Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Jean Chauvineau

Quelques remarques sur les applications isométriques et la répartition dans un corps p-adique

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 6, n° 2 (1964-1965), exp. n° 12, p. 1-13

<http://www.numdam.org/item?id=SDPP_1964-1965__6_2_A3_0>

Séminaire DELANGE-PISOT
(Théorie des nombres)
6e année, 1964/65, n° 12

29 mars 1965

QUELQUES REMARQUES SUR LES APPLICATIONS ISOMÉTRIQUES ET LA RÉPARTITION DANS UN CORPS p-ADIQUE

par Jean CHAUVINEAU

1. Notations.

$\underset{\sim}{Z}$ désigne l'anneau des entiers rationnels, $\underset{\sim}{Z}^+$ l'ensemble des entiers naturels ; on pose $\underset{\sim}{N} = \underset{\sim}{Z}^+ \cup \{0\}$.

Soient K un corps p-adique complet contenant $\underset{\sim}{Q}_p$, A l'anneau des entiers de K , G le groupe des unités de K , P l'idéal maximal de A . En particulier, K pourra être $\underset{\sim}{Q}_p$ (on posera alors $A = \underset{\sim}{Z}_p$, $G = \underset{\sim}{U}_p$ et on aura $P = p\underset{\sim}{Z}_p$), ou encore la clôture algébrique complétée $\overset{\wedge}{\underset{\sim}{\Omega}}_p$ de $\underset{\sim}{Q}_p$ (on posera alors $A = \overset{\wedge}{\underset{\sim}{A}}_p$, $G = \overset{\wedge}{\underset{\sim}{G}}_p$, $P = \overset{\wedge}{\underset{\sim}{P}}_p$). Si $x \in K$, $v(x)$ désigne la valuation de x .

Si $X \subseteq K$, $\mathfrak{I}(X)$ désigne la classe des isométries de X . Si $o \in X$, on pose $X^* = X - \{0\}$. Si $x = (x_n)_{n \in \underset{\sim}{Z}^+}$ est une suite de $\underset{\sim}{Z}_p$, par exemple, et si $N \in \underset{\sim}{Z}^+$, $\alpha \in \underset{\sim}{Z}_p$, $k \in \underset{\sim}{N}$, on désigne par $(N , \alpha , k)_x$ le nombre des x_n tels que $1 \leqslant n \leqslant N$ et $x_n \in \alpha + p^k \underset{\sim}{Z}_p$. On s'intéresse aux suites équiréparties (e. r.) et et aux suites très bien réparties (t. b. r.).

2. Isométries analytiques de A .

Soit une suite $(a_k)_{k \in \underset{\sim}{N}}$ de K telle que $\lim_{k \to \infty} |a_k|_p = 0$; on pose

$$f(x) = \sum_{k \in \underset{\sim}{N}} a_k x^k \qquad \text{pour tout } x \in A . \tag{1}$$

(a) Pour que f définie par (1), à coefficients dans K , soit une isométrie de A , il suffit que l'on ait

$$a_0 \in A , \quad a_1 \in G , \quad a_k \in P \quad \text{pour} \quad k \geqslant 2 . \tag{2}$$

Formons, pour $x \in A$, $y \in A$:

$$f(x) - f(y) = (x - y)(a_1 + \sum_{k \geqslant 2} a_k z_k) ,$$

en posant $z_k = x^{k-1} + x^{k-2} y + \ldots + xy^{k-2} + y^{k-1}$; puisque $a_1 \in G$ et

$\sum_{k\geqslant 2} a_k z_k \in P$, on a

$$v(f(x) - f(y)) = v(x - y) \qquad \text{pour} \quad x \in A , \quad y \in A$$

et puisque $a_0 \in A$, f est une application isométrique de A dans A , donc $f \in \mathfrak{I}(A)$.

Ainsi les conditions (2) fournissent une classe d'isométries analytiques de A , et notamment d'isométries polynomiales de A ; si on les renforce, en exigeant plus particulièrement $a_0 \in P$, les restrictions à P et à G de ces isométries sont alors respectivement des isométries de P et des isométries de G .

(b) Lorsque K contient toutes les racines de $f - a_0$ de valuation $\geqslant 0$, les conditions (2) sont aussi nécessaires.

D'abord $f(0) = a_0 \in A$. Pour $x \in A$, on a $v(f(x) - a_0) = v(x)$, d'où, en posant $f(x) - a_0 = xg(x)$:

$$g(x) = \sum_{k\geqslant 1} a_k x^{k-1} \in G \qquad \text{pour tout} \quad x \in A ,$$

et notamment $g(0) = a_1 \in G$. On voit que g n'a pas de racine dans A ; dès lors g n'a pas non plus de racine dans $\underset{\sim}{A}_p$, et le polygone de Newton de g n'a aucun côté de pente $\leqslant 0$; puisque $a_1 \in G$, il en résulte que $a_k \in P$ pour $k \geqslant 2$.

Lorsque $K = \hat{\underset{\sim}{\Omega}}_p$, les conditions (2), alors nécessaires et suffisantes, fournissent l'expression générale des isométries analytiques de $\hat{\underset{\sim}{A}}_p$, et notamment l'expression générale des isométries polynomiales de $\hat{\underset{\sim}{A}}_p$.

3. Isométries réciproques.

Lorsque les conditions (2) sont satisfaites, $f \in \mathfrak{I}(A)$, et par conséquent f est univalente sur A ; f admet alors une fonction réciproque, dont la valeur au point $x \in A$ est l'unique racine dans A de $\varphi(y) = \sum_{k\geqslant 0} a_k y^k - x$, et cette fonction, notée f_A^{-1} , est elle aussi une isométrie de A .

