PUBLICATIONS MATHÉMATIQUES ET INFORMATIQUES DE RENNES

PIERRE BERTHELOT

Systèmes de Honda des schémas en $\mathbb{F}_q$-vectoriels

Publications des séminaires de mathématiques et informatique de Rennes, 1975, fascicule 2
« Séminaires d'algèbre et de logique », , exp. n° 1, p. 1-19
<http://www.numdam.org/item?id=PSMIR_1975___2_A1_0>

SYSTEMES DE HONDA DES SCHEMAS EN $\mathbb{F}_q$-VECTORIELS

par

Pierre BERTHELOT

Soient k un corps parfait de caractéristique p > 0, W l'anneau des vecteurs de Witt à coefficients dans k, K son corps des fractions. Généralisant les résultats de Grothendieck [5] sur la classification des groupes p-divisibles, Fontaine a montré [4] que la classification des schémas en groupes commutatifs, finis et plats sur W, peut se faire au moyen du "système de Honda" d'un tel schéma en groupes G, système formé du module de Dieudonné M de la réduction G_k de G sur k, et d'un sous-W-module $L \subset M$ vérifiant des conditions rappelées plus bas. De plus, la théorie de Fontaine permet de répondre, dans le cas fini comme dans le cas p-divisible, à la question posée par Grothendieck dans [5] : comment construire la représentation de Gal $(\overline{K}/K)$ fournie par la fibre générique de G, à partir du couple (M,L) classifiant G ?

Nous donnons ici un exemple indiquant comment cette construction peut être utilisée pour obtenir des informations sur la représentation galoisienne définie par G. Si H est un quotient de Jordan-Hölder de G, il existe un corps fini F et une structure de schéma en F-vectoriels sur H, de rang 1 sur F, telle que la restriction au groupe d'inertie I de la représentation galoisienne définie par H se fasse par un caractère $\Psi : I \longrightarrow F^*$ (cf. [7]). Répondant à une question de Serre, Raynaud a montré [6] que le caractère Ψ peut s'écrire comme produit des caractères fondamentaux de I, chaque caractère ayant pour exposant 0 ou 1 (W étant ici absolument non ramifié). A partir des résultats de Fontaine, on obtient une autre démonstration de ce résultat, ainsi qu'une description très simple du caractère Ψ à partir du système de Honda de H, et de l'action de F sur ce système (théorème 3.8).

On peut d'autre part espérer que cette méthode se généraliserait au cas où l'on remplace le groupe G par l'homologie étale $H_*(X_K, \mathbb{Z}/p\mathbb{Z})$ de la fibre générique d'un schéma X propre et lisse sur W (comme le demande Serre dans [7]), si l'on disposait d'une construction analogue à celle de Fontaine, reliant la cohomologie cristalline de X_k, munie de la filtration de Hodge définie par X, à la cohomologie étale p-adique de X_K (voir l'introduction de [1]).

1 - Représentation galoisienne associée à un système fini de Honda.

Rappelons brièvement la classification des schémas en groupes commutatifs finis et plats sur l'anneau des vecteurs de Witt d'un corps parfait, d'après Fontaine ([2], [4]).

1.1. Soient k un corps parfait de caractéristique $p > 0$, $W = W(k)$ l'anneau des vecteurs de Witt à coefficients dans k. Pour toute k-algèbre artinienne R, on note CW(R) l'ensemble des suites

$$x = (\ldots, x_{-i}, \ldots, x_o) = (x_{-i})_{i \in \mathbb{N}}$$

telles que, pour presque tout i, x_{-i} appartienne au radical de R.

Les applications

$$W_n(R) \longrightarrow CW(R)$$

qui associent à $y = (y_j)_{0 \leq j \leq n-1}$ la suite $(x_{-i})_{i \in \mathbb{N}}$ définie par

$$x_{-i} = y_{n-1-i} \quad \text{pour} \quad 0 \leq i \leq n-1, \quad x_{-i} = 0 \quad \text{si} \quad i \geq n,$$

définissent une injection

$$\underset{\rightarrow}{W}(R) = \varinjlim_n W_n(R) \hookrightarrow CW(R),$$

identifiant $\underset{\rightarrow}{W}(R)$ à l'ensemble des suites (x_{-i}) telles que $x_{-i} = 0$ pour presque tout i.

