Thème de recherche n°2: les BRENOMS

Vincent Lefèvre

24, rue Louis Blanc
31400 Toulouse

vlefevre@ens-lyon.fr

Janvier 1994

0 Introduction

Dans le sujet, les brenoms ont été définis en base 10. Mais on peut définir des brenoms en base k, pour tout entier $k \geq 2$. Et on peut définir de même la somme et le produit de 2 brenoms en base k, selon les modes opératoires habituels en base k (ces deux opérations seront définies plus précisément au §1.2). Mais on s'intéressera un peu plus à la base 10, et aux bases p, pour p premier (§5, §6).

Attention! on verra que, contrairement à l'anneau $\mathbb{Z}$ des entiers relatifs, l'anneau des brenoms dépend de la base choisie (i.e. ces anneaux ne sont pas tous isomorphes). Ici, la base n'est donc plus seulement un système de notation.

On cherchera d'abord quelle est la structure de l'ensemble des brenoms muni de l'addition et de la multiplication (§2): a-t-on un groupe? un anneau? un corps? quel est l'ensemble des brenoms inversibles? Puis on définira des brenoms *fractionnaires*; on obtiendra ainsi un ensemble encore plus grand, sur lequel on définira une distance ultramétrique (§3). On s'intéressera ensuite aux brenoms dont l'écriture est périodique à partir d'un certain rang (§4). Puis on étudiera le cas où la base est un nombre premier (§5), car on peut ramener l'étude des brenoms en base k à celle des brenoms en base p, où p décrit l'ensemble des facteurs premiers de k (§6). On pourra alors résoudre certaines équations en base k (en particulier, on cherchera les racines carrées d'un brenom), en se ramenant aux cas p premier (§7).

Remarque: le résultat le plus important pour l'étude des brenoms est le §6.2. Certaines sections situées avant auraient pu être étudiées après (j'ai préféré laisser les résultats dans l'ordre dans lequel je les ai trouvés, jusqu'au §3.2). Mais les paragraphes §6.1 et §6.2 reposent uniquement sur §1, §2.1, et pour k premier: §2.2, §2.5, §2.6, §3.1 et §3.2.

1 Définitions, notations

1.1 Ensemble des brenoms

On considère une base $k \geq 2$. On appelle *brenom* a une suite $(a_n)_{n\in\mathbb{N}}$ où $a_n \in [\![0; k-1]\!]$. Il sera noté $\ldots a_3 a_2 a_1 a_0$. On note $\mathbb{B}(k)$, ou plus simplement $\mathbb{B}$ (s'il n'y a pas d'ambiguïté, par exemple si k est fixé), l'ensemble des brenoms en base k.

On identifiera les brenoms a pour lesquels la suite (a_n) est nulle à partir d'un certain rang aux entiers naturels. Ces brenoms seront appelés brenoms *naturels*, et leur ensemble sera noté $\mathbb{N}$.

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

On dira qu'un brenom a est *périodique* lorsque la suite (a_n) est périodique à partir d'un certain rang, et on note $\mathbb{P}$ l'ensemble des brenoms périodiques. Si la suite (a_n) est immédiatement périodique, on dira que le brenom a est *immédiatement périodique*. Les brenoms périodiques seront notés: $\ldots(a_{n+p-1}\ldots a_{n+1}a_n)a_{n-1}\ldots a_1 a_0$, la séquence entre parenthèses étant une partie périodique. On a l'inclusion évidente: $\mathbb{N} \subset \mathbb{P}$.

Remarque: les brenoms en base k sont plus couramment appelés *nombres k-adiques*; mais pour k non premier, je continuerai à les appeler *brenoms* pour bien les différencier des nombres p-adiques (p premier).

1.2 Addition et multiplication

On définit la somme $c = a + b$ de deux brenoms a et b de la façon suivante:

$$q_{-1} = 0 \text{ et } \forall\, n \in \mathbb{N},\ c_n + q_n k = q_{n-1} + a_n + b_n \text{ avec } c_n \in [\![0; k-1]\!]$$

On définit le produit $c = a.b$ de deux brenoms a et b de la façon suivante:

$$q_{-1} = 0 \text{ et } \forall\, n \in \mathbb{N},\ c_n + q_n k = q_{n-1} + \sum_{i=0}^{n} a_i b_{n-i} \text{ avec } c_n \in [\![0; k-1]\!]$$

1.3 Complémentaire

On définit le complémentaire $\overline{a}$ d'un brenom a de la façon suivante:

$$\overline{a} = (\overline{a_n})_{n\in\mathbb{N}} \text{ avec } \overline{a_n} = k - 1 - a_n$$

Par exemple, en base 10, $\overline{1234} = \ldots 9998765$.

1.4 Congruences modulo k^n

Soit $n \in \mathbb{N}^*$. On note $[a]_n = (a_i)_{i<n}$ et $\mathbb{B}_n = \{[a]_n\}$.

L'application $[.]_n : \mathbb{B} \to \mathbb{B}_n$ définit une relation d'équivalence sur $\mathbb{B}$: $a \mathrel{\mathcal{R}} b \Leftrightarrow [a]_n = [b]_n$. Cette relation d'équivalence sera appelée “congruence modulo k^n”, comme sur $\mathbb{Z}$. On identifiera les éléments de $\mathbb{B}_n$ aux classes d'équivalence.

D'après les définitions de l'addition et de la multiplication (données au §1.2), il suffit de connaître les n premiers chiffres de a et de b pour connaître les n premiers chiffres de la somme et du produit. L'addition et la multiplication sur $\mathbb{B}$ sont donc compatibles avec la relation d'équivalence définie ci-dessus, i.e. si $[a]_n = [a']_n$ et $[b]_n = [b']_n$, alors $[a+b]_n = [a'+b']_n$ et $[ab]_n = [a'b']_n$. On peut alors définir sur $\mathbb{B}_n$ une addition et une multiplication:

$$[a]_n + [b]_n = [a+b]_n \quad , \quad [a]_n[b]_n = [ab]_n$$

On fera les identifications suivantes: $\mathbb{B}_n = \mathbb{B}/k^n\mathbb{B} = \mathbb{Z}/k^n\mathbb{Z}$.

On a la propriété suivante, qui sera utile par la suite :

$$\boxed{a = b \iff \forall\, n \in \mathbb{N}^*,\ [a]_n = [b]_n} \tag{1}$$

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

1.5 Notations

On note $\overline{\mathbb{N}} = \mathbb{N} \cup \{+\infty\}$ et $\overline{\mathbb{Z}} = \mathbb{Z} \cup \{-\infty; +\infty\}$.

On pose $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

On pose

$$\varepsilon_p = 1 + \delta_{p,2}$$

que l'on notera aussi ε (pour une question de clarté) quand il est en indice ou en exposant.

La notation a_n peut désigner soit un chiffre d'un brenom a (surtout au début), soit un terme d'une suite de brenoms (qui peut être aussi noté a^n); $a^{(p)}$ (avec des parenthèses) désignera encore autre chose (cf §6.2).

Si a est un brenom, a pourra aussi désigner une classe d'équivalence s'il n'y a pas d'ambiguïté. Par exemple, si f est une fonction dont l'ensemble de départ est $\mathbb{B}_n$, on pourra écrire $f(a)$ au lieu de $f([a]_n)$.

2 Structure algébrique de l'ensemble des brenoms

2.1 Structure d'anneau commutatif

$(\mathbb{B}, +)$ est un groupe abélien :

- Commutativité: évidente, d'après la définition de l'addition de deux brenoms.
- Associativité: on utilise l'associativité de l'addition sur $\mathbb{Z}/m\mathbb{Z}$ pour tout m, et la propriété (1) appliquée aux brenoms $(a + b) + c$ et $a + (b + c)$.
- Elément neutre: 0.
- Opposé d'un brenom a: $-a = \overline{a} + 1$.

$(\mathbb{B}, +, .)$ est un anneau commutatif:

- $(\mathbb{B}, +)$ est un groupe abélien.
- Commutativité de la multiplication: évidente, d'après la définition.
- Associativité: on utilise la propriété (1), comme pour l'addition.
- Distributivité par rapport à l'addition: on utilise encore la propriété (1).
- Elément neutre: 1.

On identifiera l'anneau $(\mathbb{Z}, +, .)$ au sous-anneau de $(\mathbb{B}, +, .)$ engendré par 1.

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

2.2 Cas où la base k est un nombre primaire

On rappelle qu'un nombre primaire est un nombre de la forme p^α, où p est un nombre premier et α un entier strictement positif.

On peut alors définir la p-valuation d'un brenom a, comme sur $\mathbb{Z}$:

$$\mathrm{v}_p(a) = \sup\{n \in \mathbb{N} \mid a \equiv 0 \pmod{p^n}\} \in \overline{\mathbb{N}}$$

Si $a \neq 0$ et $b \neq 0$, alors $\mathrm{v}_p(ab) = \mathrm{v}_p(a) + \mathrm{v}_p(b) \neq +\infty$, donc $ab \neq 0$. Par conséquent, si k est un nombre primaire, alors $(\mathbb{B}, +, .)$ est un anneau intègre.

Remarque: on verra au §2.6 qu'on aurait pu se ramener au cas où la base k est un nombre premier.

2.3 Cas où la base k n'est pas un nombre primaire

Dans ce cas, il existe deux entiers p et q premiers entre eux et ≥ 2 tels que $k = pq$. Cherchons deux brenoms a et b non nuls tels que $ab = 0$.

Soient $a_0 = p$ et $b_0 = q$. Construisons (a_n, b_n) par récurrence, en utilisant la définition de la multiplication donnée au §1.2:

Supposons que $a_0,\ a_1,\ \ldots,\ a_{n-1}$ et $b_0,\ b_1,\ \ldots,\ b_{n-1}$ soient construits tels que $[ab]_{n-1} = 0$. Or

$$\forall\, x_n \in \mathbb{Z}/k\mathbb{Z},\ \ \exists\ (a_n, b_n) \in (\mathbb{Z}/k\mathbb{Z})^2,\ \ q.a_n + p.b_n = x_n$$

On pourra donc trouver a_n et b_n tels que $[ab]_n = 0$, et on aura $ab = 0$ d'après la propriété (1).

Par conséquent, si k n'est pas un nombre primaire, alors l'anneau $(\mathbb{B}, +, .)$ n'est pas intègre.

2.4 Conclusion

On vient de trouver une C.N.S. pour que l'anneau $(\mathbb{B}, +, .)$ soit intègre :

Théorème 2.1 *L'anneau $(\mathbb{B}, +, .)$ est intègre ssi k est un nombre primaire.*

Ainsi, on voit bien que les anneaux $(\mathbb{B}(k), +, .)$ ne sont pas tous isomorphes.

Cherchons maintenant l'ensemble des brenoms inversibles.

2.5 Ensemble des brenoms inversibles

Soit $a \in \mathbb{B}$. Cherchons si a admet un inverse, i.e. cherchons $x \in \mathbb{B}$ tel que $ax = 1$.

Là encore, trouver x revient à résoudre une succession d'équations dans $\mathbb{Z}/k\mathbb{Z}$ de la forme: $a_0 x_n = c_n$ où x_n est l'inconnue et c_n dépend de $[a]_n$ et $[x]_{n-1}$. Puisque $c_0 = 1$, alors pour que a admette un inverse, il faut que $a_0 \wedge k = 1$. Réciproquement, si $a_0 \wedge k = 1$, alors l'équation $a_0 x_n = c_n$ aura toujours une solution (unique). D'où le théorème :

Théorème 2.2 *Un brenom a est inversible ssi $a_0 \wedge k = 1$.*

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

2.6 Cas où la base est une puissance

Soient $k \geq 2$ et $\alpha \in \mathbb{N}^*$. Considérons l'application $\varphi : \mathbb{B}(k) \to \mathbb{B}(k^\alpha)$ définie par $b = \varphi(a)$ avec :

$$\forall\, n \in \mathbb{N}, \quad b_n = \sum_{i=0}^{\alpha-1} a_{n\alpha+i} k^i$$

On peut vérifier que cette application φ est un isomorphisme.

3 Brenoms fractionnaires

3.1 Définition, structure de l'ensemble

On pourrait penser à généraliser la notion de brenom en introduisant une "partie fractionnaire" illimitée, comme on peut le faire pour les entiers relatifs (on obtient alors l'ensemble des réels; mais en pratique, pour la construction de cet ensemble, on s'y prend autrement). Mais on aurait du mal à définir une multiplication. En revanche, on peut essayer d'étudier le cas où la "partie fractionnaire" reste "limitée" (i.e. à partir d'un certain rang, il n'y a que des 0). On verra que, d'après les propriétés de l'ensemble ainsi obtenu (notamment en ce qui concerne la topologie), il s'agit de la généralisation la plus intéressante.

Pour cela, considérons les ensembles $k^n\mathbb{B}$ pour $n \leq 0$, définis, de façon analogue à $\mathbb{B}$ mais avec une partie fractionnaire de $-n$ chiffres, par les suites $(a_i)_{i \in [\![n;+\infty[\![}$. En ajoutant des termes nuls aux suites, on a $\mathbb{B} \subset k^{-1}\mathbb{B} \subset k^{-2}\mathbb{B} \subset \ldots$, et on peut définir les éléments k^n par $k^n_i = \delta_{ni}$ (symbole de Kronecker). On peut définir une addition, loi interne sur $k^n\mathbb{B}$, et une multiplication, loi interne sur la réunion des ensembles $k^n\mathbb{B}$, que l'on notera $\mathbb{A}$. On a $k^n\mathbb{B} = \{k^n x\}_{x \in \mathbb{B}}$, ce qui justifie les notations employées. On peut facilement vérifier que l'ensemble $\mathbb{A}$ muni de l'addition et de la multiplication (définies précédemment) est un anneau, que l'on appellera *anneau des brenoms fractionnaires.*

On peut généraliser la définition de $[.]_n$ au cas $n \in \mathbb{Z}$ (et non plus seulement $n \in \mathbb{N}$). De même, §2.6 se généralise en prenant l'ensemble $\mathbb{A}$ au lieu de $\mathbb{B}$.

Remarque: au §4.6, on s'intéressera à l'ensemble des brenoms fractionnaires périodiques et on verra que c'est un corps isomorphe à $\mathbb{Q}$ (et il sera noté $\mathbb{Q}$).