4. Isométries polynomiales particulières de A .

(a) Soit

$$(3) \qquad f(x) = a_0 + a_1 x \prod_{1\leqslant k\leqslant m} (1 + \alpha_k x) \qquad a_0 , a_1 , \alpha_k \in K , \quad \alpha_k \neq 0 .$$

Les conditions (2) sont nécessaires et suffisantes ; elles sont d'ailleurs équivalentes aux suivantes

(4) $\qquad a_0 \in A\ ,\ a_1 \in G\ ,\ \alpha_k \in P \qquad \text{pour}\ \ 1 \leqslant k \leqslant m$

évidemment suffisantes, puisqu'elles entraînent (2), et d'autre part nécessaires, car s'il existait h tel que $1 \leqslant h \leqslant m$ et $v(\alpha_h) \leqslant 0$, on aurait $-\frac{1}{\alpha_h} \in A^*$ et $f(C) = f(-\frac{1}{\alpha_h}) = a_0$, de sorte que f ne serait pas une isométrie de A.

Le critère (4) s'étend aussitôt aux fonctions construites en remplaçant dans (3) le produit fini qui y figure par un produit infini convergent sur A.

En particulier, les conditions $a_0 \in A$, $a_1 \in G$, $a_2 \in P$ fournissent l'expression générale des isométries $x \rightsquigarrow a_0 + a_1 x + a_2 x^2$ de A.

(b) Soit $K = \underset{\sim}{Q}_p$, et soit

$$f(x) = a_0 + a_1 x + bx^{p^m+1} \qquad a_0, a_1, b \in \underset{\sim}{Q}_p\ ,\ m \in \underset{\sim}{N}\ .$$

Les conditions suffisantes $a_0 \in \underset{\sim}{Z}_p$, $a_1 \in \underset{\sim}{U}_p$, $b \in p\underset{\sim}{Z}_p$ sont aussi nécessaires pour que $f \in \mathfrak{I}(\underset{\sim}{Z}_p)$, car alors on a d'abord $f(0) = a_0 \in \underset{\sim}{Z}_p$, $g(0) = a_1 \in \underset{\sim}{U}_p$ et par conséquent $b \in \underset{\sim}{Z}_p$; d'autre part, on a $g(x) = a_1 + bx^{p^m} \in \underset{\sim}{U}_p$ pour tout $x \in \underset{\sim}{Z}_p$, ce qui, d'après FERMAT qui donne $x^{p^m} \in x + p\underset{\sim}{Z}_p$, équivaut à $a_1 + bx \in \underset{\sim}{U}_p$ pour tout $x \in \underset{\sim}{Z}_p$; mais cela serait impossible si l'on avait $b \in \underset{\sim}{U}_p$, donc $b \in p\underset{\sim}{Z}_p$.

Ainsi les conditions $a_0 \in \underset{\sim}{Z}_p$, $a_1 \in \underset{\sim}{U}_p$, $b \in p\underset{\sim}{Z}_p$ fournissent l'expression générale des isométries $x \rightsquigarrow a_0 + a_1 x + bx^{p^m+1}$ de $\underset{\sim}{Z}_p$ $(m \in \underset{\sim}{N})$.

5. Isométries analytiques de P.

Des remarques analogues s'appliquent aux isométries analytiques de P, avec les nouvelles conditions :

$$a_0 \in P\ ,\ a_1 \in G\ ,\ a_k \in A \qquad \text{pour}\ \ k \geqslant 2$$

qui fournissent l'expression générale des isométries analytiques (notamment polynomiales) de $\hat{\underset{\sim}{P}}_p$ et celle des isométries du second degré de P. Mais lorsque K est à valuation discrète, on dispose de conditions plus avantageuses. Soit q l'indice de ramification de K, et supposons ici que $|a_k|_p = o(p^{k/q})$ quand $k \to \infty$.

(a) Pour que f définie par (1), à coefficients dans K d'indice de ramification q, soit une isométrie de $P = p^{1/q} A$, il suffit que l'on ait

(5) $\qquad a_0 \in p^{1/q} A\ ,\ a_1 \in G\ ,\ a_k \in p^{(2-k)/q} A \qquad \text{pour}\ \ k \geqslant 2\ .$

En effet, pour $x \in P$, $y \in P$, on a $v(z_k) \geqslant \frac{k-1}{q}$, d'où $v(a_k z_k) \geqslant \frac{1}{q}$ pour $k \geqslant 2$, ce qui entraîne $v(f(x) - f(y)) = v(x - y)$ pour $x \in P$, $y \in P$.

(b) Lorsque K contient toutes les racines de $f - a_0$ de valuation $\geqslant \frac{1}{q}$, les conditions (5) sont aussi nécessaires.

En effet, g n'a pas de racine dans $p^{1/q} \underset{\sim}{A}_p$, donc le polygone de Newton de g n'a aucun côté de pente $\leqslant -\frac{1}{q}$; puisque $a_1 \in G$, il en résulte que

$$\frac{v(a_k)}{k-1} > -\frac{1}{q} , \qquad \text{donc} \quad v(a_k) \geqslant \frac{2-k}{q} .$$

6. Exemples d'applications isométriques ou homométriques dans $\underset{\sim}{Q}_p$ $(p \neq 2)$.

Posons $B_{h,k} = hp^k + p^{k+1} \underset{\sim}{Z}_p$, où $h = 1 , \dots , p-1$, $k \in \underset{\sim}{Z}$.

(a) $x \rightsquigarrow x|x|_p$ est une application homométrique de $B_{h,k}$ sur $B_{h,0}$ (ici p quelconque).

