Nombres p-adiques et ultramétricité
Gilles Christol

A. Espaces ultramétriques

Le but de cette première partie est de définir les ensembles ultramétriques classiques et particulièrement les nombres p-adiques. Cela sera réalisé au moyen d'une procédure générale décrite en Section 2. En Section 1 sont données des définitions générales au sujet des ensembles ultramétriques. Ces définitions pourront sembler dénuées de sens à la lectrice non avertie. Aussi suggérons-nous de commencer la lecture au paragraphe 2.1.2, en lisant la Section 1 quand nécessaire. L'anneau $\mathbb{Z}_p$ des nombres p-adiques est introduit en Section 3.2 et l'anneau $\widehat{\mathbb{Z}}$, une généralisation de $\mathbb{Z}_p$, sans aucun nombre premier privilégié, est introduit en Section 3.3. L'anneau $\widehat{\mathbb{Z}}$ a déjà été utilisé par les physiciens, comme expliqué en 3.4.

1. Distances ultramétriques

1.1. Définitions

1.1.1. Une distance d sur un ensemble E est dite ultramétrique si elle satisfait les conditions habituelles :

$$d(a,b) \geq 0\ ; d(a,b) = 0 \iff a = b\ ; d(a,b) = d(b,a),$$

et si l'inégalité triangulaire est remplacée par l'inégalité plus forte :

$$d(a,c) \leq \max[d(a,b), d(b,c)], \tag{1.1}$$

appelée l'*inégalité ultramétrique*.

1.1.2. Comme conséquence de l'inégalité (1.1), il est facile de voir que :

$$d(a,b) < d(b,c) \implies d(a,c) = d(b,c),$$

Si on pense géométriquement, cela signifie que "tous les triangles sont isocèles". Une conséquence amusante est que tout point d'un disque est son centre. Car soient

$$D_a(r) = \{x\ ; d(a,x) \leq r\}$$
$$D_a(r^-) = \{x\ ;\ d(a,x) < r\}.$$

Alors pour tout b dans $D_a(r)$, $D_b(r) = D_a(r)$. De plus, si la "circonférence" $\{x\ ;\ d(a,x) = r\}$ est non vide, elle contient tout "disque ouvert" $D_b(r^-)$ de n'importe lequel de ses points b, et est plus grande (souvent beaucoup plus grande) que l'"intérieur" $D_a(r^-)$.

Référence : Gilles Christol, "p-adic numbers and ultrametricity", dans Waldschmidt, Luck, Moussa, Itzykson (éds.), From Number Theory to Physics, Les Houches 1989, Springer Verlag, 1992, p. 440-475.
Traduction : Denise Vella-Chemla, 26.4.2022.

Remarques.

* L'ensemble E est muni de sa topologie d'espace métrique, et des propriétés topologiques comme la complétude de E feront référence à la topologie en question.

* Les notions de "disque ouvert", "intérieur", "circonférence" sont mises entre guillemets parce qu'elles *ne sont pas prises dans leur sens topologique*. En fait tout disque $D_a(r)$ ou $D_a(r^-)$ est à la fois ouvert et fermé.

  Par définition de la topologie métrique, chaque point de E a un système fondamental de voisinages qui consiste en des disques qui sont à la fois ouverts et fermés. Un espace topologique avec cette propriété est dit *totalement déconnecté*.

1.2. Valeur absolue et valuations

1.2.1. Si l'ensemble E est un groupe commutatif (avec la composition dénotée additivement), il est naturel de se demander si la distance est compatible avec l'addition :

$$d(a+c, b+c) = d(a, b).$$

Alors la distance est entièrement déterminée par les nombres $d(a, 0) = d(0, a)$. Une autre conséquence amusante de l'ultramétricité est qu'une série converge dans un groupe ultramétrique dès que son terme général converge vers zéro.

1.2.2. Si l'ensemble E est un anneau commutatif, la compatibilité s'exprime ainsi :

$$d(a, b) = |a - b|,$$

où $|.|$ est une *valeur absolue ultramétrique*, i.e. satisfait :

$$\begin{cases} |a| \geq 0\ ; \quad |a| = 0 \iff a = 0; \\ |a+b| \leq \max(|a|, |b|)\ ;\ |ab| = |a||b|. \end{cases} \tag{1.2}$$

Un anneau muni d'une valeur absolue ultramétrique est appelé *anneau valué*. Un anneau peut être valué si et seulement s'il n'a pas de diviseur de zéro, en effet, sur tout anneau sans diviseur de zéro, il y a une valuation triviale définie par :

$$\forall (a \neq 0), |a| = 1.$$

De ce fait, un anneau valué a un corps de fractions auquel la valeur absolue peut être étendue par :

$$|a/b| = |a|/|b|$$

Ainsi, les anneaux valués sont les sous-anneaux de corps valués. De tels corps sont souvent appelés *non archimédiens* par référence à la propriété archimédienne de $\mathbb{R}$ muni de la valeur absolue classique (ou $\mathbb{C}$ muni de la norme, ...) qui est qu'on peut atteindre tous les points à partir de zéro avec des marches de n'importe quelle longueur.

1.2.3. Si K est un corps valué, l'ensemble $\{|a| \ ; a \in K\}$ est un sous-groupe multiplicatif de $\mathbb{R}^+$. Dans de nombreuses circonstances, il est plus pratique d'utiliser des notations "additives"[1]. Dans ce but, on choisit un nombre $\alpha > 1$, et on définit :

$$v(a) = \begin{cases} -\log_\alpha(|a|) & \text{si } a \neq 0 \\ \infty & \text{si } a = 0. \end{cases}$$

En traduisant les propriétés ultramétriques, on obtient :

$$\begin{array}{ll} & v(a) = \infty \iff a = 0 \ ; \\ (1.3) & v(a+b) \geq \inf(v(a), v(b)) \ ; \\ & v(ab) = v(a) + v(b). \end{array}$$

Une application d'un corps K vers $\mathbb{R} \cup \{\infty\}$ qui vérifie (1.3) est appelée une *valuation*. Étant donnée une valuation v, on obtient en retour une distance ultramétrique par

$$d(a,b) = \alpha^{-v(a-b)}.$$

Clairement les distances construites de cette manière avec des nombres α différents sont toutes équivalentes (i.e. elles définissent la même topologie).

2. Une procédure générale pour obtenir des espaces ultramétriques

2.1. Construction

2.1.1. Nous donnerons une description générale d'une large classe d'espaces ultramétriques qui contient, entre autres, les anneaux complets valués *discrètement* (i.e. des anneaux valués avec valuations dans $\mathbb{N}$). Nous pensons que la vision que cela donne des espaces ultramétriques est plus réaliste que la représentation géométrique. Les exemples de 3) illustrent la "théorie" suivante.

2.1.2. Examinons un objet selon différents grossissements. Selon chaque grossissement, l'objet semble être composé d'un ensemble (fini ou pas) de points. Par exemple, selon le grossissement "zéro", il y a seulement un point, notamment l'objet lui-même. Maintenant en augmentant petit à petit le grossissement, on voit chaque point être un ensemble de points plus petits, chacun d'eux pouvant à son tour être séparé en sous-points et etc. Notre but est de décrire l'objet comme il apparaît selon un grossissement infini. On construit un modèle mathématique de la situation en donnant une séquence infinie E_n $(n = 0, 1, ...)$ d'ensembles reliés par des applications φ_n de E_{n+1} vers E_n. La situation peut aussi être représentée par un arbre dont les nœuds sont les éléments de $\bigcup E_n$ et dont les branches (dirigées) relient $a_{n+1} \in E_{n+1}$ à $\varphi_n(a_{n+1})$. Sur la fig. 1, on représente le cas où chaque point de E_n est l'image d'exactement deux éléments de E_{n+1}.

[1]Dans le but de simplifier, on définit v seulement dans le cas des valeurs absolues, mais la notation additive est utile en général, comme on le verra en 2.

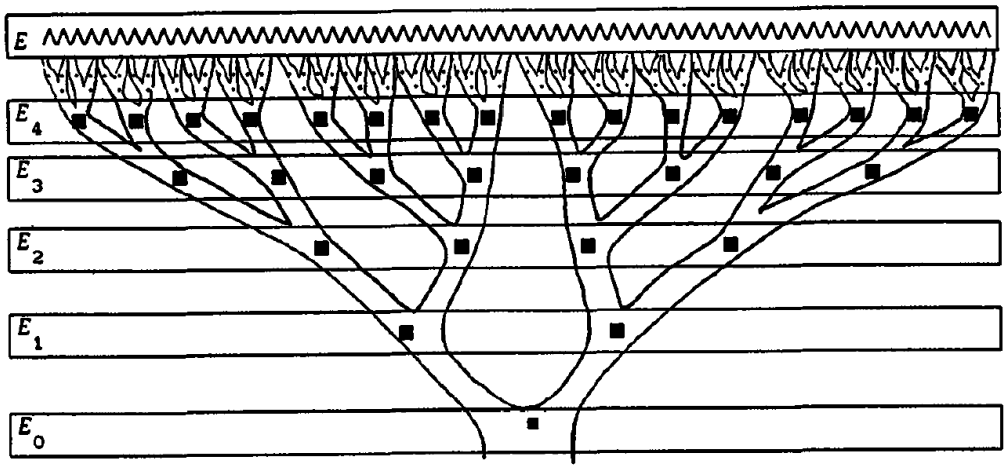


FIG. 1.

Maintenant pour représenter notre objet, on considère l'ensemble E des "feuilles de l'arbre" (ou des chemins partant de la racine E_0 et de longueur infinie) i.e. plus précisément, l'ensemble des séquences $a = \{a_n\}$ telles que :

$$a_n \in E_n \ ; \ \varphi_n(a_{n+1}) = a_n. \tag{2.1}$$

Classiquement, on utilise la notation:

$$E = \varprojlim E_n$$

et on appelle E la *limite inverse* des E_n.

2.1.3. Vérifions que l'ensemble E est équipé d'une topologie ultramétrique. Dans ce but, définissons d'abord une distance "naturelle" sur l'arbre qu'on vient de définir : soit $\{d_n\}$ n'importe quelle séquence décroissante de nombres réels convergeant vers zéro (par exemple, $d_n = \alpha^n$ pour tout $\alpha < 1$), et admettons que toute arête reliant un sommet de E_{n+1} à un sommet de E_n a une longueur égale à $\frac{1}{2}(d_n - d_{n+1})$. Alors tout chemin dirigé infini se terminant dans E_n a une longueur de $\frac{1}{2}d_n$ et tout chemin dans l'arbre a une longueur finie. Maintenant, il y a une distance triviale sur E, notamment la longueur du (plus court) chemin allant d'une "feuille" à une autre et passant à travers l'arbre. Cette définition peut facilement s'exprimer en termes mathématiquement corrects. Soient a et b deux éléments distincts de E, i.e. deux séquences $\{a_n\}$ et $\{b_n\}$ vérifiant (2.1) (par conséquent $a_n = b_n$ implique $a_i = b_i$ pour $i \leq n$), appelons :

$$v(a, b) = \sup\{n \ ; a_n = b_n\}$$

(c'est le niveau auquel l'"ancêtre commun" de a et b appartient). Alors la formule :

$$d(a, b) = d_{v(a,b)}$$

définit une distance ultramétrique sur E. De plus, l'espace topologique E ainsi obtenu est indépendant de la séquence $\{d_n\}$ et il est *complet*. En effet, si $a(m)$ est une séquence de Cauchy dans E, alors, pour m suffisamment grand, les $a(m)$ restent dans le même disque (comme E est ultramétrique, pour sortir du disque on a besoin de faire un saut plus grand que son rayon) i.e. la séquence $a(m)_n$,

est finalement constante. Ainsi, si a est défini par $a_n = \lim a(m)_n$ pour tout n, on voit aisément que $a = \lim a(m)$. L'espace E est un espace *compact* si et seulement si les ensembles E_n sont finis. En effet, si E est compact, les disques "ouverts" de rayons d_n sont en correspondance bijective avec les éléments sur E_n, mais ils forment un recouvrement disjoint de E. Donc les E_n doivent être finis. Inversement, si les E_n sont finis, pour toute séquence $a(m)$ dans E, on peut trouver a dans E tel que pour tout n on a $a(m)_n = a_n$ pour un nombre infini de m. Ainsi a est un point limite de la séquence et E est compact. Si v est une valuation, on doit choisir $d_n = \alpha^n$ pour un certain $\alpha < 1$ pour que la distance devienne une valeur absolue.

2.2. Propriétés supplémentaires

2.2.1. Si les E_n sont des groupes (commutatifs) et si les φ_n sont des homomorphismes de groupes alors E lui-même est un groupe avec la règle de composition :

$$\{a_n\} + \{b_n\} = \{a_n + b_n\}$$

avec laquelle la distance est compatible au sens de 1.2.1.

2.2.2. De la même manière, si les E_n sont des anneaux et si les φ_n sont des homomorphismes d'anneaux, alors E devient un anneau pour le produit :

$$\{a_n\}\{b_n\} = \{a_n b_n\}.$$

Mais il n'y a pas de raison que ce produit soit compatible avec la distance au sens de 1.2.2, i.e. pour :

$$v(a) = v(a, 0) = \inf\{n \ ; \ a_n \neq 0\}$$

pour satisfaire $v(ab) = v(a)v(b)$. Par exemple, si les E_n n'ont pas de diviseurs de zéro, on obtient seulement :

$$v(ab) \geq \sup(v(a), v(b)),$$

qui est suffisant pour assurer la continuité du produit.

2.2.3. Dans de nombreux exemples, il est possible, pour chaque sommet, de sélectionner une arête parmi celles aboutissant à ce sommet. En d'autres termes, E_n peut être "relevé" en E_{n+1}, i.e. il existe des applications ψ_n de E_n dans E_{n+1} telles que $\varphi_n \circ \psi_n =$ Identité. Si cette situation advient, lorsqu'on décrit E il est plus concis d'omettre à chaque niveau l'information déjà connue du niveau précédent. Plus précisément, les éléments de E peuvent être donnés de la manière suivante : soit $E_{[n]}$ le groupe quotient $E_{n+1}/\psi_n(E_n)$ (isomorphe au noyau de φ_n), alors l'élément $\{a_n\}$ de E est entièrement déterminé par la séquence $a_{[0]}, \ldots, a_{[n]}, \ldots$, où $a_{[0]} = a_1$ et $a_{[n]}$ est l'image de a_{n+1} dans $E_{n+1}/\psi(E_n)$.