3.2 Corps p-adiques

Considérons le cas où $\mathbb{B}(k)$ est un anneau intègre, i.e. k est un nombre primaire: $k = p^\alpha$. D'après §2.6, on peut se ramener au cas où $\alpha = 1$, i.e. k est un nombre premier p. $\mathbb{B}(p)$ sera alors noté $\mathbb{Z}_p$, anneau des entiers p-adiques. Puisque cet anneau est intègre, on peut construire son corps des fractions, noté $\mathbb{Q}_p$: corps p-adique. Puisque les éléments non inversibles a de $\mathbb{Z}_p$ sont tels que $a_0 = 0$, alors $\mathbb{Q}_p = \mathbb{A}(p)$.

Théorème 3.1 *Si la base est un nombre premier p, alors l'anneau $\mathbb{A}(p)$ des brenoms fractionnaires est un corps: c'est le corps p-adique.*

Tout élément $a \in \mathbb{Q}_p$ s'écrit de façon unique $a = p^n u$ avec $n \in \mathbb{Z}$ et $u \in \mathbb{Z}_p^*$ (élément inversible de l'anneau $\mathbb{Z}_p$).

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

3.3 Valuation

3.3.1 Définition

Soit $a \in \mathbb{A}(k)$. On pose :

$$\mathrm{v}(a) = \sup\{n \in \mathbb{Z} \mid [a]_n = 0\} \ \in \ \mathbb{Z} \cup \{+\infty\}$$

On a :

$$\begin{cases} \mathrm{v}(a) = +\infty \ \Leftrightarrow \ a = 0. \\ \mathrm{v}(ab) \geq \mathrm{v}(a) + \mathrm{v}(b), \text{ et si } k \text{ est premier, il y a égalité.} \\ \mathrm{v}(a+b) \geq \inf(\mathrm{v}(a), \mathrm{v}(b)), \text{ et si } \mathrm{v}(a) \neq \mathrm{v}(b), \text{ il y a égalité.} \end{cases}$$

et

$$\mathrm{v}(a) \geq 0 \ \Leftrightarrow \ a \in \mathbb{B}(k)$$

Si k est un nombre premier, $\mathrm{v}(a)$ est appelée *valuation* de a.

3.3.2 Valuation de $n!$

Soit p un nombre premier. On note $\mathrm{v}_p(n!)$ la p-valuation de $n!$, i.e. l'exposant de p dans la décomposition de $n!$ en facteurs premiers.

Théorème 3.2

$$v_p(n!) \leq \frac{n}{p-1}$$

Démonstration :

$$\mathrm{v}_p(n!) \ = \ \sum_{i=1}^{+\infty} \left[\frac{n}{p^i}\right] \ \leq \ \frac{n}{p} \sum_{i=0}^{+\infty} \frac{1}{p^i} \ = \ \frac{n}{p} \, \frac{1}{1-1/p} \ = \ \frac{n}{p-1}$$

Théorème 3.3

$$v_p(n!) \sim \frac{n}{p-1} \ \ \textit{quand} \ \ n \to +\infty$$

Démonstration :

$$\mathrm{v}_p(n!) \ \geq \ \sum_{i=1}^{m} \frac{n}{p^i} - m \ = \ \frac{n}{p} \, \frac{1-1/p^m}{1-1/p} - m \ = \ \frac{n}{p-1} - \frac{n.p^{-m}}{p-1} - m$$

On prend m tel que $p^m \leq n < p^{m+1}$. D'après le théorème (3.2) :

$$\left|\frac{\mathrm{v}_p(n!)}{n} - \frac{1}{p-1}\right| \ \leq \ \frac{p^{-m}}{p-1} + \frac{m}{n} \ \leq \ p^{-m}\left(\frac{1}{p-1} + m\right) \ \to \ 0 \text{ quand } m \to +\infty.$$

Or quand $n \to +\infty$, $m \to +\infty$. Donc

$$\lim_{n\to+\infty} \frac{\mathrm{v}_p(n!)}{n} = \frac{1}{p-1}$$

d'où le théorème.

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

3.4 Espace ultramétrique

3.4.1 Définitions, propriétés

Soit $\alpha \in \,]0;1[$. On définit sur $\mathbb{A}$ une distance :

$$\forall\,(x,y) \in \mathbb{A}^2,\ \mathrm{d}(x,y) = \alpha^{\mathrm{v}(x-y)}$$

On a évidemment :

$$\mathrm{d}(x,y) = 0 \quad \Leftrightarrow \quad x = y$$

et

$$\mathrm{d}(x,y) = \mathrm{d}(y,x)$$

De plus,

$$\mathrm{d}(x,y) \leq \sup(\mathrm{d}(x,z), \mathrm{d}(y,z))$$

car

$$\mathrm{v}(x-y) \geq \inf(\mathrm{v}(x-z), \mathrm{v}(z-y))$$

Muni de cette distance, $\mathbb{A}$ est donc un espace ultramétrique, et cette distance définit une topologie sur $\mathbb{A}$.

Pour $a \in \mathbb{A}$ et $n \in \overline{\mathbb{Z}}$, on pose

$$B(a,n) = \{x \in \mathbb{A} \mid [x]_n = [a]_n\}$$

($B(a,-\infty) = \mathbb{A}$ et $B(a,+\infty) = \{a\}$). Ces ensembles seront appelés *boules* d'ordre n. Ce sont des fermés; pour $n \neq +\infty$, ce sont aussi des ouverts; pour $n \in \mathbb{Z}$, ce sont des compacts (démonstration: cf §3.4.2 pour $B(0,0) = \mathbb{B}$). On a :

$$\forall\,x \in B(a,n),\ B(x,n) = B(a,n)$$

Attention! si une suite (x^n) de rationnels converge vers un rationnel a pour la topologie p-adique, et vers un rationnel b pour la topologie classique, alors on n'a pas forcément $a = b$ (cf §3.6.7).

3.4.2 Propriétés de $\mathbb{B}$ et $\mathbb{A}$

$\mathbb{B}$ est compact, i.e. de toute suite à éléments dans $\mathbb{B}$, on peut extraire une sous-suite convergente dans $\mathbb{B}$: en effet, soit (x^n) une suite à éléments dans $\mathbb{B}$. Il existe $a_0 \in [\![0;k-1]\!]$ et une sous-suite $(x^{\varphi(n)})$ tels que $\forall\,n,\ [x^{\varphi(n)}]_1 = [a]_1$. De même, il existe $a_1 \in [\![0;k-1]\!]$ et une sous-suite $(x^{\varphi(\psi(n))})$ tels que $\forall\,n,\ [x^{\varphi(\psi(n))}]_2 = [a]_2$. On obtient ainsi une suite $(a_n)_{n\in\mathbb{N}}$ à éléments dans $[\![0;k-1]\!]$, qui définit un élément $a \in \mathbb{B}$. En prenant le n-ième terme de chaque sous-suite définie ci-dessus, on obtient une sous-suite de (x^n) convergeant vers $a \in \mathbb{B}$.

$\mathbb{B}$ est complet, car compact.

$\mathbb{A}$ est complet: soit (x^n) une suite de Cauchy. Alors $\exists m,\ \forall\,n \geq m,\ \forall\,q \in \mathbb{N},\ \mathrm{d}(x^n, x^{n+q}) \leq 1$. En particulier, $\mathrm{d}(x^m, x^{m+q}) \leq 1$, i.e. $[x^m]_0 = [x^{m+q}]_0$. Or la suite $(x^{m+q} - x^m)_{q\in\mathbb{N}}$ de $\mathbb{B}^{\mathbb{N}}$ converge dans $\mathbb{B}$, car c'est une suite de Cauchy et $\mathbb{B}$ est complet. Donc la suite (x^n) converge dans $\mathbb{A}$.

De plus, puisque $\mathbb{A}$ est un espace ultramétrique complet, une suite (x^n) converge ssi

$$\lim_{n\to+\infty} (x^{n+1} - x^n) = 0$$

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

Par conséquent, une série converge ssi son terme général tend vers 0, toute "sous-série" d'une série convergente est convergente, et toute série est commutativement convergente. Le produit de Cauchy de deux séries convergentes converge vers le produit des limites de ces deux séries.

On peut facilement vérifier que $\mathbb{N}$ et $\mathbb{Z}$ sont denses dans $\mathbb{B}$, et que $\mathbb{Q}$ est dense dans $\mathbb{A}$.

3.4.3 Fonctions continues

Soit une application $f : D \to \mathbb{A}$ où $D \subset \mathbb{A}$. Soit $a \in D$.

$$f \text{ est continue en } a \text{ ssi } \forall\, n \in \mathbb{Z},\ \exists\, p \in \mathbb{Z},\ \forall\, x \in B(a,p) \cap D,\ f(x) \in B(f(a),n)$$

On pose :

$$p(n) \ = \ \inf \{p \in \mathbb{Z} \mid \forall\, x \in B(a,p) \cap D,\ f(x) \in B(f(a),n)\} \ \in \ \overline{\mathbb{Z}}.$$

C'est une fonction croissante de n (qui dépend de a).

$$f \text{ est continue en } a \text{ ssi } \forall\, n \in \mathbb{Z},\ p(n) \neq +\infty.$$

3.4.4 Dérivabilité

Soit $a \in \operatorname{Int} D$ (intérieur de D), et $\ell = \lim_{n \to +\infty} p(n)$.

- Si $\ell \neq +\infty$, f est constante et donc continue sur $B(a,\ell) \cap D$, et f est dérivable sur $\operatorname{Int}(B(a,\ell) \cap D)$.
- Si $\ell = +\infty$, pour que f soit dérivable en a, il est nécessaire que $n - p(n)$ ait une limite $m \in \mathbb{Z} \cup \{+\infty\}$ quand $n \to +\infty$. Si f est dérivable en a, on a: $\mathrm{v}(f'(a)) = m$.

En effet, pour n_0 tel que $B(a, p(n_0) - 1) \subset D$, on a pour tout $n \geq n_0$:

$$\begin{cases} \exists\, h \in \mathbb{A},\ \mathrm{v}(h) = p(n) \text{ et } \mathrm{v}(\frac{f(a+h)-f(a)}{h}) \geq n - p(n) \\ \exists\, h \in \mathbb{A},\ \mathrm{v}(h) = p(n) - 1 \text{ et } \mathrm{v}(\frac{f(a+h)-f(a)}{h}) \leq n - p(n) \end{cases}$$

Attention! si $f' = 0$ sur une boule, f n'est pas forcément constante sur cette boule.

Exemple :
Soit $n \in \mathbb{Z} \cup \{+\infty\}$, et $m \in \mathbb{Z}$ tel que $m > n$. Soit $f : B(a,n) \to \{x \in \mathbb{A} \mid \forall\, k \geq m,\ x_k = 0\}$ définie par $f(x) = [x]_m$. Si $\mathrm{v}(h) \geq m$, $[x+h]_m = [x]_m$, donc $\frac{f(x+h)-f(x)}{h} = 0$. Donc $f'(x) = 0$, bien que f ne soit pas constante.

Ceci vient du fait que les boules d'ordre $n \in \mathbb{Z} \cup \{-\infty\}$ sont à la fois des ouverts et des fermés, et sont donc non connexes.

3.4.5 Connexité

Théorème 3.4 *Tout sous-ensemble E de $\mathbb{A}$ contenant au moins 2 éléments est non connexe.*

Démonstration :

Soient x et y deux éléments distincts de E. Soit $n \in \mathbb{Z}$ tel que $y \notin B(x,n)$. Soit $V = B(x,n)$ et $W = \mathbb{A} \backslash V$. V et W sont deux ouverts disjoints, et $\{V \cap E\ ,\ W \cap E\}$ réalise une partition de E, ce qui prouve le théorème.

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

3.5 Brenoms algébriques, brenoms transcendants

Soit $a \in \mathbb{A}$. On pose :

$$\mathcal{I} \;=\; \{P \in \mathbb{Q}[X] \mid P(a) = 0\}$$

$\mathcal{I}$ est un idéal de $\mathbb{A}$, et puisque $\mathbb{Q}[X]$ est un anneau principal, il existe un polynôme $P \in \mathbb{Q}[X]$ tel que $\mathcal{I} = P.\mathbb{Q}[X]$. Si $P \neq 0$, on pourra choisir P unitaire, et il y a unicité; on dit alors que a est *algébrique*, que P est le polynôme minimal de a, et que $\deg P$ est le degré de a. Si $P = 0$, alors $\mathcal{I} = \{0\}$; on dit alors que a est *transcendant*.

Puisque l'ensemble des brenoms algébriques est dénombrable, et celui des brenoms fractionnaires est non dénombrable, alors on sait qu'il existe des brenoms transcendants. On donnera plus tard des exemples de brenoms transcendants (cf §5.8 et §6.7).

3.6 Séries entières

3.6.1 Définitions

On appelle *série entière* de $\mathbb{A}$ toute série

$$S(x) = \sum_{i=0}^{+\infty} a_i x^i$$

où $(a_i)_{i\in\mathbb{N}}$ est une suite d'éléments de $\mathbb{A}$.

On appelle *valuation* de S l'élément

$$\operatorname{val} S = \inf\{i \in \mathbb{N} \mid a_i \neq 0\} \in \overline{\mathbb{N}}$$

3.6.2 Disque et rayon de convergence

On rappelle que dans $\mathbb{A}$, une série converge ssi son terme général converge vers 0.

Soit $S(x) = \sum_{i=0}^{+\infty} a_i x^i$ une série entière de $\mathbb{A}$. Soit

$$n_S = n = \inf\left\{m \in \mathbb{Z} \mid \lim_{i\to+\infty} \mathrm{v}(a_i) + im = +\infty\right\} \in \overline{\mathbb{Z}}$$

On appelle *rayon de convergence* le nombre $R_S = \alpha^n \in \overline{\mathbb{R}_+}$ (il s'agit du α défini au §3.4).

Alors l'ensemble des $x \in \mathbb{A}$ pour lesquels $S(x)$ converge est le disque de centre 0 et de rayon R_S. Cet ensemble est appelé *disque de convergence* et noté D_S.