(b) Soit $\exp x - 1 = \sum_{k \geqslant 1} \frac{x^k}{k!}$ série convergente sur $p\underset{\sim}{Z}_p$; on a $a_0 = 0$, $a_1 = 1$, et pour $k \geqslant 2$:

$$v(a_k) = -v(k!) \geqslant \frac{1-k}{p-1} > 1 - k$$

d'où $v(a_k) \geqslant 2 - k$; donc $x \rightsquigarrow \exp x$ est une application isométrique de $p\underset{\sim}{Z}_p$ sur $B_{1,0}$.

(c) L'application réciproque $\log$, définie sur $B_{1,0}$, peut être prolongée sur $\underset{\sim}{Q}_p^*$. En effet, on sait qu'à tout $x \in \underset{\sim}{U}_p$ est associée une racine $(p-1)$-ième de 1 , soit ζ_x , telle que $\zeta_x x \in B_{1,0}$. Dès lors, la fonction F définie par

$$F(x) = \log \zeta_{x|x|_p} x|x|_p \qquad \text{pour tout} \quad x \in \underset{\sim}{Q}_p^*$$

vérifie la relation fonctionnelle $F(x) + F(y) = F(xy)$; elle fournit donc un prolongement du logarithme sur $\underset{\sim}{Q}_p^*$ et sera notée $\log$ dans tout ce qui suit. Les zéros de cette fonction prolongée sont les nombres $\zeta^h p^k$, où ζ désigne une racine $(p-1)$-ième primitive de 1 , $h = 1 , \dots , p-1$, $k \in \underset{\sim}{Z}$.

Si $x , y \in B_{h,k}$, on a

$$v(\log x - \log y) = v(\log \tfrac{x}{y}) = v(\tfrac{x}{y} - 1) = v(x - y) - k ,$$

donc $x \rightsquigarrow \log x$ est une application homométrique de $B_{h,k}$ sur $p\underset{\sim}{Z}_p$.

(d) $x \rightsquigarrow x \exp x$ est une isométrie de $p\underset{\sim}{Z}_p$.

(e) On en déduit que $x \rightsquigarrow x \log x$ est une application isométrique de $B_{h,k}$ sur $p^{k+1}\underset{\sim}{Z}_p$.

(f) Si $x , y \in B_{1,0}$, alors la valuation $v(\log x^x - \log y^y)$ est égale à $v(x - y)$ et comme elle est aussi égale à $v(x^x - y^y)$, on voit que $x \rightsquigarrow x^x$ est une isométrie de $B_{1,0}$.

(g) Soit

$$\sin x = \sum_{h \geqslant 0} (-1)^h \frac{x^{2h+1}}{(2h+1)!}$$

série convergente sur $p\underset{\sim}{Z}_p$; on a $a_0 = 0$, $a_1 = 1$, et pour $k \geqslant 2$, on a

$$v(a_k) = \infty \quad \text{si} \quad k \quad \text{pair},$$

$$v(a_k) = -v(k!) \geqslant 2 - k \quad \text{si} \quad k \quad \text{impair} ;$$

donc $x \rightsquigarrow \sin x$ est une isométrie de $p\underset{\sim}{Z}_p$, et par itération $x \rightsquigarrow \sin^{(k)} x$, où $k \in \underset{\sim}{Z}^+$, est une isométrie de $p\underset{\sim}{Z}_p$.

(h) $x \rightsquigarrow x \cos x$ est une isométrie de $p\underset{\sim}{Z}_p$.

(i) Si $x , y \in p\underset{\sim}{Z}_p$, on a

$$v(\operatorname{tg} x - \operatorname{tg} y) = v\left(\frac{\sin(x - y)}{\cos x \cos y}\right) = v(\sin(x - y)) = v(x - y) ,$$

donc $x \rightsquigarrow \operatorname{tg} x$ est une isométrie de $p\underset{\sim}{Z}_p$, et par itération $x \rightsquigarrow \operatorname{tg}^{(k)} x$, où $k \in \underset{\sim}{Z}^+$, est une isométrie de $p\underset{\sim}{Z}_p$.

7. Exemples d'équirépartition ou de très bonne répartition sur des compacts de $\underset{\sim}{Z}_p$ $(p \neq 2)$.

7.1. - Les conditions $a_0 \in \underset{\sim}{Z}_p$, $a_1 \in \underset{\sim}{U}_p$, $a_2 \in p\underset{\sim}{Z}_p$ sont suffisantes pour que la suite $f(n) = a_0 + a_1 n + a_2 n^2$ soit t. b. r. sur $\underset{\sim}{Z}_p$. Mais, si $p \neq 2$, ces conditions sont aussi nécessaires pour que la suite $f(n)$, à coefficients dans $\underset{\sim}{Q}_p$, soit e. r. sur $\underset{\sim}{Z}_p$. En effet, montrons d'abord que les trois coefficients sont alors dans $\underset{\sim}{Z}_p$: on a

$$a_0 \in \underset{\sim}{Z}_p , \quad a_1 + a_2 \in \underset{\sim}{Z}_p \quad \text{et} \quad f(n+1) - f(n) = a_1 + a_2 + 2a_2 n \in \underset{\sim}{Z}_p ,$$

d'où $2a_2 n \in \underset{\sim}{Z}_p$ pour tout $n \in \underset{\sim}{Z}^+$, ce qui exige, puisque $p \neq 2$, qu'on ait $a_2 \in \underset{\sim}{Z}_p$; finalement aussi $a_1 \in \underset{\sim}{Z}_p$. Cela posé, quel que soit $h \in \underset{\sim}{N}$, la suite

