

# 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](http://www.numdam.org/item?id=SDPP_1964-1965__6_2_A3_0)

© Séminaire Delange-Pisot-Poitou. Théorie des nombres  
(Secrétariat mathématique, Paris), 1964-1965, tous droits réservés.

L'accès aux archives de la collection « Séminaire Delange-Pisot-Poitou. Théorie des nombres » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques  
<http://www.numdam.org/>

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

par Jean CHAUVINEAU

1. Notations.

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

Soient  $K$  un corps  $p$ -adique complet contenant  $\mathbb{Q}_p$ ,  $A$  l'anneau des entiers de  $K$ ,  $G$  le groupe des unités de  $K$ ,  $P$  l'idéal maximal de  $A$ . En particulier,  $K$  pourra être  $\mathbb{Q}_p$  (on posera alors  $A = \mathbb{Z}_p$ ,  $G = \mathbb{U}_p$  et on aura  $P = p\mathbb{Z}_p$ ), ou encore la clôture algébrique complétée  $\hat{\mathbb{Q}}_p$  de  $\mathbb{Q}_p$  (on posera alors  $A = \hat{\mathbb{A}}_p$ ,  $G = \hat{\mathbb{G}}_p$ ,  $P = \hat{P}_p$ ). 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  $X^* = X - \{o\}$ . Si  $x = (x_n)_{n \in \mathbb{Z}^+}$  est une suite de  $\mathbb{Z}_p$ , par exemple, et si  $N \in \mathbb{Z}^+$ ,  $\alpha \in \mathbb{Z}_p$ ,  $k \in \mathbb{N}$ , on désigne par  $(N, \alpha, k)_x$  le nombre des  $x_n$  tels que  $1 \leq n \leq N$  et  $x_n \in \alpha + p^k \mathbb{Z}_p$ . On s'intéresse aux suites équiréparties (e. r.) et aux suites très bien réparties (t. b. r.).

2. Isométries analytiques de  $A$ .

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

$$(1) \quad f(x) = \sum_{k \in \mathbb{N}} a_k x^k \quad \text{pour tout } x \in A.$$

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

$$(2) \quad a_0 \in A, \quad a_1 \in G, \quad a_k \in P \quad \text{pour } k \geq 2.$$

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

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

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

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

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

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  $\geq 0$ , 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  $f(x) - a_0 = xg(x)$ :

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

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  $\hat{A}_p$ , et le polygone de Newton de  $g$  n'a aucun côté de pente  $\leq 0$ ; puisque  $a_1 \in G$ , il en résulte que  $a_k \in P$  pour  $k \geq 2$ .

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

### 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  $\varphi(y) = \sum_{k \geq 0} a_k y^k - x$ , et cette fonction, notée  $f_A^{-1}$ , est elle aussi une isométrie de  $A$ .

### 4. Isométries polynomiales particulières de $A$ .

(a) Soit

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

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

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

évidemment suffisantes, puisqu'elles entraînent (2), et d'autre part nécessaires, car s'il existait  $h$  tel que  $1 \leq h \leq m$  et  $v(\alpha_h) \leq 0$ , 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  $x \mapsto a_0 + a_1 x + a_2 x^2$  de  $A$ .

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

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

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

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

## 5. Isométries analytiques de $P$ .

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

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

qui fournissent l'expression générale des isométries analytiques (notamment polynomiales) de  $\hat{P}_p$  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  $k \rightarrow \infty$ .

(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

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

En effet, pour  $x \in P$ ,  $y \in P$ , on a  $v(z_k) \geq \frac{k-1}{q}$ , d'où  $v(a_k z_k) \geq \frac{1}{q}$  pour  $k \geq 2$ , 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  $\geq \frac{1}{q}$ , les conditions (5) sont aussi nécessaires.

