Bull. Soc. math. France
133 (4), 2005, p. 601–618

REPRÉSENTATIONS DE DE RHAM ET NORMES UNIVERSELLES

PAR LAURENT BERGER

RÉSUMÉ. — On calcule le module des normes universelles pour une représentation p-adique de de Rham. Le calcul utilise la théorie des (φ, Γ)-modules (la formule de réciprocité de Cherbonnier-Colmez) et l'équation différentielle associée à une représentation de de Rham.

ABSTRACT (*De Rham representations and universal norms*). — We compute the module of universal norms for a de Rham p-adic representation. The computation uses the theory of (φ, Γ)-modules (Cherbonnier-Colmez's reciprocity formula) and the differential equation attached to a de Rham representation.

Table des matières

Texte reçu le 23 janvier 2004, accepté le 5 avril 2004.

LAURENT BERGER, IHES, Le Bois-Marie, 35 route de Chartres, 91440 Bures-sur-Yvette, France • *E-mail :* `laurent.berger@ihes.fr` • *Url :* `www.ihes.fr/~lberger`

Classification mathématique par sujets (2000). — 11F80, 11R23, 11S25, 12H25, 14F30.
Mots clefs. — Représentations p-adiques, normes universelles, théorie d'Iwasawa.

Introduction

Dans tout cet article, p est un nombre premier, k est un corps parfait de caractéristique p, et K est une extension finie du corps des fractions F de l'anneau des vecteurs de Witt sur k. On se fixe une clôture algébrique $\overline{K}$ de K, et on pose $G_K = \mathrm{Gal}(\overline{K}/K)$. Rappelons qu'en utilisant l'anneau de périodes p-adiques $\mathbf{B}_{\mathrm{dR}}$, Fontaine a défini la notion de représentation de *de Rham* de G_K. Si V est une telle représentation et si L est une extension finie de K, on définit $H^1_g(L,V)$ comme étant l'ensemble des classes de cohomologie qui déterminent une extension $0 \to V \to E \to \mathbb{Q}_p \to 0$ de représentations de G_L telle que E est une représentation de de Rham de G_L.

On écrit $\mu_{p^n} \subset \overline{K}$ pour désigner l'ensemble des racines p^n-ièmes de l'unité et on définit $K_n = K(\mu_{p^n})$ ainsi que $K_\infty = \bigcup_{n=0}^{+\infty} K_n$. On pose $H_K = \mathrm{Gal}(\overline{K}/K_\infty)$ et $\Gamma_K = \mathrm{Gal}(K_\infty/K)$. L'algèbre d'Iwasawa est l'algèbre de groupe complétée $\Lambda_K = \mathbb{Z}_p[[\Gamma_K]]$. La cohomologie d'Iwasawa de V est définie par

$$H^1_{\mathrm{Iw}}(K,V) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^1_{\mathrm{Iw}}(K,T)$$

où T est un réseau de V stable par G_K et $H^1_{\mathrm{Iw}}(K,T) = \varprojlim_n H^1(K_n,T)$ est la limite projective pour les applications « corestriction » ce qui fait de $H^1_{\mathrm{Iw}}(K,V)$ un $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \Lambda_K$-module. Par construction, on a des applications $\mathrm{pr}_{K_n,V} : H^1_{\mathrm{Iw}}(K,V) \to H^1(K_n,V)$ et l'objet de cet article est l'étude du module $H^1_{\mathrm{Iw}}(K,V)_g$ des « normes universelles », l'ensemble des $y \in H^1_{\mathrm{Iw}}(K,V)$ tels que pour tout $n \geqslant 0$ on ait $\mathrm{pr}_{K_n,V}(y) \in H^1_g(K_n,V)$.

Si $\mathrm{Fil}^1 V$ est la plus grande sous-représentation de V dont tous les poids de Hodge-Tate sont $\geqslant 1$, alors $\mathrm{Fil}^1 V$ est de de Rham et on peut montrer que $H^1_{\mathrm{Iw}}(K,\mathrm{Fil}^1 V)_g = H^1_{\mathrm{Iw}}(K,\mathrm{Fil}^1 V)$. Le résultat principal de cet article est le suivant :

