Théorie des nombres/*Number Theory*

Le corps des périodes p-adiques

Pierre COLMEZ

Résumé – On démontre que $\bar{\mathbf{Q}}_p$ est dense dans l'anneau $\mathbf{B}_{\mathrm{DR}}^+$ construit par Fontaine et on en déduit une nouvelle construction de cet anneau comme complété de $\bar{\mathbf{Q}}_p$ pour une certaine topologie.

The field of p-adic periods

Abstract – *We prove that $\bar{\mathbf{Q}}_p$ is dense in the ring $\mathbf{B}_{\mathrm{DR}}^+$ constructed by Fontaine and we use this fact to give a new construction of this ring as the completion of $\bar{\mathbf{Q}}_p$ for a certain topology.*

1. RAPPELS CONCERNANT $\mathbf{B}_{\mathrm{DR}}^+$. – Rappelons brièvement la construction, due à Fontaine (*cf.* [1]), de l'anneau $\mathbf{B}_{\mathrm{DR}}^+$. Soient p un nombre premier, $\bar{\mathbf{Q}}_p$ une clôture algébrique de $\mathbf{Q}_p$, $\mathcal{O}$ l'anneau des entiers de $\bar{\mathbf{Q}}_p$, $\mathbf{Q}_p^{nr}$ l'extension maximale non ramifiée de $\mathbf{Q}_p$, $\mathbf{C}_p$ le complété p-adique de $\bar{\mathbf{Q}}_p$, $\hat{\mathcal{O}}$ son anneau d'entiers et v_p la valuation de $\mathbf{C}_p$ normalisée par $v_p(p)=1$. Soit R l'ensemble des suites $x=(x^{(n)})$, $n\in\mathbf{N}$ d'éléments de $\hat{\mathcal{O}}$ vérifiant $(x^{(n+1)})^p=x^{(n)}$. On fait de R un anneau de caractéristique p valué et complet en posant

$$v_{\mathrm{R}}(x)=v_p(x^{(0)}),$$

puis

$$x+y=s \qquad \text{avec} \qquad s^{(n)}=\lim_{m\to\infty}(x^{(n+m)}+y^{(n+m)})^{p^m}$$

et

$$xy=t \qquad \text{avec} \quad t^{(n)}=x^{(n)}y^{(n)}.$$

Soit W(R) l'anneau des vecteurs de Witt à coefficients dans R et si $x\in\mathrm{R}$, soit $[x]$ son représentant de Teichmüller dans W(R). Soit θ l'homomorphisme de W(R) dans $\hat{\mathcal{O}}$ qui à $(x_0, x_1, \ldots, x_n, \ldots)=\sum_{n=0}^{\infty} p^n[x_n^{p^{-n}}]$ associe $\sum_{n=0}^{\infty} p^n x_n^{(n)}$. Alors θ est surjectif et son noyau I_+ est un idéal principal. Notons encore θ l'homomorphisme de $\mathrm{W}(\mathrm{R})[p^{-1}]$ dans $\mathbf{C}_p$ et soit $\mathbf{B}_{\mathrm{DR}}^+=\varprojlim_n \mathrm{W}(\mathrm{R})[p^{-1}]/(\ker\theta)^n$. On peut prolonger θ par continuité à $\mathbf{B}_{\mathrm{DR}}^+$ et on note I son noyau. Alors $\mathbf{B}_{\mathrm{DR}}^+$ est un anneau de valuation discrète, d'idéal maximal I et de corps résiduel $\mathbf{C}_p$. De plus, si pour k, $n\in\mathbf{N}$, on pose $\mathrm{U}_{n,k}=p^k\mathrm{W}(\mathrm{R})+\mathrm{I}^n$, alors $\mathbf{B}_{\mathrm{DR}}^+$ est aussi le séparé complété de $\mathrm{W}(\mathrm{R})[p^{-1}]$ pour la topologie obtenue en prenant comme système fondamental de voisinages les $x+\mathrm{U}_{n,k}$, pour $x\in\mathrm{W}(\mathrm{R})[p^{-1}]$ et n, $k\in\mathbf{N}$. D'après le théorème de structure des anneaux de valuation discrète complets en égale caractéristique, le morphisme θ de $\mathbf{B}_{\mathrm{DR}}^+$ sur $\mathbf{C}_p$ possède une section (non canonique), mais cette section ne peut être choisie ni continue, ni même compatible à l'action de $\mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$. Par contre, $\bar{\mathbf{Q}}_p$ s'identifie canoniquement à la clôture intégrale de $\mathbf{Q}_p$ dans $\mathbf{B}_{\mathrm{DR}}^+$.