En particulier :

- Si $n = -\infty$, $D_S = \mathbb{A}$ (rayon de convergence infini).
- Si $n \in \mathbb{Z}$, $D_S = k^n\mathbb{B}$.
- Si $n = +\infty$, $D_S = 0$ (rayon de convergence nul).

D'après ce qui précède, pour $m \geq n_S$ (avec $m \in \mathbb{Z}$), $\mathrm{v}(S(x))$ est minorée sur $k^m\mathbb{B}$.

On dira qu'une fonction $f : \mathbb{A} \to \mathbb{A}$ est *développable en série entière* lorsqu'il existe une série entière S de rayon de convergence non nul telle que $\forall\, x \in D_S,\ f(x) = S(x)$.

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

3.6.3 Equivalent de $S(x)$ quand $x \to 0$

Soit une série entière $f(x) = \sum_{i=0}^{+\infty} a_i x^i$ telle que $n_f \neq +\infty$ et $\exists\, j \in \mathbb{N},\ a_j \neq 0$. Soit $\ell = \operatorname{val} f$.

On a :

$$f(x) = a_\ell x^\ell + g(x) \ \text{ avec } \ \operatorname{val} g > \ell$$

On peut écrire :

$$f(x) = x^\ell [a_\ell + x.h(x)]$$

où h est une série entière.

Soient $m \in \mathbb{Z}$ tel que $m \geq n_f$, et $q \in \mathbb{Z}$ un minorant de $\mathrm{v}(h(x))$ sur $k^m\mathbb{B}$. On a alors :

$$\mathrm{v}(g(x)) - \mathrm{v}(a_\ell x^\ell) = \mathrm{v}(x) + \mathrm{v}(h(x)) - \mathrm{v}(a_\ell) \geq \mathrm{v}(x) + q - \mathrm{v}(a_\ell)$$

Donc $\mathrm{v}(g(x)) - \mathrm{v}(a_\ell x^\ell) \to +\infty$ quand $x \to 0$, i.e. $f(x) \sim a_\ell x^\ell$ quand $x \to 0$.

3.6.4 Unicité du développement en série entière

Soient une série entière $f(x) = \sum_{i=0}^{+\infty} a_i x^i$ telle que $n_f \neq +\infty$, et $m \in \mathbb{Z}$ tel que $m \geq n_f$.

D'après §3.6.3, si $\forall\, x \in k^m\mathbb{B},\ f(x) = 0$, alors $\forall\, i \in \mathbb{N},\ a_i = 0$.

On en déduit que si une fonction f, définie sur un voisinage de 0 (ou sur un ensemble pour lequel 0 est un point d'accumulation), est développable en série entière, alors son développement en série entière est unique.

3.6.5 Dérivation d'une série entière

Théorème 3.5 *Soit une série entière $f(x) = \sum_{i=0}^{+\infty} a_i x^i$ de rayon de convergence non nul. Alors f est dérivable et*

$$f'(x) = \sum_{i=0}^{+\infty} a_i.i.x^{i-1}$$

Démonstration :

On fixe $x \in D_f$. Soit $M : \mathbb{Z} \to \mathbb{Z}$ telle que

$$\forall\, i > M(n),\ \mathrm{v}(a_i x^i) > n$$

Donc

$$[f(x)]_n = \sum_{i=0}^{M(n)} a_i x^i$$

h désigne un élément inversible de $\mathbb{A}$ tel que $\mathrm{v}(h) > \mathrm{v}(x)$, si bien que la série $f(x+h)$ converge. On pose :

$$T(h) = \frac{f(x+h) - f(x)}{h}$$

On a alors :

$$T(h) = \sum_{i=1}^{+\infty} a_i \frac{(x+h)^i - x^i}{h}$$

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

et

$$[T(h)]_n = \sum_{i=1}^{M(n-\mathrm{v}(x))} a_i \frac{(x+h)^i - x^i}{h}$$

Quand $h \to 0$, le second membre tend vers :

$$\sum_{i=1}^{M(n-\mathrm{v}(x))} a_i.i.x^{i-1}$$

donc $T(h)$ reste dans une boule d'ordre n quand $h \to 0$, et ceci pour tout $n \in \mathbb{Z}$. Donc $T(h)$ a une limite quand $h \to 0$, qui est :

$$f'(x) = \sum_{i=0}^{+\infty} a_i.i.x^{i-1}$$

3.6.6 Exemples de séries entières

Cf exponentielles au §5.7.2.

On peut construire d'autres séries entières, comme sur $\mathbb{R}$, ayant certaines propriétés. En général, les séries entières à coefficients dans $\mathbb{Q}$ auront les mêmes propriétés algébriques (i.e. qui ne font pas intervenir la topologie) sur $\mathbb{R}$ et sur un corps p-adique. Il en est de même si les coefficients s'expriment à l'aide d'éléments de $\mathbb{Q}$ et de paramètres réels ou p-adiques (cf exponentielles). Il suffira alors de connaître certains résultats sur $\mathbb{R}$ pour les exploiter sur les corps p-adiques. La plus grande différence est le disque de convergence (car il est lié à la topologie).

Par exemple, considérons le développement en série entière de la fonction $f(x) = \sqrt{1+x}$, définie sur un sous-ensemble de $\mathbb{R}$. On a :

$$\sqrt{1+x} = 1 + \sum_{n=1}^{+\infty} \mathrm{C}_{2n-2}^{n-1} \frac{(-1)^{n-1}}{n.2^{2n-1}} x^n$$

Dans un corps p-adique, le membre de droite (s'il y a convergence) définit une des deux racines carrées de $1+x$: en effet, si on élève au carré la série entière définie ci-dessus, on trouve la série entière $1+x$ (il s'agit ici d'opérations effectuées sur des séries entières, et non sur des nombres p-adiques).

Puisque $\mathrm{C}_{2n-2}^{n-1}/n = \mathrm{C}_{2n-2}^{n}/(n-1)$ et $n \wedge (n-1) = 1$, alors $\mathrm{C}_{2n-2}^{n-1}/n \in \mathbb{N}$. Donc si $p \neq 2$: si $\mathrm{v}(x) \geq 1$, alors la série converge (il y a en fait équivalence); et si $p = 2$: si $\mathrm{v}(x) \geq 3$, alors la série converge (il y a encore équivalence). Ainsi, on peut retrouver partiellement le résultat de §5.5.

3.6.7 Série entière de $\sqrt{(1+x)}$ pour les topologies p-adique et classique

Considérons la série entière

$$1 + \sum_{n=1}^{+\infty} \mathrm{C}_{2n-2}^{n-1} \frac{(-1)^{n-1}}{n.2^{2n-1}} x^n$$

où $x \in \mathbb{Q}$. Elle converge dans $\mathbb{R}$ (pour la topologie classique) ssi $|x| < 1$. Elle converge dans $\mathbb{Q}_p$ (pour la topologie p-adique) ssi $\mathrm{v}_p(x) \geq v$, où

$$v = \begin{cases} 1 & \text{si } p \neq 2, \\ 3 & \text{si } p = 2. \end{cases}$$

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

L'ensemble des racines carrées rationnelles positives (dans $\mathbb{R}$) de $1+x$, où x vérifie les conditions ci-dessus, est

$$\left\{r \in \mathbb{Q} \mid \exists\, a, b \in \mathbb{N}^*,\ r = \frac{a}{b} \text{ et } a \wedge b = 1 \text{ et } p^v|(a-b)(a+b) \text{ et } a^2 < 2b^2\right\}$$

Soient $r = \frac{a}{b}$ un élément de cet ensemble (avec $a, b \in \mathbb{N}^*$ et $a \wedge b = 1$), $x = r^2 - 1$ et r' la limite de la série pour la topologie p-adique. Cherchons des C.N.S. pour que $r = r'$ (dans le cas contraire, on a $r = -r'$).

On a :

$$x = r^2 - 1 = \frac{a^2}{b^2} - 1 = \frac{a^2 - b^2}{b^2} = \frac{(a-b)(a+b)}{b^2}$$

donc b n'est pas divisible par p; et a n'est pas divisible par p non plus.

Si $p \neq 2$, alors $[r']_0 = 1$. $p \mid a^2 - b^2$, donc $p \mid a-b$ ou $p \mid a+b$. Si $p \mid a-b$, alors $a \equiv b \pmod{p}$, donc $r \equiv 1 \pmod{p}$, et $r = r'$ (car $-1 \not\equiv 1 \pmod{p}$). Si $p \mid a+b$, alors $a \equiv -b \pmod{p}$, donc $r \equiv -1 \pmod{p}$, et $r = -r'$.

Si $p = 2$, alors $[r']_1 = 1$. b est impair et $8 \mid a^2 - b^2$, donc $4 \mid a-b$ ou $4 \mid a+b$. Si $4 \mid a-b$, alors $a \equiv b \pmod{4}$, donc $r \equiv 1 \pmod{4}$, et $r = r'$ (car $-1 \not\equiv 1 \pmod{4}$). Si $4 \mid a+b$, alors $a \equiv -b \pmod{4}$, donc $r \equiv -1 \pmod{4}$, et $r = -r'$.

En conclusion:

- $r = r'$ ssi $p^\varepsilon \mid a - b$.
- $r \neq r'$ ssi $p^\varepsilon \mid a + b$.

4 Brenoms périodiques

Note: cette section n'utilise pas les résultats de la section 3, sauf §4.6, qui utilise §3.1 et §3.2.

4.1 Inverse d'un brenom naturel inversible

Soit a un brenom naturel inversible dans $\mathbb{B}$, et $b_{p-1} \dots b_0$ la partie périodique du réel a^{-1} écrit en base k, en commençant par le premier chiffre après la virgule (par exemple, en base 10 pour $a = 7$: 142857). Alors

$$a.(b_{p-1} \dots b_0) = k^p - 1$$

Donc

$$a^{-1} = -\dots(b_{p-1} \dots b_0)$$

Par exemple, en base 10, $7^{-1} = \dots(857142)857143$.

D'où le théroème suivant :

Théorème 4.1 *L'inverse d'un brenom naturel inversible est un brenom périodique.*

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

4.2 Expression d'un brenom périodique à l'aide de brenoms naturels

Théorème 4.2 *Si a est un brenom périodique, alors on peut mettre a sous la forme $a = \pm c.d^{-1}$, où c et d sont des brenoms naturels.*

Démonstration :

Soit $a = \ldots(a_{n+p-1}\ldots a_n)a_{n-1}\ldots a_0$. Alors

$$a = a_{n-1}\ldots a_0 - k^n(a_{n+p-1}\ldots a_n)(k^p-1)^{-1} = b(k^p-1)^{-1}$$

avec

$$b = (k^p-1)(a_{n-1}\ldots a_0) - k^n(a_{n+p-1}\ldots a_n)$$

d'où le théorème avec $c = \pm b$ et $d = k^p - 1$.

4.3 Structure de $(\mathbb{P}, +)$

Considérons 2 brenoms immédiatement périodiques, et soit m une période commune (par exemple, le PPCM des plus petites périodes des 2 brenoms). On effectue alors l'addition des 2 brenoms, par tranches de m chiffres (ce qui revient à effectuer une addition de 2 brenoms en base k^m, chacun étant associé à une suite constante); la retenue est soit 0, soit 1. On vérifie immédiatement que la somme est un brenom périodique (à partir de la première ou deuxième tranche), dont m est une période (pas forcément la plus petite).

On vérifie de même que la somme d'un brenom périodique et d'un brenom naturel est un brenom périodique.

Soient a et b deux brenoms périodiques. En écrivant $a = k^n.a' + a''$ et $b = k^n.b' + b''$, où les brenoms a' et b' sont immédiatement périodiques, et les brenoms a'' et b'' sont naturels, on voit que $a + b$ est un brenom périodique.

On vient de montrer que la somme de deux brenoms périodiques est un brenom périodique, i.e. $\mathbb{P}$ est stable par addition. De plus, le complémentaire d'un brenom périodique est encore un brenom périodique. Donc l'opposé d'un brenom périodique est un brenom périodique. D'où le théorème suivant :

Théorème 4.3 $(\mathbb{P}, +)$ *est un sous-groupe de* $(\mathbb{B}, +)$.

4.4 Structure de $(\mathbb{P}, +, .)$

Soient a et b deux brenoms périodiques. Montrons que ab est un brenom périodique. Pour cela, on écrit a et b sous la forme

$$a = a_{m-1}\ldots a_0 - k^m(a_{m+p-1}\ldots a_m)(k^p-1)^{-1}$$

et

$$b = b_{n-1}\ldots b_0 - k^n(b_{n+q-1}\ldots b_n)(k^q-1)^{-1}$$

Or

$$(k^p-1)^{-1}(k^q-1)^{-1} = [(k^p-1)(k^q-1)]^{-1}$$

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

Ce brenom, inverse d'un brenom naturel inversible, est périodique, d'après §4.1. De plus, le produit d'un brenom périodique par un brenom naturel c est un brenom périodique, car il s'agit en fait d'une somme de c brenoms périodiques. Donc ab est un brenom périodique. On vient de montrer que $\mathbb{P}$ est stable par multiplication.

L'élément neutre pour la multiplication, 1, est un brenom périodique.

Donc $(\mathbb{P}, +, .)$ est un sous-anneau de $(\mathbb{B}, +, .)$.

Montrons maintenant que $\mathbb{P}$ ne contient pas de diviseur de 0 de $(\mathbb{B}, +, .)$.

Soient $a \in \mathbb{P} - \{0\}$ et $b \in \mathbb{B}$ tels que $ab = 0$. Montrons que $b = 0$. D'après §4.2, a s'écrit $\pm c.d^{-1}$, où c est un brenom naturel. On a alors $bc = 0$. Puisque c peut être identifié à un entier naturel, on peut écrire $c = e.c'$, avec $(e, c') \in \mathbb{N}^2$ tel que $\exists\ n \in \mathbb{N},\ e|k^n$ et $c' \wedge k = 1$. Donc on a $be = 0$, et en multipliant par k^n/e, $b.k^n = 0$. Donc $b = 0$.