Cette représentation peut être vue comme une sorte de développement décimal généralisé. De plus, pour chaque n il y a un "relèvement canonique" de E_n vers E où $\psi(a_n)$ est donné par le chemin infini passant par a_n et contenant les sommets choisis.

2.2.4. Une situation analogue advient dans les circonstances suivantes. Soit A un anneau et I_n une séquence d'idéaux de A telle que :

$$I_{n+1} \subset I_n \qquad \text{et} \qquad \bigcap I_n = \{0\}.$$

Soit E_n l'anneau A/I_n. La réduction modulo I_n donne un homomorphisme φ_n de E_{n+1} dans E_n, et ainsi une distance sur l'anneau $E = \varprojlim E_n$ comme montré en 2.1. Il y a un encastrement canonique de A dans E : chaque a dans A est relié à la séquence $\{a \bmod I_n\}$. Alors A est un sous-ensemble topologique dense de E. En d'autres termes, E est la complétion de A pour la topologie construite à partir des I_n. Le v défini en 2.2.2 est effectivement une valuation quand $I_n = I^n$ pour un certain idéal $I \neq A$ (tel que $\cap I^n = 0$).

3. Exemples élémentaires

3.1. Polynômes et séries de puissances

3.1.1. Soit k un corps et soit E_n le groupe additif des polynômes à coefficients dans k de degré inférieur ou égal à n. La projection naturelle de E_{n+1} dans E_n, notamment "oublier le terme de degré $n+1$", permet de construire un groupe E selon la démarche de 2.1 (utiliser 2.2.1 pour la structure de groupe).

3.1.2. La description de cet ensemble est plus concrète si on utilise la ruse de 2.2.3 (en effet, E_n est un sous-ensemble de E_{n+1}): il s'avère être l'ensemble $k[[x]]$ des "séries formelles de puissances sur k" i.e. l'ensemble des séries de puissances :

$$a = \sum_{n=0}^{\infty} a_{[n]} x^n \ , \qquad a_{[n]} \in k$$

sans aucune condition sur les $a_{[n]}$ (ils sont formels parce que, par exemple, si $k = \mathbb{C}$, la plupart d'entre eux sont convergents nulle part). La distance entre deux séries de puissances a et b est $\alpha^{v(a-b)}$ ($\alpha < 1$) où $v(a-b)$ est la valuation de $a-b$, notamment le plus petit entier tel que le coefficient du terme de degré n dans $a-b$ est non nul.

3.1.3. Maintenant, il y a un produit classique sur $k[[z]]$ donné par :

$$ab_{[n]} = \sum_{k=0}^{\infty} a_{[k]} b_{[n-k]}$$

qui est une extension du produit des polynômes. Pour cette loi, la valuation qui vient d'être définie respecte la condition (1.3) et est effectivement une valuation ! Cette valuation est appelée la *valuation x-adique*. Cette désignation rappelle que l'on est dans une situation dans laquelle 2.2.4 s'applique, en prenant pour A l'anneau $k[x]$ de tous les polynômes à coefficients dans k et pour I l'idéal $xk[x]$ (alors $I_n = I^n$ est l'idéal $x^n k[x]$). Dans cette description, E_n est l'ensemble des polynômes modulo x^n et $k[[x]]$ est la complétion de $k[x]$ selon la valuation x-adique (un polynôme est une série de puissances dont les coefficients sont finalement nuls !).

3.1.4. Comme $k[[x]]$ est un anneau valué il a un corps de fractions, notamment le corps $k((z))$ de séries formelles de puissances sur k, dont les éléments sont :

$$a = \sum_{n=v(a)}^{\infty} a_{[n]} x^n \ , \qquad a_{[n]} \in k \ , \qquad a_{a[v(a)]} \neq 0$$

où $v(a)$ appartient à $\mathbb{Z}$ et est, trivialement, la valuation de a. Le corps $k(x)$ des fractions rationnelles sur k est le corps de fractions de l'anneau des polynômes qui est alors contenu dans $k((x))$. La valuation x-adique d'une fraction rationnelle f s'obtient en l'écrivant sous la forme :

$$x^{v(f)} P(x)/Q(x) \ ; \ P(0) \neq 0 \ ; \ Q(0) \neq 0$$

(ce qui nous permet de la développer en série de Laurent "près de 0"). Il y a réellement de nombreuses autres valuations définies sur $k(x)$ notamment une pour chaque polynôme irréductible de $k[x]$. Par exemple, si k est algébriquement fermé, les valuations de $k(x)$ sont en correspondance bijective avec les points de la "droite projective" sur k, i.e. $k \cup \{\infty\}$: la valuation associée au point ξ est donnée par le développement de la fraction rationnelle en série de Laurent près de ξ (i.e. dans $k((x-\xi))$ pour ξ fini et dans $k((1/x))$ si $\xi = \infty$).

3.2. Nombres p-adiques

3.2.1. Soit p un nombre premier et soit $E_n = \mathbb{Z}/p^n\mathbb{Z}$ l'anneau des "entiers modulo p^n". La projection[2] de E_{n+1} dans E_n donnée par le reste lorsqu'on divise par p^n nous permet de construire un anneau E selon les étapes vues en 2.1 (utiliser 2.2.1 et 2.2.2 pour la structure d'anneau). La Figure 2 montre la construction quand $p = 2$. L'anneau est dénoté par $\mathbb{Z}_p$, et est appelé *anneau des entiers p-adiques*.

3.2.2. Décrivons maintenant $\mathbb{Z}_p$ plus concrètement. En utilisant $[0, 1, \ldots, p^n - 1]$ comme ensemble de représentants, E_n s'avère être un sous-ensemble de E_{n+1}. Même si cette injection n'est pas un homomorphisme d'anneaux (par exemple $1 + (p^n - 1)$ est égal à 0 dans E_n mais pas dans E_{n+1}), cela nous permet d'appliquer la ruse de 2.2.3. L'anneau $\mathbb{Z}_p$ s'avère être l'ensemble des *séries de Hensel* :

$$a = \sum_{n=0}^{\infty} a_{[n]} p^n \ , \qquad a_{[n]} \in [0, \ldots, p-1].$$

Avec ces notations, la valuation (p-adique) d'un entier p-adique a est le plus petit entier n tel que $a_{[n]} \neq 0$. Il n'est pas difficile de prouver que ceci est effectivement une valuation. Classiquement, le nombre α utilisé pour définir la valeur absolue correspondante est choisi comme étant égal à $\frac{1}{p}$ de telle façon que la *distance* (*p-adique*) entre deux entiers p-adiques a et b est $p^{-v(a-b)}$.

[2] Il y a une autre projection naturelle donnée par le quotient en divisant par p, mais cette seconde projection n'est pas un homomorphisme d'anneaux et ne nous intéresse pas.

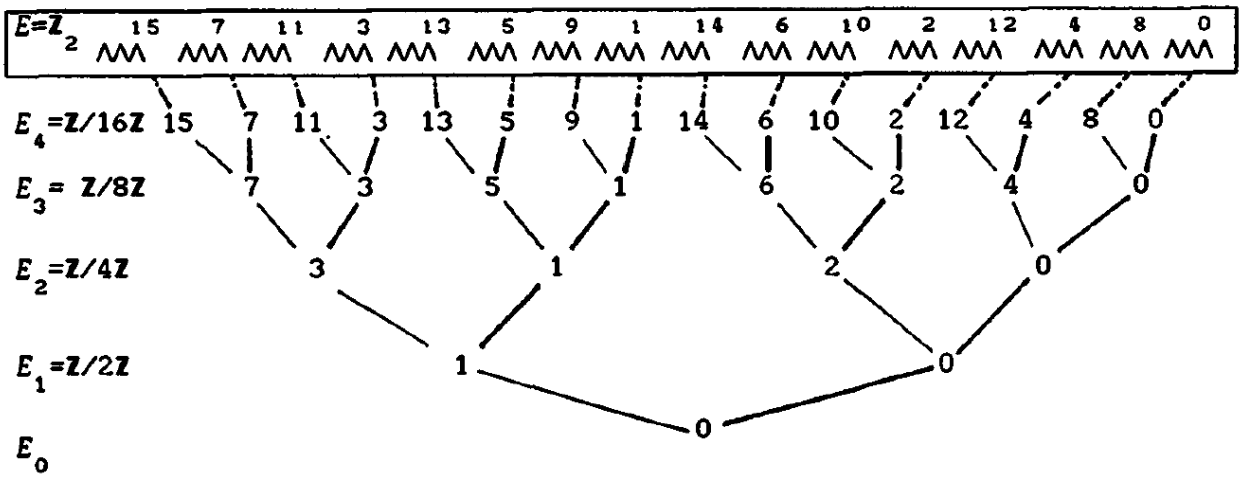


FIG. 2. L'"arbre" des nombres 2-adiques

Remarques.

* Une séquence infinie $a_{[n]}$ de chiffres dans $[0, \ldots, p-1]$ peut représenter un élément de trois groupes additifs distincts :

  1) un nombre réel $a_{[0]}, a_{[1]} \ldots a_{[n]}$ de $\mathbb{R}/p\mathbb{Z}$,
  2) une série de puissances $a_{[0]} + a_{[1]}x + \ldots + a_{[n]}x^n + \ldots$ de $\mathbb{Z}/p\mathbb{Z}[[x]]$,
  3) un entier p-adique $a_{[0]} + a_{[1]}p + \ldots + a_{[n]}p^n + \ldots$ de $\mathbb{Z}_p$.

  Chacun de ces groupes est caractérisé par la manière dont on y effectue les additions. Pour les séries de puissances, on se comporte comme les cancres et on oublie les retenues, pour les nombres réels, comme tout le monde le sait, on reporte la retenue à gauche et pour les entiers p-adiques, on reporte la retenue sur la droite. Ce fait explique pourquoi de petites perturbations peuvent changer tous les chiffres dans le cas réel mais pas dans les deux autres cas, où l'on ne peut pas modifier des nombres avant celui qui a été modifié.

* On utilise $[0, 1, ..., p^n-1]$ comme ensemble de représentants, mais d'autres choix sont possibles, par exemple $[(1-p)/2, ...(p-1)/2]$ quand $p \neq 2$. Chaque choix amène à une représentation différente de Z_p au moyen d'un développement de Hensel. Les différences n'apparaissent que dans les calculs explicites.

3.2.3. Dans la description ci-dessus, un entier positif m appartient à E_n dès que $p^n > m$. Alors, en utilisant 2.2.3, il peut être vu comme un élément de $\mathbb{Z}_p$. Sa série (finie) de Hensel est son développement en base p. On voit facilement que sa valuation p-adique est la puissance du nombre premier p qui apparaît dans sa factorisation : par exemple, la valuation 3-adique de $2250 = 2.3^2.5^3$ est 2. De cette manière, $\mathbb{Z}_p$ devient la complétion de l'ensemble $\mathbb{N}$ des entiers naturels muni de la distance p-adique.

Comme exercice, on laisse la lectrice vérifier que les entiers négatifs correspondent aux séries de Hensel dont les coefficients sont finalement égaux à $(p-1)$: par exemple, dans $\mathbb{Z}_3$ on a :

$$-5 = 1 + 1.3 + 2.3^2 + 2.3^3 + 2.3^4 + ...$$

3.2.4. Puisque $\mathbb{Z}_p$ est un anneau valué, il a un corps de fractions, notamment le corps $\mathbb{Q}_p$ de *nombres p-adiques*. En utilisant les représentations de Hensel, les éléments de $\mathbb{Q}_p$ sont

$$a = \sum_{n=v(a)}^{\infty} a_{[n]} p^n \ , \qquad a_{[n]} \in [0, \ldots, p-1] \ , \qquad a_{[v(a)]} \neq 0 \ ,$$

où $v(a)$ appartient à $\mathbb{Z}$ et est, de façon évidente, la valuation (p-adique) de a. Le corps $\mathbb{Q}$ des nombres rationnels est contenu dans $\mathbb{Q}_p$, les rationnels apparaissant comme les séquences terminales de Hensel. Par exemple, dans $\mathbb{Q}_3$ on a :

$$\frac{1}{24} = \frac{2}{3} + \frac{2+3}{1-9} = 2.\frac{1}{3} + 2 + 3 + 2.3^2 + 3^3 + \ldots .$$

La valuation p-adique $v(r)$ d'un nombre rationnel r est donnée en l'écrivant sous la forme :

$$p^{v(r)} \frac{m}{d} \ ; \qquad \text{avec } m \text{ et } d \text{ premiers à } p.$$

3.2.5. Pour chaque nombre premier p on a défini une valuation p-adique (resp. une valeur absolue) sur $\mathbb{Q}$. Nous la dénoterons v_p (resp. $|.|_p$) quand il peut y avoir confusion. Outre la valeur absolue classique (souvent dénotée par $|.|_\infty$ par analogie avec l'exemple 3.1) ce sont principalement les seules, plus précisément toute valuation non triviale sur $\mathbb{Q}$ doit être équivalente à l'une d'entre elles. De plus elles sont reliées par la *formule du produit* :

$$|r|_\infty \prod_{p \text{ premier}} |r|_p = 1.$$

3.3. L'anneau $\widehat{\mathbb{Z}}$ et les nombres adéliques

3.3.1. Comme il est difficile de croire que n'importe quel nombre premier à lui tout seul jouerait un rôle particulier dans la nature, on généralise la construction de l'exemple 3.2 sans privilégier aucun nombre premier. Le point de départ est la famille d'ensembles finis $E_n = \mathbb{Z}/n\mathbb{Z}$ d'"entiers modulo n". Pour tout entier k il y a une projection de E_{kn} vers E_n donné par le reste obtenu en divisant par n. Ces projections nous permettent de construire un anneau, dénoté par $\widehat{\mathbb{Z}}$, selon une méthode qui généralise celle de 2.1. Pourtant les choses sont un peu plus compliquées parce que les ensembles E_n ne sont plus empilés mais ordonnés d'une manière plus intriquée comme cela est montré sur la Figure 3.