Si $x\in\mathbf{B}_{\mathrm{DR}}^+$, soit $s_n(x)=\sup\{k\in\mathbf{Z}\,|\,x\in p^k\mathrm{W}(\mathrm{R})+\mathrm{I}^{n+1}\}$. On appelle écriture minimale de x toute série $\sum_{n=0}^{\infty} x_n$ dont la somme est x et telle que $x_n\in p^{s_n(x)}\mathrm{I}_+^n$ (notons que cette condition implique la convergence de la série). Si A est un $\mathbf{Z}_p[\mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)]$-module, on

Note présentée par Jean-Marc FONTAINE.

0764-4442/90/03100321 $ 2.00 © Académie des Sciences

Source gallica.bnf.fr / Archives de l'Académie des sciences

note $A(n)$ le module tordu par la puissance n-ième du caractère cyclotomique. Soient

$$\mathbf{a}^n = \left\{ x \in \bar{\mathbf{Q}}_p \,|\, v_p(x) \geqq -\frac{n}{p-1} \right\} \quad \text{et} \quad m \in \mathbf{Z};$$

alors, $I^n/(p^m I_+^n + I^{n+1})$ s'identifie à $(\bar{\mathbf{Q}}_p/p^m \mathbf{a}^n)(n)$ (*cf.* [2]). Si $\sum_{n=0}^{s} x_n$ est une écriture minimale de x et si $m \leqq s_{n-1}(x)$, alors l'image de x_n dans $(\bar{\mathbf{Q}}_p/p^m \mathbf{a}^n)(n)$ ne dépend que de x. Pour $n \in \mathbf{N}$, on pose $\mathcal{O}_n = \bar{\mathbf{Q}}_p \cap (W(R) + I^{n+1})$; on a $\mathcal{O}_0 = \mathcal{O}$. Si $n \geqq 1$, si $x \in \mathcal{O}_{n-1}$ et si $\sum_{n=0}^{s} x_n$ est une écriture minimale de x, l'image $\partial_n(x)$ de x_n dans $(\bar{\mathbf{Q}}_p/\mathbf{a}^n)(n)$ ne dépend que de x et ∂_n est une dérivation sur $\mathcal{O}_{n-1}$ dont le noyau est $\mathcal{O}_n$.

2. GÉNÉRALITÉS SUR LES ANNEAUX DE SÉRIES FORMELLES. — Soient K un corps commutatif de caractéristique 0, $P \in K[X]$ un polynôme irréductible, $K[X]_P$ le complété du localisé de $K[X]$ en l'idéal engendré par P, $L = K[X]/P$ le corps résiduel de cet anneau de valuation discrète complet et π l'image de X dans L. Alors $Y = X - \pi$ est une uniformisante de $K[X]_P$ qui s'identifie donc à $L[[Y]]$. Notons que si $D = d/dP(X)$ est l'unique dérivation de $K[X]_P$ de noyau L vérifiant $D(P) = 1$, si $y \in L$ et si $Q \in K[X]$ vérifie $Q(\pi) = y$, alors l'application $y \to F_y = \sum_{n=0}^{\infty} (-1)^n/n!\, D^n(Q) P^n$ est la section de la projection de $K[X]_P$ sur L. En effet, $D(F_y) = 0$, ce qui implique $F_y \in L$ et de plus, $F_y(\pi) = y$.

Tout élément de $K[X]_P$ s'écrit de manière unique $\sum_{n=0}^{s} Q_n P^n$ avec $Q_n \in K[X]$ et $\deg(Q_n) < \deg(P)$. Une telle écriture sera dite minimale. Si $y \in L$, on note $\sum_{n=0}^{\infty} \delta_P^n(y) P^n$ son écriture minimale.

Supposons dorénavant que K est un corps local de caractéristique 0, que L est une extension totalement ramifiée de K et que $P \in K[X]$ est le polynôme minimal d'une uniformisante π de L. Soit v la valuation de L normalisée par $v(K^*) = \mathbf{Z}$. Si $Q = \sum_{i=0}^{n} a_i X^i \in K[X]$, soit $v(Q) = \inf_{0 \leqq i \leqq n} v(a_i)$. Si $x \in \mathbf{R}$, on note $E(x)$ sa partie entière. Alors si $\deg(Q) < \deg(P)$, on a $v(Q) = E(v(Q(\pi)))$.