D'où le théorème suivant :

Théorème 4.4 *$(\mathbb{P}, +, .)$ est un sous-anneau intègre de $(\mathbb{B}, +, .)$. De plus, $\mathbb{P}$ ne contient pas de diviseur de 0 de l'anneau $(\mathbb{B}, +, .)$.*

4.5 Inverse d'un brenom périodique inversible

D'après §4.2, un brenom périodique a peut s'écrire $a = \pm c.d^{-1}$. On a: $a^{-1} = \pm d.c^{-1}$. Or d et c^{-1} sont des brenoms périodiques. Donc le brenom a^{-1} est périodique, d'où le théorème suivant :

Théorème 4.5 *L'inverse d'un brenom périodique inversible est un brenom périodique.*

4.6 Corps des fractions

Puisque $\mathbb{Z}$ est un anneau intègre, on peut construire son corps des fractions: $\mathbb{Q}$. De même, puisque $\mathbb{P}$ est un anneau intègre, il admet un corps des fractions, qui est aussi $\mathbb{Q}$, car d'après §4.2, $\mathbb{P} \subset \mathbb{Q}$.

On vérifie rapidement que l'anneau engendré par $\mathbb{P}$ et $\{k^{-n}\}_{n\in\mathbb{N}}$ (anneau des brenoms fractionnaires périodiques) et l'anneau engendré par $\mathbb{P}$ et $\{1/k^n\}_{n\in\mathbb{N}}$ (sous-anneau de $\mathbb{Q}$) sont isomorphes et que l'isomorphisme permet d'identifier les éléments k^{-n} et $1/k^n$, et ces 2 anneaux à un anneau unique. Montrons alors que tout élément de $\mathbb{Q}$ appartient à cet anneau. Il suffit en fait de faire la vérification pour les éléments $1/b$ avec $b \in \mathbb{N}^*$. On écrit, comme au §4.4, $b = e.b'$ avec $b' \wedge k = 1$ et $e|k^n$, i.e. $k^n = d.e$ (tous ces brenoms étant des brenoms naturels). Puisque b' est inversible dans $\mathbb{P}$, $b'^{-1} \in \mathbb{P}$. Alors

$$1/b = (1/e).(1/b') = (d/k^n).b'^{-1} = (d.b'^{-1})/k^n$$

c'est un brenom fractionnaire périodique.

En conclusion :

Théorème 4.6 *L'ensemble des brenoms fractionnaires périodiques (muni de l'addition et de la multiplication) est un corps, qui peut être identifié à $\mathbb{Q}$, corps des fractions de $\mathbb{Z}$ et de $\mathbb{P}$.*

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

5 Corps p-adiques

Bibliographie:

Jean-Pierre Serre: *Cours d'arithmétique* (chapitre 2).

5.0 Rappels

On note $\mathbb{Z}_p = \mathbb{B}(p)$ l'anneau des entiers p-adiques et $\mathbb{Q}_p = \mathbb{A}(p)$ le corps p-adique (corps des fractions de $\mathbb{Z}_p$), qui, muni de la distance p-adique définie au §3.4, est un espace ultramétrique complet. $\mathbb{Z}_p$ est compact (donc complet). $\mathbb{Z}$ est dense dans $\mathbb{Z}_p$, et $\mathbb{Q}$ est dense dans $\mathbb{Q}_p$ ($\mathbb{Q}_p$ est parfois défini comme le complété de $\mathbb{Q}$ pour la distance p-adique).

5.1 Quelques propriétés de l'anneau $\mathbb{Z}_p$

Théorème 5.1 *L'anneau $\mathbb{Z}_p$ des entiers p-adiques est principal (donc factoriel) et local.*

Démonstration :

Pour montrer que $\mathbb{Z}_p$ est principal, il suffit de montrer que tout idéal de $\mathbb{Z}_p$ est principal (on a déjà vu que $\mathbb{Z}_p$ est intègre).

Soit $\mathcal{I}$ un idéal non nul. Soit

$$n = \inf_{x \in \mathcal{I}} \mathrm{v}_p(x)$$

Alors $\mathcal{I} = p^n \mathbb{Z}_p$ (les deux inclusions sont évidentes), i.e. $\mathcal{I}$ est un idéal principal.

L'anneau $\mathbb{Z}_p$ admet une seule classe d'irréductibles: $p\mathbb{Z}_p^*$ (deux irréductibles sont équivalents ssi l'un est le produit de l'autre par une unité). Par conséquent, $\mathbb{Z}_p$ a un seul idéal maximal: $p\mathbb{Z}_p$. Donc $\mathbb{Z}_p$ est un anneau local.

Soit $x \in \mathbb{Z}_p$ (resp. $x \in \mathbb{Q}_p$). L'unicité de la décomposition en facteurs premiers dans $\mathbb{Z}_p$ implique qu'il existe un unique $u \in \mathbb{Z}_p^*$ et un unique $n \in \mathbb{N}$ (resp. $n \in \mathbb{Z}$), tels que $x = p^n u$.

5.2 Zéros d'un polynôme

Théorème 5.2 *Soit $f \in \mathbb{Z}_p[X]$, et soit f' sa dérivée. Soient $x \in \mathbb{Z}_p$ et $\ell, n \in \mathbb{N}$ tels que $[f(x)]_n = 0$, $\mathrm{v}(f'(x)) = \ell$ et $2\ell < n$. Alors $\exists\ y \in \mathbb{Z}_p,\ f(y) = 0$ et $[y]_{n-\ell} = [x]_{n-\ell}$.*

Démonstration :

Montrons d'abord que

$$\exists\ x' \in \mathbb{Z}_p,\ [f(x')]_{n+1} = 0, \mathrm{v}(f'(x')) = \ell \text{ et } [x']_{n-\ell} = [x]_{n-\ell}$$

Prenons x' de la forme $x + p^{n-\ell}z$, avec $z \in \mathbb{Z}_p$. D'après la formule de Taylor, on a :

$$f(x') = f(x) + p^{n-\ell}z.f'(x) + p^{2n-2\ell}a, \text{ avec } a \in \mathbb{Z}_p$$

Par hypothèse, on a $f(x) = p^n b$ avec $b \in \mathbb{Z}_p$, et $f'(x) = p^\ell c$, avec $c \in \mathbb{Z}_p^*$. Cela permet de choisir $z \in \mathbb{Z}_p$ de telle sorte que $b + zc \equiv 0 \pmod p$.

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

Dès lors

$$f(x') = p^n(b + zc) + p^{2n-2\ell}a \equiv 0 \pmod{p^{n+1}}$$

puisque $2n - 2\ell > n$.

Enfin, la formule de Taylor appliquée à f' montre que

$$f'(x') \equiv p^\ell c \pmod{p^{n-\ell}}$$

Comme $n - \ell > \ell$, on en déduit bien que $\mathrm{v}(f'(x')) = \ell$.

On peut alors construire une suite $(x^n)_{n\in\mathbb{N}}$ à éléments dans $\mathbb{Z}_p$ telle que :

$$x^0 = x, \quad \text{et} \quad \forall\, q \in \mathbb{N},\ [x^{q+1}]_{n+q-\ell} = [x^q]_{n+q-\ell} \text{ et } [f(x^q)]_{n+q} = 0$$

C'est une suite de Cauchy, et si on note y sa limite, on a évidemment $f(y) = 0$ et $[y]_{n-\ell} = [x]_{n-\ell}$, d'où le théorème.

5.3 Conséquence sur les racines $(p-1)$-ièmes de l'unité

Théorème 5.3 *Le corps p-adique $\mathbb{Q}_p$ contient les racines $(p-1)$-ièmes de l'unité.*

Démonstration :

On applique le théorème (5.2) au polynôme $f(X) = X^{p-1} - 1$ pour $n = 1$. Soit $x \in [\![1; p-1]\!]$.

D'après le théorème de Fermat, on a $x^{p-1} \equiv 1 \pmod{p}$. Donc $[f(x)]_1 = 0$.

$f'(x) = (p-1).x^{p-2} \not\equiv 0 \pmod{p}$, donc $\ell = \mathrm{v}(f'(x)) = 0 < n$.

Donc $\exists\, y \in \mathbb{Z}_p$, $y^{p-1} = 1$ et $y \equiv x \pmod{p}$. Le polynôme f a donc au moins $p-1$ zéros. Il en a donc exactement $p-1$: ce sont les racines $(p-1)$-ièmes de l'unité.

5.4 Groupe multiplicatif de $\mathbb{Q}_p$

On note $\mathbb{U} = \mathbb{Z}_p^*$ (groupe des unités p-adiques), $\mathbb{U}_1 = 1 + p\mathbb{Z}_p$ et $\mathbb{V} = \{x \in \mathbb{U} \mid x^{p-1} = 1\}$. $\mathbb{V}$ est le seul sous-groupe de $\mathbb{U}$ isomorphe à $\mathbb{F}_p^*$.

Tout élément $x \in \mathbb{Q}_p^*$ s'écrit de façon unique sous la forme $x = p^n.u$ avec $n \in \mathbb{Z}$ et $u \in \mathbb{U}$. On a donc $\mathbb{Q}_p^* \simeq \mathbb{Z} \times \mathbb{U}$. D'autre part, d'après le théorème (5.3), il existe un unique $v \in \mathbb{V}$ tel que $v \equiv u \pmod{p}$. Et il existe un unique $u_1 \in \mathbb{U}_1$ tel que $u = v.u_1$. Donc $\mathbb{Q}_p^* \simeq \mathbb{Z} \times \mathbb{V} \times \mathbb{U}_1$. On démontrera au §5.7 le théorème suivant :

Théorème 5.4

$$\mathbb{U}_1 \simeq \begin{cases} \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z} & si\ p = 2, \\ \mathbb{Z}_p & si\ p \neq 2. \end{cases}$$

Par conséquent :

Théorème 5.5

$$\mathbb{Q}_p^* \simeq \begin{cases} \mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z} & si\ p = 2, \\ \mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z} & si\ p \neq 2. \end{cases}$$

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

5.5 Carrés de $\mathbb{Q}_p^*$

5.5.1 Cas $p \neq 2$

Théorème 5.6 *Supposons $p \neq 2$, et soit $x = p^n.u \in \mathbb{Q}_p^*$ avec $n \in \mathbb{Z}$ et $u \in \mathbb{U}$. Pour que x soit un carré, il faut et il suffit que n soit pair et que l'image de u dans $\mathbb{F}_p^*$ soit un carré.*

Démonstration :

Décomposons u sous la forme $u = v.u_1$, avec $v \in \mathbb{V}$ et $u_1 \in \mathbb{U}_1$. D'après §5.4, x est un carré ssi n est pair et v et u_1 sont des carrés. Mais $\mathbb{U}_1 \simeq \mathbb{Z}_p$ et 2 est inversible dans $\mathbb{Z}_p$; tout élément de $\mathbb{U}_1$ est donc un carré. Comme $\mathbb{V} \simeq \mathbb{F}_p^*$, le théorème en résulte.

Autre démonstration (celle-ci n'utilise pas le théorème (5.4)) :

L'élément x est un carré ssi n est pair et u est un carré. Pour que u soit un carré, il est évidemment nécessaire que l'image de u dans $\mathbb{Z}/p\mathbb{Z}$ soit un carré. C'est aussi une condition suffisante: on applique le théorème (5.2) à $f(X) = X^2 - u$, $n = 1$, x tel que $x^2 \equiv u \pmod p$, et $\ell = 0$: $f'(x) = 2x \not\equiv 0 \pmod p$ car $x \not\equiv 0 \pmod p$ et $p \neq 2$.

5.5.2 Cas $p = 2$

Théorème 5.7 *Pour qu'un élément $x = 2^n.u \in \mathbb{Q}_2^*$ soit un carré, il faut et il suffit que n soit pair et que $u \equiv 1 \pmod 8$.*

Démonstration :

L'élément x est un carré ssi n est pair et u est un carré. Pour que u soit un carré, il est évidemment nécessaire que $u \equiv 1 \pmod 8$. C'est aussi une condition suffisante: on applique le théorème (5.2) à $f(X) = X^2 - u$, $n = 3$, $x = 1$, et $\ell = \mathrm{v}(f'(1)) = \mathrm{v}(2) = 1$.

5.6 Racines de l'unité dans $\mathbb{Q}_p$

5.6.1 Cas $p = 2$

Cherchons toutes les racines de l'unité dans $\mathbb{Q}_2$, i.e. les $x \in \mathbb{Q}_2$ tels que $\exists\ n \in \mathbb{N}^*,\ x^n = 1$.

1 et -1 sont des racines de l'unité. S'il en existait une autre, celle-ci engendrerait un sous-groupe fini de $\mathbb{Q}_2^*$ d'ordre > 2. Mais d'après le théorème (5.4), $\mathbb{Q}_2^*$ n'a pas de sous-groupe fini d'ordre > 2, car pour tout élément $(\alpha; \beta; \gamma)$ appartenant à un sous-groupe fini de $\mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$, on a $\alpha = 0$ et $\beta = 0$. D'où le théorème suivant :

Théorème 5.8 *Les seules racines de l'unité dans $\mathbb{Q}_2$ sont 1 et -1.*

On peut aussi démontrer ce théorème sans utiliser le théorème (5.4) :

On a :

$$x^n - 1 = (x - 1)(x^{n-1} + \ldots + x + 1)$$

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

mais si n est impair, alors
$$\forall\, x \in \mathbb{Z}/2\mathbb{Z},\ x^{n-1} + \ldots + x + 1 = 1$$
Donc, si n est impair, l'équation $x^n = 1$ a comme seule solution: $x = 1$. Par conséquent, si x est une racine de l'unité, alors il existe $k \in \mathbb{N}$ tel que x soit une racine 2^k-ième de l'unité. 1 et -1 sont les 2 racines carrées de l'unité. Cherchons alors les racines quatrièmes de l'unité. Il y a 1 et -1, et les autres sont des racines carrées de -1. Mais, d'après §5.5.2, -1 n'a pas de racine carrée dans $\mathbb{Q}_2$, car $-1 \not\equiv 1 \pmod 8$. Donc 1 et -1 sont les seules racines quatrièmes de l'unité, et le théorème en résulte.