$$f(n + h) = f(h) + nf'(h) + a_2 n^2$$

est e. r. sur $\underset{\sim}{Z}_p$. Supposons qu'on ait $f'(h) \in p\underset{\sim}{Z}_p$, et soit $(N , f(h) , 2)$ le

nombre des termes $f(n + h)$ tels que $1 \leqslant n \leqslant N$ et

$$v(f(n + h) - f(h)) = v(nf'(h) + a_2 n^2) \geqslant 2 .$$

On aurait évidemment $(N , f(h) , 2) \geqslant \left[\frac{N}{p}\right]$, d'où

$$\frac{1}{N}(N , f(h) , 2) \geqslant \frac{1}{N}\left[\frac{N}{p}\right] \to \frac{1}{p} \quad \text{quand} \quad N \to \infty ;$$

comme d'autre part $\frac{1}{N}(N , f(h) , 2) \to \frac{1}{p^2}$, on devrait avoir $\frac{1}{p^2} \geqslant \frac{1}{p}$, ce qui est impossible. Donc

$$f'(h) = a_1 + 2a_2 h \in \underset{\sim}{U}_p \qquad \text{pour tout} \quad h \in \underset{\sim}{N} ,$$

ce qui exige $a_1 \in \underset{\sim}{U}_p$ et $a_2 \in p\underset{\sim}{Z}_p$.

Ainsi les conditions $a_0 \in \underset{\sim}{Z}_p$, $a_1 \in \underset{\sim}{U}_p$, $a_2 \in p\underset{\sim}{Z}_p$ fournissent l'expression générale des suites $a_0 + a_1 n + a_2 n^2$ qui sont t. b. r. [resp. e. r.] sur $\underset{\sim}{Z}_p$.

7.2. - Les applications isométriques obtenues dans le § 6 donnent immédiatement des suites t. b. r. :

(a) la suite $\exp pn$ est t. b. r. sur $1 + p\underset{\sim}{Z}_p$;

(b) les suites $n \exp pn$, $n \cos pn$ sont t. b. r. sur $\underset{\sim}{Z}_p$;

(c) les suites $\sin^{(k)} pn$, $\mathrm{tg}^{(k)} pn$, où $k \in \underset{\sim}{Z}^+$, sont t. b. r. sur $p\underset{\sim}{Z}_p$.

7.3. - Les applications homométriques obtenues dans le § 6 fournissent aisément des suites e. r..

Par exemple, soit une suite x_n e. r. sur $\underset{\sim}{Z}_p^*$, et posons $y_n = \log x_n$. Choisissant $\alpha \in p\underset{\sim}{Z}_p$, $k \in \underset{\sim}{Z}^+$, on a

$$(N , \alpha , k)_y = \sum_{\ell=0}^{\infty} \sum_{h=1}^{p-1} (N , \beta_{h,\ell} , k + \ell)_x$$

où $\beta_{h,\ell} \in B_{h,\ell}$, et on justifie sans peine que, quand $N \to \infty$:

$$\frac{1}{N}(N , \alpha , k)_y \to \sum_{\ell=0}^{\infty} \sum_{h=1}^{p-1} \frac{1}{p^{k+\ell}} = \frac{p-1}{p^k} \sum_{\ell=0}^{\infty} \frac{1}{p^\ell} = \frac{1}{p^{k-1}}$$

ce qui montre que la suite y_n est e. r. sur $p\underset{\sim}{Z}_p$. Attribuant au besoin un sens au symbole $\log 0$ (convention $\log 0 \in p\underset{\sim}{Z}_p$), ce résultat sera applicable aux suites x_n e. r. sur $\underset{\sim}{Z}_p$. Il peut d'ailleurs être itéré, car si la suite $\log^{(k)} x_n$, où $k \in \underset{\sim}{Z}^+$, est e. r. sur $p\underset{\sim}{Z}_p$, il en est de même de la suite

$$\log \frac{\log^{(k)} x_n}{p} = \log^{(k+1)} x_n ,$$

puisque $\log p = 0$.

Cet argument, et d'autres qui lui sont analogues, montrent (on suppose ci-dessous $n \geqslant 1$) que

(a) <u>la suite</u> $\log^{(k)} n$, <u>où</u> $k \in \underset{\sim}{Z}^+$, <u>est e. r. sur</u> $p\underset{\sim}{Z}_p$ (convention $\log 0 \in p\underset{\sim}{Z}_p$ si $k \geqslant 2$) ;

(b) <u>la suite</u> $n|n|_p$ <u>est e. r. sur</u> $\underset{\sim}{U}_p$ (ici p quelconque) ;

(c) <u>la suite</u> $n|n|_p \log n$ <u>est e. r. sur</u> $p\underset{\sim}{Z}_p$.

7.4. - Des sommations classiques montrent que <u>les suites</u> $\sum_{0\leqslant k\leqslant n} \exp(\alpha k + \beta)$, $\sum_{0\leqslant k\leqslant n} \cos(\alpha k + \gamma)$, <u>où</u> $\alpha \in p\underset{\sim}{Z}_p$, $\beta \in p\underset{\sim}{Z}_p$, $\gamma \in p^{v(\alpha)}\underset{\sim}{Z}_p$, <u>sont t. b. r. sur</u> $\underset{\sim}{Z}_p$.

8. <u>Applications isométriques par boules maximales de</u> A <u>dans</u> A.

Revenons à (1), et appelons boules maximales de **A** les boules de la forme $\alpha + P$, où $\alpha \in A$.