Les formules universelles définissant la somme dans $\underset{\rightarrow}{W}(R)$ gardent un sens pour les éléments de CW(R), munissant cet ensemble d'une structure de groupe abélien. On définit d'autre part des opérateurs F, V prolongeant ceux de $\underset{\rightarrow}{W}(R)$ par

$$F((a_{-i})_{i \in \mathbb{N}}) = (a^p_{-i})_{i \in \mathbb{N}} ,$$
$$V((a_{-i})_{i \in \mathbb{N}}) = (a_{-i-1})_{i \in \mathbb{N}} .$$

Enfin, on vérifie qu'il existe sur CW(R) une unique structure de W-module telle que pour $a = (a_o, 0, \ldots, 0, \ldots) \in W(k)$, on ait

$$a.(x_{-i})_{i \in \mathbb{N}} = (a_o^{p^{-i}} x_{-i})_{i \in \mathbb{N}} ,$$

et les compatibilités usuelles avec les opérateurs F et V. Si D_k est l'anneau de Dieudonné de k, CW est ainsi un foncteur sur la catégorie des k-algèbres artiniennes, à valeurs dans la catégorie des D_k-modules.

Soit G un schéma en groupes (commutatif) fini sur k. Le module de Dieudonné de G est alors le D_k-module

$$M(G) = \mathrm{Hom}(G, CW) ,$$

où Hom désigne l'ensemble des morphismes de foncteurs en groupes abéliens. Si R est l'algèbre de G, M(G) s'identifie naturellement à un sous D_k-module de CW(R).

Théorème 1.2. (cf. [2]) : *Le foncteur qui à G associe M(G), est une équivalence de catégories de la catégorie des k-schémas en groupes finis commutatifs dans la catégorie des D_k-modules qui sont de longueur finie comme W-modules.*

Un foncteur quasi-inverse peut se décrire comme suit : soit A une k-algèbre artinienne ; si M = M(G), alors

$$G(A) = \mathrm{Hom}_{D_k}(M, CW(A)).$$

1.3. Soit maintenant A une W-algèbre libre finie. On définit une application

$$w_A : CW(A/pA) \longrightarrow (A \otimes_W K)/A ,$$

où K = Frac(W), en posant, pour $a_{-i} \in A/pA$, et b_{-i} relevant a_{-i} dans A,

$$w_A((a_{-i})_{i \in \mathbb{N}}) = \sum_{i=0}^{\infty} p^{-i-1} b_{-i}^{p^i} .$$

La série obtenue converge pour la topologie p-adique de $A \otimes_W K$, et sa somme ne dépend pas modulo A du choix des relèvements b_{-i}. De plus, w_A est un homomorphisme W-linéaire, fonctoriel en A.

Soient G un schéma en groupe commutatif, fini et plat sur W, R son algèbre, G_k sa fibre spéciale, d'algèbre R/pR. On considère l'homomorphisme composé

$$M(G_k) \subset CW(R/pR) \xrightarrow{w_R} (R \otimes_W K)/R,$$

et on note L(G) son noyau, qui est donc un sous-W-module de $M(G_k)$.
Le couple $(M,L) = (M(G_k),L(G))$ vérifie alors les propriétés suivantes :

Théorème 1.4. ([4]) :

a) $F(M) \cap L = pL$;

b) $M = F(M) \oplus L$;

c) *la restriction de* V *à* L *est injective.*

Un couple formé d'un D_k-module M de longueur finie sur W et d'un sous-W-module L de M vérifiant les conditions de 1.4 est appelé système fini de Honda. Les conditions de 1.4 sont encore équivalentes aux conditions suivantes :

i) $F(M) \cap L = pL$;

ii) $Ker(p) = Ker(p|_L) \oplus Ker(V)$;

iii) $Ker(F) \subset Im(V)$.