On en déduit aussi le théorème suivant :

Théorème 5.9 *Les seuls sous-groupes finis de $\mathbb{Q}_2^*$ sont $\{1\}$ et $\{1, -1\}$.*

5.6.2 Cas $p \neq 2$

Cherchons toutes les racines de l'unité dans $\mathbb{Q}_p$, i.e. les $x \in \mathbb{Q}_p$ tels que $\exists\, n \in \mathbb{N}^*,\ x^n = 1$. On peut utiliser le théorème (5.4) dans le cas $p \neq 2$ pour démontrer que les seules racines de l'unité dans $\mathbb{Q}_p$ sont les racines $(p-1)$-ièmes de l'unité, exactement comme on l'a fait pour le cas $p = 2$. Ici aussi, on peut donner une démonstration ne faisant pas intervenir le théorème (5.4).

Soit p un nombre premier quelconque (pas forcément différent de 2). Soit $q \in \mathbb{N}^*$ tel que
$$q \wedge p(p-1) = 1$$
(par exemple, q peut être un nombre premier différent de p, et ne divisant pas $p-1$). Cherchons les solutions de l'équation $x^q = 1$ dans $\mathbb{Q}_p$ (racines q-ièmes de l'unité).

Soit $x \in \mathbb{Q}_p$ tel que $x^q = 1$ (alors $x \in \mathbb{Z}_p$). Soit r l'ordre de x dans $\mathbb{Z}/p\mathbb{Z}$. $r|q$ et $r \mid p-1$, donc $r = 1$, et $x \equiv 1 \pmod p$. Supposons que x s'écrive
$$x = p^n.y + 1 \ \text{ avec } \ n \geq 1 \ \text{ et } \ y \in \mathbb{Z}_p$$
(c'est vrai pour $n = 1$). Alors
$$(p^n.y + 1)^q \equiv 1 \pmod{p^{n+1}}$$
Donc, en développant,
$$1 + q.p^n.y \equiv 1 \pmod{p^{n+1}}$$
donc $p|qy$. Puisque $p \wedge q = 1$, alors $p|y$. Donc x s'écrit sous la forme
$$x = p^{n+1}.y' + 1 \ \text{ avec } \ y' \in \mathbb{Z}_p$$
Par récurrence, on a :
$$\forall\, n \in \mathbb{N}^*,\ \mathrm{v}(x-1) \geq n$$
Donc $x = 1$. En conclusion :

Si $q \in \mathbb{N}^*$ est premier avec $p(p-1)$, alors 1 est la seule racine q-ième de l'unité dans $\mathbb{Q}_p$.

Cherchons maintenant les solutions de l'équation $x^p = 1$, i.e. les racines p-ièmes de l'unité, dans le cas $p \neq 2$ (le cas $p = 2$ a été étudié au §5.6.1).

Soit x une solution (alors $x \in \mathbb{Z}_p$). $x^p \equiv 1 \pmod p$ et $x^p \equiv x \pmod p$, donc $x \equiv 1 \pmod p$. Alors x s'écrit sous la forme $x = py + 1$ avec $y \in \mathbb{Z}_p$. On a :
$$(py+1)^p \equiv 1 \pmod{p^3}$$

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

donc

$$1 + p^2.y + \frac{p(p-1)}{2}p^2.y^2 \equiv 1 \pmod{p^3}$$

Or $2 \mid p-1$. Donc $p^2.y \equiv 0 \pmod{p^3}$. Donc x s'écrit sous la forme $x = p^2.y' + 1$ avec $y' \in \mathbb{Z}_p$.

Supposons que x s'écrive sous la forme

$$x = p^n.y + 1 \ \text{ avec } \ n \geq 2 \ \text{ et } \ y \in \mathbb{Z}_p$$

(c'est vrai pour $n = 2$). Alors

$$1 + p^{n+1}.y \equiv 1 \pmod{p^{n+2}}$$

Donc $p|y$, et x s'écrit

$$x = p^{n+1}.y' + 1 \ \text{ avec } \ y' \in \mathbb{Z}_p$$

Par récurrence, on a :

$$\forall\, n \in \mathbb{N}^*,\ \mathrm{v}(x-1) \geq n$$

Donc $x = 1$. En conclusion :

Si $p \neq 2$, alors 1 est la seule racine p-ième de l'unité dans $\mathbb{Q}_p$.

Maintenant, on sait que si x est une racine de l'unité, alors il existe n de la forme $n = (p-1)^h$ avec $h \in \mathbb{N}$, tel que $x^n = 1$.

Soit x une racine de l'unité telle que $x^{p-1} \neq 1$ (on devra aboutir à une contradiction). Soit n l'ordre de x, i.e. $x^\ell = 1 \Leftrightarrow n|\ell$. Soit

$$m = \frac{p-1}{n \wedge (p-1)}$$

Alors $p-1 \mid mn$ et $p-1 \neq mn$ (car n ne divise pas $p-1$). Soit r tel que

$$mn = (p-1)qr \ \text{ avec } q \text{ premier et } q \mid p-1$$

On a $x^{p-1} \equiv 1 \pmod{p}$. Donc

$$x^{(p-1)r} \equiv 1 \pmod{p}$$

Or $x^{(p-1)r}$ est une racine q-ième de l'unité, donc c'est une racine $(p-1)$-ième de l'unité; et puisque $x^{(p-1)r} \equiv 1 \pmod{p}$, alors

$$x^{(p-1)r} = 1$$

(cf démonstration du théorème (5.3)). Donc $n \mid (p-1)r$; d'où $qn \mid mn$, et $q|m$, i.e.

$$q \mid \frac{p-1}{n \wedge (p-1)}$$

On a aussi

$$q \mid \frac{mn}{p-1} = \frac{n}{n \wedge (p-1)}$$

d'où une contradiction, car ces 2 nombres sont premiers entre eux. En conclusion :

Théorème 5.10 *Pour $p \neq 2$, les seules racines de l'unité dans $\mathbb{Q}_p$ sont les racines $(p-1)$-ièmes de l'unité.*

On en déduit le théorème suivant :

Théorème 5.11 *Pour $p \neq 2$, les sous-groupes finis de $\mathbb{Q}_p^*$ sont les sous-groupes du groupe $\mathbb{V}$ des racines $(p-1)$-ièmes de l'unité, qui est isomorphe à $\mathbb{F}_p^*$.*

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

5.7 Exponentielles et logarithmes

5.7.1 Définition

Cas $p \neq 2$ Soit p un nombre premier différent de 2. Soit $\alpha = 1 + \beta.p$ avec $\beta \in \mathbb{Z}_p^*$. Cherchons un isomorphisme $\exp_\alpha$ de $\mathbb{Z}_p$ sur $\mathbb{U}_1$ tel que $\exp_\alpha(1) = \alpha$.

Supposons que $\alpha^{p^{r-1}}$ s'écrive sous la forme

$$\alpha^{p^{r-1}} = 1 + \beta.p^r \text{ avec } \beta \in \mathbb{Z}_p^*$$

(c'est vrai pour $r = 1$). Alors

$$\alpha^{p^r} = (1 + \beta.p^r)^p = 1 + \beta p^{r+1} + \ldots + \beta^p p^{pr}$$

et les exposants de p dans les termes non écrits sont $\geq 2r + 1 > r + 2$. D'autre part, $pr \geq r + 2$, car $p \geq 3$ (mais cela reste vrai pour $p = 2$ si $r \geq 2$). Donc α^{p^r} s'écrit sous la forme

$$\alpha^{p^r} = 1 + \beta'.p^{r+1} \text{ avec } \beta' \in \mathbb{Z}_p^*$$

Par récurrence, ceci est vrai pour tout $r \in \mathbb{N}$; et si $h \in \mathbb{Z}$ n'est pas divisible par p, alors α^{hp^r} s'écrit sous la forme

$$\alpha^{hp^r} = 1 + \beta.p^{r+1} \text{ avec } \beta \in \mathbb{Z}_p^*$$

Par conséquent,

$$\alpha^m \equiv \alpha^n \pmod{p^{r+1}} \iff m \equiv n \pmod{p^r}$$

On peut alors définir un homomorphisme

$$\varphi_r : \mathbb{Z}/p^r\mathbb{Z} \to 1 + p(\mathbb{Z}/p^r\mathbb{Z}), \; \varphi_r(n) = \alpha^n$$

(à cause de l'implication $\Leftarrow$ démontrée ci-dessus). Or cet homomorphisme est injectif (à cause de l'implication $\Rightarrow$). C'est donc un isomorphisme, car les ensembles de départ et d'arrivée sont finis et équipotents.

Considérons maintenant un élément $x \in \mathbb{Z}_p$. D'après ce qui précède, il existe un unique élément $x' \in \mathbb{U}_1$ tel que

$$\forall\, r \in \mathbb{N}, \; \varphi_r(x) = [x']_{r+1}$$

Notons $\exp_\alpha$ l'application de $\mathbb{Z}_p$ dans $\mathbb{U}_1$ ainsi définie. D'après la propriété (1), cette application est injective.

Inversement, à tout élément $x' \in \mathbb{U}_1$, on peut associer une suite unique (x'_r) d'éléments de $1 + p(\mathbb{Z}/p^r\mathbb{Z})$ telle que $\forall\, r \in \mathbb{N}$, $[x']_{r+1} = x'_r$; et il existe une suite unique (x_r) d'éléments de $\mathbb{Z}/p^r\mathbb{Z}$ telle que $\forall\, r \in \mathbb{N}$, $\varphi_r(x_r) = x'_r$. Soit x l'élément de $\mathbb{Z}_p$ tel que $\forall\, r \in \mathbb{N}^*$, $[x]_r = x_r$. Par construction, on a alors $\exp_\alpha(x) = x'$. L'application $\exp_\alpha$ est donc bijective. On note $\log_\alpha$ l'application réciproque.

On peut vérifier facilement, en faisant intervenir les isomorphismes φ_r et la propriété (1), que les applications $\exp_\alpha$ et $\log_\alpha$ sont continues, et que ce sont des isomorphismes. On les appellera *exponentielle* et *logarithme* en base α (par analogie avec les isomorphismes $\exp_a$ et $\log_a$ que l'on peut définir sur $\mathbb{R}$ et sur $\mathbb{R}_+^*$).

Remarque: le théorème (5.4) est ainsi démontré dans le cas $p \neq 2$.

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

Cas $p = 2$ On note $\mathbb{U}_2 = 1 + p^2\mathbb{Z}_p$. Pour $p = 2$, on prend $\alpha = 1 + \beta.p^2$ avec $\beta \in \mathbb{Z}_p^*$. On peut construire, comme au paragraphe précédent, les isomorphismes continus $\exp_\alpha : \mathbb{Z}_p \to \mathbb{U}_2$ et $\log_\alpha : \mathbb{U}_2 \to \mathbb{Z}_p$.

On peut démontrer le théorème (5.4) dans le cas $p = 2$. Soit $x \in \mathbb{U}_1$. Alors $x \equiv 1 \pmod 2$. Donc x s'écrit de façon unique sous la forme $x = \varepsilon.x'$ avec $\varepsilon = \pm 1$ et $x' \in \mathbb{U}_2$, i.e. $x' \equiv 1 \pmod 4$. Par conséquent, $\mathbb{U}_1 = \{1, -1\} \times \mathbb{U}_2$. Or $\{1, -1\} \simeq \mathbb{Z}/2\mathbb{Z}$ et $\mathbb{U}_2 \simeq \mathbb{Z}_2$. Donc $\mathbb{U}_1 \simeq \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$.

Conclusion Soit p un nombre premier. On note $\mathbb{L}_p = 1 + p\mathbb{Z}_p^*$ et $\mathbb{Y}_p = \mathbb{U}_1$ si $p \neq 2$, et $\mathbb{L}_2 = 1 + 2^2\mathbb{Z}_2^*$ et $\mathbb{Y}_2 = \mathbb{U}_2$, i.e.

$$\mathbb{L}_p = 1 + p^\varepsilon \mathbb{Z}_p^* \text{ et } \mathbb{Y}_p = \mathbb{U}_\varepsilon$$

Théorème 5.12 *Soit p un nombre premier et $\alpha \in \mathbb{L}_p$. Alors il existe un unique isomorphisme continu* $\exp_\alpha : \mathbb{Z}_p \to \mathbb{Y}_p$ *tel que* $\exp_\alpha(1) = \alpha$. *Cet isomorphisme est appelé* exponentielle *en base α. L'isomorphisme réciproque est noté* $\log_\alpha$ *et appelé* logarithme *en base α; il est continu, et on a* $\log_\alpha(\alpha) = 1$.

Démonstration :

L'existence et les propriétés ont été démontrées aux paragraphes précédents. Puisque $\exp_\alpha$ doit être un isomorphisme (par hypothèse), alors $\forall\, n \in \mathbb{Z}$, $\exp_\alpha(n) = \alpha^n$. Il y a donc unicité sur $\mathbb{Z}$. Mais $\overline{\mathbb{Z}} = \mathbb{Z}_p$ et $\exp_\alpha$ doit être continu (par hypothèse). Il y a donc unicité sur $\mathbb{Z}_p$.

On a aussi les résultats suivants, pour p premier et $r \in \mathbb{N}$:

$$x \equiv 0 \pmod{p^r} \quad \Leftrightarrow \quad \exp_\alpha(x) \equiv 1 \pmod{p^{r+\varepsilon}}$$

et

$$x \in p^r\mathbb{Z}_p^* \quad \Leftrightarrow \quad \exp_\alpha(x) \in 1 + p^{r+\varepsilon}\mathbb{Z}_p^*$$

Remarque: on peut prolonger de façon unique l'application $\log_\alpha$ sur $\mathbb{Z}_p^*$. En effet, si $x^n = 1$, alors

$$\log_\alpha(x) = \frac{\log_\alpha(x^n)}{n} = 0$$

En mettant un élément $x \in \mathbb{Z}_p^*$ sous la forme $x = v.u_\varepsilon$, v étant une racine de l'unité et $u_\varepsilon \in \mathbb{Y}_p = \mathbb{U}_\varepsilon$, on a :

$$\log_\alpha(x) = \log_\alpha(u_\varepsilon)$$

Dans le paragraphe suivant, on cherchera à exprimer l'exponentielle sous la forme d'une série convergente (ce sera une série entière), comme on peut le faire sur $\mathbb{R}$.

5.7.2 Développement en série entière des exponentielles

Cas où l'exponentielle est un isomorphisme Soit $f = \exp_\alpha$ telle que f soit développable en série entière. On note a_k ses coefficients (il y a unicité, d'après §3.6.4).