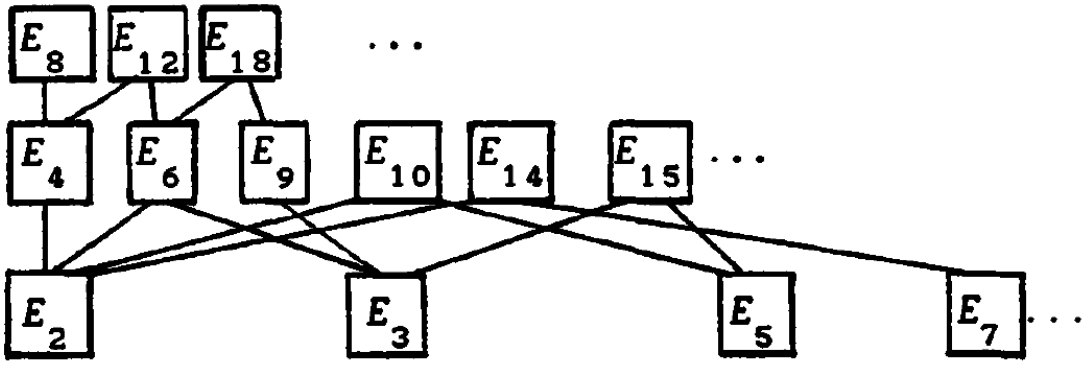


FIG. 3.

Notons qu'utiliser deux chemins différents de E_n à E_m donne la même projection. En effectuant un choix arbitraire, on travaillera dans une sous-pile du tableau et alors on retrouvera la construction "classique" 2.1.

3.3.2. Une séquence d'entiers $\{u_n\}$ est dite aller *multiplicativement à l'infini* si, pour n'importe quel entier donné k, il existe un entier N tel que, pour $n > N$, u_n devient un multiple de k. Par exemple, la séquence $n!$ va multiplicativement à l'infini. On choisit une fois pour toutes une séquence $\{u_n\}$ parmi les nombreuses séquences, qui satisfait les deux conditions :

$$\begin{cases} (3.3.2.1) & \{u_n\} \text{ va à l'infini multiplicativement} \\ (3.3.2.2) & u_0 = 1 \text{ et pour tout } n,\ u_n \text{ divise } u_{n+1}. \end{cases}$$

3.3.3. Changeons légèrement les notations et dénotons par E_n l'ensemble $\mathbb{Z}/u_n\mathbb{Z}$. La condition (3.3.2.2) implique que nous pouvons appliquer la construction de 2.1 et les remarques algébriques de 2.2 à la suite d'anneaux E_n et obtenir un anneau $E = \widehat{\mathbb{Z}}$. En choisissant par exemple la séquence $\{1, 2, 6, 12, 60, ...\}$ pour u_n, on obtient l'"arbre" de la Fig.4.

Alors la condition (3.3.2.1) dit que des entiers distincts seront finalement séparés dans la construction, et par conséquent que $\mathbb{Z}$ est un sous-anneau de $\widehat{\mathbb{Z}}$. La topologie induite sur $\mathbb{Z}$ est décrite par la remarque suivante : *une séquence d'entiers converge vers 0 dans $\widehat{Z}$ si et seulement si elle converge multiplicativement vers l'infini* (notons que ceci est indépendant de la séquence choisie $\{u_n\}$. On a effectivement un cas particulier de 2.2.4 avec $A = \mathbb{Z}$ et $I_n = u_n\mathbb{Z}$. Par conséquent $\mathbb{Z}$ est dense dans $\widehat{\mathbb{Z}}$ et $\widehat{\mathbb{Z}}$ apparaît comme le sous-ensemble des "limites" des séquences $\{s_n\}$ d'entiers telles que $s_n - s_m$ devient un multiple de n'importe quel entier fixé quand n et m sont suffisamment grands.

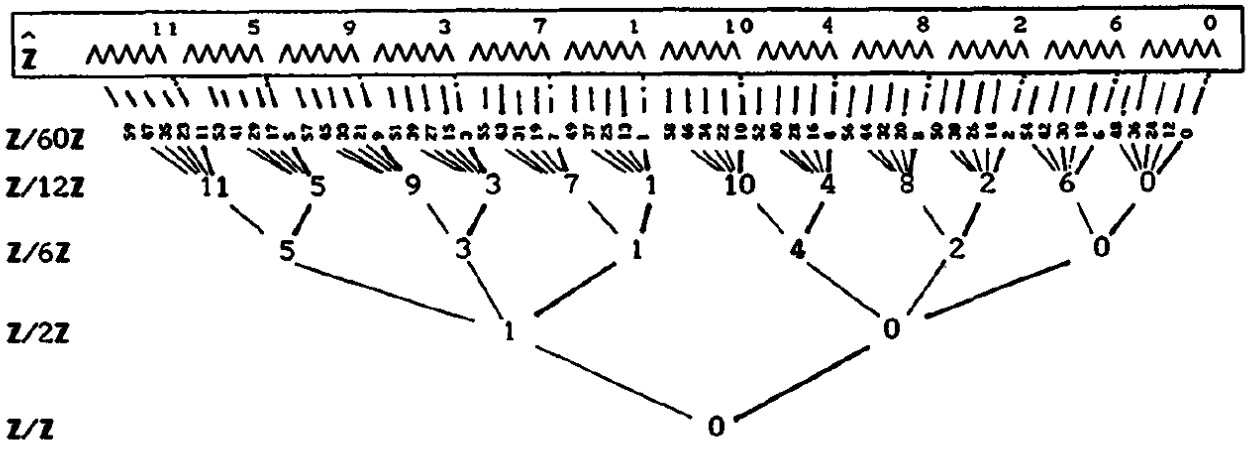


FIG. 4. Un $\widehat{\mathbb{Z}}$-arbre

Remarque. Comme il y a toujours de nouveaux nombres premiers disponibles, on ne peut pas avoir $I_{n+m} \supset I_n.I_m$ pour tous les entiers n et m, par conséquent, le v défini en 2.2.2 n'est pas une valuation, et $\widehat{\mathbb{Z}}$ n'est pas un anneau valué mais seulement un anneau ultramétrique compact et complet.

3.3.4. Soit n un entier ; à partir de sa factorisation :

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

on obtient la décomposition (c'est le théorème des restes chinois) :

$$\mathbb{Z}/n\mathbb{Z} = \prod_{p \text{ premier}} \mathbb{Z}/p^{v_p(n)}\mathbb{Z}$$

(il y a effectivement seulement un nombre fini de nombres premiers dans le produit, notamment ceux divisant n). On peut appliquer cette décomposition pour chaque u_n. Pour n'importe quel nombre premier p, la condition 3.3.2.2 dit que la séquence $v_p(u_n)$ augmente et la condition 3.1.2.1 dit qu'il tend vers l'infini. Alors la décomposition donne la limite :

$$\widehat{\mathbb{Z}} = \prod_{p \text{ premier}} \mathbb{Z}_p \ ;$$

Ici $\widehat{\mathbb{Z}}$ est un ensemble compact, ainsi qu'un produit (infini) d'ensembles compacts. Cela nous permet d'écrire un élément a de $\widehat{\mathbb{Z}}$ comme une famille $(a_2, a_3, a_5, \ldots, a_p, \ldots)$ de nombres p-adiques. Les lois d'addition et multiplication agissent composante par composante. Comme exercice, le lecteur peut retrouver les a_n de la construction 2.1 à partir des a_p qui viennent d'être définis.

3.3.5. L'anneau $\widehat{\mathbb{Z}}$ a de nombreux diviseurs de zéro, comme on peut facilement le voir à partir de 3.3.4 (par conséquent il ne peut être valué !). Donc il n'a pas de corps de fractions. Pourtant, une sorte de "corps de fractions" peut être défini, notamment l'anneau des *adèles finies* :

$$A_f = (a_2, a_3, \ldots, a_p, \ldots) \ ;$$
$$a_p \in \mathbb{Q}_p, a_p \in \mathbb{Z}_p \qquad \text{pour tous les p sauf un nombre fini d'entre eux.}$$

Les *adèles* $\mathbb{A}$ sont construites de la même manière mais avec une composante de plus a_∞ appartenant à $\mathbb{R}$, de telle façon que toutes les complétions de $\mathbb{Q}$ soient considérées. Le groupe des *idèles (finies)* est le sous-groupe multiplicatif des éléments inversibles des adèles (finies). Ce sont les adèles (finies) n'ayant aucune composante nulle et toutes les composantes sauf un nombre fini d'entre elles de valuation (p-adique) 0 (ou de manière équivalente de valeur absolue 1). Étant donnée une idèle, le nombre :

$$|a_\infty|_\infty \prod_{p \text{ premier}} |a_p|_p$$

est appelé son volume. Tout nombre rationnel a est identifié avec l'adèle (finie) dont toutes les composantes sont égales à a (si a est un entier, on obtient l'élément de $\widehat{\mathbb{Z}}$ déjà obtenu dans 3.3.3.). Si $a \neq 0$ on obtient une idèle et la formule du produit affirme qu'elle a un volume unitaire. Il vaut la peine de signaler que $\mathbb{Q}$ est un sous-groupe discret de $\mathbb{A}$ pour l'addition, comme $\mathbb{Z}$ est un sous-groupe discret de $\mathbb{R}$ (en effet, deux nombres rationnels sont à distance 1 l'un de l'autre pour toutes les distances p-adiques sauf pour un nombre fini d'entre elles). De plus, l'analogie va plus loin et le quotient dans les deux cas est compact (en utilisant le théorème des restes chinois on prouve que $\mathbb{A}/\mathbb{Q} = \mathbb{R}/\mathbb{Z} \prod \mathbb{Z}_p$).

3.4. Matrices de Parisi

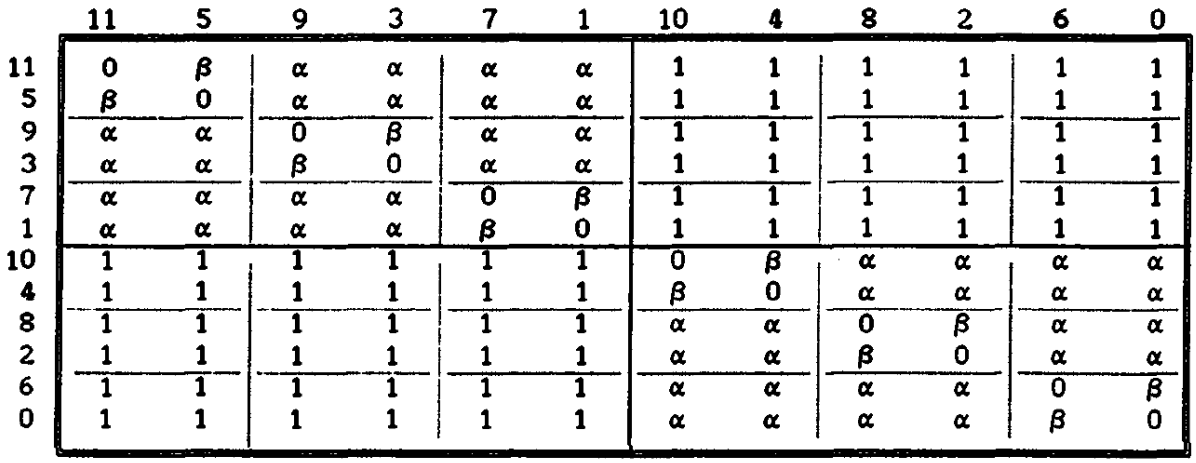
3.4.1. Rappelons la définition des matrices introduites par Parisi comme "brisure de symétrie des répliques" dans le modèle du champ moyen d'un verre de spins de Sherrington-Kirkpatrick (pour des détails, voir Rammal, Toulouse, et Virasoro 1986). Soient $1 = m_N \leq \ldots \leq m_0 = n$ des entiers tels que m_i est un multiple de m_{i+1} et soit Q_i $(0 \leq i \leq N-1)$ une séquence de nombres réels. À partir de ces données, pour $0 \leq i \leq N$, on peut construire une matrice $(n/m_i) \times (n/m_i)$, $\mathbf{Q}^{(i)}$, en suivant les règles récursives suivantes :

a) $\mathbf{Q}^{(0)} = [0]$,

b) La matrice $\mathbf{Q}^{(i+1)}$ est construite en substituant à l'entrée $\mathbf{Q}^{(i)}_{a,b}$ de la matrice $\mathbf{Q}^{(i)}$ de taille $(m_i/m_{i+1}) \times (m_i/m_{i+1})$ l'élément $\mathbf{P}^{(i),a,b}$ défini par :

$$\mathbf{P}^{(i),a,b}_{c,d} = \begin{cases} \mathbf{Q}^{(i)}_{a,b} & \text{si } a \neq b \\ Q_i & \text{si } a = b \text{ et } c \neq d \\ 0 & \text{si } a = b \text{ et } c = d \end{cases}$$

À la fin du processus, on obtient une matrice appelée *matrice de Parisi* $\mathbf{Q} = \mathbf{Q}^{(N)}$.



	11	5	9	3	7	1	10	4	8	2	6	0
11	0	β	α	α	α	α	1	1	1	1	1	1
5	β	0	α	α	α	α	1	1	1	1	1	1
9	α	α	0	β	α	α	1	1	1	1	1	1
3	α	α	β	0	α	α	1	1	1	1	1	1
7	α	α	α	α	0	β	1	1	1	1	1	1
1	α	α	α	α	β	0	1	1	1	1	1	1
10	1	1	1	1	1	1	0	β	α	α	α	α
4	1	1	1	1	1	1	β	0	α	α	α	α
8	1	1	1	1	1	1	α	α	0	β	α	α
2	1	1	1	1	1	1	α	α	β	0	α	α
6	1	1	1	1	1	1	α	α	α	α	0	β
0	1	1	1	1	1	1	α	α	α	α	β	0

FIG. 5.