(a) <u>Pour que</u> f <u>définie par (1), à coefficients dans</u> K , <u>soit une application isométrique par boules maximales de</u> A <u>dans</u> A , <u>il suffit que l'on ait</u>

(6) $\qquad a_1 \in G$, $a_k \in A$ si $p|k$, $\qquad a_k \in P$ si $p\not|k$ et $k \neq 1$.

En effet, z_k se met sous la forme $z_k = kx^{k-1} + (x - y)t_k$, où $t_k \in A$; si l'on suppose $x - y \in P$, alors on a, pour $k \geqslant 2$,

$$v(a_k z_k) > v(a_k) \geqslant 0 \qquad \text{si } p|k$$

$$v(a_k z_k) \geqslant v(a_k) > 0 \qquad \text{si } p\not|k$$

d'où $v(f(x) - f(y)) = v(x - y)$ pour $x \in A$, $y \in A$, $x - y \in P$.

(b) <u>Lorsque</u> K <u>contient toutes les racines de</u> $f - a_0$ <u>de valuation</u> > 0 , <u>et toutes les racines de</u> f' <u>de valuation</u> $\geqslant 0$, <u>les conditions (6) sont aussi nécessaires.</u>

En effet, $g(x) \in G$ pour tout $x \in P$; g n'a pas de racine dans $\underset{\sim}{P}_p$, donc le polygone de Newton de g n'a aucun côté de pente < 0 ; puisque $a_1 \in G$, il en résulte que $a_k \in A$ pour $k \geqslant 2$.

D'autre part, pour $x \in A$, $y \in A$, $x - y \in P$, on a

$$v(f(y) - f(x)) = v(y - x)$$

c'est-à-dire $\frac{f(y) - f(x)}{y - x} \in G$; faisant tendre y vers x fixé, on obtient

$$f'(x) = \sum_{k \geqslant 1} k a_k x^{k-1} \in G \qquad \text{pour tout } x \in A .$$

f' n'a pas de racine dans $\underset{\sim}{A}_p$, donc le polygone de Newton de f' n'a aucun côté de pente $\leqslant 0$; puisque $a_1 \in G$, il en résulte que $k a_k \in P$ pour $k \geqslant 2$, et notamment $a_k \in P$ si $p \nmid k$ et $k \neq 1$.

9. Isométries polynomiales particulières de $\underset{\sim}{Z}_p$.

Soit $K = \underset{\sim}{Q}_p$ et soit

$$f(x) = a_0 + a_1 x + b x^{p^m} \qquad a_0 , a_1 , b \in \underset{\sim}{Q}_p , \quad m \in \underset{\sim}{Z}^+ .$$

Supposons réalisées les conditions suffisantes (6), qui s'écrivent ici $a_0 \in \underset{\sim}{Z}_p$, $a_1 \in \underset{\sim}{U}_p$, $b \in \underset{\sim}{Z}_p$. D'après FERMAT, on a $x^{p^m} \in x + p\underset{\sim}{Z}_p$, de sorte que

$$f(x) \in a_0 + (a_1 + b)x + p\underset{\sim}{Z}_p \qquad \text{pour tout } x \in \underset{\sim}{Z}_p .$$

Si $a_1 + b \in p\underset{\sim}{Z}_p$, alors f applique isométriquement chaque boule maximale de $\underset{\sim}{Z}_p$ sur la boule $a_0 + p\underset{\sim}{Z}_p$.

Si $a_1 + b \in \underset{\sim}{U}_p$, alors f opère une permutation sur l'ensemble des boules maximales de $\underset{\sim}{Z}_p$, et $f \in \mathfrak{I}(\underset{\sim}{Z}_p)$.

Il en résulte que les conditions $a_0 \in \underset{\sim}{Z}_p$, $a_1 \in \underset{\sim}{U}_p$, $a_1 + b \in \underset{\sim}{U}_p$ sont suffisantes pour que $f \in \mathfrak{I}(\underset{\sim}{Z}_p)$. Elles sont aussi nécessaires pour que $f \in \mathfrak{I}(\underset{\sim}{Z}_p)$, car alors on a

$$f(0) = a_0 \in \underset{\sim}{Z}_p , \quad g(0) = a_1 \in \underset{\sim}{U}_p , \quad g(1) = a_1 + b \in \underset{\sim}{U}_p .$$

Ainsi les conditions $a_0 \in \underset{\sim}{Z}_p$, $a_1 \in \underset{\sim}{U}_p$, $a_1 + b \in \underset{\sim}{U}_p$ fournissent l'expression générale des isométries $x \rightsquigarrow a_0 + a_1 x + b x^{p^m}$ de $\underset{\sim}{Z}_p$ $(m \in \underset{\sim}{Z}^+)$.

10. Applications isométriques par boules maximales de G dans G.

Soit une suite $(a_k)_{k \in \underset{\sim}{Z}}$ de K telle que $\lim_{|k| \to \infty} |a_k|_p = 0$; on pose

$$f(x) = \sum_{k \in \underset{\sim}{Z}} a_k x^k \qquad \text{pour tout } x \in G . \tag{7}$$

(a) Pour que f définie par (7), à coefficients dans K, soit une application isométrique par boules maximales de G dans G, il suffit qu'il existe