En particulier, si $p.M = 0$, $F \circ V = V \circ F = 0$, de sorte que la condition iii) équivaut à $Ker(F) = Im(V)$, ou encore $Ker(V) = Im(F)$.

Théorème 1.5 ([4]) :

i) *Supposons* $p \neq 2$. *Alors le foncteur qui à* G *associe* $(M(G_k),L(G))$, *est une équivalence de catégories de la catégorie des* W-*schémas en groupes commutatifs, finis et plats sur la catégorie des systèmes finis de Honda.*

ii) *Supposons* p=2. *Alors le même énoncé reste vrai si on se restreint à la catégorie des schémas en groupes unipotents, resp. à celle des systèmes finis de Honda tels que* V *soit nilpotent sur* M.

Un foncteur quasi-inverse peut se décrire de la façon suivante : soient G un schéma en groupes fini et plat sur W, de système de Honda (M,L), et A une W-algèbre finie et libre. Posons

$$L_A = \mathrm{Ker}(CW(A/pA) \xrightarrow{w_A} (A \otimes K)/A).$$

Alors

$$G_A \simeq \mathrm{Hom}_{D_k,\mathrm{filt}}((M,L), (CW(A/pA),L_A)),$$

où $\mathrm{Hom}_{D_k,\mathrm{filt}}$ désigne le groupe des homomorphismes D_k-linéaires $\varphi : M \longrightarrow CW(A/pA)$ tels que $\varphi(L) \subset L_A$.

1.6. Soient en particulier K' une extension finie de K, A' la clôture intégrale de W dans K' ; on a donc, si $G_K = G \times_W K$,

$$G_K(K') = G(A') \simeq \mathrm{Hom}_{D_k,\mathrm{filt}}((M,L),(CW(A'/pA'),L_{A'})).$$

L'action de $\mathcal{G}_{K'} = \mathrm{Gal}(K'/K)$ sur $G_K(K')$ se fait par l'intermédiaire de son action sur A', donc sur le couple $(CW(A'/pA'),L_{A'})$. Posons

$$\mathcal{CW}_K = \varinjlim_{K'/K} CW(A'/pA') \ , \qquad \mathcal{L}_K = \varinjlim_{K'/K} L_{A'} \ ,$$

(on notera l'injectivité des flèches de transition), de sorte qu'il existe une action naturelle de $\mathcal{G} = \mathrm{Gal}(\bar{K}/K)$ sur le couple $(\mathcal{CW}_K, \mathcal{L}_K)$. Par passage à la limite, on obtient l'expression du module galoisien $G_K(\bar{K})$ à partir du système de Honda de G :

$$G_K(\bar{K}) \simeq \mathrm{Hom}_{D_k,\mathrm{filt}}((M,L) \ , \ (\mathcal{CW}_K, \mathcal{L}_K)).$$

2 - Structure du système de Honda d'un schéma en $\mathbb{F}_q$-vectoriels.

2.1. Soit $\mathbb{F}_q$ un corps fini à $q = p^r$ éléments. On appellera *schéma en $\mathbb{F}_q$-vectoriels* sur un schéma S, la donnée d'un S-schéma en groupes commutatifs G, fini et plat sur S, et d'un homomorphisme d'anneaux $\mathbb{F}_q \longrightarrow \mathrm{End}_S(G)$. Pour tout $\lambda \in \mathbb{F}_q$, on notera $[\lambda]$ l'endomorphisme de G correspondant.

