$, on a $\mathcal{N}(f) = \mathbb{Z}$. Autrement dit, on trouve des zéros non triviaux de tels polynômes dans des extensions de degrés premiers entre eux.

Proposition 3.6. *$\mathbb{Q}_p$ n'est pas C_1^0. Et même, tout f homogène de degré 2 en 3 variables sans zéro non trivial dans $\mathbb{Q}_p$ n'a de zéro non trivial que dans des extensions de degré pair.*

Démonstration. Quitte à réduire la forme homogène f, on peut se ramener à l'équation $ax^2 + by^2 + cz^2 = 0$, sans zéro non trivial dans $\mathbb{Q}_p$, et même $x^2 - ay^2 = bz^2$.
Remarquons que si K est un corps p-adique, cette équation a une solution non triviale dans K si et seulement si b est une norme de $K \hookrightarrow K(\sqrt{a})$.
Si a est un carré, les deux propriétés sont vraies. Sinon on remarque que $N_{K(\sqrt{a})/K}(x + \sqrt{a}y) = x^2 - ay^2$. Donc comme a n'est pas un carré dans K, si (x, y, z) est une solution non triviale, $z \neq 0$ et :

$$b = N_{K(\sqrt{a})/K}\left(\frac{x + y\sqrt{a}}{z}\right).$$

Si b est une norme, alors b s'écrit $u^2 - av^2$, et donc $(u, v, 1)$ est une solution non triviale.
Supposons alors que $[K : \mathbb{Q}_p]$ soit impair et que $b = N_{K(\sqrt{a})/K}(\omega)$, montrons qu'on arrive à une contradiction. En prenant les normes :

$$\begin{aligned} b^{[K:\mathbb{Q}_p]} &= N_{K/\mathbb{Q}_p}(b) \\ &= N_{K(\sqrt{a})/\mathbb{Q}_p}(\omega) \\ &= N_{\mathbb{Q}_p(\sqrt{a})/\mathbb{Q}_p}\left(N_{K(\sqrt{a})/\mathbb{Q}_p(\sqrt{a})}(\omega)\right). \end{aligned}$$

Or :

$$b^{[K:\mathbb{Q}_p]} = bN_{\mathbb{Q}_p(\sqrt{a})/\mathbb{Q}_p}\left(b^{\frac{[K:\mathbb{Q}_p]-1}{2}}\right),$$

donc b est une norme de $\mathbb{Q}_p \hookrightarrow \mathbb{Q}_p(\sqrt{a})$, ce qui est absurde. □

L'objet de la partie suivante est l'étude de la propriété C_2^0 sur $\mathbb{Q}_p$. Kato et Kuzumaki ont conjecturé que $\mathbb{Q}_p$ est C_2^0, et l'ont démontré pour les polynômes homogènes de degré premier. Dans le cas général, la conjecture est toujours ouverte, même pour les formes de degré 4.

4 Théorème de Kato et Kuzumaki

Soit K un corps p-adique. Le but de cette section est de démontrer le théorème suivant :

Théorème 4.1 (Kato et Kuzumaki)**.** *K vérifie la propriété C_2^0 pour les polynômes de degré premier.*

Autrement dit, on souhaite montrer que pour tout polynôme f homogène de degré d premier en n variables tel que $d^2 < n$, on a $\mathcal{N}(f) = \mathbb{Z}$.

Commençons par faire l'observation suivante :

Proposition 4.2. *On a $d \in \mathcal{N}(f)$.*

Démonstration. Déjà, si $(0, 1..., 1)$ est un zéro de f, alors on a le résultat.
Dans le cas contraire, on remarque que X_1 n'apparaît pas dans tous les monômes de f et que le coefficient devant le terme de degré d de $g := f(1, X, \ldots, X)$ est non nul.
Le polynôme g est ainsi de degré d. Soient $h_1, ..., h_s$ irréductibles tels que $g = h_1...h_s$. Pour tout i, g admet un zéro dans une extension de K de degré le degré de h_i. Or $d = \deg(h_1) + ... + \deg(h_s)$. □

Il suffit donc de montrer que $\mathcal{N}(f)$ contient un entier premier avec d. Comme d est premier, si $\mathcal{N}(f)$ contient un entier $< d$, c'est terminé. Dans le cas contraire, on va utiliser le résultat suivant :

Lemme 4.3. *Soient $n \in \mathbb{N}^*$, $V = K^n$ et v la valuation sur K qui prolonge la valuation p-adique. Soit f un polynôme de degré d à n variables sur K. Supposons que f n'a de zéro non trivial dans aucune extension finie de K de degré $< d$. Posons, pour tout $k \in \mathbb{Z}$, $V^{(k)} = f^{-1}(\pi^k \mathcal{O}_K)$. On a les propriétés suivantes :*