$m \in \underset{\sim}{Z} - p\underset{\sim}{Z}$ tel que

(8) $$a_m \in G , \quad a_k \in P \quad \text{pour} \quad k \neq m .$$

Formons, pour $x \in G$, $y \in G$:

$$f(x) - f(y) = (x - y)\Big(- \sum_{k\geqslant 1} \frac{a_{-k}\, z_k}{x^k\, y^k} + \sum_{k\geqslant 1} a_k\, z_k\Big)$$

en posant $z_1 = 1$ et comme plus haut $z_k = x^{k-1} + x^{k-2}\, y + \ldots + xy^{k-2} + y^{k-1}$ pour $k \geqslant 2$, de sorte que $z_k = kx^{k-1} + (x - y)t_k$ où $t_k \in A$; si l'on suppose $x - y \in P$, alors on a, pour $k \geqslant 1$:

$$v(z_k) = 0 \quad \text{si} \quad p\not| k , \qquad v(z_k) > 0 \quad \text{si} \quad p|k .$$

Définissons u_n pour $n \neq 0$ en posant $u_k = a_k\, z_k$ et $u_{-k} = - \frac{a_{-k}\, z_k}{x^k\, y^k}$ pour $k \geqslant 1$; on a alors, pour $n \neq 0$:

$$v(u_n) = v(a_n) \quad \text{si} \quad p\not| n , \qquad v(u_n) > v(a_n) \quad \text{si} \quad p|n .$$

Les conditions (8) entraînent $v(u_m) = v(a_m) = 0$ et $v(u_n) \geqslant v(a_n) > 0$ pour $n \neq 0$, $n \neq m$, de sorte que $\sum_{n\neq 0} u_n \in G$ et

$$v(f(x) - f(y)) = v(x - y) \qquad \text{pour} \quad x \in G , \quad y \in G , \quad x - y \in P .$$

Dès lors, puisque $a_0 \in P$, d'où $f(x) \in G$ pour $x \in G$, f est une application isométrique par boules maximales de G dans G .

(b) Lorsque K contient toutes les racines de f et de f' de valuation nulle, les conditions (8) sont aussi nécessaires.

En effet, f n'a pas de racine dans $\underset{\sim}{G}_p$, donc le polygone de Newton de f n'a aucun côté de pente nulle ; alors $\min_{k\in\underset{\sim}{Z}} v(a_k)$ est atteint pour une seule valeur de k , soit m , et l'on a

$$v(a_m) = v(f(x)) = 0 , \quad v(a_k) > 0 \quad \text{pour} \quad k \neq m .$$

D'autre part $f'(x) = \sum_{k\in\underset{\sim}{Z}} ka_k\, x^{k-1} \in G$ pour tout $x \in G$; f' n'a pas de racine dans $\underset{\sim}{G}_p$, donc le polygone de Newton de f' n'a aucun côté de pente nulle ; alors $\min_{k\in\underset{\sim}{Z}} v(ka_k)$ est atteint pour une seule valeur de k , soit m' , et l'on a

$$v(m'a_{m'}) = v(f'(x)) = 0 , \quad v(ka_k) > 0 \quad \text{pour} \quad k \neq m' .$$

Si l'on avait $m \neq m'$, on aurait à la fois $v(m'a_{m'}) = 0$ et $v(a_{m'}) > 0$, d'où $v(m') < 0$, ce qui est impossible ; donc $m = m'$, et finalement il existe $m \in \underset{\sim}{Z}$

tel que

$$v(a_m) = 0 \ , \quad v(m) + v(a_m) = 0 \ , \quad v(a_k) > 0 \qquad \text{pour} \quad k \neq m$$

autrement dit, il existe $m \in \underset{\sim}{Z} - p\underset{\sim}{Z}$ tel que l'on ait (8).

11. Isométries de $\underset{\sim}{U}_p$.

11.1. - Soit $K = \underset{\sim}{Q}_p$ et supposons satisfaites les conditions (8) ; alors $f(x) \in a_m x^m + p\underset{\sim}{Z}_p$ pour tout $x \in \underset{\sim}{U}_p$. Si le nombre $\frac{p-1}{(m \ , \ p-1)}$ des résidus (mod p) de degré $|m|$ atteint son maximum $p - 1$, c'est-à-dire si $(m \ , \ p - 1) = 1$, alors f opère une permutation sur l'ensemble des boules maximales de $\underset{\sim}{U}_p$, donc $f \in \mathfrak{I}(\underset{\sim}{U}_p)$. Posant

$$E_p = \{k : \ k \in \underset{\sim}{Z} \ \text{ et } \ (k \ , \ p) = (k \ , \ p - 1) = 1\} \ ,$$

on a finalement :

Pour que f définie par (7), à coefficients dans $\underset{\sim}{Q}_p$, soit une isométrie de $\underset{\sim}{U}_p$, il suffit qu'il existe $m \in E_p$ tel que l'on ait

$$a_m \in \underset{\sim}{U}_p \ , \quad a_k \in p\underset{\sim}{Z}_p \qquad \text{pour} \quad k \neq m \ . \tag{9}$$

Ainsi les conditions (9) fournissent une classe d'isométries de $\underset{\sim}{U}_p$ développables en série de Laurent, et notamment d'isométries quasi-polynomiales de $\underset{\sim}{U}_p$.

11-2. - Lorsque les conditions (9) sont satisfaites, $f \in \mathfrak{I}(\underset{\sim}{U}_p)$ et par conséquent f est univalente sur $\underset{\sim}{U}_p$; f admet alors une fonction réciproque, dont la valeur au point $x \in \underset{\sim}{U}_p$ est l'unique racine dans $\underset{\sim}{U}_p$ de $\varphi(y) = \sum_{k \in \underset{\sim}{Z}} a_k y^k - x$, et cette fonction, notée $f^{-1}_{\underset{\sim}{U}_p}$, est elle aussi une isométrie de $\underset{\sim}{U}_p$.