THÉORÈME A. — *Si V est une représentation de de Rham, alors :*

1) *si V n'a pas de sous-quotient fixé par H_K, alors on a*

$$H^1_{\mathrm{Iw}}(K,V)_g = H^1_{\mathrm{Iw}}(K,\mathrm{Fil}^1 V);$$

2) *en général, $H^1_{\mathrm{Iw}}(K,\mathrm{Fil}^1 V) \subset H^1_{\mathrm{Iw}}(K,V)_g$ et le quotient est un $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \Lambda_K$-module de torsion (c'est en fait un $\mathbb{Q}_p$-espace vectoriel de dimension finie).*

La démonstration est très similaire à celle qu'en a donnée Perrin-Riou dans [22] pour les représentations cristallines, et dans [23] pour les représentations semi-stables, du groupe de Galois d'un corps non-ramifié mais au lieu d'utiliser son « exponentielle élargie », on utilise les constructions de [2] (qui

redonnent l'exponentielle élargie d'ailleurs, comme on le montre dans [3]) et au lieu d'utiliser des considérations de « cran de la filtration » et d'ordre, on utilise la théorie des (φ,Γ)-modules qui encodent toutes ces informations. Cela simplifie la démonstration de Perrin-Riou et nous permet de plus de l'étendre au cas des représentations de de Rham du groupe de Galois d'un corps éventuellement ramifié. Remarquons que l'on n'utilise pas le fait que les représentations de de Rham sont potentiellement semi-stables.

Indiquons brièvement d'où provient cette conjecture. On renvoie à l'article [22] de Perrin-Riou pour plus d'informations. Si E est une courbe elliptique définie sur K, on s'intéresse au module des « normes universelles » $\mathcal{N}_{K_\infty/K}(E) = \varprojlim E(K_n)$, limite projective pour les applications $\mathrm{Tr}_{K_n/K_{n-1}}$. Le calcul de ce module a été fait (pour une courbe elliptique, une variété abélienne ou même un groupe formel, et pour une $\mathbb{Z}_p$-extension quelconque) dans certains cas par Mazur [18], puis par Hazewinkel [14], [15], Schneider [24] et Perrin-Riou [20] entre autres. Dans [7], Coates et Greenberg ont formulé une conjecture assez générale décrivant le module des normes universelles. La formulation du résultat que nous démontrons est due à Nekovář et concerne les normes universelles dans l'extension cyclotomique pour une représentation p-adique de de Rham. Si on l'applique au module de Tate d'une courbe elliptique E, définie sur une extension finie K de $\mathbb{Q}_p$, on retrouve, via la théorie de Kummer, certains résultats des auteurs cités précédemment : si E est ordinaire, alors $\mathcal{N}_{K_\infty/K}(E)$ est un Λ_K-module de rang $[K:\mathbb{Q}_p]$ et si E est supersingulière, alors il est nul.

Remerciements. — Je remercie Pierre Colmez pour ses nombreuses suggestions, de la démonstration du théorème principal à la rédaction finale de cet article. Je remercie aussi Jan Nekovář pour ses encouragements et ses commentaires, ainsi que le *referee* pour ses remarques pertinentes qui ont permis d'améliorer la clarté de cet article.

I. Algèbre différentielle des (φ,Γ)-modules

L'objet de ce premier chapitre est de rappeler et compléter certains points de la théorie des (φ,Γ)-modules. Ensuite, on résout un problème d'algèbre différentielle. Dans le deuxième chapitre, on verra comment cela s'applique aux représentations p-adiques.

I.1. Les (φ,Γ)-modules. — Dans tout cet article, k désigne un corps parfait de caractéristique p et K est une extension finie de F, le corps des fractions de l'anneau des vecteurs de Witt sur k. On écrit $\mu_{p^n}\subset\overline{K}$ pour désigner l'ensemble des racines p^n-ièmes de l'unité et on définit

$$K_n = K(\mu_{p^n}),\quad K_\infty = \bigcup_{n=0}^{+\infty} K_n.$$

Soient $G_K = \mathrm{Gal}(\overline{K}/K)$ et $H_K = \mathrm{Gal}(\overline{K}/K_\infty)$ le noyau du caractère cyclotomique $\chi : G_K \to \mathbb{Z}_p^*$ et $\Gamma_K = G_K/H_K$ le groupe de Galois de K_∞/K, qui s'identifie via le caractère cyclotomique à un sous-groupe ouvert de $\mathbb{Z}_p^*$. Enfin, soient F' l'extension maximale non-ramifiée de F contenue dans K_∞ et k' le corps résiduel de F'. On note σ le Frobenius absolu (qui relève $x \mapsto x^p$ sur k').