Soit G un schéma en $\mathbb{F}_q$-vectoriels sur W, qu'on suppose unipotent si p=2. Si (M,L) est le système de Honda de G, $\mathbb{F}_q$ opère sur (M,L) par fonctorialité, et on notera encore $[\lambda]$ l'endomorphisme de (M,L) défini par $\lambda \in \mathbb{F}_q$. Comme G est annulé par p, il en est de même de M, qui est donc un k-espace vectoriel. Pour tout $\lambda \in \mathbb{F}_q$, $[\lambda]$ est donc un endomorphisme k-linéaire de M, commutant à F et V, pour lequel L est stable.

Pour tout caractère $\chi : \mathbb{F}_q^* \longrightarrow k^*$, soit M_χ le sous-espace de M sur lequel $\mathbb{F}_q$ agit par l'intermédiaire de χ. Rappelons que χ est dit *fondamental* si l'application $\overline{\chi} : \mathbb{F}_q \longrightarrow k$ prolongeant χ par $\overline{\chi}(0) = 0$ est additive ; il existe r caractères fondamentaux, induits par les r plongements du corps $\mathbb{F}_q$ dans le corps k, et qu'on peut noter χ_i, $i \in \mathbb{Z}/r$, en choisissant un plongement particulier $\chi_o : \mathbb{F}_q \hookrightarrow k$, et en imposant $\chi_{i+1} = \chi_i^p$.
On posera $M_i = M_{\chi_i}$.

Lemme 2.2. : *Avec les notations précédentes,*

$$M = \bigoplus_{i \in \mathbb{Z}/r} M_i .$$

Un argument classique montre que si l'on pose

$$\pi_\chi = \frac{1}{q-1} \sum_{\lambda \in \mathbb{F}_q^*} \chi(\lambda)^{-1} \, [\lambda] ,$$

l'image de π_χ est M_χ, et les π_χ constituent une famille d'idempotents orthogonaux, de somme l'identité. Par suite,

$$M = \bigoplus_{\chi : \mathbb{F}_q^* \longrightarrow k^*} M_\chi ,$$

et il suffit de voir que si $M_\chi \neq 0$, χ est un caractère fondamental. Soient $\lambda,\mu \in \mathbb{F}_q$, et $x \in M_\chi$, $x \neq 0$. La relation $[\lambda+\mu] = [\lambda] + [\mu]$ dans End(M,L) donne

$$[\lambda+\mu](x) = [\lambda](x) + [\mu](x) ,$$

soit

$$\chi(\lambda+\mu)x = (\chi(\lambda)+\chi(\mu))x ,$$

d'où l'additivité de χ.

Lemme 2.3 : *Pour tout* i,

$$F(M_i) \subset M_{i+1} , \quad V(M_i) \subset M_{i-1}.$$

Puisque l'action de $\mathbb{F}_q$ commute à F et V, on a, pour $x \in M_i$,

$$[\lambda](F(x)) = F([\lambda](x)) = F(\chi_i(\lambda)x) = \chi_i(\lambda)^p.F(x) = \chi_{i+1}(\lambda).F(x),$$

de sorte que $F(x) \in M_{i+1}$; de même, $V(x) \in M_{i-1}$.

Corollaire 2.4 : *Supposons que* G *soit de rang* r *sur* k. *Alors, pour tout* i, $\dim_k M_i = 1$.

Supposons que $M_i = 0$. D'après 2.3, F est nul sur M_{i-1}. Si $x \in M_{i-1}$, x est donc de la forme V(y), d'après 1.4 iii). Quitte à remplacer y par sa composante sur M_i, on peut d'après 2.3 supposer que $y \in M_i$, donc $y = 0$, $x = 0$, et par suite $M_{i-1} = 0$. Par récurrence, on en déduit que $M = 0$, ce qui est absurde. Donc, pour tout i, $\dim_k M_i \geq 1$. Or la dimension de M sur k est égale au rang de G, soit r, et il y a r caractères fondamentaux, d'où le résultat.

On suppose désormais que G est de rang r sur k.

Lemme 2.5 : *Supposons* k *algébriquement clos. Alors* M *possède une base* $(e_i)_{i \in \mathbb{Z}/r}$, *telle que*

a) e_i *engendre* M_i ;

b) *soit* $F(e_i) = e_{i+1}$, *soit* $V(e_{i+1}) = e_i$.