11-3. - La condition $m \in E_p$, suffisante pour que $f(x) = x^m$ soit une isométrie de $\underset{\sim}{U}_p$, est aussi nécessaire pour que $f \in \mathfrak{I}(\underset{\sim}{U}_p)$, car alors il existe $p - 1$ résidus (mod p) de degré $|m|$, de sorte que $(m \ , \ p - 1) = 1$; d'autre part, on a

$$x^m - y^m = (x - y)z_m = (x - y)(mx^{m-1} + (x - y)t_m) \quad \text{pour} \quad x \in \underset{\sim}{U}_p \ , \quad y \in \underset{\sim}{U}_p \ ,$$

d'où, si de plus $x - y \in p\underset{\sim}{Z}_p$:

$$v(x^m - y^m) \geqslant v(x - y) + \min(v(m) \ , \ 1)$$

et, puisque le premier membre est égal à $v(x - y)$, cela entraîne $\min(v(m) \ , \ 1) \leqslant 0$, ce qui exige $v(m) = 0$; finalement on a $m \in E_p$. Ainsi $x \rightsquigarrow x^m$, où $m \in \underset{\sim}{Z}$, est une isométrie de $\underset{\sim}{U}_p$ si et seulement si $m \in E_p$.

11-4. - Il en résulte que, si $m \in E_p$, tout $x \in U_p$ admet une seule racine m-ième dans U_p, qu'on notera $x^{1/m}$, et alors $x \rightsquigarrow x^{1/m}$, où $m \in E_p$, est une isométrie de U_p.

12. Exemples d'équirépartition ou de très bonne répartition sur U_p.

(a) Mme Y. AMICE a montré [1] que, si $p \neq 2$, pour que la suite α^n, où $\alpha \in h + pZ_p$, $h = 1, \ldots, p-1$, soit t. b. r. [resp. e. r.] sur U_p, il faut et il suffit que $\alpha^{p-1} \in 1 + pU_p$ et que h engendre multiplicativement toutes les classes résiduelles (mod p) non nulles. La 1re condition équivaut à $\log \alpha \in pU_p$, c'est-à-dire encore $\zeta_h \alpha = \exp \log \alpha \in 1 + pU_p$, ou enfin $\alpha \in \zeta_h^{-1} + pU_p$, où ζ_h^{-1} est la racine $(p-1)$-ième de 1 située dans $h + pZ_p$. La 2e condition exprime que cette racine ζ_h^{-1} est une racine primitive. Ainsi la suite α^n, où $\alpha \in U_p$, est t. b. r. [resp. e. r.] sur U_p si et seulement si $\alpha \in \zeta + pU_p$, où ζ désigne une racine $(p-1)$-ième primitive quelconque de 1 $(p \neq 2)$.

(b) Soit ν_n le n-ième entier naturel non divisible par p ; les suites ν_n^m, $\nu_n^{1/m}$, où $m \in E_p$, sont t. b. r. sur U_p.

(c) Les suites $(n|n|_p)^m$, $(n|n|_p)^{1/m}$, $(n|n|_p)^m \exp pmn$, $(n|n|_p)^{1/m} \exp \frac{pn}{m}$, où $m \in E_p$, sont e. r. sur U_p ($p \neq 2$ pour les deux dernières).

13. Un théorème d'équivalence concernant la répartition sur A de certaines suites polynomiales à coefficients dans A.

13-1. - Supposons K à valuation discrète ; soient q son indice de ramification, p^s le cardinal du corps des restes $\overline{K}$ de K, $\vec{\omega} = (\omega_0, \ldots, \omega_{s-1})$ une base de $\overline{K}$ considéré comme espace vectoriel de dimension s sur le corps $Z/(p)$ des entiers (mod p).

A tout $n \in Z^+$, on associe les $c_\ell(n)$, où $\ell \in N$, définis par

$$n = \sum_{\ell \geqslant 0} c_\ell(n)\, p^\ell \qquad \text{où } 0 \leqslant c_\ell(n) \leqslant p-1 \text{ pour tout } \ell \in N,$$

c'est-à-dire qu'on écrit n dans le système de numération à base p, et on construit la suite u_n de A, dite suite associée à la base $\vec{\omega}$ de $\overline{K}$, en posant

$$u_n = \sum_{\ell \geqslant 0} c_\ell(n)\, \omega_{s\{\frac{\ell}{s}\}}\, p^{\frac{1}{q}[\frac{\ell}{s}]}$$

où $[r]$ et $\{r\}$ désignent respectivement la partie entière et la partie fractionnaire du réel r. Par construction même, la suite u_n est t. b. r. sur A.

Quel que soit $k \in \underset{\sim}{Z}^+$, les ks premiers "chiffres" de $n + p^{ks}$ sont respectivement égaux aux ks premiers "chiffres" de n :

$$c_\ell(n + p^{ks}) = c_\ell(n) \qquad \text{pour } \ell = 0 , 1 , \dots , ks - 1 , \text{ pour } n , k \in \underset{\sim}{Z}^+ .$$

On en déduit aussitôt que $u_{n+p^{ks}} \in u_n + p^{k/q} A$ et plus généralement, en élevant à la puissance $j \in \underset{\sim}{Z}^+$:

$$u^j_{n+p^{ks}} \in u^j_n + p^{k/q} A \qquad \text{pour } n , k , j \in \underset{\sim}{Z}^+ .$$

Soit alors $f(X) = \sum_{0 \leqslant j \leqslant m} a_j X^j$ un polynôme formel en X à coefficients dans A .