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

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

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

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

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

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

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

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

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

$$F(x) = \log \zeta_x |x|_p \quad \text{pour tout } x \in \mathbb{Q}_p^*$$

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

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

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

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

(d)  $x \mapsto x \exp x$  est une isométrie de  $\mathbb{p}\mathbb{Z}_{\mathbb{p}}$ .

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

(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  $x \mapsto x^x$  est une isométrie de  $B_{1,0}$ .

(g) Soit

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

série convergente sur  $\mathbb{p}\mathbb{Z}_{\mathbb{p}}$ ; on a  $a_0 = 0$ ,  $a_1 = 1$ , et pour  $k \geq 2$ , on a

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

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

donc  $x \mapsto \sin x$  est une isométrie de  $\mathbb{p}\mathbb{Z}_{\mathbb{p}}$ , et par itération  $x \mapsto \sin^{(k)} x$ , où  $k \in \mathbb{Z}^+$ , est une isométrie de  $\mathbb{p}\mathbb{Z}_{\mathbb{p}}$ .

(h)  $x \mapsto x \cos x$  est une isométrie de  $\mathbb{p}\mathbb{Z}_{\mathbb{p}}$ .

(i) Si  $x, y \in \mathbb{p}\mathbb{Z}_{\mathbb{p}}$ , 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  $x \mapsto \operatorname{tg} x$  est une isométrie de  $\mathbb{p}\mathbb{Z}_{\mathbb{p}}$ , et par itération  $x \mapsto \operatorname{tg}^{(k)} x$ , où  $k \in \mathbb{Z}^+$ , est une isométrie de  $\mathbb{p}\mathbb{Z}_{\mathbb{p}}$ .

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

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

$$a_0 \in \mathbb{Z}_{\mathbb{p}}, \quad a_1 + a_2 \in \mathbb{Z}_{\mathbb{p}} \quad \text{et} \quad f(n+1) - f(n) = a_1 + a_2 + 2a_2 n \in \mathbb{Z}_{\mathbb{p}},$$

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

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

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

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

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

On aurait évidemment  $(N, f(h), 2) \geq \left\lfloor \frac{N}{p} \right\rfloor$ , d'où

$$\frac{1}{N} (N, f(h), 2) \geq \frac{1}{N} \left\lfloor \frac{N}{p} \right\rfloor \rightarrow \frac{1}{p} \text{ quand } N \rightarrow \infty;$$

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

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

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

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

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  $1 + p\underline{Z}_p$  ;
- (b) les suites  $n \exp pn$ ,  $n \cos pn$  sont t. b. r. sur  $\underline{Z}_p$  ;
- (c) les suites  $\sin^{(k)} pn$ ,  $\text{tg}^{(k)} pn$ , où  $k \in \underline{Z}^+$ , sont t. b. r. sur  $p\underline{Z}_p$ .

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  $\underline{Z}_p^*$ , et posons  $y_n = \log x_n$ . Choisisant  $\alpha \in p\underline{Z}_p$ ,  $k \in \underline{Z}^+$ , 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  $N \rightarrow \infty$  :

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

ce qui montre que la suite  $y_n$  est e. r. sur  $p\underline{Z}_p$ . Attribuant au besoin un sens au symbole  $\log 0$  (convention  $\log 0 \in p\underline{Z}_p$ ), ce résultat sera applicable aux suites  $x_n$  e. r. sur  $\underline{Z}_p$ . Il peut d'ailleurs être itéré, car si la suite  $\log^{(k)} x_n$ , où  $k \in \underline{Z}^+$ , est e. r. sur  $p\underline{Z}_p$ , 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  $n \geq 1$ ) que

(a) la suite  $\log^{(k)} n$ , où  $k \in \mathbb{Z}^+$ , est e. r. sur  $\mathbb{P}_{\mathbb{Z}_p}$  (convention  $\log 0 \in \mathbb{P}_{\mathbb{Z}_p}$  si  $k \geq 2$ ) ;

(b) la suite  $n|n|_p$  est e. r. sur  $\mathbb{U}_p$  (ici  $p$  quelconque) ;

(c) la suite  $n|n|_p \log n$  est e. r. sur  $\mathbb{P}_{\mathbb{Z}_p}$ .