3.4.2. On vérifie maintenant que, au moyen d'un léger changement de notation, une matrice de Parisi, obtenue à partir d'une séquence strictement décroissante Q_i de nombres réels positifs, n'est rien d'autre que la table des distances mutuelles "au niveau n" de $\widehat{\mathbb{Z}}$ muni d'une des distances définies en 3.3.3. Il n'est donc pas surprenant que les calculs basés sur de telles matrices amènent à un espace ultramétrique. Plus précisément, choisissons une séquence $\{u_n\}$ d'entiers vérifiant (3.3.2.1) et (3.3.2.2) et une séquence strictement décroissante $\{d_n\}$ de nombres réels tendant vers zéro telle que, pour $0 \leq i \leq N$:

$$u_1 = m_{N-i} \; ; \; d_i = Q_{N-i}$$

et construisons la distance associée sur $\widehat{\mathbb{Z}}$ en suivant les étapes de 3.3.2 et 2.1.3. Alors, si nous ordonnons le sous-ensemble $(0, 1, ..., n-1)$ de $\widehat{\mathbb{Z}}$ selon le reste des divisions par les u_i, la table des distances mutuelles est exactement la matrice de Parisi. Nous pensons qu'un exemple est mieux qu'une explication compliquée. La Figure 5 donne la matrice de Parisi pour les séquences $\{1, 2, 6, 12, ...\}$ et $\{1, \alpha, \beta, ...\}$. On doit noter que les matrices de Parisi sont habituellement construites à partir des séquences croissantes Q_i et que la distance associée est en fait donnée par $1 - Q_i$. Quand on travaille dans cette dernière situation, il peut être plus pratique d'avoir des entrées sur la diagonale égales à 1 plutôt qu'à 0.

B. Corps valués non archimédiens complets

4. Propriétés générales

4.1. Définitions

4.1.1. Soit K un corps valué non archimédien i.e. (voir 1.2.2) un corps muni d'une valeur absolue $|.|$ satisfaisant (1.2). L'ensemble :

$$\mathcal{O}_K = \{a \in K; |a| \leq 1\}$$

est un anneau valué (l'ultramétricité implique la stabilité selon l'addition). Il est appelé l'*anneau de valuation de* K. L'ensemble :

$$\mathcal{M}_K = \{a \in K; |a| < 1\}$$

est un idéal de $\mathcal{O}_K$. En fait c'est *l'*idéal maximal parce que tout élément u de $\mathcal{O}_K$ qui n'est pas dans $\mathcal{M}_K$ est inversible.

Par conséquent, l'ensemble :

$$k = \mathcal{O}_K/\mathcal{M}_K$$

est un corps appelé le *corps résiduel de* K. Par exemple, pour $k((x))$, l'anneau de valuation est $k[[x]]$ et le corps résiduel est k. Pour $\mathbb{Q}_p$ l'anneau de valuation est $\mathbb{Z}_p$, et le corps résiduel est $\mathbb{Z}/p\mathbb{Z}$, i.e. *le* corps avec p éléments, aussi dénoté par $\mathbb{F}_p$. On utilisera la notation habituelle suivante :

Si $a \in \mathcal{O}_K$, son image dans k est dénotée par $\overline{a}$.

Par exemple si a est un entier dans $\mathbb{Z}_p$, alors $\overline{a}$ est son résidu (mod p) dans $\mathbb{Z}/p\mathbb{Z}$.

4.1.2. Un corps est dit de caractéristique zéro s'il contient $\mathbb{Z}$. Sinon, sa caractéristique est le plus petit entier p pour lequel on a $p.1 = 0$. Cet entier doit être un nombre premier. Dénotons par $\mathrm{ch}(K)$ la caractéristique de K. L'examen des caractéristiques d'un corps valué non archimédien et de son corps résiduel amène à trois possibilités :

1) $\mathrm{ch}(K) = \mathrm{ch}(k) = 0$,
2) $\mathrm{ch}(K) = \mathrm{ch}(k) = p$,
3) $\mathrm{ch}(K) = 0; \mathrm{ch}(k) = p$.

Supposons de plus que le corps K est complet (pour la topologie définie par sa valuation) ; alors :

* Dans le cas de *caractéristiques égales* (cas 1 ou 2), le corps K contient des sous-corps isomorphes à $k((x))$. Plus explicitement, pour tout a dans l'idéal maximal, il y a un encastrement i, donné par $i(x) = a$, de $k((x))$ dans K. L'image de i est dénotée par $k((a))$.

* Dans le cas de *caractéristiques inégales* (cas 3), le corps K contient un sous-corps isomorphe à $\mathbb{Q}_p$.

4.2. Rechercher des carrés dans $\mathbb{Q}_p$

Notre prochain but est de résoudre des équations algébriques dans les corps complets valués non archimédiens. Commençons par le cas le plus simple, notamment les équations du second degré dans le corps des nombres p-adiques. Un calcul élémentaire réduit la question de résoudre l'équation $x^2 = a$. L'existence de solution(s) dans le corps $\mathbb{Q}_p$ sera étudiée en trois étapes :

4.2.1. Comme la valuation de tout élément de $\mathbb{Q}_p$ est un nombre entier, pour que a soit un carré, sa valuation doit être un entier *pair* (le cas trivial $a = 0$ étant omis). Par exemple p n'est pas un carré dans $\mathbb{Q}_p$.

4.2.2. Supposons que $v(a)$ soit paire, i.e., $a = p^{2n}u$, $|u| = 1$. Alors il suffit de résoudre $x^2 = u$. En prenant les restes, on obtient $\overline{x}^2 = \overline{u}$ (dans$\mathbb{F}_p$) et on trouve une seconde condition pour que a soit un carré dans $\mathbb{Q}_p$, notamment que $\overline{u}$ doit être un carré dans $\mathbb{F}_p$. Par exemple ni 2 ni -1 ne sont des carrés dans $\mathbb{Q}_3$ parce que 2 n'est pas un carré dans $\mathbb{F}_3$.

Remarque. Les carrés dans $\mathbb{F}_p$ peuvent être trouvés directement en élevant au carré tous les nombres dans $\mathbb{F}_p$ ou mieux en utilisant la loi de réciprocité bien connue de Gauss, que nous rappelons pour des raisons de complétude. Soit p un nombre premier et n un nombre entier premier à p. Le *symbole de Legendre* $\left(\frac{n}{p}\right)$ est 1 (resp. -1) si n est (resp. n'est pas) un carré dans $\mathbb{F}_p$. Le symbole de Legendre peut être facilement calculé au moyen des règles suivantes où p et q sont des nombres premiers distincts :

$$\left(\frac{n+p}{p}\right) = \left(\frac{n}{p}\right) \ , \ \left(\frac{n.m}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{m}{p}\right)$$

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \ , \ \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$$

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4} \qquad \text{(loi de réciprocité)}.$$

4.2.3. Maintenant $\overline{u}$ est un carré dans $\mathbb{F}_p$ si et seulement s'il existe α dans $\mathbb{Z}_p$ tel que $u - \alpha^2$ appartient à $p\mathbb{Z}_p$. Comme $\overline{u} \neq 0$, α est inversible dans $\mathbb{Z}_p$ et l'application :

$$\ell(x) = \frac{1}{2\alpha}\left(\frac{u-\alpha^2}{p} - px^2\right)$$

est une contraction de $\mathbb{Z}_p$. Son point fixe unique v satisfait :

$$u = (\alpha + pv)^2$$

et donne une racine carrée de u (commençant avec $-\alpha$ on obtient $-v$ et l'autre racine carrée). Nous résumons notre discussion par l'équivalence suivante :

$$\exists b \in \mathbb{Q}_p \ : \ a = b^2 \iff a = 0 \text{ ou } \begin{cases} a = p^{2n}u, |u| = 1 \\ \overline{u} = \alpha^2 \text{ (dans } \mathbb{F}_2). \end{cases}$$

Remarque. Dans $\mathbb{R}$ il y a seulement une condition à satisfaire pour que x soit un carré, notamment $x \geq 0$, mais dans $\mathbb{Q}_p$ il faut satisfaire deux conditions. Pour le dire brièvement, la moitié des nombres réelles sont des carrés (comparé à un quart des nombres p-adiques).

4.2.4. Exemple. Comme $-1 = 2 \times 2 \pmod 5$ le polynôme $x^2 + 1$ a une racine carrée a dans $\mathbb{Z}_5$ telle que $\overline{a} = 2$. C'est un bon exercice de faire de tels calculs explicites. En supposant que la racine soit $2 + 5b$, on trouve $b = 1 + 5(b + b^2)$, ce qui nous permet de trouver récursivement la séquence de Hensel :

$$a = 2 + 5 + 2.5^2 + 5^3 + 3.5^4 + 4.5^5 + 2.5^6 + 3.5^7 + \ldots$$

4.3. Lemme de Hensel

Fondamentalement, le lemme de Hensel fournit une généralisation de tout polynôme unitaire P à coefficients dans $\mathbb{Z}_p$ à partir du principe expliqué en 4.2.3 : grosso modo, pour toute racine α de $\overline{P}$ (le polynôme obtenu en prenant à la place les résidus des coefficients) il existe dans $\mathbb{Z}_p$ une racine a de P telle que $\overline{a} = \alpha$. Cela représente un outil encore plus basique pour résoudre les équations

algébriques dans un corps ultramétrique *complet* K puisque tout polynôme P dont les coefficients sont dans K peut être scindé en un produit de polynômes dont chacun a toutes ses racines de même valuation.

4.3.1. *Lemme de Hensel.* Soit K un corps complet ultramétrique et soit $P = \sum a_i x^i$ un polynôme dont les coefficients a_i sont dans $\mathcal{O}_K$. Supposons qu'il existe deux polynômes q et r dont les coefficients sont dans le corps résiduel k, respectivement premier, et tel que $\overline{P} = \sum \overline{a}_i x^i = qr$. Alors il existe deux polynômes Q et R dont les coefficients sont dans $\mathcal{O}_K$ et satisfaisant :

$$P = QR, \overline{Q} = q, \overline{R} = r, deg(Q) = deg(q).$$

La preuve de ce lemme est basée sur l'algorithme de Newton.

Remarques.

* La condition de primalité signifie que q et r n'ont pas de facteur commun ; il est essentiel comme montré par le polynôme $P = x^2 + p$ de $\mathbb{Z}_p[x]$ qui est irréductible mais vérifie $\overline{P} = xx$.

* Il y a plusieurs autres lemmes de Hensel (qui concernent les fonctions analytiques, les opérateurs différentiels,... au lieu des polynômes) ; chacun d'eux affirme, sous certaines légères conditions (ici la primalité), que toute cassure au niveau du corps résiduel est vraiment une cassure "totale".

4.3.2. Quand le polynôme q est de degré un, le lemme de Hensel devient : soit K un corps ultramétrique complet et soit P un polynôme dont les coefficients sont dans $\mathcal{O}_K$. Soit α une racine simple de $\overline{P}$ (i.e. $\overline{P}(\alpha) = 0$ mais $\overline{P}'(\alpha) \neq 0$). Alors il existe une racine a de P dans $\mathcal{O}_K$ telle que $\overline{a} = \alpha$.

4.3.3 Exemple. On peut appliquer la méthode donnée dans la preuve du lemme de Hensel (i.e. la méthode de Newton) pour trouver les racines du polynôme $x^2 + 1$. La racine qui est "proche de 2" s'avère être la limite de la séquence :

$$u_0 = 2, u_{n+1} = u_n - (u_n^2 + 1)/2u_n.$$

Dans ce cas particulier, des calculs explicites sont davantage nécessités si cette méthode générale est utilisée plutôt que la méthode du paragraphe 4.2.3.

4.3.4 Le polygone de Newton. À chaque polynôme :

$$P = \sum a_n x^n$$

(plus généralement avec chaque puissance ou série de Laurent) on associe l'ensemble Δ des points Δ_n avec coordonnées $(n, v(a_n))$. Soit x dans K. Un calcul direct montre que la droite $L_n(x)$ de pente $v(x)$ qui passe par le point Δ_n intersecte l'axe des y en le point $(0, v(a_n x^n))$. Par l'inégalité ultramétrique (1.3) on sait que le point $(0, v(P(x)))$ est au-dessus d'une droite $L_n(x)$ au moins. De plus, l'inégalité ultramétrique est réellement une égalité quand seulement un terme de la somme a la valuation la plus petite. En d'autres termes, *s'il y a seulement un point de* Δ *sur la droite la plus basse* $L_n(x)$ *alors cette droite intersecte l'axe des* y *en le point* $(0, v(P(x)))$.

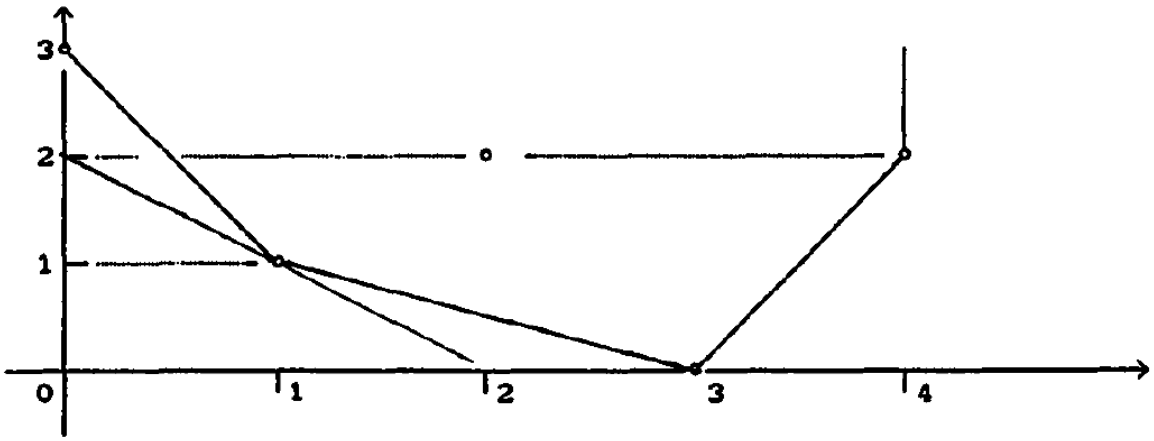


FIG. 6. Polygone de Newton pour le polynôme $P(x) = 25x^4 + 2x^3 + 25x^2 + 5x + 250$, et calcul graphique de la valuation de $P(5)$.