La relation $f(2x) = f(x)^2$ et l'unicité du développement en série entière donnent :

$$\forall\, n \in \mathbb{N},\ 2^n a_n = \sum_{k=0}^{n} a_k a_{n-k}$$

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

Il est alors facile de prouver que :

$$\exists\, a \in \mathbb{Q}_p,\ \forall\, n \in \mathbb{N},\ a_n = \frac{a^n}{n!}$$

Alors

$$\exp_\alpha(x) = f(x) = \sum_{k=0}^{+\infty} \frac{(ax)^k}{k!}$$

et pour $x = 1$:

$$\sum_{k=0}^{+\infty} \frac{a^k}{k!} = \alpha$$

On doit avoir nécessairement $\mathrm{v}(a) \geq \varepsilon_p$ pour assurer la convergence de cette série; et de plus,

$$\alpha \in \mathbb{L}_p \quad\Leftrightarrow\quad \mathrm{v}(a) = \varepsilon_p$$

On définit ainsi une application $\alpha\ :\ p^\varepsilon\mathbb{Z}_p^* \ \to\ \mathbb{L}_p$. On note $\alpha_a = \alpha(a)$. Réciproquement, on vérifie facilement (comme sur $\mathbb{R}$ ou $\mathbb{C}$), que pour tout $a \in p^\varepsilon\mathbb{Z}_p^*$, l'application définie par la série entière est bien une exponentielle.

L'application α est injective (ceci est dû à l'unicité du développement en série entière). Montrons qu'elle est surjective.

On pose

$$\beta = \sum_{k=0}^{+\infty} \frac{p^{\varepsilon k}}{k!}$$

Soit $a \in p^\varepsilon\mathbb{Z}_p^*$. On pose $a' = p^{-\varepsilon}a \in \mathbb{Z}_p^*$. Alors $\alpha_a = \exp_\beta(a')$. Soit $\alpha \in 1 + p^\varepsilon\mathbb{Z}_p^*$. Alors $\log_\beta(\alpha) \notin p\mathbb{Z}_p$. Donc $\log_\beta(\alpha) \in \mathbb{Z}_p^*$.

Donc l'application α est surjective. Elle est donc bijective. En conclusion :

Théorème 5.13

$$\forall\, \alpha \in \mathbb{L}_p,\ \exists!\ a \in p^\varepsilon\mathbb{Z}_p^*,\ \forall\, x,\ \exp_\alpha(x) = \sum_{k=0}^{+\infty} \frac{(ax)^k}{k!}$$

et réciproquement.

Cas général Soit $f(x) = \sum_{k=0}^{+\infty} a_k x^k$ développable en série entière telle que :

$$\forall\, x, y \in D_f,\ f(x+y) = f(x).f(y)$$

Alors

$$\exists\, a \in \mathbb{Q}_p,\ \forall\, n \in \mathbb{N},\ a_n = \frac{a^n}{n!}$$

(cf paragraphe précédent). On définit alors :

$$\exp\ :\ p^\varepsilon\mathbb{Z}_p \ \to\ \mathbb{Y}_p = 1 + p^\varepsilon\mathbb{Z}_p,\ \ \exp a = \sum_{k=0}^{+\infty} \frac{a^k}{k!}$$

Il s'agit du prolongement "naturel" de l'application α définie au paragraphe précédent. On a: $f(x) = \exp ax$. D'après §5.7.1, l'application exp est bijective. On note alors log l'application réciproque. D'après §5.7.1, on a :

$$\forall\, r \geq \varepsilon,\ \ x \in p^r\mathbb{Z}_p^* \Leftrightarrow \exp x \in 1 + p^r\mathbb{Z}_p^*$$

Soit $\alpha \in \mathbb{Y}_p$. Alors $\exp_\alpha(x) = \exp ax$, où $a = \log \alpha$.

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

5.8 Nombres p-adiques transcendants

Dans ce paragraphe, on donne des exemples de nombres p-adiques transcendants, analogues aux nombres de Liouville sur $\mathbb{R}$.

Soit $(r_i) \in \mathbb{N}^{\mathbb{N}}$ une suite strictement croissante telle que :

$$\limsup_{k \to +\infty} \frac{r_{k+1}}{r_k} = +\infty$$

Montrons que le nombre p-adique

$$x = \sum_{i=0}^{+\infty} p^{r_i}$$

est transcendant.

Supposons au contraire que x soit algébrique. Alors il existe un polynôme non nul $P(X) = \sum_{i=0}^{d} a_i X^i$ de $\mathbb{Z}[X]$ tel que $P(x) = 0$. Soit $\alpha \in \mathbb{N}$ tel que

$$\sum_{i=0}^{d} |a_i| < p^{\alpha}$$

On pose :

$$m_k = \sum_{i=0}^{k} p^{r_i} \quad \text{et} \quad \beta_k = \alpha + d.(r_k + 1)$$

Alors

$$|P(m_k)| \quad \leq \quad \sum_{i=0}^{d} |a_i|.|m_k|^i \quad < \quad p^{\alpha}.|m_k|^d \quad \leq \quad p^{\beta_k}$$

Or

$$P(m_k) \equiv P(x) \equiv 0 \pmod{p^{r_{k+1}}}$$

Donc, pour tout k tel que $r_{k+1} \geq \beta_k$ (il y en a une infinité), $P(m_k) = 0$. Contradiction.

Donc x est transcendant.

5.9 Factorisation d'un polynôme de $\mathbb{Q}[X]$ dans un corps p-adique

5.9.1 Existence d'un corps p-adique tel que le polynôme ait une racine

Lemme 5.1 *Soit P un polynôme irréductible de $\mathbb{Z}[X]$, de degré ≥ 1. Alors il existe une infinité de nombres premiers p tels qu'il existe un élément $x \in \mathbb{Z}/p\mathbb{Z}$ tel que $P(x) = 0$ et $P'(x) \neq 0$ (dans $\mathbb{Z}/p\mathbb{Z}$).*

Démonstration :

Evident si $\deg P = 1$.

On suppose maintenant $\deg P > 1$. Alors $P(0) \neq 0$. P est irréductible. Donc P et P' sont premiers entre eux, et il existe $Q, R \in \mathbb{Z}[X]$ et $a \in \mathbb{Z}^*$ tels que $PQ + P'R = a$. Pour $k \in \mathbb{Z}^*$, on a :

$$P(a.k.P(0)^2) = P(0).[c.a.k.P(0) + 1]$$

avec $c \in \mathbb{Z}$. Supposons qu'il n'existe qu'un nombre fini de nombres premiers p_1, p_2, ..., p_r vérifiant les conditions demandées ($r \geq 0$). On peut choisir k tel que

$$p_1 p_2 \dots p_r \mid k \text{ et } |c.a.k.P(0) + 1| \geq 2$$

Soient p un facteur premier de $c.a.k.P(0) + 1$ et x l'image de $a.k.P(0)^2$ dans $\mathbb{Z}/p\mathbb{Z}$. On a $P(x) = 0$ dans $\mathbb{Z}/p\mathbb{Z}$, et $a \not\equiv 0$ (sinon $p|1$). Donc $P'(x) \neq 0$ dans $\mathbb{Z}/p\mathbb{Z}$. Contradiction: on vient de trouver un autre nombre premier vérifiant les conditions demandées. Donc il existe une infinité de nombres premiers vérifiant les conditions.

Théorème 5.14 *Soit P un polynôme non constant de $\mathbb{Q}[X]$. Alors il existe une infinité de nombres premiers p tels que P admette au moins une racine dans $\mathbb{Q}_p$.*

Démonstration :

Soit Q un facteur irréductible de P dans $\mathbb{Q}[X]$, et $R = d.Q$ avec $d \in \mathbb{Z}^*$ tel que $R \in \mathbb{Z}[X]$. D'après le lemme (5.1), il existe une infinité de nombres premiers p tels que $\exists\, x \in \mathbb{Z}/p\mathbb{Z}$, $R(x) = 0$ et $R'(x) \neq 0$. D'après le théorème (5.2), R a une racine dans $\mathbb{Q}_p$, donc P aussi.

5.9.2 Racines de l'unité

Théorème 5.15 *Soit $n \in \mathbb{N}^*$. Alors il existe une infinité de nombres premiers p tels que $\mathbb{Q}_p$ contient les racines n-ièmes de l'unité, i.e. le polynôme $X^n - 1$ se décompose en produit de facteurs du premier degré.*

Démonstration :

D'après le théorème de Dirichlet, il existe une infinité de $q \in \mathbb{N}$ tels que le nombre $p = qn + 1$ soit premier. Le théorème (5.15) résulte alors du théorème (5.3).

5.10 Décomposition d'un nombre p-adique en une somme de carrés

Notation: si $u \in \mathbb{Z}_p$, on note u_0 l'image de u dans $\mathbb{F}_p$.

5.10.1 Lemme

Lemme 5.2 *Dans $\mathbb{F}_p$, tout élément est somme de 2 carrés.*

Démonstration :

Soit $a \in \mathbb{F}_p$. On pose :

$$X_a = \left\{ x^2 \in \mathbb{F}_p \mid 0 \leq x \leq \frac{p-1}{2} \right\}$$

et

$$Y_a = \left\{ a - y^2 \in \mathbb{F}_p \mid 0 \leq y \leq \frac{p-1}{2} \right\}$$

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

Soient $0 \leq x \leq y \leq (p-1)/2$ tels que $x^2 \equiv y^2 \pmod{p}$. Alors $(y-x)(y+x) \equiv 0 \pmod{p}$. Puisque $\mathbb{F}_p$ est un corps, $0 \leq y+x < p$ et $0 \leq y-x < p$, alors $x = y$. Donc

$$\operatorname{card} X_a = \operatorname{card} Y_a = \frac{p-1}{2}$$

Or

$$\operatorname{card}(X \cup Y) \leq \operatorname{card} \mathbb{F}_p = p$$

Donc $X \cap Y \neq \emptyset$. Donc $\exists\ (x, y) \in {\mathbb{F}_p}^2$, $x^2 = a - y^2$, i.e. a est somme de 2 carrés.

5.10.2 Sommes de 2, 3 et 4 carrés de $\mathbb{Q}_p$

Cherchons les éléments de $\mathbb{Q}_p$ qui peuvent se décomposer en une somme de 2 carrés de $\mathbb{Q}_p$, ceux qui peuvent se décomposer en une somme de 3 carrés de $\mathbb{Q}_p$, et montrons que tout élément de $\mathbb{Q}_p$ est somme de 4 carrés de $\mathbb{Q}_p$.

Soit $x = p^n.u \in \mathbb{Q}_p$, avec $n \in \mathbb{Z}$ et $u \in \mathbb{Z}_p^*$. On suppose que x n'est pas un carré (donc si x est somme de 2 carrés, ces carrés sont non nuls).

Si x est somme de 2 carrés $p^\ell.v$ et $p^m.w$, avec $m < \ell$, alors $m = n$, et m et ℓ sont pairs.

Supposons d'abord n pair.

Si $p \neq 2$, x est somme de 2 carrés: en effet, d'après le lemme (5.2), il existe $a, b \in \mathbb{F}_p^*$ tels que $u_0 = a^2 + b^2$; soient alors $v \in \mathbb{Z}_p^*$ tel que $v_0 = a^2$, et $w = u - v$; $p^n.v$ et $p^n.w$ sont des carrés de $\mathbb{Q}_p$, et $x = p^n.v + p^n.w$.

Si $p = 2$: si $u \equiv 5 \pmod{8}$, alors on prend $v \in \mathbb{Z}_p$ tel que $v \equiv 4 \pmod{32}$, par exemple $v = 4$, et $w = u - v$, donc x est somme de 2 carrés. Si $u \equiv 3 \pmod{4}$: si x est somme de 2 carrés $p^\ell.v$ et $p^m.w$ avec $m \leq \ell$, le cas $m \neq \ell$ est impossible car on aurait $w \equiv 3 \pmod{4}$, et le cas $m = \ell$ est aussi impossible car 3 n'est pas somme de 2 carrés dans $\mathbb{Z}/4\mathbb{Z}$; donc x n'est pas somme de 2 carrés. Si $u \equiv 3 \pmod{8}$, x est somme de 3 carrés, car on a $u = 1 + 1 + v$ avec $v \equiv 1 \pmod{8}$. Si $u \equiv 7 \pmod{8}$, x n'est pas somme de 3 carrés: en effet, si

$$x = 4^m.u = 4^q.a + 4^r.b + 4^s.c \ \text{ avec } q \leq r \leq s$$

on ne peut pas avoir $q \geq m$ car 7 ne peut pas se décomposer dans $\mathbb{Z}/8\mathbb{Z}$ en une somme de 3 éléments égaux à 0, 1 ou 4, et si $q < m$, alors

$$\mathrm{v}_4(4^q.a + 4^r.b + 4^s.c) = q \neq m$$

mais x est somme de 4 carrés, car on a $u = 4 + 1 + 1 + v$ avec $v \equiv 1 \pmod{8}$.

Supposons maintenant n impair.

Cherchons si x peut se décomposer en une somme de 2 carrés, i.e. s'il existe v et w carrés de $\mathbb{Z}_p^*$ tels que l'on puisse écrire

$$x = p^n.u = p^{2k}(v + w)$$

Nécessairement, $w_0 = -v_0$. Si $p \equiv 1 \pmod{4}$, -1 est un carré dans $\mathbb{F}_p^*$; on choisit un carré v quelconque de $\mathbb{Z}_p^*$; alors $w = p.u - v$ est aussi un carré, donc x est somme de 2 carrés.

Mais si $p \equiv 3 \pmod{4}$, -1 n'est pas un carré dans $\mathbb{F}_p^*$, et l'égalité $w_0 = -v_0$ est impossible. Donc x n'est pas somme de 2 carrés. Soit $y = p^{n-1}.u'$, u' étant un carré de $\mathbb{Z}_p^*$. $x - y$ est somme de 2 carrés (cas n pair), donc x est somme de 3 carrés.

