Théorie des nombres/ *number theory*

Sur un résultat de S. Sen

Pierre Colmez

résumé: Nous construisons un anneau permettant de passer d'une représentation p-adique à son module de Sen

On a result of S. Sen

abstract: We construct a ring giving a bridge between a p-adic Galois representation and its Sen-module

Soient p un nombre premier et $\mathcal{G}$ le groupe de Galois de $\overline{\mathbf{Q}}_p$ sur $\mathbf{Q}_p$. Si $n \in \mathbf{N}$, soit $F_n = \mathbf{Q}_p(\mu_{p^n}) \subset \overline{\mathbf{Q}}_p$ et $F_\infty = \cup F_n$. Si $K \subset \overline{\mathbf{Q}}_p$ est une extension finie de $\mathbf{Q}_p$, soit $\mathcal{G}_K$ le sous-groupe de $\mathcal{G}$ fixant K et si $n \in \mathbf{N} \cup \{\infty\}$, soit $K_n = KF_n \subset \overline{\mathbf{Q}}_p$. Soient $\chi : \mathcal{G} \to \mathbf{Z}_p^*$ le caractère cyclotomique, $\tau : \mathcal{G} \to \mathbf{Z}_p$ le caractère (additif) de $\mathcal{G}$ défini par $\tau(g) = \log_p \chi(g)$ et $\mathcal{H}_K \subset \mathcal{G}_K$ le noyau de χ.

Si K est une extension finie de $\mathbf{Q}_p$, un $\mathbf{Q}_p$-espace vectoriel V de dimension finie sera appelé représentation p-adique de $\mathcal{G}_K$, si on a un morphisme continu de $\mathcal{G}_K$ dans $Aut(V)$. Le théorème suivant est dû à Sen [Se80 Th.2 et Th.4].

Théorème 1: *Soient $K \subset \overline{\mathbf{Q}}_p$ une extension finie de $\mathbf{Q}_p$ et V une représentation p-adique de $\mathcal{G}_K$ de dimension d. Il existe une base $e_1, \ldots, e_d$ de $\mathbf{C}_p \otimes V$, un entier $n \geq 0$ et une application linéaire φ_V dont la matrice dans la base $e_1, \ldots, e_d$ est à coefficients dans K_n tels que, si $g \in \mathcal{G}_{K_n}$, alors $g(e_i) = \exp(\tau(g)\varphi_V)e_i$.*

Notre but est de réinterpréter ce résultat à la Fontaine (cf. [Fo82]). Notons $D_{\mathrm{Sen}}(V)$ le sous-K_∞-espace vectoriel de $\mathbf{C}_p \otimes V$ engendré par les e_i et muni de l'opérateur φ_V. Nous allons construire un anneau $\mathbf{B}_{\mathrm{Sen}}$ muni d'un germe d'action de $\mathcal{G}$ et d'un opérateur Θ commutant à l'action de $\mathcal{G}$ permettant de passer directement de V à $D_{\mathrm{Sen}}(V)$.

Un $\mathbf{Q}_p$-espace vectoriel topologique sera dit muni d'une action de $\mathcal{G}_{K_\infty}$, s'il existe sur M une filtration croissante par des sous-$\mathbf{Q}_p$-espaces vectoriels M_n fermés telle que chaque M_n soit muni d'une action continue de $\mathcal{G}_{K_n}$ et telle que $M = \cup_{n\geq 0} M_n$. Notons que cette condition est plus forte que de demander que M soit muni d'une action continue de $\mathcal{H}_K$. On notera alors $M^{\mathcal{G}_{K_\infty}} = \cup_{n\geq 0} M_n^{\mathcal{G}_{K_n}}$.