1. *Les $V^{(k)}$ sont des sous-$\mathcal{O}_K$-modules de V libres de type fini tels que*
$$K \otimes_{\mathcal{O}_K} V^{(k)} = V.$$
2. *Si $x \in V^{(k)}$ et $y \in V^{(k+1)}$ alors $f(x + y) = f(x) \pmod{\pi^{k+1}\mathcal{O}_K}$.*

On parle ici de produit tensoriel de modules. La définition est exactement la même que pour les espaces vectoriels, à savoir la satisfaction du problème universel de factorisation pour les applications bilinéaires.
Dans la suite, on utilisera les deux propriétés suivantes, où A est un anneau intègre de corps de fractions K' et M un A-module :

1. $K' \otimes_A M$ est canoniquement un K'-espace vectoriel, avec si $\lambda \in K'$ et $x \in M$, $\lambda(1 \otimes x) = \lambda \otimes x$.
2. Si M est libre de type fini, alors la dimension du K'-espace vectoriel $K' \otimes_A M$ est égale au rang de M.

Montrons maintenant le lemme :

Démonstration. Soit $e \in \mathbb{N}^*$ tel que $\frac{1}{e}$ soit la valuation d'une uniformisante π de v. Montrons le premier point. Soient $x \in V^{(k)}$ et $\lambda \in \mathcal{O}_K$. Par homogénéité, $f(\lambda x) = \lambda^d f(x)$, donc :

$$v(f(\lambda x)) = dv(\lambda) + v(f(x)) \geqslant \frac{k}{e}.$$

Ainsi, $\lambda x \in V^{(k)}$.
Soient $x, y \in V$ tels que $\frac{k}{e} \leqslant v(f(x)) \leqslant v(f(y))$. Pour monter que $V^{(k)}$ est un sous-$\mathcal{O}_K$-module de V, il ne reste plus qu'à monter que $v(f(x+y)) \geqslant \frac{k}{e}$. Si x et y sont liés sur K, on a le résultat. Supposons donc (x, y) libre sur K.
Posons $P = f(Tx + y) \in K[T]$. Comme $f(x)$ est non nul par hypothèse, P est de degré d et son coefficient dominant est $f(x)$. Montrons que P est irréductible.
Supposons à l'inverse qu'on ait une racine α de P qui soit de degré $< d$ sur K. Alors $f(\alpha x_1 + y_1, ..., \alpha x_n + y_n) = 0$ et donc par l'hypothèse faite sur f on a :

$$\forall i \in \{1, ..., n\},\ \alpha x_i + y_i = 0.$$

Comme x est non nul, il vient $\alpha \in K$ et donc $\alpha x + y = 0$ contredit la liberté de (x, y).
Soient maintenant α une racine de P dans un corps de rupture et $L := K(\alpha)$. Montrons que :

$$f(Tx + y) = f(x) N_{L(T)/K(T)}(T - \alpha).$$

Le polynôme $f(x)^{-1} f(Tx + y)$ est unitaire, irréductible et a α pour racine : c'est donc son polynôme minimal. Mais α annule le terme constant du polynôme minimal sur $K(T)$ de $T - \alpha$ donc annule $N_{L(T)/K(T)}(T - \alpha)$. Donc on a :

$$f(x)^{-1} f(Tx + y) \mid N_{L(T)/K(T)}(T - \alpha).$$

Or ces deux polynômes sont unitaires et :

$$N_{L(T)/K(T)}(T-\alpha) = \det(TId_{L(T)} - m_\alpha),$$

où m_α est la multiplication par α. On en déduit qu'ils sont aussi de même degré, d'où l'égalité attendue.
De plus, $N_{L/K}(-\alpha) = f(y)f(x)^{-1}$, et donc, en notant toujours v la valuation de L qui prolonge celle de K, la définition de v donne $v(\alpha) \geqslant 0$, l'inégalité étant stricte si $v(f(y)) > v(f(x))$.
Notons X l'ensemble des K-morphismes de corps de L dans $\overline{K}$. Par séparabilité, et le degré de $1-\alpha$ étant $[L : K]$, l'application naturelle entre X et les conjugués de $1-\alpha$ est bijective. Par ailleurs, pour tout $\sigma \in X$, $v \circ \sigma$ est une valuation sur le corps de décomposition de P qui prolonge celle de K donc par unicité, $v \circ \sigma = v$. On a :

$$\begin{aligned} N_{L/K}(1-\alpha) &= \prod_{\sigma\in X} \sigma(1-\alpha) \\ &= \prod_{\sigma\in X} (1-\sigma(\alpha)) \\ &\in \mathcal{O}_L. \end{aligned}$$