LEMME 1. — *Soient* A, $B \in K[X]$ *satisfaisant* $\deg(A) < \deg(P)$, $\deg(B) < \deg(P)$ *et* $(A, P) = 1$. *Soient* Q *et* R *les éléments de* $K[X]$ *caractérisés par* $\deg(Q) < \deg(P)$, $\deg(R) < \deg(A)$ *et* $B = AQ + PR$. *Alors* $v(Q) \geqq v(B) - v(A) - 1$ *et* $v(R) \geqq v(B) - 1$.

Démonstration. — On a

$$v(Q) = E(v(Q(\pi)) = E(v(B(\pi)) - v(A(\pi))) \geqq E(v(B(\pi))) + E(-v(A(\pi))) \geqq v(B) - v(A) - 1,$$

ce qui donne le résultat concernant $v(Q)$. Celui concernant $v(R)$ s'obtient en remarquant que $v(B - AQ) \geqq v(B) - 1$ et que la division par P n'introduit pas de dénominateurs car P est unitaire et $v(P) \geqq 0$.

COROLLAIRE. — *Soit* $\sum_{n=0}^{\infty} Q_n P^n$ *l'écriture minimale de* $A^{-1} B$. *Alors*

$$v(Q_n) \geqq v(B) - v(A) - n - 1.$$

LEMME 2. — *Soient* $Q \in K[X]$ *avec* $\deg(Q) < \deg(P)$, $k \geq 1$ *et* $\sum_{i=0}^{\infty} F_{i,k} P^i$ *l'écriture minimale de* $d^k Q/(dP(X))^k$. *Alors on a l'inégalité* $v(F_{i,k}) \geq v(Q') - kv(P') - i - k$.

Démonstration. — Si $k=1$, c'est une conséquence immédiate du corollaire précédent. Supposons l'inégalité vraie pour k; on peut alors écrire :

$$\frac{d^{k+1}Q}{(dP(X))^{k+1}} = \frac{1}{P'}\frac{d}{dX}\left(\frac{d^kQ}{(dP(X))^k}\right) = \sum_{i=0}^{\infty}\left(\frac{1}{P'}F'_{i,k}P^i + iF_{i,k}P^{i-1}\right).$$

Soit $\sum_{j=0}^{\infty} H_{i,j,k} P^j$ l'écriture minimale de $F'_{i,k}/P'$; alors on a

$$F_{i,k+1} = (i+1)F_{i+1,k} + \sum_{j_1+j_2=i} H_{j_1,j_2,k}$$

et l'inégalité cherchée est une conséquence des inégalités

$$v((i+1)F_{i+1,k}) \geq v(F_{i+1,k}) \geq v(Q') - kv(P') - (i+k+1)$$

et

$$v(H_{j_1,j_2,k}) \geq v(F'_{j_1,k}) - v(P') - j_2 - 1 \geq v(F_{j_1,k}) - v(P') - j_2 - 1$$
$$\geq v(Q') - (k+1)v(P') - (j_1+j_2+k+1).$$

COROLLAIRE. — *Si* $r \in \mathbf{Z}$, *soit* $J[r]$ *l'idéal fractionnaire de* L *des éléments de valuation supérieure ou égale à* r. *Alors on a, pour* $n \geq 1$,

(i) $$v(\delta_P^n(y)) \geq v(Q') - n(v(P')+1) - v(n!);$$

(ii) $$\delta_P^n(y)(\pi) \equiv \frac{(-1)^n}{n!}\frac{d^nQ}{(dP(X))^n}(\pi) \mod J[v(Q') - (n-1)v(P') - n - v((n-1)!))].$$

Démonstration. — On a $\delta_P^n(y) = \sum_{k=1}^{n} (-1)^k/k!\, F_{n-k,k}$ et $F_{0,n}(\pi) = d^nQ/(dP(X))^n(\pi)$ et on conclut en utilisant les majorations obtenues au lemme précédent.

3. $\bar{\mathbf{Q}}_p$ COMME SOUS-ANNEAU DE $\mathbf{B}_{DR}^+$. — Nous allons appliquer les résultats précédents à $K = \mathbf{Q}_p^{nr}$ et nous noterons v_p au lieu de v la valuation de $\bar{\mathbf{Q}}_p$ normalisée par $v_p(p) = 1$. Soient $y \in \bar{\mathbf{Q}}_p$, $L \neq \mathbf{Q}_p^{nr}$ une extension finie de $\mathbf{Q}_p^{nr}$ contenant y, π une uniformisante de L et P le polynôme minimal de π sur $\mathbf{Q}_p^{nr}$.