En tant qu'anneau, $\mathbf{B}_{\mathrm{Sen}}$ s'identifie à l'anneau $\mathbf{C}_p\{\{u\}\}$ des séries formelles à coefficients dans $\mathbf{C}_p$ dont le rayon de convergence est non-nul. On munit $\mathbf{B}_{\mathrm{Sen}}$ d'une filtration croissante par les $\mathbf{B}_{\mathrm{Sen}}^n$, pour $n \in \mathbf{N}$, en identifiant $\mathbf{B}_{\mathrm{Sen}}^n$ au sous-anneau des série dont le rayon de convergence est supérieur ou égal à $p^{-\sup(1,n)}$ (si $p = 2$, il faut remplacer $\sup(1, n)$ par $\sup(2, n)$). On note Θ l'opérateur $\mathbf{C}_p$-linéaire de $\mathbf{B}_{\mathrm{Sen}}$ induit par $-\frac{d}{du}$ et on fait agir $\mathcal{G}$ sur u par $g(u) = u + \tau(g)$, ce qui fait de u un analogue p-adique de $\log 2i\pi$. Comme on a $\tau(g) \in p^{\sup(1,n)}\mathbf{Z}_p$ si $g \in \mathcal{G}_{K_n}$, la série $\sum_{i=0}^{+\infty} g(a_i)(u + \tau(g))^i$ est convergente si $\sum_{i=0}^{+\infty} a_i u^i \in \mathbf{B}_{\mathrm{Sen}}^n$ et $g \in \mathcal{G}_{F_n}$, ce qui munit $\mathbf{B}_{\mathrm{Sen}}^n$ d'une action continue de $\mathcal{G}_{K_n}$ et $\mathbf{B}_{\mathrm{Sen}}$ d'une action de $\mathcal{G}_{K_\infty}$, qui commute de manière évidente à l'action de Θ.

Théorème 2: *(i)* $(\mathbf{B}_{\mathrm{Sen}})^{\mathcal{G}_{K_\infty}} = K_\infty$.

(ii) Si V est une représentation p-adique de $\mathcal{G}_K$, alors on a $D_{\mathrm{Sen}}(V) \cong (\mathbf{B}_{\mathrm{Sen}} \otimes V)^{\mathcal{G}_{K_\infty}}$, l'opérateur φ_V étant induit par l'action de Θ sur $\mathbf{B}_{\mathrm{Sen}}$.

Démonstration: (i) Soit $x = \sum_{i=0}^{+\infty} a_i u^i$ un élément de $\mathbf{B}^n_{\mathrm{Sen}}$ fixe par l'action de $\mathcal{G}_{K_n}$. Comme u est invariant par $\mathcal{H}_K$, les a_i doivent l'être aussi; et donc si on note $\hat{K}_\infty$ l'adhérence de K_∞ dans $\mathbf{C}_p$, on doit avoir $a_i \in \hat{K}_\infty$ pour tout $i \in \mathbf{N}$. Maintenant, si l'on identifie les coefficients de u^i dans l'équation $g^{-1}(x) = x$, on obtient:

$$a_i = \sum_{k \geq i} g^{-1}(a_k) \binom{k}{i} (-\tau(g))^{k-i},$$

ou encore, appliquant g aux deux membres,

$$g(a_i) = \sum_{k \geq i} a_k \binom{k}{i} (-\tau(g))^{k-i}. \tag{1}$$

Soient $m \geq n+1$, $a \in K_\infty$ et $m' \geq m$ tel que $a \in K_{m'}$. On vérifie facilement que $p^{m-m'} Tr_{K_{m'}/K_m}(a)$ ne dépend pas du choix de m' et on note Tr_m l'application linéaire de K_∞ sur K_m ainsi définie. On vérifie facilement que Tr_m s'étend par continuité à $\hat{K}_\infty$, que si $a \in \hat{K}_\infty$, alors a est la limite de $Tr_m(a)$ quand m tend vers l'infini et que, si $g \in \mathcal{G}_{K_n}$, alors $Tr_m(g(a)) = g(Tr_m(a))$. Appliquant alors Tr_m à l'identité (1), on obtient

$$g(Tr_m(a_i)) = \sum_{k \geq i} Tr_m(a_k) \binom{k}{i} (-\tau(g))^{k-i}.$$

Le premier membre de cette équation est une fonction localement constante de g tandis que le second est analytique; on en déduit que les deux membres sont des fonctions constantes de g et donc que $Tr_m(a_i) = 0$ pour tout $m \geq n$ et tout $i \geq 1$. Laissant tendre alors m vers $+\infty$, on en tire $a_i = 0$ si $i \geq 1$, c'est à dire $x \in \hat{K}_\infty$. Le (i) s'en déduit aisément.