7.4. - Des sommations classiques montrent que les suites  $\sum_{0 \leq k \leq n} \exp(\alpha k + \beta)$ ,  $\sum_{0 \leq k \leq n} \cos(\alpha k + \gamma)$ , où  $\alpha \in \mathbb{P}_{\mathbb{Z}_p}$ ,  $\beta \in \mathbb{P}_{\mathbb{Z}_p}$ ,  $\gamma \in p^{v(\alpha)} \mathbb{Z}_p$ , sont t. b. r. sur  $\mathbb{Z}_p$ .

### 8. Applications isométriques par boules maximales de $A$ dans $A$ .

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

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

(6)  $a_1 \in G$ ,  $a_k \in A$  si  $p|k$ ,  $a_k \in P$  si  $p \nmid k$  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  $k \geq 2$ ,

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

$$v(a_k z_k) \geq v(a_k) > 0 \quad \text{si } p \nmid k$$

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

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

En effet,  $g(x) \in G$  pour tout  $x \in P$ ;  $g$  n'a pas de racine dans  $\mathbb{P}_p$ , 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  $k \geq 2$ .

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

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

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

### 9. Isométries polynomiales particulières de $\underline{\underline{Z}}_p$ .

Soit  $K = \underline{\underline{Q}}_p$  et soit

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

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

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

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

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

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

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

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

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

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

$$(7) \quad f(x) = \sum_{k \in \underline{\underline{Z}}} a_k x^k \quad \text{pour tout } x \in G .$$

(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

$m \in \underline{\mathbb{Z}} - p\underline{\mathbb{Z}}$  tel que

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

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

$$f(x) - f(y) = (x - y) \left( - \sum_{k \geq 1} \frac{a_{-k} z_k}{x^k y^k} + \sum_{k \geq 1} a_k z_k \right)$$

en posant  $z_1 = 1$  et comme plus haut  $z_k = x^{k-1} + x^{k-2} y + \dots + xy^{k-2} + y^{k-1}$  pour  $k \geq 2$ , 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  $k \geq 1$  :

$$v(z_k) = 0 \text{ si } p \nmid k, \quad v(z_k) > 0 \text{ si } p \mid k.$$

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  $k \geq 1$ ; on a alors, pour  $n \neq 0$  :

$$v(u_n) = v(a_n) \text{ si } p \nmid n, \quad v(u_n) > v(a_n) \text{ si } p \mid n.$$

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

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

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

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

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

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

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  $m \in \underline{\mathbb{Z}}$

tel que

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

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

### 11. Isométries de $\mathbb{U}_p$ .

11.1. - Soit  $K = \mathbb{Q}_p$  et supposons satisfaites les conditions (8) ; alors  $f(x) \in a_m x^m + p\mathbb{Z}_p$  pour tout  $x \in \mathbb{U}_p$ . 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  $\mathbb{U}_p$ , donc  $f \in \mathfrak{I}(\mathbb{U}_p)$ . Posant

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

on a finalement :

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

$$(9) \quad a_m \in \mathbb{U}_p, \quad a_k \in p\mathbb{Z}_p \quad \text{pour } k \neq m.$$