LEMME 3. — *Si* $\tilde{\pi} \in W(R)$ *est tel que* $\theta(\tilde{\pi}) = \pi$, *alors* $P(\tilde{\pi})$ *est un générateur de* I_+.

Démonstration. — Soit $u \in R$ tel que $u^{(0)} = \pi$. On a $\tilde{\pi} = [u] + \alpha$ avec $\alpha \in I_+$ et si $e = [L : \mathbf{Q}_p^{nr}]$, alors $P([u]) \equiv [u^e] \bmod pW(R)$. Comme $v_R(u^e) = 1$ et $P([u]) \in I_+$, ceci implique ([1], prop. 2.4) que $P([u])$ est un générateur de I_+. On peut donc écrire $\alpha = \beta P([u])$ avec $\beta \in W(R)$ et on a $P(\tilde{\pi}) = P([u])(1 + P'([u])\beta) \bmod I_+^2$. Pour conclure, il suffit de remarquer que $\theta(1 + P'([u])\beta) = 1 + P'(\pi)\theta(\beta)$ est une unité p-adique car L est totalement ramifiée et donc $1 + P'([u])\beta \in W(R)^*$.

PROPOSITION 4. — $\sum_{n=0}^{\infty} \delta_P^n(y)(\tilde{\pi})P(\tilde{\pi})^n$ *est une écriture minimale de* y.

Démonstration. — C'est une écriture car $P(\tilde{\pi}) \in I - I^2$ implique que le morphisme $F \to F(\tilde{\pi})$ est une injection de $\mathbf{Q}_p^{nr}[X]_P$ dans $\mathbf{B}_{DR}^+$ et donc que $F_y(\tilde{\pi}) = y$. Elle est minimale car $P(\tilde{\pi})$ est un générateur de I_+ et $\deg(\delta_P^n(y)) < \deg(P)$.

Remarque 1. — On peut définir $s_n(y)$ et $\mathcal{C}_n$ sans recours à $\mathbf{B}_{\mathrm{DR}}^+$: en effet, $s_n(y)$ n'est rien d'autre que le minimum de $v_p(\delta_{\mathrm{P}}^i(y))$ pour $0 \leqq i \leqq n$ et $\mathcal{C}_n$ est l'ensemble des $x \in \bar{\mathbf{Q}}_p$ vérifiant $s_n(x) \geqq 0$.

Remarque 2. — Si $y \in \mathcal{C}_{n-1}$, l'image de $\delta_{\mathrm{P}}^n(y)(\pi)\,\mathrm{P}(\tilde{\pi})^n$ dans $(\bar{\mathbf{Q}}_p/\mathbf{a}^n)(n)$ est égale à $\hat{c}_n(y)$ et donc ne dépend ni du choix de L, ni du choix de π ni de celui de $\tilde{\pi}$.

Soit $\mathcal{U} = \{\alpha \in \mathcal{C} \mid \alpha$ est une uniformisante de $\mathbf{Q}_p^{nr}(\alpha)\}$. Si $\alpha \in \mathcal{U}$, soit $\mathrm{R}_\alpha = \{x \in \mathrm{R} \mid x^{(0)} = \alpha\}$.

Lemme 5. — *Soient* $\alpha \in \mathcal{U}$ *et* $x = (x^{(n)}) \in \mathrm{R}_\alpha$. *Soient* P *le polynôme minimal de* α *sur* $\mathbf{Q}_p^{nr}$, $k \in \mathbf{N}$, $l(k)$ *le plus grand entier* l *tel que* $p^l \leqq k$ *et* $m \in \mathbf{N}$ *satisfaisant*

$$m \geqq k(n + v_p(\mathrm{P}') + 2) + v_p(k!) + 1.$$

Soit $x_{n,m} \in \mathcal{C}$ *vérifiant* $(x_{n,m})^{p^m} + p x_{n,m} = x^{(n)}$. *Alors*

$$(x^{(n)} - p x_{n,m})^{p^n} = (x_{n,m})^{p^{n+m}} \text{ est congru à } [x] \bmod p^{n-l(k)}\mathrm{W}(\mathrm{R}) + \mathrm{I}^{k+1}.$$