(ii) Soit $e_1, \ldots, e_d$ la base de $\mathbf{C}_p \otimes V$ fournie par le théorème de Sen et soit $f_i = \exp(-u\varphi_V)e_i \in \mathbf{B}_{\mathrm{Sen}} \otimes V$. On vérifie facilement que f_i est fixe par $\mathcal{G}_{K_\infty}$ et donc que $(\mathbf{B}_{\mathrm{Sen}} \otimes V)^{\mathcal{G}_{K_\infty}}$ est de dimension au moins d. D'autre part, le (i) du théorème permet de démontrer l'autre inégalité, ce qui implique que l'application K_∞-linéaire ι envoyant e_i sur f_i est un isomorphisme de $D_{\mathrm{Sen}}(V)$ sur $(\mathbf{B}_{\mathrm{Sen}} \otimes V)^{\mathcal{G}_{K_\infty}}$. De plus, on a $\Theta(f_i) = \varphi_V(f_i)$ et donc par linéarité, on voit que si $x \in D_{\mathrm{Sen}}(V)$, alors $\Theta(\iota(x)) = \iota(\varphi_V(x))$, ce qui permet de terminer la démonstration.

Remarque 1: Si on appelle périodes de la représentation V les coefficients de la matrice de passage de V à $D_{\mathrm{Sen}}(V)$, on peut réinterpréter le théorème en disant que les périodes de toutes les représentations p-adiques vivent dans $\mathbf{B}_{\mathrm{Sen}}$. Une question naturelle est alors de se demander si les périodes varient de manière continue en fonction de la représentation (cf. Th.3).

Remarque 2: Soit $\omega : \mathbf{Z}_p^* \to \mu_{p-1} \subset \mathbf{Z}_p^*$ le caractère de Teichmüller envoyant x sur la racine $p-1$-ième de l'unité congrue à x modulo p. Notons encore ω le caractère d'ordre fini de $\mathcal{G}$ donné par la formule $\omega(g) = \omega(\chi(g))$. Si $p \geq 3$ (resp. $p = 2$), soit α_p une solution de l'équation $\alpha_p^{p-1} = -p$ (resp. $\alpha_2^2 = -4$). Soit $t_p = \alpha_p u \in \mathbf{B}_{\mathrm{Sen}}$; comme on a $\chi(g) = \omega(g)\exp(\tau(g))$ si $g \in \mathcal{G}$ et que $\mathcal{G}$ agit sur α_p par $g(\alpha_p) = \omega(g)\alpha_p$, on voit que $\mathcal{G}$ agit sur t_p par multiplication par le caractère cyclotomique et donc que t_p est un analogue p-adique de $2i\pi$. En particulier, $\mathbf{B}_{HT}$ s'injecte dans $\mathbf{B}_{\mathrm{Sen}}$. Notons que la formule donnée pour $t_p \in \mathbf{B}_{\mathrm{Sen}}$ est compatible avec la formule $v_p(t_p) = \frac{1}{p-1}$ valable dans $\mathbf{B}_{DR}$ (moralement, une exponentielle est une unité et a une valuation nulle).

Remarque 3: On obtiendrait les mêmes conclusions que celles du théorème 2 en remplaçant $\mathbf{B}_{\mathrm{Sen}}$ par son sous-anneau engendré par $\mathbf{C}_p, u$ et les $\exp(\alpha u)$, où α décrit $\overline{\mathbf{Q}}_p$. L'inconvénient est que cet anneau est très loin d'être complet. On peut remédier à cet inconvénient en prenant une solution intermédiaire. Notons $\mathbf{B}_{\mathrm{ult}}$ le sous-anneau de $\mathbf{B}_{\mathrm{Sen}}$ engendré par $\mathbf{B}^0_{\mathrm{Sen}}$ et par les $\exp(\alpha u)$, où α décrit $\overline{\mathbf{Q}}_p$. Comme $\exp(\alpha u)$ est algébrique sur $\mathbf{B}^0_{\mathrm{Sen}}$ (on a $(\exp(\alpha u))^{p^n} = \exp(p^n\alpha u) \in \mathbf{B}^0_{\mathrm{Sen}}$ si n est assez grand) et que $\mathbf{B}^0_{\mathrm{Sen}}$ est muni d'une action continue de $\mathcal{G}$, on peut munir $\mathbf{B}_{\mathrm{ult}}$ d'une action d'un groupe $\tilde{\mathcal{G}}$ extension de $\mathcal{G}$ par $Gal(\mathbf{B}_{\mathrm{ult}}/\mathbf{B}^0_{\mathrm{Sen}})$. Mais, le groupe $\tilde{\mathcal{G}}$ n'est pas un produit semi-direct et on ne peut donc pas étendre l'action de $\mathcal{G}$ à $\mathbf{B}_{\mathrm{ult}}$ tout entier.