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

Il reste le cas $p=2$. Si $u \equiv 1 \pmod 4$, alors on choisit $v \equiv 1 \pmod 8$ et on prend $w = 2u - v \equiv 1 \pmod 8$, donc x est somme de 2 carrés. Si $u \equiv 3 \pmod 4$, alors $2u \equiv 6 \pmod 8$, donc x n'est pas somme de 2 carrés (car 6 n'est pas somme de 2 carrés dans $\mathbb{Z}/8\mathbb{Z}$); mais x est somme de 3 carrés: on choisit $y = 2^{n-1}.u'$ avec $u' \equiv 4 \pmod{32}$, et $x - y$ est somme de 2 carrés (cf cas précédent).

En conclusion :

Théorème 5.16 *Suivant la valeur de p, on sait quels sont les éléments qui sont somme de 2, 3 ou 4 carrés :*

- *Si $p=2$: tout élément de $\mathbb{Q}_2$ est somme de 4 carrés. Les éléments de $\mathbb{Q}_2^*$ qui sont somme de 3 carrés sont ceux qui s'écrivent $x = 4^m.a$ avec $a \not\equiv 7 \pmod 8$, où $m = \mathrm{v}_4(x)$. Les éléments de $\mathbb{Q}_2^*$ qui sont somme de 2 carrés sont ceux qui s'écrivent $x = 2^n.u$ avec $u \equiv 1 \pmod 4$, où $n = \mathrm{v}_2(x)$.*
- *Si $p \equiv 1 \pmod 4$: tout élément de $\mathbb{Q}_p$ est somme de 2 carrés.*
- *Si $p \equiv 3 \pmod 4$: tout élément de $\mathbb{Q}_p$ est somme de 3 carrés. Les éléments de $\mathbb{Q}_p^*$ qui sont somme de 2 carrés sont ceux dont la valuation n est paire.*

Remarque: cette conclusion persiste si on prend l'ensemble $\mathbb{Z}_p$ au lieu de $\mathbb{Q}_p$, ou si on prend l'ensemble $\mathbb{Q}$, $\mathbb{Z}$ ou $\mathbb{N}$ (dans ce cas, les carrés considérés sont les éléments de $\mathbb{Q}$, $\mathbb{Z}$ ou $\mathbb{N}$ qui ont au moins une racine carrée dans $\mathbb{Q}_p$).

5.11 Puissances k-ièmes

(Ce paragraphe utilise les résultats de §5.7.1.)

Soient $k \in \mathbb{N}^*$ et $a \in \mathbb{Q}_p^*$. Cherchons une C.N.S. pour qu'il existe $x \in \mathbb{Q}_p$ tel que $x^k = a$.

On pose: $a = p^n.u$ avec $u \in \mathbb{Z}_p^*$, et $k = p^r.k'$ avec $k' \wedge p = 1$.

Pour que a soit une puissance k-ième, il est nécessaire que $k|n$ et que l'image de u dans $\mathbb{F}_p^*$ soit une puissance k-ième. Supposons ces conditions vérifiées. Cherchons alors une C.N.S. pour que u soit une puissance k-ième dans $\mathbb{Z}_p^*$.

Soit $f(x) = x^k - u$. $f'(x) = k.x^{k-1}$. Si $r = 0$, alors d'après le théorème (5.2), u est une puissance k-ième dans $\mathbb{Z}_p^*$. Supposons maintenant $r \neq 0$. u est une puissance k-ième ssi il existe $x \in \mathbb{Z}_p^*$ tel que $\log_\alpha u = k.\log_\alpha x$ (où α est un élément quelconque de $\mathbb{L}_p$), i.e. $[\log_\alpha u]_r = 0$.

Dans $\mathbb{Q}_2$: nécessairement, $u \equiv 1 \pmod 8$. Alors, d'après §5.7.1, la condition équivaut à

$$u \equiv 1 \pmod{2^{r+2}}$$

On a $u = x^k$, avec $x = \exp_\alpha(k^{-1}.\log_\alpha u)$.

Dans $\mathbb{Q}_p$ ($p \neq 2$): on écrit $u = v.u_1$ avec $v \in \mathbb{V}$ et $u_1 \in \mathbb{U}_1$. v est une puissance k-ième ssi l'image de u dans $\mathbb{F}_p^*$ est une puissance k-ième. D'après §5.7.1, la condition équivaut à

$$u_1 \equiv 1 \pmod{p^{r+1}}$$

On a $u_1 = x^k$, avec $x = \exp_\alpha(k^{-1}.\log_\alpha u_1)$.

Pour tout p premier, la condition équivaut donc à

$$u_1 \equiv 1 \pmod{p^{r+\varepsilon}}$$

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

(si $p = 2$, $u_1 = u$). Pour la vérifier, on n'a pas besoin de calculer u_1. En effet, elle équivaut à

$$u \equiv v \pmod{p^{r+\varepsilon}}$$

(si $p = 2$, $v = 1$).

En conclusion :

Théorème 5.17 *$a = p^n.u$ ($u \in \mathbb{Z}_p^*$) est une puissance k-ième ssi les 3 conditions suivantes sont vérifiées :*

- *$k|n$.*
- *L'image de u dans $\mathbb{F}_p^*$ est une puissance k-ième (condition toujours vérifiée si $p = 2$).*
- *$r = 0$ ou $\exists\ v \in \mathbb{V},\ u \equiv v \pmod{p^{r+\varepsilon}}$.*

La vérification de la troisième condition nécessite de connaître les $r+\varepsilon$ premiers chiffres des éléments de $\mathbb{V}$. Le paragraphe suivant donne une méthode simple et rapide de calcul approché de ces nombres.

5.12 Calcul approché des éléments de $\mathbb{V}$

Le but de ce paragraphe est de calculer rapidement les n premiers chiffres des éléments de $\mathbb{V}$ (racines $(p-1)$-ièmes de l'unité). Comme $\mathbb{V}$ est un groupe cyclique, il suffit de calculer les n premiers chiffres d'un seul élément (qui est un générateur).

Soit $p \neq 2$ (pour $p = 2$, $\mathbb{V} = \{1\}$). Soit $v \in \mathbb{V}$. D'après le paragraphe précédent, on a :

$$[v]_n = \left[z^{p^{n-1}}\right]_n \quad \text{où} \quad z \equiv v \pmod{p}$$

On peut prendre $z \in [\![1; p-1]\!]$, par exemple.

Remarque: si $v \equiv 1 \pmod{p}$, alors $v = 1$; et si $v \equiv -1 \pmod{p}$ avec $p \neq 2$, alors $v = -1$.

6 Projection d'un brenom fractionnaire sur les corps p-adiques

6.1 Projection sur un corps p-adique

Soit k un nombre non primaire. L'objet de ce paragraphe est de définir un homomorphisme surjectif de l'anneau des brenoms fractionnaires $\mathbb{A}(k)$ sur le corps p-adique $\mathbb{Q}_p = \mathbb{A}(p)$ où p est un facteur premier de k. De plus, l'anneau $\mathbb{B}(k)$ sera envoyé sur $\mathbb{Z}_p = \mathbb{B}(p)$.

Soient p un facteur premier de k, $\alpha = \mathrm{v}_p(k)$: valuation p-adique de k, $q = p^\alpha$ et k' tel que $k = q.k'$. Alors $k' \wedge p = 1$. Définissons d'abord un homomorphisme $\varphi\ :\ \mathbb{B}(k)\ \to\ \mathbb{B}(q)$, $\varphi(a) = a'$ tel que

$$\forall\, n \in \mathbb{N}^*,\ [a']_n \equiv [a]_n \pmod{q^n}$$

Avec cette définition, la surjectivité de φ est évidente.

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

Montrons ensuite (par récurrence) que l'élément a' ainsi défini existe et est unique. Pour $n = 0$, il n'y a rien à démontrer. Supposons que $[a']_n$ soit déterminé de façon unique (i.e. on connaît les n premiers chiffres de a'). Cherchons le chiffre a'_n. On pose :

$$s_n = \sum_{i<n} a'_i q^i \ \in \mathbb{N}$$

On cherche a'_n tel que :

$$a'_n q^n + s_n \equiv [a]_{n+1} \pmod{q^{n+1}}$$

Or

$$[a]_{n+1} \equiv [a]_n \equiv [a']_n \equiv s_n \pmod{q^n}$$

Donc

$$\exists!\ x_n \in [\![0; q-1]\!],\ [a]_{n+1} - s_n \equiv x_n q^n \pmod{q^{n+1}}$$

On a ainsi l'existence et l'unicité de a'_n ($a'_n = x_n$).

Montrons maintenant que l'application φ est bien un homomorphisme. Soient $a, b \in \mathbb{B}(k)$. On note: $c = a + b$, $a' = \varphi(a)$, $b' = \varphi(b)$, $c' = \varphi(c)$. Montrons que $c' = a' + b'$. On a :

$$[c']_n \equiv [c]_n \equiv [a]_n + [b]_n \equiv [a']_n + [b']_n \equiv [a' + b']_n \pmod{q^n}$$

Donc

$$\forall\, n \in \mathbb{N}^*,\ [c']_n = [a' + b']_n$$

Donc, d'après la propriété (1), $c' = a' + b'$.

On vient de montrer que $\varphi(a) + \varphi(b) = \varphi(a + b)$. On démontrerait de même que $\varphi(a).\varphi(b) = \varphi(a.b)$. Enfin, $\varphi(1) = 1$.

On a ainsi défini un homomorphisme d'anneaux surjectif de $\mathbb{B}(k)$ sur $\mathbb{B}(q)$, qui est isomorphe (d'après §2.6) à $\mathbb{Z}_p = \mathbb{B}(p)$.

Considérons maintenant l'application $\Phi : \mathbb{A}(k) \to \mathbb{A}(q)$ définie par :

$$\Phi(a) = k^{-r}\varphi(k^r a) = q^{-r}\varphi(q^r a)$$

où $r \in \mathbb{N}$ est tel que $k^r a \in \mathbb{B}(k)$. Il est clair que cette application Φ est un homomorphisme surjectif.

Comme $\mathbb{A}(q)$ est isomorphe à $\mathbb{A}(p)$, alors on peut définir ainsi un homomorphisme surjectif de l'anneau $\mathbb{A}(k)$ sur le corps p-adique $\mathbb{Q}_p = \mathbb{A}(p)$.

Cet homomorphisme est appelé *projection* de l'anneau des brenoms fractionnaires $\mathbb{A}(k)$ sur le corps p-adique $\mathbb{Q}_p = \mathbb{A}(p)$. On peut vérifier que c'est une application continue.

Notons que les éléments de $\mathbb{Q}$ sont invariants par projection, avec les identifications que l'on a faites. Comme $\mathbb{P}(k) = \mathbb{B}(k) \cap \mathbb{Q}$, la projection d'un élément de $\mathbb{P}(k)$ est un élément de $\mathbb{P}(p)$.

6.2 Projection sur une base de corps p-adiques

Soit $k \geq 2$ (base quelconque) et $\mathcal{P}$ l'ensemble des facteurs premiers positifs de k. L'objet de ce paragraphe est de définir un isomorphisme de l'anneau des brenoms fractionnaires $\mathbb{A}(k)$ sur le produit des corps p-adiques pour $p \in \mathcal{P}$ (base de corps p-adiques).

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

Décomposons k en produit de facteurs premiers :

$$k = \prod_{p \in \mathcal{P}} p^{\alpha(p)} = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \ldots {p_r}^{\alpha_r} = q_1 q_2 \ldots q_r$$

avec

$$q_i = {p_i}^{\alpha_i} \ , \ \alpha_i \in \mathbb{N}^* \ , \ r = \operatorname{card} \mathcal{P}$$

On définit les homomorphismes :

$$\varphi \ : \ \mathbb{B}(k) \ \rightarrow \ \prod_{p \in \mathcal{P}} \mathbb{Z}_p \ \text{ et } \ \Phi \ : \ \mathbb{A}(k) \ \rightarrow \ \prod_{p \in \mathcal{P}} \mathbb{Q}_p$$

par

$$\forall\, a \in \mathbb{B}, \ \varphi(a) = (a^{(p)})_{p \in \mathcal{P}} \ \text{ et } \ \forall\, a \in \mathbb{A}, \ \Phi(a) = (a^{(p)})_{p \in \mathcal{P}}$$

où $a^{(p)}$ désigne la projection du brenom fractionnaire a sur le corps p-adique $\mathbb{Q}_p$. Montrons qu'il s'agit en fait d'isomorphismes.

Soit $(x_p)_{p \in \mathcal{P}} \in \prod_{p \in \mathcal{P}} \mathbb{Z}_p$. Cherchons $a \in \mathbb{B}(k)$ tel que $\forall\, p \in \mathcal{P}$, $a^{(p)} = x_p$, i.e. tel que

$$\forall\, n \in \mathbb{N}^*, \ \forall\, i \in [\![1; r]\!], \ [a]_n \equiv [x_p]_n \pmod{{q_i}^n}$$

ce qui définit $[a]_n$ de façon unique, puisque

$$\mathbb{Z}/k^n\mathbb{Z} \simeq \prod_{i=1}^{r} \mathbb{Z}/{q_i}^n\mathbb{Z}$$

En utilisant la propriété (1), on en déduit que a existe et est unique. Donc φ est un isomorphisme.

En utilisant le fait que

$$\forall\, a \in \mathbb{B}(k), \ \forall\, x_p \in \mathbb{Z}_p, \ \forall\, s \in \mathbb{N}, \ \Phi(k^{-s} a) = (k^{-s} x_p)_{p \in \mathcal{P}} \Leftrightarrow \varphi(a) = (x_p)_{p \in \mathcal{P}}$$

on prouve que Φ est un isomorphisme.

En conclusion :

Théorème 6.1

$$\mathbb{B}(k) \simeq \prod_{p \in \mathcal{P}} \mathbb{Z}_p \ \textit{ et } \ \mathbb{A}(k) \simeq \prod_{p \in \mathcal{P}} \mathbb{Q}_p$$

On note

$$\mathbb{S}(k) = \{x \in \mathbb{A}(k) \mid \forall\, p \in \mathcal{P}, \ x^{(p)} \in \mathbb{Q}\}$$

C'est un sous-anneau de $\mathbb{A}(k)$ isomorphe à $\mathbb{Q}^r$.