Définissons ici quelques anneaux de séries formelles (ces constructions sont faites en détail dans [9]) : si r est un réel positif, soit $\mathbf{B}_F^{\dagger,r}$ l'anneau des séries formelles $f(X) = \sum_{k\in\mathbb{Z}} a_k X^k$ où $\{a_k \in F\}_{k\in\mathbb{Z}}$ est une suite bornée telle que $f(X)$ converge sur la couronne $0 < v_p(X) \leqslant 1/r$. Cet anneau est muni d'une action de Γ_F, qui est triviale sur les coefficients et donnée par

$$\gamma(X) = (1+X)^{\chi(\gamma)} - 1$$

et on peut définir un Frobenius $\varphi : \mathbf{B}_F^{\dagger,r} \to \mathbf{B}_F^{\dagger,pr}$ qui est σ-semi-linéaire sur les coefficients et tel que $\varphi(X) = (1+X)^p - 1$. Le « théorème de préparation de Weierstrass » montre que

$$\mathbf{B}_F^\dagger = \bigcup_{r\geqslant 0} \mathbf{B}_F^{\dagger,r}$$

est un corps. Ce corps n'est pas complet pour la norme de Gauss et on appelle $\mathbf{B}_F$ son complété qui est un corps local de dimension 2 dont le corps résiduel s'identifie à $k((\overline{X}))$.

L'extension K_∞/F_∞ est une extension finie de degré de ramification $e_K \leqslant [K_\infty : F_\infty]$ et par la théorie du corps de normes de [13], [25] il lui correspond une extension séparable $k'((\overline{Y}))/k((\overline{X}))$ de degré $[K_\infty : F_\infty]$ qui nous permet de définir des extensions non-ramifiées $\mathbf{B}_K/\mathbf{B}_F$ et $\mathbf{B}_K^\dagger/\mathbf{B}_F^\dagger$ de degré $[K_\infty : F_\infty]$. On peut montrer que

$$\mathbf{B}_K^\dagger = \bigcup_{r\geqslant 0} \mathbf{B}_K^{\dagger,r}$$

où $\mathbf{B}_K^{\dagger,r}$ est un $\mathbf{B}_F^{\dagger,r}$-module libre de rang $[K_\infty : F_\infty]$ qui s'identifie à un anneau de séries formelles $f(Y) = \sum_{k\in\mathbb{Z}} a_k Y^k$ où $\{a_k \in F'\}_{k\in\mathbb{Z}}$ est une suite bornée telle que $f(Y)$ converge sur la couronne $0 < v_p(Y) \leqslant 1/e_K r$. L'élément $\overline{Y}$ vérifie une équation d'Eisenstein sur $k'((\overline{X}))$ qu'on peut relever en une équation sur $\mathbf{B}_{F'}^{\dagger,r}$; l'action de Γ_K s'étend naturellement à $\mathbf{B}_K^{\dagger,r}$ de même que le Frobenius $\varphi : \mathbf{B}_K^{\dagger,r} \to \mathbf{B}_K^{\dagger,pr}$.

Un (φ,Γ)-module est un $\mathbf{B}_K^\dagger$-espace vectoriel $D^\dagger$ de dimension finie, muni d'un Frobenius $\varphi : D^\dagger \to D^\dagger$ et d'une action de Γ_K qui sont semi-linéaires par rapport à ceux de $\mathbf{B}_K^\dagger$. On dit que $D^\dagger$ est *étale* si

$$D = \mathbf{B}_K \otimes_{\mathbf{B}_K^\dagger} D^\dagger$$

possède un réseau D_0 stable par φ sur l'anneau des entiers $\mathbf{A}_K$ de $\mathbf{B}_K$, tel que $\varphi(D_0)$ engendre D_0 sur $\mathbf{A}_K$.

Définissons l'opérateur $\psi : D^\dagger \to D^\dagger$ qui nous servira dans la suite. On peut montrer que tout élément $x \in D^\dagger$ s'écrit de manière unique sous la forme $x = \sum_{i=0}^{p-1}(1+X)^i\varphi(x_i)$.

DÉFINITION I.1.1. — Si $x = \sum_{i=0}^{p-1}(1+X)^i\varphi(x_i)$, alors on pose $\psi(x) = x_0$.

Ceci fait de ψ un inverse à gauche de φ qui commute à l'action de Γ_K et qui vérifie $\psi(\varphi(x)y) = x\psi(y)$ si $x \in \mathbf{B}_K^\dagger$ et $y \in D^\dagger$.