Et si $v(f(y)) > v(f(x))$, alors on a même $N_{K/L}(1-\alpha) = 1 \pmod{\mathfrak{m}_K}$.
Ceci montre donc que $f(x+y) \in V^{(k)}$ et que, si $v(f(y)) > v(f(x))$, alors :

$$f(x+y) = f(x) \pmod{\pi^{k+1}\mathcal{O}_K}.$$

Montrons que $V^{(k)}$ est un $\mathcal{O}_K$-module libre de type fini. Si $(e_i)_{1\leqslant i\leqslant n}$ est la base canonique de V et $k \in \mathbb{Z}$, alors $\bigoplus_{i=1}^n \pi^k \mathcal{O}_K e_i$ est un $\mathcal{O}_K$-module libre de type fini. Il suffit donc de montrer que, pour tout m, il existe k tel que :

$$V^{(m)} \subset \bigoplus_{i=1}^n \pi^k \mathcal{O}_K e_i.$$

Pour tout $x \in V$, on notera $\nu(x) = \min\{v(x_i)\}$. Montrons que si une suite $(x_k)_k$ de V vérifie $\nu(x_k) \to -\infty$, $(v(f(x_k)))_k$ est non minorée, ce qui montrera le résultat. En posant $y_k = \pi^{-e\nu(x_k)} x_k$ on remarque qu'il suffit de montrer que si $(\nu(y_k))_k = 0$, alors $(v(f(y_k)))_k$ est majorée.
Supposons par l'absurde que cette suite soit non majorée, quitte à extraire on suppose qu'elle diverge vers $+\infty$, ce qui signifie que $f(y_k) \to 0$. Mais y_k est à valeur dans une partie compacte, donc on peut supposer qu'elle converge vers y, nécessairement non nul. Mais alors $f(y) = 0$, ce qui est absurde.

Montrons enfin $K \otimes_{\mathcal{O}_K} V^{(k)} = V$. Notons B l'application produit : $K \times V^{(k)} \to V$, qui est $\mathcal{O}_K$-bilinéaire. Soit $g : K \times V^{(k)} \to V$ une application $\mathcal{O}_K$-bilinéaire. On peut étendre g en $\widehat{g}$ définie sur V en posant, pour $x \in V$:

$$\widehat{g}(x) = g\left(\frac{1}{\pi^m}, \pi^m x\right),$$

où l'entier m est choisi de sorte que $\pi^m x \in V^{(k)}$. La $\mathcal{O}_K$-bilinéarité de g assure que $\widehat{g}(x)$ est bien définie, et $\mathcal{O}_K$-linéaire. On a alors $g = \widehat{g} \circ B$.
De plus si $g = h \circ B$ alors nécessairement $h = \widehat{g}$.
Autrement dit, (V, B) vérifie la propriété universelle du produit tensoriel. Donc :

$$K \otimes_{\mathcal{O}_K} V^{(k)} = V.$$

□

Soit f un polynôme homogène de degré d à n variables sur K, sans zéro non trivial dans des extensions de K de degré premier à d. On est alors dans les conditions du lemme 4.3. Pour finir la démonstration du théorème, il suffit de montrer que $d^2 \geqslant n$. Notons F le corps résiduel de K. On remarque déjà que si $\lambda \in \mathfrak{m}_K$ et $x \in V^{(0)}$, alors $\lambda x \in V^{(d)}$ et donc que $V^{(0)}/V^{(k)}$ est un F-espace vectoriel dès que $k \leqslant d$.

De plus, f induit une forme homogène, $f_0 : V^{(0)}/V^{(1)} \to F$ de degré d.
En effet, par le deuxième point du lemme 4.3, si $x \in V^{(0)}$ et $y \in V^{(1)}$, la valeur de $f(x + y) \pmod{\mathfrak{m}_K}$ est indépendante de y, donc f_0 est une application bien définie.
Reste à montrer que f_0 est bien une forme homogène.
Soit $(\varepsilon_i)_{1 \leqslant i \leqslant r} \in \left(V^{(0)}\right)^r$ tel que $(\varepsilon_i \pmod{V^{(1)}})_i$ soit une F-base de $V^{(0)}/V^{(1)}$; soient $(e_j)_{1 \leqslant j \leqslant n}$ la base canonique de V et $\lambda_{i,j} \in K$ tels que $\varepsilon_i = \sum_{i=1}^n \lambda_{i,j} e_j$.
On a alors :