Inversement, si x est une racine de P, lorsque $v(P(x)) = \infty$, la situation précédente ne peut avoir lieu et la droite la plus basse doit rencontrer deux points de Δ au moins. Par conséquent, sa droite la plus basse doit être une arête de l'enveloppe convexe $\mathcal{N}(P)$ de l'ensemble $\Delta \cup \{\infty\}$ où ∞ représente un point à l'infini dans la direction $0y$. En enlevant les arêtes verticales de la frontière de $\mathcal{N}(P)$ on obtient une droite polygonale appelée *le polygone de Newton de* P. Ainsi nous prouvons que les pentes des arêtes du polygone de Newton sont les valuations (possibles) des racines du polynôme. On peut réellement aller plus loin en appliquant le lemme de Hensel. Choisissons une arête du polygone de Newton de P. Soit λ sa pente et m sa longueur. Alors il existe des polynômes Q et R tels que :

1) $P = QR$.

2) Le polynôme Q est de degré m et a un polygone de Newton constitué d'une seule arête de pente λ,

3) Les pentes des côtés du polygone de Newton de R sont distinctes de λ.

De cela on obtient un résultat de base : les polynômes irréductibles de $K(x)$ ont des polygones de Newton constitués d'une seule arête. Donc leur racines dans n'importe quel corps valué non archimédien contenant K (et dont la valuation étend celle de K) ont la même valuation, notamment la pente des arêtes du polygone de Newton.

5. Extensions

5.1. Extensions finies

5.1.1. Soit K un corps valué complet non archimédien et soit L une extension finie (algébrique) de K, disons de degré n. Alors il existe une unique valeur absolue sur L qui étend la valeur absolue de K. Soit α appartenant à L et soit $P(x) = x^d + \ldots + a_0$ le polynôme unitaire minimal de $K[x]$ tel que $P(\alpha) = 0$. Alors la valuation de α est donnée par la pente de l'unique arête du polygone de Newton de P et on doit avoir :

(5.1) $$|\alpha| = |a_0|^{1/d} \text{ ou } v(\alpha) = v(\alpha_0)/d.$$

Il reste à vérifier que cela donne effectivement une valeur absolue sur L.

Remarque. Pour tout α dans L, le degré d de $K(\alpha)$ sur K divise le degré n de L sur K (n/d est le degré de L sur $K(\alpha)$).

5.1.2. Supposons maintenant que K est *valué discrètement* i.e. que l'ensemble $v(K)$ des valuations de ses éléments est un sous-groupe discret de $\mathbb{R}$ (par exemple $\mathbb{Q}_p$ est valué discrètement parce que $v(\mathbb{Q}_p) = \mathbb{Z}$) et que L/K est une extension finie de degré n. Par construction l'ensemble $v(L)$ est un sous-groupe additif de $\frac{1}{n}v(K)$ et par conséquent doit être $\frac{1}{e}v(K)$ pour un certain entier e. Cet entier est appelé l'*indice de ramification* de L/K. D'un autre côté, le corps résiduel $\overline{L}$ s'avère être une extension finie du corps résiduel $\overline{K}$. Soit f son degré. Alors on peut démontrer que $n = ef$.

5.1.3. Soit maintenant L une extension de $\mathbb{Q}_p$ de degré fini n et l'indice de ramification e. Choisissons un élément π de L tel que $v(\pi) = 1/e$. Comme $\overline{L}$ est une extension de $\mathbb{F}_p$, disons de degré f, ce doit être un corps fini à p^f éléments. Pour chaque élément α de $\overline{L}$ choisissons un *antécédent* $\underline{\alpha}$ tel que $\overline{\underline{a}} = a$ et dénotons par U l'ensemble de tous les antécédents (il a exactement p^f éléments). Il est facile de démontrer que chaque élément a de L a un développement unique :

$$a = \sum_{ev(a)\leq i}^{\infty} a_i \pi^i \ ; \ a_i \in U$$

qui ressemble beaucoup à un développement de Hensel.

5.2. Extensions algébriquement fermées. Construction de $\mathbb{C}_p$

5.2.1. Soit K un corps quelconque. Sa *fermeture algébrique* K^{alg} est, pour le dire rapidement, l'ensemble de toutes les racines des polynômes dans $K[x]$. C'est aussi le plus petit corps contenant K qui est *algébriquement fermé* i.e. dans lequel n'importe quel polynôme est le produit de polynômes de degré un.

5.2.2. Quand K est un corps complet non archimédien, il existe une valeur absolue unique sur K^{alg}, donnée par la formule (5.1), qui étend la valeur absolue de K. Par conséquent le corps K^{alg} est un corps non archimédien mais malheureusement il n'est pas complet en général. Pourtant, un résultat profond de Krasner dit que *la complétion* de K^{alg} est un corps complet non archimédien algébriquement fermé.

5.2.3. La complétion de la fermeture algébrique de $\mathbb{Q}_p$ est "classiquement" dénotée par $\mathbb{C}_p$ parce que ce corps joue le rôle de $\mathbb{C}$ à plusieurs égards. L'ensemble des valuations $v(\mathbb{C}_p)$ est $\mathbb{Q}$ et donc $\mathbb{C}_p$ n'est pas discrètement valué. Le corps résiduel de $\mathbb{C}_p$ est la fermeture algébrique du corps $\mathbb{F}_p$. Différemment de $\mathbb{Q}_p$, ou plus généralement de n'importe quel corps complet discrètement valué, il y a, à isomorphisme près, plusieurs *extensions immédiates* de $\mathbb{C}_p$, i.e. les corps avec le même ensemble de valuations et de corps résiduel comme $\mathbb{C}_p$. Ce phénomène sera clarifié au prochain paragraphe.

5.3. Extensions sphériquement complètes

5.3.1. Une propriété curieuse de $\mathbb{C}_p$ est qu'il contient des séquences décroissantes de disques avec une intersection vide, i.e. les disques :

$$D_n = D(a_n, r_n^-) = \{x \in \mathbb{C}_p \ ; \ 0 \leq |x - a_n| < r_n)$$

tels que $D_{n+1} \subseteq D_n$ mais $\cup D_n = \varnothing$. Comme $\mathbb{C}_p$ est un corps complet, quand cette situation advient, la séquence r_n est strictement décroissante mais elle ne tend pas vers 0 (et ainsi la situation ne peut pas arriver dans $\mathbb{Q}_p$ où les r_n appartiennent à $p^{\mathbb{Z}}$!).

5.3.2. Un espace métrique est dit *sphériquement complet* si toute séquence décroissante de disques dans cet espace a une intersection non vide. Les espaces sphériquement complets sont complets (appliquer la définition aux séquences de disques avec des rayons tendant vers zéro) mais le contraire n'est pas vrai. Pourtant, on peut prouver les résultats suivants :

* Tout corps complet non archimédien et *valué discrètement* est sphériquement complet (facile),
* Tout corps non archimédien algébriquement clos qui est *maximalement complet* i.e. sans extension immédiate (extension stricte avec les mêmes ensembles de valuations et corps résiduel) est sphériquement complet (pas très difficile),
* Tout corps algébriquement fermé non archimédien est contenu dans un corps maximalement complet. Ce dernier est algébriquement fermé puisque sphériquement complet (le point très technique à démontrer est que la famille des extensions immédiates est réellement un ensemble !).

Ces résultats montrent l'existence d'un corps, dénoté par Ω_p, qui contient $\mathbb{C}_p$ (et $\mathbb{Q}_p$) et qui est à la fois algébriquement complet et sphériquement complet. Ce corps est utile dans certaines circonstances, mais il est difficile à visualiser car il est si gros.

5.4. Espaces de Banach ultramétriques

5.4.1. Un espace vectoriel E sur le corps valué non archimédien K est dit ultramétrique s'il est muni d'une norme $\|.\|$ satisfaisant les propriétés classiques mais dans lequel l'inégalité triangulaire est remplacé par l'inégalité ultramétrique :

$$\|v + w\| \leq \text{Max}(\|v\|, \|w\|).$$

Un espace vectoriel est dit être un espace de Banach s'il est complet. Même si les preuves peuvent être différentes, les espaces de Banach ultramétriques ont la plupart des propriétés des espaces de Banach classiques. Par exemple, si E est un espace K-vectoriel de *dimension finie* et si K est un corps valué *complet* non archimédien, alors toutes les normes ultramétriques sur E sont équivalentes.

5.4.2. Pourtant il y a certaines exceptions notables. La plus célèbre est le théorème de Hahn-Banach[3], qui est faux pour les corps complets non sphériques. En effet, soit L un corps sphériquement

[3]Toute forme linéaire définie sur un certain espace sous-vectoriel F de E et bornée par M sur F peut être étendue à une forme linéaire sur E bornée par M.

complet et soit K un sous-corps de L complet mais non sphériquement complet ; alors il n'y a aucune application K-linéaire bornée par 1 sur L qui étend l'application Identité de K.

5.4.3. Soit E un espace K-Banach. La famille (e_i) est dite être une *base normale* de E si pour tout x dans E il existe x_i dans K tel que :

$$x = \sum_{i \in I} x_i e_i \ ; \ \|x\| = \sup_{i \in I} |x_i|.$$

L'existence et la construction de bases normales est un problème fondamental lorsqu'on étudie les espaces de Banach. Comme exemple, soit $\mathcal{C}$ l'ensemble des fonctions continues de $\mathbb{Z}_p$ dans $\mathbb{C}_p$. C'est un espace $\mathbb{C}_p$-Banach pour la norme :

$$\|f\| = \sup_{x \in \mathbb{Z}_p} |f(x)|$$

de convergence uniforme et on démontre que la famille (e_i) donnée par :

$$e_i(x) = x(x-1)\dots(x-i+1)/i!$$

en est une base normale. Plus précisément si f appartient à $\mathcal{C}$ on a :

$$f = \sum_{i=0}^{\infty} a_i e_i \ ; \ a_n = \sum_{i=0}^{\infty} (-1)^{n-i} e_i(n) f(i).$$

Inversement cette formule (l'interpolation de Newton) permet de décider si une fonction de $\mathbb{N}$ dans $\mathbb{C}_p$ peut être prolongée en une fonction de $\mathcal{C}$: les coefficients de son interpolation a_i, définis par la formule ci-dessus, doivent tendre vers zéro. Par exemple, la fonction :

$$n \longrightarrow a^n = \sum_{i=0}^{\infty} (a-1)^i e_i(n)$$

est la restriction à $\mathbb{N}$ d'une fonction de $\mathcal{C}$ si et seulement si $|a-1| < 1$. En d'autres termes, le nombre a^x peut être défini pour a dans $1 + p\mathbb{Z}_p$, et x dans $\mathbb{Z}_p$.

6. Fonctions analytiques

6.1. Généralités

6.1.1. Choisissons une fois pour toutes un corps complet algébriquement fermé non archimédien K, par exemple $K = \mathbb{C}_p$. La série de puissances :

$$f(x) = \sum_{n=0}^{\infty} a_n (x-\alpha)^n$$

converge si et seulement si son terme général converge vers zéro i.e. il converge dans le disque "ouvert" :

$$D(\alpha, r^-) \ ; \ r = 1/\limsup \sqrt[n]{|a_n|}$$

comme dans le cas complexe. De plus, la série de puissances converge pour x tel que $|x-\alpha| = r$ si et seulement si :

$$\lim |a_n| r^n = 0$$

cas dans lequel elle converge dans le disque "fermé" $D(a, r)$.

6.1.2. Une fonction f définie dans un certain disque ("ouvert" ou "fermé") $D(\alpha, r)$ de K est dite être *analytique* si elle est la somme d'une série de puissances convergeant dans ce disque. Maintenant à cause de la nature ultramétrique de la distance dans K, tout point β dans $D(\alpha, r)$ est un centre et f peut être développée en une série de puissances autour de β. Cette série de puissances converge dans le disque $D(\beta, r) = D(\alpha, r)$.

6.1.3. Une fonction définie sur une union de disques et analytique sur chacun d'eux est dite *localement analytique*. À nouveau du fait de l'ultramétricité, deux disques sont soit concentriques[4] soit disjoints. Par conséquent si une fonction est définie sur deux disques non concentriques et est analytique sur chacun d'eux, il n'y a pas de connexion entre les valeurs de f dans les deux disques (comme dans le cas complexe pour les fonctions holomorphes sur un ensemble avec deux composantes connectées). Comme conséquence de cela, on ne peut pas construire un prolongement analytique en utilisant la même ruse que dans le cas complexe. Pourtant des théories du prolongement analytique existent (voir 6.2 par exemple) mais sont d'une nature assez différente.

6.2. Exemples élémentaires

Pour illustrer les propriétés générales donnons des exemples basiques de fonctions analytiques sur $\mathbb{C}_p$.

6.2.1. L'exponentielle. Dénotons par $[r]$ la partie entière du réel r. Un simple calcul montre que :

$$v(n!) = [n/p] + [n/p^2) + \ldots + [n/p^h] + \ldots.$$

De cela, on déduit que la fonction :

$$\exp(x) = \sum_{n=0}^{\infty} x^n/n!$$

est seulement définie dans un petit disque notamment le disque $D(0, \rho^-)$ avec :

$$\rho = |p|^{1/(p-1)} < 1.$$

De plus pour tout x dans ce disque, on a :

$$|\exp(x) - 1| \leq p < 1.$$

Par conséquent :

$$|\exp(x)| = 1.$$

En d'autres termes, la fonction exponentielle est *bornée* (par 1) sur son disque de convergence et n'a pas de zéro sur lui. Plus généralement une fonction analytique bornée dont les coefficients sont

[4] Au sens où il existe un centre commun aux deux disques.

dans un corps valué discrètement a seulement un nombre fini de zéros sur son disque de convergence (preuve au moyen du polygone de Newton). Pourtant les fonctions non bornées peuvent avoir un nombre infini de zéros comme on le montrera pour la fonction logarithme. De plus une fonction bornée avec des coefficients dans un corps non discrètement valué peut aussi avoir un nombre infini de zéros, par exemple la fonction : $\sum a_n x^n$; $a_n^n = p, a_n \in \mathbb{C}_p$.