Il existe $r(K)$ tel que si $p^{n-1}(p-1) \geqslant r \geqslant r(K)$, alors on a une application injective $\iota_n : \mathbf{B}_K^{\dagger,r} \to K_n[[t]]$ (c'est l'application φ^{-n} de [6, § III.2]). Par exemple si $K = F$, alors $\iota_n(X) = \varepsilon^{(n)}\exp(t/p^n) - 1$ où $\varepsilon^{(n)}$ est une racine primitive p^n-ième de 1 et ι_n agit par σ^{-n} sur les coefficients.

On peut montrer (voir pour cela [4]) que l'ensemble des sous $\mathbf{B}_K^{\dagger,r}$-modules de type fini M de $D^\dagger$ tels que $\varphi(M) \subset \mathbf{B}_K^{\dagger,pr} \otimes_{\mathbf{B}_K^{\dagger,r}} M$ admet un plus grand élément $D^{\dagger,r}$ et qu'il existe $r(D)$ que l'on peut supposer $\geqslant r(K)$ tel que si $r \geqslant r(D)$, alors

$$D^\dagger = \mathbf{B}_K^\dagger \otimes_{\mathbf{B}_K^{\dagger,r}} D^{\dagger,r}.$$

On utilise alors ι_n pour définir $K_n[[t]] \otimes^{\iota_n}_{\mathbf{B}_K^{\dagger,r}} D^{\dagger,r}$ et $K_n((t)) \otimes^{\iota_n}_{\mathbf{B}_K^{\dagger,r}} D^{\dagger,r}$.

Le lemme suivant sera utile par la suite :

LEMME I.1.2. — *Si $y \in (D^\dagger)^{\psi=1}$, alors il existe $P(\gamma) \in F'[\Gamma_K]$ tel que $P(\gamma)y = 0$ si et seulement si $y \in (D^\dagger)^{\varphi=1}$.*

Démonstration. — Un petit calcul montre que $(D^\dagger)^{\varphi=1}$ est un $\mathbb{Q}_p$-espace vectoriel de dimension $\leqslant \dim(D^\dagger)$ (il suffit de remarquer que des éléments de $(D^\dagger)^{\varphi=1}$ qui sont liés sur $\mathbf{B}_K^\dagger$ le sont sur $\mathbb{Q}_p = (\mathbf{B}_K^\dagger)^{\varphi=1}$) qui est stable par Γ_K (puisque φ commute à l'action de Γ_K) et donc qu'il existe $P(\gamma) \in \mathbb{Q}_p[\Gamma_K]$ en fait tel que $P(\gamma)$ annule $(D^\dagger)^{\varphi=1}$. Montrons donc la réciproque.

Supposons que $(\sum a_i\gamma^i)y = 0$ est une relation de longueur minimale avec $a_i \in F'$. On peut supposer que l'un des a_i est égal à 1. En appliquant ψ et en utilisant le fait que d'une part $\psi(y) = y$ et que d'autre part ψ commute à l'action de Γ_K et agit par σ^{-1} sur F', on voit que $a_i \in \mathbb{Q}_p$ pour tout i et on suppose donc à partir de maintenant que $P(\gamma) \in \mathbb{Q}_p[\Gamma_K]$.

Nous utiliserons ci-dessous le résultat suivant : si $P(\gamma) \in \mathbb{Q}_p[\Gamma_K]$, alors il existe une constante $C(P,d)$ telle que pour tout M qui est un $K_\infty[[t]]$-module libre de rang d, muni d'une action semi-linéaire de Γ_K par automorphismes, le F-espace vectoriel $M^{P(\gamma)=0}$ est de dimension $\leqslant C(P,d)$.

Fixons $r \geqslant r(D)$ et considérons, pour n tel que $p^{n-1}(p-1) \geqslant r$, le $K_n[[t]]$-module libre $K_n[[t]] \otimes^{\iota_n}_{\mathbf{B}_K^{\dagger,r}} D^{\dagger,r}$ de rang d défini ci-dessus. On voit que l'on a une injection

$$(D^{\dagger,r})^{P(\gamma)=0} \hookrightarrow \bigl(K_\infty[[t]] \otimes_{K_n[[t]]} K_n[[t]] \otimes^{\iota_n}_{\mathbf{B}_K^{\dagger,r}} D^{\dagger,r}\bigr)^{P(\gamma)=0},$$