$$\forall x_1, ..., x_r, f(x_1\varepsilon_1 + ... + x_r\varepsilon_r) = f(\sum_{i=1}^r \lambda_{i,1} x_i, \ldots, \sum_{i=1}^r \lambda_{i,n} x_i),$$

que l'on regarde comme un polynôme homogène en les x_i.
Pour pouvoir regarder modulo $\mathfrak{m}_K$ les coefficients du polynôme obtenu, il suffit de remarquer que si h est un polynôme homogène à r variables sur K dont l'image restreinte à $\mathcal{O}_K^r$ est dans $\mathcal{O}_K$, alors les cefficients de h sont dans $\mathcal{O}_K$.
Si h non nul est un tel polynôme, notons $a_1, ..., a_s \in K$ les coefficients de h de valuation minimale. Or $\mathcal{O}_K$ est infini, on peut donc trouver $(x_1, ..., x_r) \in \mathcal{O}_K^r$ qui n'annule pas la somme des monômes dont les coefficients sont les a_i. Et donc, on a trouvé $(x_1, ..., x_r) \in \mathcal{O}_K^r$ tel que la valuation de $h(x_1, ..., x_r)$ est

celle des a_i, qui est donc positive.

On remarque que f_0 n'a pas de zéro non trivial, en effet, s'il existe $x \in V^{(0)}$ tel que $f(x) \in \mathfrak{m}_K$, alors $x \in V^{(1)}$.
Or F est un corps fini donc est C_1. En regardant les formes :

$$(\pi^{-k} f)_0 : V^{(k)}/V^{(k+1)} \to F,$$

on a pour tout k :

$$\dim_F \left(V^{(k)}/V^{(k+1)}\right) \leqslant d.$$

Or, si K' est un corps, E un K'-espace vectoriel de dimension finie et G un sous-espace vectoriel de E, alors E/G est un K'-espace vectoriel de dimension $\dim_{K'}(E) - \dim_{K'}(G)$. De plus, pour tout $k \leqslant d$ on a :

$$V^{(0)}/V^{(k)} \simeq \left(V^{(0)}/V^{(k+1)}\right) / \left(V^{(k)}/V^{(k+1)}\right).$$

Et donc, par récurrence :

$$\dim_F \left(V^{(0)}/V^{(d)}\right) = \dim_F \left(V^{(0)}/V^{(1)}\right) + \dim_F \left(V^{(1)}/V^{(2)}\right) + \ldots + \dim_F \left(V^{(d-1)}/V^{(d)}\right).$$

Ce qui donne :

$$\begin{aligned} \dim_K (V) &= \dim_K \left(K \otimes_{\mathcal{O}_K} V^{(0)}\right) \\ &= \mathrm{rg}_{\mathcal{O}_K} \left(V^{(0)}\right) \\ &= \dim_F \left(V^{(0)}/\mathfrak{m}_K V^{(0)}\right) \\ &= \dim_F \left(V^{(0)}/V^{(d)}\right) \\ &\leqslant d^2, \end{aligned}$$

et permet de conclure.

Références

1. K. Kato, T. Kuzumaki, The dimension of fields and algebraic K-theory, J. Number Theory 24 (1986), no. 2, 229-224.
2. S. Lang, On quasi-algebraic closure, Ann. of Math. (2) 55 (1952), 373-390.
3. G. Terjanian, Un contre-exemple à la conjecture d'Artin, C. R. Acad. Sci. Paris Sér. A-B 262 (1966), A612.
4. N. Koblitz, p-adic numbers, p-adic analysis, and zeta-functions (1984).
5. Y. Amice, Les nombres p-adiques (1975).
6. O. Wittenberg, La connexité rationnelle en arithmétique, Variétés rationellement connexes : aspects géométriques et arithmétiques, Panoramas et Synthèses 31, Soc. Math. de Fr. (2010), 61-114.
7. Y. Alemu, On zeros of forms over local fields, Acta Arith. 45 (1985), no. 2, 163–171.
8. G. I. Arkhipov et A. A. Karatsuba, On local representation of zero by a form, Izv. Akad. Nauk SSSR Ser. Mat. 45 (1981), no. 5, 948–961 (en russe), traduit dans Math. USSR Izv. 19 (1982), no. 2, 231–240.
9. D. J. Lewis, Cubic homogeneous polynomials over p-adic number fields, Ann. of Math. (2) 56 (1952), no. 3, 473–478.
10. H. Hasse, Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper, J. reine angew. Math. 153 (1924), 113–130.