6.2.2. Le logarithme. La fonction logarithme est définie par :

$$\log(x) = -\sum_{n=1}^{\infty} \frac{(-1)^n}{n}(x-1)^n.$$

Elle converge sur le disque $D(1, 1^-)$ et pour x et y sur ce disque, on a

$$\log(xy) = \log(x) + \log(y).$$

En particulier, si ζ est une racine $k^{\text{ième}}$ de l'unité dans $D(1, 1^-)$ on a :

$$\log(\zeta) = \frac{1}{k}\log(\zeta^k) = \frac{1}{k}\log(1) = 0.$$

Pour trouver les zéros de la fonction logarithme on doit imaginer quelles racines $k^{\text{ièmes}}$ de l'unité sont dans $D(1, 1^-)$. Si ξ est une racine $k^{\text{ième}}$ de l'unité, $\xi - 1$ est une racine du polynôme :

$$P_k(x) = (1+x)^k - 1.$$

Soit $k = p^h d$ avec $(d, p) = 1$. On trouve :

$$\begin{aligned} P_k(x) &= P_{p^k}(x)Q(x) \\ Q(x) &= [1 + (1+x)^{p^h} + \ldots + (1+x)^{(d-1)p^h}]. \end{aligned}$$

Comme $Q(0) = d$ est premier à p, en regardant le polygone de Newton Q on voit qu'aucune racine de Q ne peut être dans $D(0, 1^-)$. Par conséquent, seules les $p^{h-\text{ièmes}}$ racines de l'unité peuvent être dans le disque $D(1, 1^-)$. Inversement, en regardant le polygone de Newton du polynôme $P_{p^k}(x)$ il est facile de montrer que les $p^{h-\text{ièmes}}$ racines de l'unité sont dans le disque $D(1, 1^-)$ et qu'il en est ainsi des zéros du logarithme. On a donc construit un ensemble infini de zéros de cette fonction. Il reste à démontrer que nous avons obtenu tous les zéros de cette manière. Dans ce but, on considère le polygone de Newton de la fonction logarithme construit sur la figure 7.

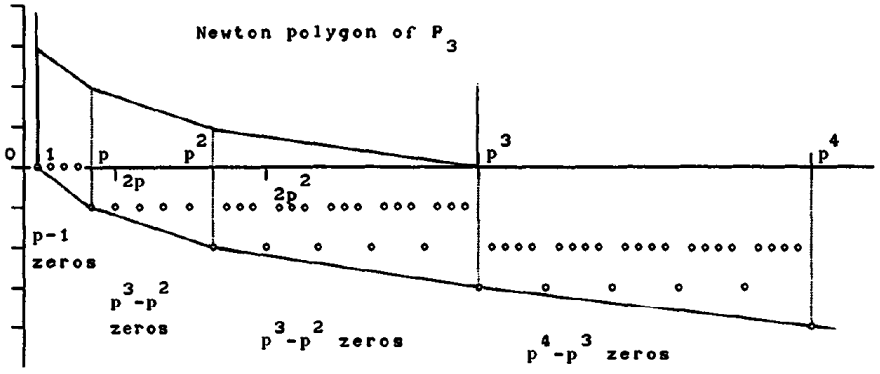


FIG. 7. Le polygone de Newton de la fonction logarithme

Le lien entre les polygones de Newton de la fonction logarithme et des polynômes P_h est contenu dans la formule utile :

$$\log(x) = \lim_{h\to\infty}[1 - x^{p^k}]/p^h \qquad \text{pour } |x| < 1.$$

Comme pour les polynômes, les pentes des arêtes du polygone de Newton de la fonction logarithme donnent les valuations des zéros. En mettant ensemble toutes les informations on obtient finalement : pour chaque entier $h \geq 0$ la fonction logarithme a exactement $p^h - p^{h-1}$ zéros tels que :

$$v(\zeta - 1) = 1/(p^h - p^{h-1}) \qquad \text{i.e. } |\zeta - 1| = |p|^{p^{1-k}/(p-1)} = \rho^{1/p^{k-1}}$$

qui sont les racines de l'unité :

$$\zeta^{p^k} = 1 \; ; \; \zeta^{p^{k-1}} \neq 1.$$

Cela épuise l'ensemble des zéros distincts de 1. Si $|x| < \rho$, de telle façon que $\exp(x)$ existe, on a :

$$\log(\exp(x)) = x.$$

Dans la direction opposée :

$$\exp(\log(x)) = x$$

est vérifiée quand $\log(x)| < \rho$ i.e. quand $|x-1| < \rho$, où ρ est le rayon de convergence de la fonction exponentielle.

6.2.3. L'exponentielle de Artin-Hasse. La fonction analytique :

$$\ell(x) = x + x^p/p + x^{p^2}/p^2 + \ldots + x^{p^k}/p^k + \ldots$$

est définie sur le disque $D(0, 1^-)$ et ressemble (p-adiquement) beaucoup au logarithme $\log(1 - x)$, car les deux fonctions ont le même polygone de Newton. Par exemple, les zéros des deux fonctions ont les mêmes valuations. Il est facile de vérifier sur le polygone de Newton que :

$$|\ell(x)| \leq |x| \qquad \text{si } |x| \leq \rho$$

où ρ est le rayon de convergence de la fonction exponentielle. On définit la fonction exponentielle de Artin-Hasse en prenant le développement formel :

$$A(x) = \exp(\ell(x)) = \sum_{n=0}^{\infty} e_n x^n. \tag{6.1}$$

A priori cette série de puissances existe pour $|x| < \rho$, mais en fait $|e_n| \leq 1$, et par conséquent $A(X)$ converge pour $|x| < 1$ (comparer avec la fonction $x = \exp(\log(\mathrm{x}))$ qui existe a priori seulement sur $D(1, \rho^-)$ mais en fait partout).

Preuve. On trouve par des calculs formels :

$$A(x)^p/A(x^p) = \exp(px) = 1 + pg(x),$$

où les coefficients de g sont des entiers p-adiques. D'un autre côté, comme pour toute série de puissances dans $\mathbb{Q}[[x]]$, il existe b_n (dans $\mathbb{Q}$) telle que :

$$A(x) = \prod_{n=1}^{\infty}(1 - b_n x^n)$$

ainsi :

$$A(x)^p/A(x^p) = \prod_{n=1}^{\infty}(1-b_nx^n)/(1-b_nx^{np}) = \prod_{n=1}^{\infty}(1+pb_nx^n+\ldots)$$

par induction sur n on déduit que les b_n sont des entiers p-adiques ainsi que les e_n. □

Comme les e_n sont des entiers et comme $e_1 = 1$, on trouve, pour $|x| < 1$:

$$|A(x) - 1 - x| \leq |x^2| \quad \text{donc} \quad |A(x) - 1| = |x|. \tag{6.2}$$

Maintenant choisissons un nombre ξ dans $\mathbb{C}_p$ tel que :

$$\ell(\xi) = 0 \; ; \; |\xi| = \rho$$

(en considérant le polygone de Newton de ℓ on voit qu'il existe exactement $p-1$ nombres avec ces propriétés). Pour calculer $A(\xi)$ on doit être très précautionneux : utiliser (6.1) permet en faisant bien attention d'obtenir $A(\xi) = 1$ ce qui contredit (6.2). En effet, la formule (6.1) est vraie seulement formellement, donc pour $|x| < \rho$. Ainsi elle ne peut pas être appliquée pour ξ. Mais on a effectivement que pour tout x dans $D(0,\rho)$:

$$A(x)^p = \exp(p\ell(x))$$

parce que maintenant $|p\ell(x)| \leq |p||x| < \rho$. Ainsi $A(\xi)$ est une racine $p^{\text{ième}}$ de l'unité. De plus, par (6.2) on sait que c'est *la* $p^{\text{ième}}$ racine de l'unité qui est dans $D(1+\xi,\rho^2)$. Ainsi l'exponentielle de Artin-Hasse fournit une représentation analytique des racines $p^{\text{ièmes}}$ de l'unité.

6.2.4. En pratique et pour rendre les calculs plus faciles, on travaille avec une fonction tronquée $\ell(x)$ en ne gardant que les deux premiers termes. On laisse cela comme un exercice de vérifier les propriétés suivantes : soit π une racine du polynôme $X^{p-1}+p=0$ ("le π de Dwork"). La fonction :

$$E_\pi(x) = \exp(\pi x - \pi x^p) = \sum_{n=0}^{\infty} f_n x^n$$

(exponentielle de Dwork) qui a priori converge dans $D(0,1^-)$, est effectivement définie dans $D(0,p^{(p-1)/p^2})$. De plus, la valeur $E(1)$ est la $p^{\text{ième}}$ racine de l'unité qui est dans le disque $D(1+\pi,\rho^2)$.

6.3. Éléments analytiques

Nous fournissons seulement un rapide survol de la théorie la plus classique du prolongement analytique. Elle est due à Krasner. Soit Δ un sous-ensemble de $\mathbb{C}_p$ et soit :

$$H_0(\Delta) = \{f \in \mathbb{C}_p(x) \quad \text{sans aucun pôle dans } \Delta\}.$$

On définit la "norme de convergence uniforme" par la formule :

$$\|f\| = \sup_{x\in\Delta} |f(x)|$$

et on considère la complétion $H(\Delta)$ de $H_0(\Delta)$ pour cette norme (de façon évidente, c'est un espace de Banach). Les fonctions dans $H(\Delta)$ sont appelées *éléments analytiques* dans Δ. Quand Δ n'est

pas trop compliquée, par exemple si c'est le complémentaire dans un disque d'une union finie de disques plus petits, $H(\Delta)$ a de bonnes propriétés, par exemple, les zéros des éléments analytiques sont isolés. Par conséquent sur un tel Δ il y a une théorie du prolongement analytique. Notamment, si deux éléments analytiques prennent les mêmes valeurs sur un petit disque, alors elles sont égales partout.

C. Intégration

Il y a deux théories complètement distinctes de l'intégration sur les groupes ultramétriques dépendant du corps sur lequel les fonctions à intégrer sont définies. Quand on traite des fonctions à valeurs dans $\mathbb{C}$, c'est un chapitre particulier de la théorie générale de l'intégration sur les groupes, mais si on traite des fonctions à valeurs dans $\mathbb{C}_p$, cela amène à un phénomène entièrement nouveau.

7. Intégration $\mathbb{C}$-valuée

7.1. Intégration sur un groupe profini

Soient G_n des groupes finis abéliens et soit :

$$G = \varprojlim G_n$$

leur limite inverse pour les homomorphismes de G_{n+1} dans G_n (voir 2.1.2 et 2.2.1). Dans cette situation G est dit être un *groupe profini*. C'est alors un groupe compact. Par conséquent il y a une (unique) mesure de Haar sur lui telle que :

$$\int_G d\mu(x) = 1.$$

La mesure de Haar sur G peut se calculer facilement. Soit a dans G_n et soit :

$$D_n(a) = \{x \in G \ ; \ x_n = a\}$$

(rappelons que les éléments x dans G sont des séquences $\{x_n \in G_n\}$). Comme les mesures de Haar sont invariantes par translation on trouve :

$$\mu(D_n(a)) = 1/\#(G_n),$$

où (E) dénote le nombre d'éléments dans E. Maintenant, soit f une fonction continue de G dans $\mathbb{C}$, et pour chaque a dans G_n choisissons un antécédent $\underline{a}$ dans G tel que $a = \underline{a}_n$. On trouve :

$$\int_G f(x)d\mu(x) = \lim_{n\to\infty} \frac{1}{(G_n)} \sum_{a\in G_n} f(a). \tag{7.1}$$

7.2. Intégration sur $\mathbb{Z}_p$

7.2.1. Par construction $\mathbb{Z}_p$ est un groupe profini. Maintenant pour tout nombre x de $\mathbb{Z}_p$ la valeur absolue $|x|$ est dans $\mathbb{R}$ de telle façon que, pour s dans $\mathbb{R}^+$, la fonction $x \longrightarrow |x|^s$ est une fonction

continue. Comme exemple, nous l'intègrerons sur $\mathbb{Z}_p$. En prenant $\{0, 1, \ldots, p^n - 1\}$ comme ensemble de représentants pour $\mathbb{Z}/p^n\mathbb{Z}$, l'équation (7.1) devient :

$$\int_{\mathbb{Z}_p} |x|^s d\mu(x) = \lim_{n\to\infty} \frac{1}{p^n} \sum_{a=0}^{p^n-1} |a|^s.$$

En regroupant ensemble les nombres ayant la même valeur absolue, on calcule facilement (se rappeler que $|p| = 1/p$) :

$$\begin{aligned}\int_{\mathbb{Z}_p} |x|^s d\mu(x) &= \lim_{n\to\infty} \frac{1}{p^n} \left[(p^n - p^{n-1})1^s + (p^{n-1} - p^{n-2})|p|^s + \ldots + (p-1)|p|^{s(n-1)}\right] \\ &= \lim_{n\to\infty} \frac{p-1}{p} \left(1 + p^{-s-1} + \ldots + p^{(-s-1)(n-1)}\right) \\ &= (1 - p^{-1})/(1 - p^{-1-s}).\end{aligned}$$

7.2.2. Le calcul ci-dessus peut être généralisé de la manière suivante. Soit $f(x_1, \ldots, x_r)$ un polynôme dans $\mathbb{Z}_p[x_1, \ldots, x_r]$ et soit :

$$N_n = \{(x_1, ..., x_r) \in (\mathbb{Z}/p^n\mathbb{Z})^r \ ; \ f(x_1, ..., x_r) = 0 \ (\text{mod } p^n)\}$$

le nombre de solutions "approximées à l'ordre n" de f[5]. Par exemple, dans le cas où $r = 1$ et $f(x) = x$, on a $N_n = 1$ pour tout n. On définit la série nommée *série de Poincaré* :

$$P(T) = \sum_{n=0}^{\infty} N_n T^n$$

et on calcule, pour s dans $\mathbb{R}^+$:

$$\sum_{\mathbb{Z}_p^r} |f(x_1, \ldots, x_r)|^s \ d\mu(x_1) \ldots d\mu(x_r) = p^s(p^s - 1)P(p^{-r-s}).$$

Cette formule a permis à Igusa de démontrer que $P(T)$ est une fraction rationnelle.