(a) On a

$$f(u_{n+p^{ks}}) = \sum_{0 \leqslant j \leqslant m} a_j u^j_{n+p^{ks}} \in f(u_n) + p^{k/q} A$$

d'où, quels que soient $\alpha \in A$, $n \in \underset{\sim}{Z}^+$, $k \in \underset{\sim}{Z}^+$:

$$f(u_n) \in \alpha + q^{k/q} A \Leftrightarrow f(u_{n+p^{ks}}) \in \alpha + p^{k/q} A .$$

On en tire immédiatement

$$(10) \quad (Hp^{ks} , \alpha , \tfrac{k}{q})_{fou} = H(p^{ks} , \alpha , \tfrac{k}{q})_{fou} \qquad \text{pour } \alpha \in A , H \in \underset{\sim}{Z}^+ , k \in \underset{\sim}{Z}^+ .$$

Dès lors, <u>pour que la suite</u> $f(u_n)$ <u>soit t. b. r. sur</u> A , il faut et il suffit que $(Hp^{ks} , \alpha , \frac{k}{q})_{fou} = H$ quels que soient $\alpha \in A$, $H \in \underset{\sim}{Z}^+$, $k \in \underset{\sim}{Z}^+$; pour cela, d'après (10), il faut et il suffit que l'on ait

$$(11) \qquad (p^{ks} , \alpha , \tfrac{k}{q})_{fou} = 1 \qquad \text{pour tout } \alpha \in A , \text{ pour tout } k \in \underset{\sim}{Z}^+ .$$

(b) Soit $N \in \underset{\sim}{Z}^+$ et posons $H = \left[\frac{N}{p^{ks}}\right]$, de sorte que $Hp^{ks} \leqslant N < (H + 1)p^{ks}$. On a alors

$$H(p^{ks} , \alpha , \tfrac{k}{q})_{fou} \leqslant (N , \alpha , \tfrac{k}{q})_{fou} \leqslant (H + 1)(p^{ks} , \alpha , \tfrac{k}{q})_{fou}$$

d'où l'on tire, quels que soient $\alpha \in A$, $k \in \underset{\sim}{Z}^+$:

$$(12) \qquad \lim_{N \to \infty} (N , \alpha , \tfrac{k}{q})_{fou} = \infty \Leftrightarrow (p^{ks} , \alpha , \tfrac{k}{q})_{fou} \geqslant 1 .$$

Dès lors, <u>pour que la suite</u> $f(u_n)$ <u>soit à répartition partout dense</u> [r. p. d.] <u>sur</u> A , il faut et il suffit que $\lim_{N \to \infty} (N , \alpha , \frac{k}{q})_{fou} = \infty$ quels que soient $\alpha \in A$, $k \in \underset{\sim}{Z}^+$; pour cela, d'après (12), il faut et il suffit que l'on ait

$$(p^{ks} , \alpha , \tfrac{k}{q})_{fou} \geqslant 1 \qquad \text{pour tout } \alpha \in A , \text{ pour tout } k \in \underset{\sim}{Z}^+$$

et cette condition équivaut évidemment à (11).

D'ailleurs, dans ce critère commun (11), on peut remplacer $\alpha \in A$ par $\alpha \in \underset{\sim}{C}_k$, en posant, pour tout $k \in \underset{\sim}{Z}^+$:

$$\underset{\sim}{C}_k = \left\{ \sum_{0 \leqslant j \leqslant k-1} \sum_{0 \leqslant i \leqslant s-1} h_{i,j}\, \omega_i\, p^{j/q} \right\}_{h_{i,j}=0,1,\ldots,p-1} .$$

La très bonne répartition sur A impliquant l'équirépartition sur A, qui implique à son tour la répartition partout dense sur A, on obtient finalement :

THÉORÈME. - Soit $(u_n)_{n \in \underset{\sim}{Z}^+}$ la suite associée à une base $\vec{\omega}$ du corps des restes de K ; pour une suite polynomiale en u_n à coefficients dans A, soit $(f(u_n))_{n \in \underset{\sim}{Z}^+}$, les propriétés d'être r. p. d. sur A, e. r. sur A, t. b. r. sur A sont équivalentes, et pour que cette suite possède ces propriétés, il faut et il suffit que l'on ait, pour tout $\alpha \in \underset{\sim}{C}_k$ et pour tout $k \in \underset{\sim}{Z}^+$:

$$\left(p^{ks}\ ,\ \alpha\ ,\ \frac{k}{q}\right)_{f \circ u} = 1 .$$

13-2. - Si $K = \underset{\sim}{Q}_p$, alors $A = \underset{\sim}{Z}_p$, $q = s = 1$; prenant $\omega_0 = 1$, on a $u_n = n$, $f \circ u = f$, $\underset{\sim}{C}_k = \{0\ ,\ 1\ ,\ \ldots\ ,\ p^k - 1\}$, et on obtient :

COROLLAIRE. - Pour une suite polynomiale en n à coefficients dans $\underset{\sim}{Z}_p$, soit $(f(n))_{n \in \underset{\sim}{Z}^+}$, les propriétés d'être r. p. d. sur $\underset{\sim}{Z}_p$, e. r. sur $\underset{\sim}{Z}_p$, t. b. r. sur $\underset{\sim}{Z}_p$ sont équivalentes, et pour que cette suite possède ces propriétés, il faut et il suffit que l'on ait, pour tout $h = 0\ ,\ 1\ ,\ \ldots\ ,\ p^k - 1$ et pour tout $k \in \underset{\sim}{Z}^+$:

$$\left(p^k\ ,\ h\ ,\ k\right)_f = 1 .$$

BIBLIOGRAPHIE

[1] AMICE (Yvette). - Interpolation p-adique, Bull. Soc. math. France, t. 92, 1964, p. 117-180 (Thèse Sc. math. Paris, 1963).