Choisissons pour tout i un générateur e'_i de M_i. Deux cas sont possibles :

i) si $F(e'_i) \neq 0$, on a $F(e'_i) = \alpha_i\, e'_{i+1}$, avec $\alpha_i \in k^*$;

ii) si $F(e'_i) = 0$, e'_i est de la forme $V(y)$, pour $y \in M_{i+1}$, et il existe un unique $\alpha_i \in k^*$ tel que $V(\alpha_i\, e'_{i+1}) = e'_i$.

Posant $e_i = \varepsilon_i\, e'_i$, avec $\varepsilon_i \in k^*$, on voit que les e_i vérifieront la condition b), si et seulement si

soit

$$e_{i+1} = F(e_i) = F(\varepsilon_i e'_i) = \varepsilon_i^p F(e'_i) = \varepsilon_i^p\, \alpha_i\, e'_{i+1} = \varepsilon_i^p\, \alpha_i\, \varepsilon_{i+1}^{-1}\, e_{i+1}\ ,$$

soit

$$e_i = V(e_{i+1}) = V(\varepsilon_{i+1}\, e'_{i+1}) = \varepsilon_{i+1}^{1/p}\, V(e'_{i+1}) = \varepsilon_{i+1}^{1/p}\, \alpha_i^{-1/p}\, e'_i =$$

$$\varepsilon_{i+1}^{1/p}\, \alpha_i^{-1/p}\, \varepsilon_i^{-1}\, e_i\ ,$$

c'est-à-dire si et seulement si pour tout i

$$\varepsilon_{i+1} = \alpha_i\, \varepsilon_i^p .$$

Par suite, ε_i doit être racine de l'équation

$$\varepsilon_i^{p^r} = (\alpha_i^{p^{r-1}}\, \alpha_{i+1}^{p^{r-2}} \cdots \alpha_{i+r-1})^{-1}\, \varepsilon_i\ ,$$

qui possède des solutions non triviales puisque k est supposé algébriquement clos. L'un des ε_i étant choisi de la sorte, les relations précédentes déterminent alors les ε_i pour tout i.

Lemme 2.6 : *Avec les notations précédentes, il existe une suite d'indices* $i_1,\ldots,i_d$ *telle que* $e_{i_1},\ldots,e_{i_d}$ *forment une base de* L, *et les* $e_{i'}$, *pour* $i' \neq i_1,\ldots,i_d$ *une base de* F(M).

Puisque L est stable sous l'action de $\mathbb{F}_q$, il admet une décomposition $L = \bigoplus_\chi L_\chi$, avec $L_\chi \subset M_\chi$. Comme $\dim M_\chi \leq 1$, on a $L_\chi = 0$ ou $L_\chi = M_\chi$. Lorsque $\chi = \chi_i$ est un caractère fondamental, on notera $L_i = L_{\chi_i}$; soient $i_1,\ldots,i_d$ les indices tels que $L_i \neq 0$; alors $L = \bigoplus_{j=1}^{d} L_{i_j}$, de sorte que $e_{i_1},\ldots,e_{i_d}$ forment une base de L.

D'après 1.4, $M = L \oplus F(M)$. Comme $F(M)$ est engendré par les $F(e_i)$, et que les $F(e_i)$ non nuls sont une partie des e_i, les e_i pour $i \neq i_1,\dots,i_d$ forment une base de $F(M)$.