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

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

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

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

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

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

et, puisque le premier membre est égal à  $v(x - y)$ , cela entraîne  $\min(v(m), 1) \leq 0$ , ce qui exige  $v(m) = 0$  ; finalement on a  $m \in E_p$ . Ainsi  $x \mapsto x^m$ , où  $m \in \mathbb{Z}$ , est une isométrie de  $\mathbb{U}_p$  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  $\alpha^n$ , où  $\alpha \in h + p\mathbb{Z}_p$ ,  $h = 1, \dots, p-1$ , soit t. b. r. [resp. e. r.] sur  $U_p$ , il faut et il suffit que  $\alpha^{p-1} \in 1 + p\mathbb{Z}_p$  et que  $h$  engendre multiplicativement toutes les classes résiduelles (mod  $p$ ) non nulles. La 1re condition équivaut à  $\log \alpha \in p\mathbb{Z}_p$ , c'est-à-dire encore  $\zeta_h \alpha = \exp \log \alpha \in 1 + p\mathbb{Z}_p$ , ou enfin  $\alpha \in \zeta_h^{-1} + p\mathbb{Z}_p$ , où  $\zeta_h^{-1}$  est la racine  $(p-1)$ -ième de 1 située dans  $h + p\mathbb{Z}_p$ . La 2e condition exprime que cette racine  $\zeta_h^{-1}$  est une racine primitive. Ainsi la suite  $\alpha^n$ , où  $\alpha \in U_p$ , est t. b. r. [resp. e. r.] sur  $U_p$  si et seulement si  $\alpha \in \zeta + p\mathbb{Z}_p$ , où  $\zeta$  désigne une racine  $(p-1)$ -ième primitive quelconque de 1 ( $p \neq 2$ ).

(b) Soit  $v_n$  le  $n$ -ième entier naturel non divisible par  $p$ ; les suites  $v_n^m$ ,  $v_n^{1/m}$ , 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  $\bar{K}$  de  $K$ ,  $\vec{\omega} = (\omega_0, \dots, \omega_{s-1})$  une base de  $\bar{K}$  considéré comme espace vectoriel de dimension  $s$  sur le corps  $\mathbb{Z}/(p)$  des entiers (mod  $p$ ).

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

$$n = \sum_{\ell \geq 0} c_\ell(n) p^\ell \quad \text{où } 0 \leq c_\ell(n) \leq p-1 \text{ pour tout } \ell \in \mathbb{N},$$

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  $\bar{K}$ , en posant

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

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  $k \in \mathbb{Z}^+$ , les  $ks$  premiers "chiffres" de  $n + p^{ks}$  sont respectivement égaux aux  $ks$  premiers "chiffres" de  $n$  :

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

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

$$u_{n+p^{ks}}^j \in u_n^j + p^{k/q} A \quad \text{pour } n, k, j \in \mathbb{Z}^+.$$

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

(a) On a

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

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

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

On en tire immédiatement

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

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

$$(11) \quad (p^{ks}, \alpha, \frac{k}{q})_{fou} = 1 \quad \text{pour tout } \alpha \in A, \text{ pour tout } k \in \mathbb{Z}^+.$$

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

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

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

$$(12) \quad \lim_{N \rightarrow \infty} (N, \alpha, \frac{k}{q})_{fou} = \infty \Leftrightarrow (p^{ks}, \alpha, \frac{k}{q})_{fou} \geq 1.$$

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

$$(p^{ks}, \alpha, \frac{k}{q})_{fou} \geq 1 \quad \text{pour tout } \alpha \in A, \text{ pour tout } k \in \mathbb{Z}^+$$

et cette condition équivaut évidemment à (11).

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

$$\underline{C}_k = \left\{ \sum_{0 \leq j \leq k-1} \sum_{0 \leq i \leq s-1} h_{i,j} \omega_i p^{j/q} \right\}_{h_{i,j}=0,1,\dots,p-1}.$$

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  $(u_n)_{n \in \underline{Z}^+}$  la suite associée à une base  $\bar{\omega}$  du corps des restes de  $K$  ; pour une suite polynomiale en  $u_n$  à coefficients dans  $A$ , soit  $(f(u_n))_{n \in \underline{Z}^+}$ , 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  $\alpha \in \underline{C}_k$  et pour tout  $k \in \underline{Z}^+$  :

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

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

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

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

#### BIBLIOGRAPHIE

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