Soit S un espace topologique. Une famille continue (indexée par S) de représentations p-adiques de $\mathcal{G}_K$ est par définition une application continue (pour la topologie produit) $\rho : S \times \mathcal{G}_K \to Aut(V)$, où V est un $\mathbf{Q}_p$ espace vectoriel de dimension finie, telle que pour tout $s \in S$ l'application $g \to \rho_s(g)$ soit un morphisme de groupe de $\mathcal{G}_K$ dans $Aut(V)$.

Théorème 3: *Soit ρ_s une famille continue de représentations p-adiques de $\mathcal{G}_K$ et $s_0 \in S$. Il existe un voisinage U de s_0 et une application continue $s \to \Omega_s$ de U dans $Aut(\mathbf{B}_{\mathrm{Sen}} \otimes V)$ telle que, si $x \in V$, alors $\Omega_s(x)$ est stable par $\mathcal{G}_{K_\infty}$. En d'autres termes, les périodes des représentations p-adiques dépendent continuement de la représentation.*

Démonstration: La continuité de l'application $(s, g) \to \rho_s(g)$ implique l'existence d'un sous-groupe d'indice fini $\mathcal{H}^0$ de $\mathcal{H}_K$ et d'un voisinage U_1 de s_0 tels que l'on ait $\rho_s(g) \equiv 1 \bmod p^2$. Si on regarde de plus près la démonstration du lemme 1 de [Se80], on s'aperçoit qu'elle ne fait intervenir que des opérations qui dépendent continuement de s. On en déduit l'existence d'une application continue $s \to B_s$ de U_1 dans $Aut(\mathbf{C}_p \otimes V)$ telle que si $x \in V$, alors $B_s(x)$ est stable par $\mathcal{H}_K$. La même remarque appliquée à la démonstration du lemme 3 de [Se80] permet de montrer l'existence d'un ouvert U_2, d'un entier n et d'une application continue $s \to C_s$ de U_2 dans $Aut((\mathbf{C}_p \otimes V)^{\mathcal{H}_K})$ tels qu'un générateur γ de $\mathcal{G}_{K_n}/\mathcal{H}_K$ agit sur $C_s B_s(V)$ par multiplication par une matrice Φ_s à coefficients dans K_n (et qui dépend de manière continue de s car ρ_s, C_s et B_s dépendent continuement de s). Quite à augmenter n, on peut supposer que Φ_s est congrue à 1 mod p et alors $\log_p \Phi_s$ dépend continuement de s. Si on pose $\Omega_s = \exp(-u\tau(\gamma)^{-1}\log_p \Phi_s)C_s B_s$, il existe $m \geq n$ tel que Ω_s soit élément de $Aut(\mathbf{B}^m_{\mathrm{Sen}} \otimes V)$ et si $x \in V$, alors $\Omega_s(x)$ est fixe par $\mathcal{G}_{K_m}$, ce qui nous dit que Ω_s est la matrice des périodes de ρ_s et permet de terminer la démonstration.

Bibliographie

[Fo82] 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, p.529-577,

1982
[Se80] S. Sen: Continuous Cohomology and p-Adic Galois Representations, Inv. Math. 62, p.89-116, 1980

P. Colmez, C.N.R.S.,
Département de Mathématiques et Informatique,
École Normale Supérieure, 45 rue d'Ulm, 75005 Paris