2.7. Supposons d'abord que $L \neq 0$ et $L \neq M$. On note α_j, $j \in \mathbb{Z}/s$, les indices tels que $L_{\alpha_j} \neq 0$, $L_{\alpha_j+1} = 0$, l'indexation par $\mathbb{Z}/s$ étant définie par l'unique application $\mathbb{Z}/s \longrightarrow \mathbb{Z}/r$ telle que l'application composée $[1,s] \longrightarrow \mathbb{Z}/s \longrightarrow \mathbb{Z}/r \longrightarrow [1,r]$ soit strictement croissante. Pour tout $j \in \mathbb{Z}/s$, on note M_j, m_j les entiers $\leq r$ définis par

$$\begin{cases} V^{m_j}(L_{\alpha_j}) \neq 0 \ , \quad V^{m_j+1}(L_{\alpha_j}) = 0 \ , \\ F^{n_j}(L_{\alpha_j}) \neq 0 \ , \quad F^{n_j+1}(L_{\alpha_j}) = 0. \end{cases}$$

On remarquera que $m_j \geq 1$, car V est injectif sur L ; de même, $n_j \geq 1$, car $L_{\alpha_j+1} = 0$, donc $e_{\alpha_j+1} \in F(M)$ d'après le lemme précédent, donc $F(e_{\alpha_j}) = e_{\alpha_j+1}$, d'où $F(L_{\alpha_j}) \neq 0$. En particulier, on peut encore caractériser les indices α_j comme étant ceux pour lesquels $F(e_{\alpha_j}) \neq 0$, $V(e_{\alpha_j}) \neq 0$.

On étend ces définitions aux cas $L = 0$ et $L = M$ en posant alors $s = 1$, et en prenant pour α_1 un indice arbitraire dans $\mathbb{Z}/r$. On a alors, si $L = 0$

$$F^r(e_{\alpha_1}) = e_{\alpha_1} \ , \quad V(e_{\alpha_1}) = 0,$$

puisque $F(M) = M$, donc F est un isomorphisme; on pose donc $m_1 = 0$, $n_1 = r$. De même, si $L = M$,

$$F(e_{\alpha_1}) = 0 \ , \quad V^r(e_{\alpha_1}) = e_{\alpha_1},$$

et on pose $m_1 = r$, $n_1 = 0$. On remarquera que ces deux cas se produisent si et seulement si la réduction G_k de G modulo p est étale, resp. de type multiplicatif.

Proposition 2.8 :

i) *Avec les notations précédentes, M est le D_k-module engendré par des générateurs $(x_i)_{i \in \mathbb{Z}/s}$, soumis aux relations*

a) $px_i = 0$

b) $F^{n_i}(x_i) = V^{m_{i+1}}(x_{i+1})$.

ii) L *est engendré par les* $V^j(x_i)$ *pour* $i \in \mathbb{Z}/s$, $0 \leq j < m_i$.

Si G_k est étale ou de type multiplicatif, on prend pour x_1 l'un quelconque des e_i, et l'assertion est claire. Sinon, on pose $x_i = e_{\alpha_i}$.

Pour prouver la relation b), observons que

$$F^{n_i}(e_{\alpha_i}) = e_{\alpha_i+n_i} \quad , \quad F^{n_i+1}(e_{\alpha_i}) = 0 \ ,$$

donc $V(e_{\alpha_i+n_i+1}) = F^{n_i}(e_{\alpha_i})$.

Si $F(e_{\alpha_i+n_i+1}) = 0$, alors $V(e_{\alpha_i+n_i+2}) = e_{\alpha_i+n_i+1}$,

donc $V^2(e_{\alpha_i+n_i+2}) = F^{n_i}(e_{\alpha_i})$; comme $F \neq 0$, on obtient en itérant m_i' tel que

$$F(e_{\alpha_i+n_i+m_i'}) \neq 0 \quad , \quad V^{m_i'}(e_{\alpha_i+n_i+m_i'}) = F^{n_i}(e_{\alpha_i}) \neq 0.$$

Ceci caractérisant les indices α_i, on a donc $\alpha_i+n_i+m_i' = \alpha_{i+1}$, et $m_i' = m_{i+1}$. D'où b), et les relations

$$\alpha_{i+1} - \alpha_i = m_i + m_{i+1} \quad , \quad \sum_i (m_i + n_i) = r.$$

On voit aussi que chacun des e_j est image par un itéré de F ou V de l'un des x_i, de sorte que les x_i engendrent M comme D_k-module.