Démonstration. — Soit $\mathrm{S}(\mathrm{X}) = \mathrm{X}^{p^m} + p\mathrm{X}$. Alors $x_{n,m}$ est une uniformisante de $\mathbf{Q}_p^{nr}(x_{n,m})$ et son polynôme minimal $\mathrm{P}_{n,m}$ sur $\mathbf{Q}_p^{nr}$ est égal à $\mathrm{P}(\mathrm{S}(\mathrm{X})^{p^n})$. On a $\mathrm{P}'_{n,m} = p^n \mathrm{S}' \mathrm{S}^{p^n-1} \mathrm{P}'(\mathrm{S}^{p^n})$ et donc $v_p(\mathrm{P}'_{n,m}) = n + 1 + v_p(\mathrm{P}')$. On a de plus $x^{(n)} - p x_{n,m} = \mathrm{Q}(x_{n,m})$ avec $\mathrm{Q}(\mathrm{X}) = \mathrm{X}^{p^m}$. On déduit alors du (i) du corollaire du lemme 2 :

$$v_p(\delta^i_{\mathrm{P}_{n,m}}(x^{(n)} - p x_{n,m})) \geqq v_p(\mathrm{Q}') - i(v_p(\mathrm{P}'_{n,m}) + 1) - v_p(i!) \geqq m - i(n + v_p(\mathrm{P}') + 2) - v_p(i!) \geqq 1,$$

si $i \leqq k$. Soit $\tilde{x}_{n,m} \in \mathrm{W}(\mathrm{R})$ vérifiant $\theta(\tilde{x}_{n,m}) = x_{n,m}$. La proposition 4 alliée à l'inégalité précédente implique $x^{(n)} - p x_{n,m} \equiv \mathrm{Q}(\tilde{x}_{n,m}) \bmod p\,\mathrm{W}(\mathrm{R}) + \mathrm{I}^{k+1}$, et comme

$$\mathrm{Q}(\tilde{x}_{n,m}) - [x]^{p^{-n}} + p\tilde{x}_{n,m} \in \mathrm{I}_+,$$

on obtient finalement

$$x^{(n)} - p x_{n,m} \equiv [x]^{p^{-n}} \bmod p\,\mathrm{W}(\mathrm{R}) + \mathrm{I}_+ + \mathrm{I}^{k+1}.$$

Le lemme s'obtient en élevant cette congruence à la puissance p^n.

Corollaire. — *Si* $\alpha \in \mathcal{U}$ *et* $x \in \mathrm{R}_\alpha$, *alors* $[x]$ *est dans l'adhérence de* $\bar{\mathbf{Q}}_p$ *dans* $\mathbf{B}_{\mathrm{DR}}^+$.

Démonstration. — Si $\varphi(n)$ est une suite d'entiers vérifiant $\lim_{n \to \infty} \varphi(n)/n = \infty$, la suite $(x^{(n)} - p x_{n,\varphi(n)})^{p^n}$ tend vers $[x]$ dans $\mathbf{B}_{\mathrm{DR}}^+$.

On obtient alors comme corollaire le théorème :

Théorème 6. — $\bar{\mathbf{Q}}_p$ *est dense dans* $\mathbf{B}_{\mathrm{DR}}^+$.

Démonstration. — Soient $\alpha \in \mathcal{U}$ et $u \in \mathrm{R}_\alpha$. D'après le corollaire précédent, l'adhérence de $\bar{\mathbf{Q}}_p$ dans $\mathbf{B}_{\mathrm{DR}}^+$ contient $[u] - \alpha$ qui est un générateur de I. D'autre part $\bar{\mathbf{Q}}_p$ est dense dans $\mathrm{B}_{\mathrm{DR}}^+/\mathrm{I} \cong \mathbf{C}_p$, ce qui permet de conclure.

Corollaire. — $\mathbf{B}_{\mathrm{DR}}^+ = \varprojlim_n (\mathbf{Q}_p \otimes \varprojlim_k (\mathcal{C}_n/p^k \mathcal{C}_n))$, *autrement dit* $\mathbf{B}_{\mathrm{DR}}^+$ *est le complété de* $\bar{\mathbf{Q}}_p$ *pour la topologie définie par le système fondamental de voisinages* $\mathrm{V}_{n,k}$ *de* 0, *où* $\mathrm{V}_{n,k} = p^k \mathcal{C}_n$.

Note remise le 26 décembre 1989, acceptée le 4 janvier 1990.

Références bibliographiques

[1] J.-M. Fontaine, Sur certains types de représentations p-adiques du groupe de Galois d'un corps local; construction d'un anneau de Barsotti-Tate, *Ann. of Math.*, 115, 1982, p. 529-577.

[2] J.-M. Fontaine, Formes différentielles et modules de Tate des variétés abéliennes sur les corps locaux, *Inv. Math.*, 65, 1982, p. 379-409.

C.N.R.S., Laboratoire de Mathématiques de l'École Normale Supérieure, U.A. n° 762, 45, rue d'Ulm, 75005 Paris.