6.3 Conséquences sur les diviseurs de 0 de $\mathbb{A}(k)$

D'après §6.2,

Théorème 6.2 *Un élément $a \in \mathbb{A}(k) - \{0\}$ est un diviseur de 0 ssi*

$$\exists\ p \in \mathcal{P}, \ a^{(p)} = 0$$

Théorème 6.3 *Soient a_1, a_2, …, a_n des éléments de $\mathbb{A}(k)$. Alors*

$$a_1 a_2 \ldots a_n = 0 \ \Leftrightarrow \ \forall\, p \in \mathcal{P}, \ \exists\ i \in [\![1; n]\!], \ {a_i}^{(p)} = 0$$

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

6.4 Conséquences sur le nombre de zéros d'un polynôme

Soit $f \in \mathbb{A}[X]$. Soient $f^{(p)} \in \mathbb{Q}_p[X]$ les projetés de f (i.e. on projette les coefficients). On a :

Théorème 6.4

$$f(x) = 0 \iff \forall\, p \in \mathcal{P},\ f^{(p)}(x^{(p)}) = 0$$

Par conséquent, en posant $r = \operatorname{card} \mathcal{P}$:

$$\operatorname{card}\{x \in \mathbb{A}(k) \mid f(x) = 0\} = \prod_{p \in \mathcal{P}} \operatorname{card}\{x \in \mathbb{Q}_p \mid f^{(p)}(x) = 0\} \le \deg(f)^r$$

d'où

Théorème 6.5 *Le nombre de zéros d'un polynôme de degré d à coefficients dans $\mathbb{A}(k)$ est inférieur ou égal à $d^{\operatorname{card} \mathcal{P}}$.*

En particulier, tout brenom de $\mathbb{A}(k)$ a soit 0, soit 2^n racines carrées, avec $0 \le n \le r$; un brenom a au moins une racine carrée ssi tous ses projetés en ont au moins une; dans ce cas, n est le nombre de projetés non nuls, et si ce brenom est un brenom naturel, alors il a exactement 2^r racines carrées. Donc en base 10, tout brenom fractionnaire non nul a soit 0, soit 2, soit 4 racines carrées, et tout brenom naturel non nul a soit 0, soit 4 racines carrées.

6.5 Calcul approché des éléments de $\mathbb{S}(k)$

Pour $p \in \mathcal{P}$, on note u_p l'élément de $\mathbb{S}(k)$ tel que

$$\forall\, q \in \mathcal{P},\ {u_p}^{(q)} = \delta_{pq}$$

Soit $x \in \mathbb{S}(k)$. On peut écrire :

$$x = \sum_{p \in \mathcal{P}} x^{(p)} u_p$$

Cette écriture permet de trouver rapidement les premiers chiffres des éléments de $\mathbb{S}(k)$, connaissant ceux de u_p.

<u>Exemple</u> en base 10 :

On donne $[u_2]_9 = 212890625$ (on peut le trouver de la façon suivante: on a $5^9 \equiv 357 \pmod{512}$ et $357^{-1} \equiv 109 \pmod{512}$, donc $[u_2]_9 = 109 \cdot 5^9$). On cherche les 9 premiers chiffres du brenom $x \in \mathbb{S}(k)$ tel que $x^{(2)} = \frac{2}{3}$ et $x^{(5)} = \frac{4}{7}$; on le note $x = (\frac{2}{3}; \frac{4}{7})$.

On a: $u_5 = 1 - u_2 = \overline{u_2} + 2$, donc $[u_5]_9 = 787109376$. D'après §4.1, on a: $\frac{2}{3} = \ldots(3)4$ et $\frac{4}{7} = \ldots(142857)2$. On en déduit: $[x]_9 = 544084822$.

On peut aussi avoir facilement les premiers chiffres des 4 racines carrées de 1 :

$$1\ ,\ -1 = \ldots(9)\ ,\ u_2 - u_5 = \ldots 425781249 \text{ et } u_5 - u_2 = \ldots 574218751$$

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

6.6 Exponentielles et logarithmes dans $\mathbb{B}(k)$

Soit

$$\mathbb{L}(k) = \{x \in \mathbb{B}(k) \mid \forall\, p \in \mathcal{P},\ \mathrm{v}_p(x-1) = \varepsilon_p\} \ \text{ et } \ \mathbb{Y}(k) = \{x \in \mathbb{B}(k) \mid \forall\, p \in \mathcal{P},\ \mathrm{v}_p(x-1) \geq \varepsilon_p\}$$

Alors

$$\mathbb{L}(k) \simeq \prod_{p\in\mathcal{P}} \mathbb{L}_p \ \text{ et } \ \mathbb{Y}(k) \simeq \prod_{p\in\mathcal{P}} \mathbb{Y}_p$$

Soit $\alpha \in \mathbb{L}(k)$. On peut définir l'exponentielle en base α: $y = \exp_\alpha(x) \in \mathbb{Y}(k)$ avec, pour tout $p \in \mathcal{P}$, $y^{(p)} = \exp_\alpha(x^{(p)})$; c'est un isomorphisme continu de $\mathbb{B}(k)$ sur $\mathbb{Y}(k)$. L'application réciproque est le logarithme en base α, qui est un isomorphisme continu de $\mathbb{Y}(k)$ sur $\mathbb{B}(k)$.

6.7 Brenoms algébriques, brenoms transcendants

Si $a \in \mathbb{A}(k)$ est algébrique, alors tous ses projetés sont aussi algébriques et leurs degrés sont inférieurs ou égaux à celui de a (car les projetés de a annulent le polynôme minimal de a). Donc si un des projetés de a est transcendant, alors a est aussi transcendant. Réciproquement, si tous les projetés de a sont algébriques, alors a est aussi algébrique et son degré est inférieur ou égal à la somme des degrés de ses projetés (car le produit des polynômes minimaux des projetés s'annule en a). En conclusion :

Théorème 6.6 *Un brenom $a \in \mathbb{A}(k)$ est algébrique si et seulement si tous ses projetés le sont.*

On peut donc facilement construire des nombres transcendants de $\mathbb{A}(k)$ à partir des projetés (on connaît des nombres p-adiques transcendants, d'après §5.8).

7 Résolution d'équations

7.1 Détermination des brenoms naturels carrés en base 10

Soit $n \in \mathbb{N}^*$. Cherchons une C.N.S. pour que n ait au moins une racine carrée (dans ce cas, il y aura exactement 4 racines carrées, d'après §6.4).

D'après §6.4, n est un carré dans $\mathbb{B}(10)$ ssi n est un carré dans $\mathbb{Q}_2$ et dans $\mathbb{Q}_5$, i.e. n s'écrit sous la forme

$$n = 2^\alpha 5^\beta n'$$

avec

$$n' \wedge 10 = 1 \ \ , \ \ 2|\alpha \ \ , \ \ 2|\beta \ \ , \ \ 5^\beta n' \equiv 1 \pmod 8 \ \text{ et } \ 2^\alpha n' \equiv \pm 1 \pmod 5$$

Ces deux congruences peuvent être remplacées par

$$n' \equiv 1 \pmod 8 \ \text{ et } \ n' \equiv \pm 1 \pmod 5$$

Finalement, on pourra prendre comme condition :

$$\boxed{n = 4^\alpha 25^\beta n' \ \text{ avec } \ \alpha, \beta \in \mathbb{N} \ \text{ et } \ n' \equiv 1 \text{ ou } 9 \pmod{40}}$$

Le plus petit brenom naturel carré qui n'est pas le carré d'un brenom naturel est 41.

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

7.2 Résolution de l'équation $x^2 = x$

Il s'agit ici de trouver tous les brenoms égaux à leur carré.

Dans les corps p-adiques $\mathbb{Q}_p$, il y a exactement 2 solutions: 0 et 1. Donc, dans $\mathbb{A}(k)$, il y a exactement 2^r solutions (chaque projeté est soit 0, soit 1), r étant le nombre de facteurs premiers (distincts) de k. Ces 2^r solutions sont dans $\mathbb{S}(k)$, mais 2 seulement sont dans $\mathbb{Q}$ (0 et 1). En base 10, les solutions sont 0, 1, u_2 et u_5.

7.3 Résolution de l'équation $x^n = a$ en base 10

7.3.1 Résolution de l'équation $x^n = 1$ en base 10

Résolvons l'équation $x^n = 1$ dans $\mathbb{A}(10)$, où $n \in \mathbb{N}^*$.

D'après §5.6.1, on sait que les racines de l'unité dans $\mathbb{Q}_2$ sont les 2 racines carrées de l'unité: -1 et 1. D'après §5.6.2, les racines de l'unité dans $\mathbb{Q}_5$ sont les 4 racines quatrièmes de l'unité; appelons ω une des 2 racines carrées de -1 (l'autre est alors $-\omega$); les racines quatrièmes de l'unité dans $\mathbb{Q}_5$ sont alors ω, -1, $-\omega$ et 1.

Résolvons l'équation $x^n = 1$ dans $\mathbb{Q}_2$. Si n est impair, 1 est la seule solution. Si n est pair, -1 et 1 sont les 2 seules solutions.

Résolvons l'équation dans $\mathbb{Q}_5$. Si n est impair, 1 est la seule solution. Si $n \equiv 2 \pmod 4$, -1 et 1 sont les 2 seules solutions. Si n est divisible par 4, les solutions sont les racines quatrièmes de l'unité.

On peut alors en déduire les solutions de cette équation dans $\mathbb{A}(10)$:

- Si n est impair, $(1;1) = 1$ est l'unique solution.
- Si $n \equiv 2 \pmod 4$, il y a 4 solutions: $(1;1) = 1$, $(1;-1)$, $(-1;1)$ et $(-1;-1) = -1$.
- Si n est divisible par 4, il y a 8 solutions: $(1;1) = 1$, $(1;\omega)$, $(1;-1)$, $(1;-\omega)$, $(-1;1)$, $(-1;\omega)$, $(-1;-1) = -1$ et $(-1;-\omega)$.

7.3.2 Puissances n-ièmes

Dans ce paragraphe, on cherchera une C.N.S. pour que l'équation $x^n = a$, où $a \in \mathbb{A}(10)\backslash\{0\}$, ait au moins une solution (i.e. pour que a soit une puissance n-ième).

On écrit $a = 2^p 5^q u$ avec $u \in \mathbb{B}(10)^*$, et $n = 2^r 5^s n'$ avec $n' \wedge 10 = 1$. D'après §5.11 et §6.2, a est une puissance n-ièmes ssi les 4 conditions suivantes sont vérifiées :

- $n|p$ et $n|q$.
- $r = 0$ ou $u \equiv 1 \pmod{2^{r+2}}$.
- L'image de u dans $\mathbb{F}_5^*$ est une puissance n-ième.
- $\exists\ v \in \mathbb{V}_5,\ u \equiv v \pmod{5^{s+1}}$, où $\mathbb{V}_5$ est l'ensemble des racines quatrièmes de l'unité dans $\mathbb{Q}_5$.

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse

Pour vérifier la quatrième condition, il faut et il suffit de connaître les $s+1$ premiers chiffres des éléments de $\mathbb{V}_5$ (cf §5.12 pour leur calcul). D'autre part, sachant que $\mathbb{F}_5^* \simeq \mathbb{Z}/4\mathbb{Z}$, on peut préciser la troisième condition. On a :

$$k.\mathbb{Z}/4\mathbb{Z} = \begin{cases} \{0\} & \text{si } 4|k. \\ \{0;2\} & \text{si } k \equiv 2 \pmod 4. \\ \mathbb{Z}/4\mathbb{Z} & \text{si } k \equiv 1 \pmod 2. \end{cases}$$

Par conséquent :

- Si $r = 0$, la troisième condition est toujours vérifié.
- Si $r = 1$, la troisième condition est vérifiée ssi $u \equiv \pm 1 \pmod 5$.
- Si $r \geq 2$, la troisième condition est vérifiée ssi $u \equiv 1 \pmod 5$.

En conclusion, a est une puissance n-ième ssi $n|p$, $n|q$ et :

- Si $r = 0$, $\exists\ v \in \mathbb{V}_5,\ u \equiv v \pmod{5^{s+1}}$; toujours vérifiée si $s = 0$.
- Si $r = 1$, $u \equiv 1$ ou $2 \cdot 5^{s+1} - 1 \pmod{8 \cdot 5^{s+1}}$.
- Si $r \geq 2$, $u \equiv 1 \pmod{2^{r+2}5^{s+1}}$.

Valeurs approchées des éléments de $\mathbb{V}_5$:

- En base 5: $\ldots 00000001$, $\ldots 32431212$, $\ldots 12013233$, $\ldots 44444444$.
- En base 10 (mod 5^8): 1, 280182, 110443, 390624.

7.3.3 Résolution de l'équation $x^n = a$

Dans le paragraphe précédent, on a trouvé une C.N.S. pour que l'équation $x^n = a$ ($a \in \mathbb{A}(10)\backslash\{0\}$) ait au moins une solution. Lorsqu'il y en a au moins une, toutes les solutions se déduisent les unes des autres par multiplication par une racine n-ième de l'unité. Le nombre de solutions est alors égal au nombres de racines n-ièmes de l'unité (cf §7.3.1).

7.4 Sommes de carrés

D'après §5.10, tout élément de $\mathbb{A}(k)$ est somme de 4 carrés de $\mathbb{A}(k)$, et tout élément de $\mathbb{B}(k)$ est somme de 4 carrés de $\mathbb{B}(k)$. Si k est impair, alors tout élément est somme de 3 carrés. Si les facteurs premiers de k sont tous congrus à 1 modulo 4, alors tout élément est somme de 2 carrés.

Si k n'est pas un nombre primaire, on ne peut pas étendre ce théorème à $\mathbb{Q}$, $\mathbb{Z}$ ou $\mathbb{N}$, car un élément de $\mathbb{A}(k)$ dont tous les projetés sont dans $\mathbb{Q}$ n'est pas forcément un élément de $\mathbb{Q}$. Mais, indépendamment des corps p-adiques, on peut dire, d'après le théorème de Lagrange, que tout élément de $\mathbb{N}$ est somme de 4 carrés de $\mathbb{N}$.

Pour savoir si un élément a de $\mathbb{A}(k)$ ou de $\mathbb{B}(k)$ est somme de 2 carrés de $\mathbb{A}(k)$ ou de $\mathbb{B}(k)$, on projette a sur les corps p-adiques et on utilise le résultat de §5.10.

Vincent Lefèvre
24, rue Louis Blanc
31400 Toulouse