7.3. Intégration sur $\widehat{\mathbb{Z}}$ et ruse des répliques

Soit $\{u_n\}$ une séquence satisfaisant les conditions 3.3.2 et soit g une fonction continue de $\widehat{\mathbb{Z}}$ dans $\mathbb{C}$. La formule 7.1 donne :

$$\begin{aligned}\int_{\widehat{\mathbb{Z}}} g(z) d\mu(z) &= \lim_{n\to\infty} \frac{1}{u_n} \sum_{a=0}^{u_n-1} g(a) \\ &= \lim_{n\times\to\infty} \frac{1}{n} \sum_{a=0}^{n-1} g(a),\end{aligned}$$

[5]attention : une solution exacte de $f(x_1, ..., x_r) = 0$ donne une solution approchée mais l'inverse est faux.

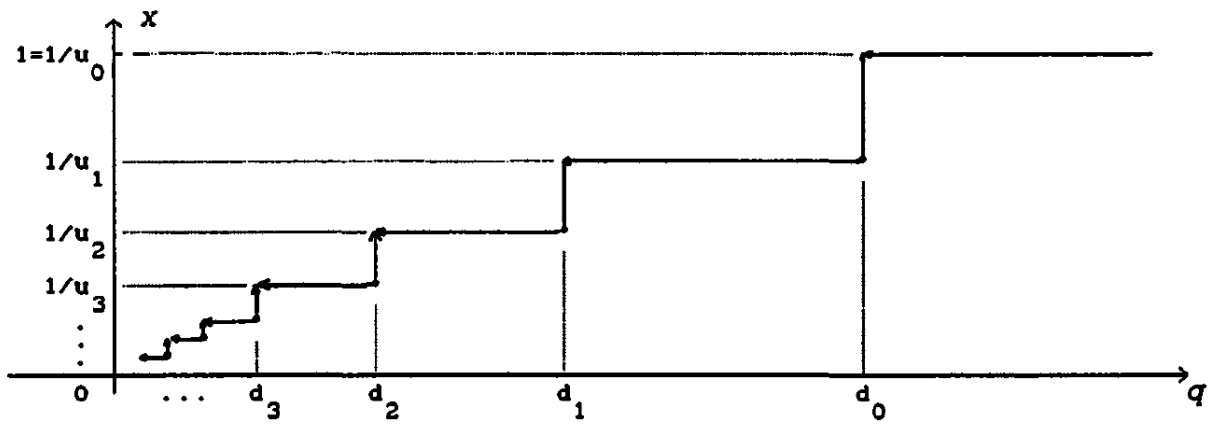


FIG. 8.

où $n\times \to \infty$ signifie que n tend multiplicativement vers l'infini. Maintenant supposons qu'une distance d a été définie sur $\widehat{\mathbb{Z}}$ au moyen d'une séquence décroissante $\{d_n\}$ comme dans 2.1.3 et 3.4.2. En utilisant les matrices de Parisi correspondantes, on calcule pour toute fonction f de $\mathbb{R}$ dans $\mathbb{C}$:

$$\begin{aligned}\int_{\widehat{\mathbb{Z}}} f(d(z,0))d\mu(z) &= \lim_{n\to\infty} \frac{1}{u_n} \sum_{a=0}^{u_n-1} f(d(a,0)) \\ &= \lim_{n\to\infty} \frac{1}{u_n(u_n-1)} \sum_{a=0}^{u_n-1}\sum_{b=0}^{u_n-1} f\left(\mathbf{Q}_{a,b}^{(n)}\right).\end{aligned} \tag{7.2}$$

D'un autre côté, l'intégrale peut être calculée par une méthode classique. Notamment, définissons une fonction x de $\mathbb{R}^+$ dans $[0,1]$ par :

$$x(q) = \mu\{z \in \widehat{\mathbb{Z}}\,;\ d(z,0) < q\}$$

et soit q la fonction "inverse" de $[0,1]$ dans $\mathbb{R}$:

$$q(x) = d_n \qquad \text{quand } \frac{1}{u_{n+1}} \le x < \frac{1}{u_n}$$

montrée sur la Fig.8. Alors on trouve facilement :

$$\begin{aligned}\int_{\widehat{\mathbb{Z}}} f(d(z,0))d\mu(z) &= \int_0^\infty f(q)dx(q) \\ &= \int_0^1 f(q(x))dx.\end{aligned} \tag{7.3}$$

Les formules (7.2) et (7.3) rappellent celles utilisées quand on travaillait avec la ruse des répliques. La principale différence est que dans notre formulation, bien que la séquence u_n tende vers zéros dans $\widehat{\mathbb{Z}}$, on doit la considérer comme une séquence à valeurs dans $\mathbb{R}$ dans la formule (7.2) et elle

tend ainsi vers l'infini.

8. Intégration $\mathbb{C}_p$-valuée

8.1. Mesures sur $\mathbb{Z}_p$

8.1.1. Une mesure "p-adique" sur Z_p étant une application bornée finiment additive de l'union infinie de disques de Z_p vers $\mathbb{C}_p$, on définit l'intégrale de f par la formule :

$$\int_{\mathbb{Z}_p} f(x)d\mu(x) = \lim_{n\to\infty} \sum_{a=0}^{p^n-1} f(a)\mu(a+p^n\mathbb{Z}_p). \tag{8.1}$$

Il n'est pas difficile de démontrer que la limite existe, mais le fait que μ soit bornée est essentiel dans la preuve.

8.1.2. Supposons qu'il existe une mesure p-adique μ invariante par translation. La mesure d'un disque devrait dépendre seulement de son rayon. Ainsi, en normalisant par $\mu(\mathbb{Z}_p) = 1$, on devrait obtenir, pour tout a dans $\mathbb{Z}_p$:

$$\mu(a+p^n\mathbb{Z}_p) = 1/p^n.$$

Comme $|1/p^n|$ tend vers l'infini avec n, la "mesure" μ ne peut être bornée. Par conséquent, *il n'y a pas de mesure de Haar p-adique !* Pourtant supposons que la mesure de Haar existe effectivement et calculons ses moments au moyen de sa fonction caractéristique. Pour tout z dans $\mathbb{C}_p$ tel que $|z| < \rho = |p|^{1/(p-1)}$ on obtient :

$$\begin{aligned}
\sum_{k=0}^{\infty} \frac{z^k}{k!} \int_{\mathbb{Z}_p} x^k d\mu(x) &= \int_{\mathbb{Z}_p} e^{xz} d\mu(x) \\
&= \lim_{n\to\infty} \frac{1}{p^n} \sum_{a=0}^{p^n-1} e^{ax} = \lim_{n\to\infty} \frac{e^{p^n x}-1}{p^n(e^x-1)} \\
&= \frac{z}{e^x-1} = \sum_{k=1}^{\infty} \frac{B_k}{k!} z^k \\
&= \sum_{k=1}^{\infty} -k\zeta(1-k)\frac{z^k}{k!},
\end{aligned}$$

où les B_k sont des nombres de Bernoulli et ζ est la fameuse fonction zeta. Le but du paragraphe suivant est de donner une version correcte de ce calcul, notamment d'exprimer les valeurs de la fonction zeta en les entiers négatifs au moyen d'une intégrale sur $\mathbb{Z}_p$.

8.2. Une fonction zeta p-adique

8.2.1. Comme $\mathbb{C}$ et $\mathbb{C}_p$ sont algébriquement fermés ils contiennent tous deux exactement $p-1$ racines $(p-1)^{\text{èmes}}$ de l'unité. De plus, par le théorème de Fermat, le polynôme $x^{p-1}-1$ a $p-1$ racines distinctes dans $\mathbb{F}_p$, (notamment $1, 2, \ldots, p-1$) par conséquent, selon le lemme de Hensel, il a $p-1$

racines dans $\mathbb{Z}_p$, une dans chaque disque $D(i,|p|)$ $(1 \leq i < p)$. Ainsi les racines $(p-1)^{\text{èmes}}$ de l'unité de $\mathbb{C}_p$, sont réellement dans $\mathbb{Z}_p$. Choisissons une application bijective entre les racines $(p-1)^{\text{èmes}}$ de l'unité dans $\mathbb{C}$ et les racines $(p-1)^{\text{èmes}}$ de l'unité dans $\mathbb{C}_p$, qui préserve la multiplication (un isomorphisme de groupes). Par exemple, pour $p=5$, il y a deux tels isomorphismes, l'un d'entre eux étant donné par :

$$1 \longrightarrow 1, -1 \longrightarrow -1, i \longrightarrow 2+\ldots, -i \longrightarrow 3+\ldots.$$

L'autre est obtenu en échangeant i et $-i$.

8.2.2. On supposera maintenant que $p > 2$. Soit α une racine $(p-1)^{ème}$ de l'unité dans $\mathbb{C}_p$, distincte de 1, et soit μ_α la mesure p-adique définie par

$$\mu_\alpha(\mathbb{Z}_p) = 1, \;\; \mu_\sigma(a+p^n\mathbb{Z}_p) = \alpha^a \qquad \text{pour } n \geq 1.$$

Comme $\alpha^p = \alpha$, la mesure de $a+p^n\mathbb{Z}_p$, ne dépend pas de (l'entier) a comme centre. De plus la formule :

$$\sum_{b=0}^{p-1} \mu(a+p^nb+p^{n+1}\mathbb{Z}_p) = \sum_{b=0}^{p-1} \alpha^{a+p^nb} = \alpha^a \frac{\alpha^{p^{n+1}}-1}{\alpha^{p^n}} - 1 = \alpha^a$$

garantit l'additivité (finie) de μ_α.

8.2.3. Calculons les moments de μ_α :

$$\begin{aligned}
\sum_{k=0}^{\infty} \frac{z^k}{k!} \int_{\mathbb{Z}_p} x^k d\mu_\alpha(x) &= \int_{\mathbb{Z}_p} e^{xz} d\mu_\alpha(x) \\
&= \sum_{n\to\infty} \sum_{a=0}^{p^n-1} e^{ax}\alpha^a = \lim_{n\to\infty} \frac{e^{p^nz}\alpha^{p^n}-1}{e^z\alpha-1} \\
&= \frac{\alpha-1}{e^z\alpha-1} = (1-\alpha)\sum_{k=0}^{\infty} L(-k,\alpha)\frac{z^k}{k!}.
\end{aligned}$$

Les nombres $L(-k,\alpha)$ définis par la dernière égalité sont dans $\mathbb{C}_p$, mais ils peuvent être exprimés comme des nombres dans $\mathbb{Q}[\alpha]$. Ainsi, au moyen de l'isomorphisme dans 8.2.1 on peut les voir comme des éléments de $\mathbb{C}$. Maintenant, cette dernière égalité devient le développement de Taylor d'une fonction holomorphe bien connue. Une formule classique affirme que les $L(-k,\alpha)$ sont les valeurs, aux entiers négatifs, d'une fonction holomorphe définie pour $\mathfrak{Re}(s) > 1$ par :

$$L(s,\alpha) = \sum_{n=1}^{\infty} \frac{\alpha^n}{n^s}$$

8.2.4. On calcule facilement (pour $\mathfrak{Re}(s) > 1$, par conséquent pour tout s par prolongement analytique) :

$$\sum_{\alpha^{p-1}=1} L(s,\alpha) = \sum_{n=1}^{\infty} \frac{p-1}{[(p-1)n]^s} = (p-1)^{1-s}\zeta(s).$$

Donc il est naturel de définir une "pseudo mesure de Haar" sur $\mathbb{Z}_p$ par :

$$\mu = \sum_{\substack{\alpha^{p-1}=1 \\ \alpha \neq 1}} \frac{1}{1-\alpha}\mu_\alpha.$$

En mettant tous ces éléments ensemble et en remarquant que $L(s,1) = \zeta(s)$ on obtient finalement pour tout entier $k \geq 0$:

$$\int_{\mathbb{Z}_p} x^k d\mu(x) = \sum_{\substack{\alpha^{p-1}=1 \\ \alpha \neq 1}} L(-k,\alpha) = [(p-1)^{1+k} - 1]\zeta(-k).$$

Comme $\zeta(-k) = -B_k(k-1)$ ces nombres sont dans $\mathbb{Q}$, donc dans $\mathbb{C}_p$. Par exemple, pour $k = 0$, on a $\mu(\mathbb{Z}_p) = (p-2)/2$.

8.2.5. Soit $\mathbb{Z}_p^* = \mathbb{Z}_p - p\mathbb{Z}_p$. Comme conséquence immédiate de la définition on a :

$$\mu(px) = \mu(x)$$

de telle façon que $\mu(\mathbb{Z}_p^*) = 0$. Plus généralement :

$$\int_{\mathbb{Z}_p^*} x^k d\mu(x) = (1-p^k)\int_{\mathbb{Z}_p} x^k d\mu(x) = [(p-1)^{1+k} - 1](1-p^k)\zeta(-k).$$

8.2.6. D'un autre côté la formule :

$$a^p = (b + a - b)^p = b^p + p(ab)[\ldots] + (a-b)^p$$

montre que pour tout a dans $\mathbb{Z}_p$, et $n \leq 1$:

$$|a-b| \leq |p|^n \implies |a^p - b^p| \leq |p|^{n+1}.$$

Mais, pour tout a in $\mathbb{Z}_p^*$, on a :

$$|a^{p-1} - 1| \leq |p|$$

donc pour tout entier $n \geq 0$:

$$|a^{(p-1)p^n} - 1| \leq |p|^n.$$

Grosso modo, cela signifie que si $k - k'$ est divisible par $(p-1)p^n$ pour n suffisamment grand alors a^k et $a^{k'}$ sont fermés dans $\mathbb{Z}_p$. En d'autres termes, la fonction $k \longrightarrow a^k$ peut être prolongée de façon à obtenir une fonction constante de

$$\varprojlim \mathbb{Z}/(p-1)p^n\mathbb{Z} = \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$$

dans $\mathbb{Z}_p$.

8.2.7. Maintenant en utilisant 8.2.6, il n'est pas difficile de prouver que :

$$\zeta_p(s) = \frac{1}{(p-1)^{1-s} - 1}\int_{\mathbb{Z}_p^*} x^{-s} d\mu(x)$$

est une fonction de $\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$, dans $\mathbb{Z}_p$, définie et continue en dehors de 1. De plus, de 8.2.5 on obtient que pour tous les entiers $k \geq 0$:

$$\zeta_p(-k) = (1-p^k)\zeta(-k).$$

Remarques.

* La fonction ζ_p a été découverte par Kubota et Leopoldt.

* Le facteur $(1-p^{-s})$ est exactement le $p^{\text{ième}}$ facteur dans le développement eulérien de ζ.

* La continuité de ζ_p donne de nombreuses congruences entres les valeurs aux entiers négatifs, donc entre les nombres de Bernoulli. Ces congruences étaient déjà connues sous le nom de congruences de Kummer.

* La formule $a^s = \exp[\log(a)s]$, vraie pour a dans $1+p\mathbb{Z}_p$ et $|s| \leq 1$, montre que la fonction ζ_p est (la restriction d') une fonction analytique sur chaque composante $\mathbb{Z}_p$ de $\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$.

8.2.8. Comme exemple typique d'un calcul p-adique nous montrons comment calculer le "résidu" de ζ_p près de 1. Clairement, on a seulement à calculer :

$$\int_{\mathbb{Z}_p^*} x^{-1} d\mu(x) = \sum_{\substack{\alpha^{p-1}=1 \\ \alpha \neq 1}} \frac{1}{1-\alpha} \lim_{n\to\infty} \sum_{\substack{a=1 \\ (a,p)=1}}^{p^n-1} \frac{\alpha^a}{a}.$$

Pour $|x| < 1$ on vérifie aisément :

$$\lim_{n\to\infty} \sum_{\substack{a=1 \\ (a,p)=1}}^{p^n-1} \frac{x^a}{a} = \sum_{\substack{a=1 \\ (a,p)=1}}^{\infty} \frac{x^a}{a}$$

$$= \log(1-x) - \frac{1}{p}\log(1-x^p) = \frac{1}{p}\log\left(\frac{(1-x)^p}{1-x^p}\right)$$

Soit :

$$\Delta = \{x \in \mathbb{C}_p \,;\, |x| \leq 1, |x-1| = 1\} = D(0,1) - D(1,1^-).$$

On a :

$$\sum_{\substack{a=1 \\ (a,p)=1}}^{p^{n+1}-1} \frac{x^a}{a} = \sum_{\substack{a=1 \\ (a,p)=1}}^{p^n-1} \frac{x^a}{a} \sum_{b=0}^{p-1} \frac{a}{a+p^n b} x^{p^n b}.$$

Mais sur Δ la séquence

$$\sum_{b=1}^{p-1} x^{p^n b} = \frac{x^{p^{n+1}} - x^{p^n}}{x^{p^n} - 1}$$

converge uniformément vers zéro. De ça, on peut facilement déduire que la séquence

$$\sum_{\substack{a=1 \\ (a,p)=1}}^{p^n-1} \frac{x^a}{a}$$

converge uniformément dans Δ, i.e., que sa limite est un élément analytique dans Δ. D'un autre côté, il existe un polynôme P dans $\mathbb{Z}[x]$ tel que :

$$\frac{(1-x)^p}{1-x^p} = 1 - p\frac{P(x)}{1-x^p}$$

et pour x dans Δ on a :

$$\left|\frac{P(x)}{1-x^p}\right| \leq 1$$

Par conséquent la fonction :

$$\log\left(\frac{(1-x)^p}{1-x^p}\right) = \lim_{n\to\infty}\sum_{k=1}^{n} p^n \left(\frac{P(x)}{1-x^p}\right)^n$$

est aussi un élément analytique dans Δ. Comme on sait que les deux éléments analytiques concordent pour $|x|<1$, par le théorème de Krasner, on sait qu'ils concordent partout dans Δ, par exemple sur les $(p-1)^{\text{ièmes}}$ racines de l'unité (différentes de 1). Finalement on obtient la formule :

$$\int_{\mathbb{Z}_p^*} x^{-1} d\mu(x) = \sum_{\substack{\alpha^{p-1}=1 \\ \alpha\neq 1}} \frac{1}{1-\alpha}\log((1-\alpha)^{p-1}).$$

Ici la $(p-1)^{\text{ième}}$ puissance doit être laissée dans l'argument pour que le logarithme soit défini.

8.3. La fonction Gamma p-adique

Pour définir une fonction Gamma p-adique, on utilise un point de vue complètement différent. Le but est de trouver un analogue p-adique à des fonctions comme $\Gamma(a) = \int x^{a-1}e^x dx$ i.e. définies en intégrant une différentielle dépendant d'un paramètre. La remarque élémentaire est qu'en intégrant sur un chemin *fermé*, les différentielles exactes donnent zéro. Ainsi, en suivant Dwork-Boyarski, on agira comme si le chemin $0-\infty$ était fermé quelque part.

8.3.1. Soit π une racine du polynôme $X^{p-1}+p$ (cf. 6.2.4) et soit $H^\dagger$ l'espace des fonctions analytiques *sur-convergentes*, i.e. les fonctions qui sont analytiques dans un disque $D(0,r)$ de $\mathbb{C}_p$ pour un certain $r>1$ (dépendant de la fonction). Pour tout "paramètre" $a\in\mathbb{Z}_p$, soit :

$$\Omega_a = x^a e^{\pi x} H^\dagger.$$

Si $f = x^a e^{\pi x} g$ est dans Ω_a alors $xf' = x^a e^{\pi x}(ag + \pi x g + x g')$ est également dans Ω_a, ainsi cela a du sens que de définir :

$$W_a = \Omega_a/(x\tfrac{d}{dx}\Omega_a).$$

En prenant $g = x^k$ $(k\geq 0)$ dans le calcul ci-dessus, on trouve :

$$x^a e^{\pi x} x^{k+1} \simeq -\frac{(a+k)}{\pi} x^a e^{\pi x} x^k \tag{8.2}$$

où $\simeq$ signifie que la différence entre les deux côtés est dans $x\frac{d}{dx}\Omega_a$. On en déduit immédiatement que W_a est de dimension un sur $\mathbb{C}_p$ avec $x^a e^{\pi x}$ comme base.

8.3.2. Définissons un opérateur, appelé le Frobenius inverse, qui agit sur les fonctions analytiques par la formule suivante :

$$\psi(\sum a_n x^n) = \sum a_{np} x^n.$$

On vérifie que cet opérateur préserve $H^\dagger$, et la formule

$$\psi(xf') = px[\psi(f)]' \tag{8.3}$$

affirme qu'il préserve les dérivées. Pour expliquer comment il agit sur Ω_a, on a besoin d'introduire l'unique nombre b de $\mathbb{Z}_p$, qui satisfait :

$$a = pb - r; r \in \mathbb{Z}, 0 \leq r < p.$$

Avec ces notations on trouve :

$$\psi(x^a e^{\pi x} g) = x^b e^{\pi x} \psi(x^{a-pb} e^{\pi(x-x^p)} g).$$

Comme expliqué en 6.2.4 la fonction $e^{\pi(x-x^p)}$ est sur-convergente de telle façon que la fonction $\psi(x^a e^{\pi x} g)$ appartient à Ω_b (comme $r < p$, les termes contenant une puissance négative de x disparaissent quand on applique ψ). La formule (8.3) affirme que l'action de ψ est compatible avec le fait de prendre les quotients. Ainsi on obtient un opérateur, dénoté α, de W_a dans W_b. Par définition, la fonction gamma p-adique est la matrice 1×1 de l'opérateur α, notamment on a :

$$\alpha(x^a e^{\pi x}) = \pi^r \Gamma_p(a) x^b e^{\pi x}. \tag{8.4}$$

8.3.3. Dans W_0, en utilisant (8.2) on obtient $x^k e^{\pi x} \simeq Cst.xe^{\pi x} \simeq 0$. Par conséquent pour $a = 0$ on a $b = r = 0$ et on calcule dans W_0 :

$$\Gamma_p(0) e^{\pi x} \simeq e^{\pi x} \psi(e^{\pi(x-x^p)}) \simeq e^{\pi x}.$$

Si $|a| = 1$, p ne divise pas a et on a $r > 0, a + 1 = pb - (r - 1)$. En utilisant la définition de Γ_p, (8.2) et (8.3), on calcule dans W_{a+1} :

$$\begin{aligned} \Gamma_p(a+1) x^b e^{\pi x} &\simeq \pi^{-r+1} \psi(x^{a+1} e^{\pi x}) \\ &\simeq \pi^{-r+1} \psi(-\frac{a}{\pi} x \hat{a} e^{\pi x}) \\ &\simeq -a \Gamma_p(a) x^b e^{\pi x}. \end{aligned}$$

Si $a < 1$, on a $a = pb, r = 0$ et $a + 1 = p(b + 1) - (p - 1)$. On calcule :

$$\begin{aligned} \Gamma_p(a+1) x^{b+1} e^{\pi x} &\simeq \pi^{-p+1} \psi(x^{a+1} e^{\pi x}) \simeq -\frac{1}{p} \psi(-\frac{a}{\pi} x^a e^{\pi x}) \\ &\simeq \frac{b}{\pi} \Gamma_p(a) x^b e^{\pi x} \simeq -\Gamma_p(a+1) x^{b+1} e^{\pi x}. \end{aligned}$$

Pour résumer, on obtient :

$$\Gamma_p(0) = 1 \ , \ \Gamma_p(a+1)/\Gamma_p(a) = \begin{cases} -1 & \text{si } |a| < 1 \\ -a & \text{si } |a| = 1. \end{cases}$$

C'était la définition originale de Morita pour la fonction gamma p-adique. Elle peut être utilisée pour calculer ses valeurs aux entiers positifs, notamment :

$$\Gamma_p(k) = (-1)^k \prod_{\substack{i=1 \\ p \nmid i}}^{k} i$$

qui nous rappelle les valeurs de la fonction Γ classique.

8.3.4. Soit

$$e^{\pi(x-x^p)} = \sum_{n=0}^{\infty} c_n x^n$$

on peut démontrer que $v(c_n) \geq n(p-1)/p^2$. En utilisant (8.2) une fois de plus, on calcule facilement, pour $r \in \mathbb{Z}, 0 \leq r < p-1, b \in \mathbb{Z}_p$:

$$\begin{aligned}
\pi^r \Gamma_p(pb-r) x^b e^{\pi x} &\simeq x^b e^{\pi x} \psi(x^{-r} e^{\pi(x-x^p)}) \\
&= x^b e^{\pi x} \psi(\sum_{n=0}^{\infty} c_n x^{n-r}) \\
&= x^b e^{\pi x} \sum_{n=0}^{\infty} c_{np+r} x^n) \\
&\simeq x^b e^{\pi x} \sum_{n=0}^{\infty} c_{np+r} (-\pi)^{-n} (b+n-1)(b+n-2)\dots(b).
\end{aligned}$$

Ainsi $\Gamma_p(pb-r) = h_r(b)$ où la fonction h_r est définie par :

$$h_r(x) = \pi^{-r} \sum_{n=0}^{\infty} c_{np+r} (-\pi)^{-n} (x+n-1)(x+n-2)\dots(x).$$

Il n'est pas très difficile de vérifier que cette formule définit une fonction h_r qui est analytique dans le disque $D(0, |p|^{e-})$ où :

$$e = p^{-1} + (p-1)^{-1} - 1 < 0.$$

Par conséquent la fonction p-adique Γ_p est dans chaque disque $r + p\mathbb{Z}_p$ la restriction d'une fonction analytique.

Bibliographie

1. Livres élémentaires pour aller plus loin.

À propos des propriétés algébriques (Section 5.1) :

→ Borevitch Z. I., Chafarevitch I. R. : *Number Theory*, Academic Press (1966) (Traduction française: Gauthier-Villars 1967).

À propos des propriétés analytiques (Section 6) :

→ Amice Y. : *Les nombres p-adiques* Collection Sup. P.U.F. (1975).

À propos des mesures p-adiques, de la fonction gamma... (Section 7, 8) :

→ Koblitz N.: *p-adic Analysis : A short Course on Recent Work*, London Math. Soc. Lecture Notes 46 (1980).

À propos des connexions avec la physique :

→ Rammal R., Toulouse G., Virasoro M. : *Ultrametricity for physicists*, Rev. Mod. Phys. 58 (1986) 765.

Chacun de ces livres contient de nombreuses références. Quelques exercices à un niveau élémentaire peuvent être trouvés dans

→ Parent D. P. : *Exercices de théorie des nombres* Gauthier Villars (1978) (traduction anglaise : Springer (1984), traduction japonaise (1987)).

2. Références plus spécifiques.

Sur les valuations :

→ Schilling O. : *The theory of valuations* Math Survey IV (1950).

Sur les espaces de Banach :

→ Monna A. F. Rapport sur la théorie des espaces linéaires topologiques sur un corps valué non archimédien.

→ Gruson L., Van Der Put M. Banach spaces.

À la fois dans *Table ronde d'analyse non archimédienne 1972 Paris*, Bull. Soc. Math. France Mémoire 39-40 (1974) p 255-278 et 55-100.

Avec une introduction à la géométrie analytique rigide, très complet et auto-suffisant, mais plutôt difficile pour des non-spécialistes :

→ Bosh S., Güntzer U., Remmert R. : *Non Archimedean Analysis* Grundlehren 261 Springer (1984).