Soit alors M' le D_k-module engendré par des générateurs x_i' soumis aux relations a) et b) ; on peut écrire

$$M' = (k[F,V]/(FV,VF))^s \ / \ (F^{n_i}(x_i') - V^{m_{i+1}}(x_{i+1}')),$$

où $k[F,V]$ est l'anneau de polynômes non commutatif tel que $Fa = a^pF$, $a^pV = Va$. Le D_k-module M est de façon naturelle un quotient de M'. Or M' est engendré sur k par les $F^j(x_i')$, $0 \leq j \leq n_i$, et les $V^j(x_i')$, $0 \leq j \leq m_i$, de sorte que

$$\dim_k(M') \leq \sum_i (m_i+n_i) = r \ ;$$

comme M est de dimension r sur k, $M' = M$.

D'autre part, L est engendré par les $e_j \notin F(M)$, et, d'après ce qui précède, ce sont exactement les vecteurs e_{α_i}, $V(e_{\alpha_i}),\dots,V^{m_i-1}(e_{\alpha_i})$, d'où l'assertion ii).

3 - La représentation galoisienne définie par un schéma en $\mathbb{F}_q$-vectoriels.

On suppose k algébriquement clos. Soit G un schéma en $\mathbb{F}_q$-vectoriels sur W, qu'on suppose de rang $q = p^r$, et unipotent dans le cas p=2. On va calculer explicitement le groupe $G_K(\overline{K})$ des points de G_K à valeurs dans la clôture algébrique $\overline{K}$ de K, qui est donc un $\mathbb{F}_q$-vectoriel de dimension 1, ainsi que l'action sur celui-ci du groupe de Galois $\mathcal{G} = \mathrm{Gal}(\overline{K}/K)$. Cette action, étant compatible à la structure $\mathbb{F}_q$-vectorielle, se fait par l'intermédiaire d'un caractère $\Psi : \mathcal{G} \longrightarrow \mathbb{F}_q^*$ que l'on cherche à expliciter à partir du système de Honda associé à G.

3.1. Soit (M,L) le système de Honda de G. D'après 1.6,

$$G_K(\overline{K}) = \mathrm{Hom}_{D_k,\mathrm{filt}}((M,L),(\mathcal{O}_{\overline{K}},\mathcal{L}_K))$$

$$= \{\varphi \in \mathrm{Hom}_{D_k}(M,\mathcal{O}_{\overline{K}}) \mid w\circ\varphi|_L = 0\},$$

où w est l'homomorphisme défini en 1.3. D'après 2.8, un tel φ est déterminé par sa valeur y_i sur les x_i, $i \in \mathbb{Z}/s$, et l'on obtient

$$\mathrm{Hom}_{D_k}(M,\mathcal{O}_{\overline{K}}) \simeq \{(y_i)_{i\in\mathbb{Z}/s} \mid y_i \in \mathcal{O}_{\overline{K}},\ py_i=0,\ F^{n_i}(y_i) = V^{m_{i+1}}(y_{i+1})\}.$$

Posons $y_i = (a_{-j,i})_{j\in\mathbb{N}}$, où les $a_{-j,i} \in A'/pA'$, A' étant l'anneau des entiers d'une extension finie K' de K. Les conditions précédentes s'écrivent :

(3.1.1) $py_i = 0 \iff \forall\ j\geq 1,\ (a_{-j,i})^p = 0$;

(3.1.2) $F^{n_i}(y_i) = V^{m_{i+1}}(y_{i+1}) \iff \forall\ j\geq 0,\ (a_{-j,i})^{p^{n_i}} = a_{-j-m_{i+1},i+1}$.

La condition $\varphi(L) \subset \mathcal{L}_K$ s'écrit d'après 2.8

$$\forall\ i,\ \forall\ j < m_i,\quad \varphi(V^j(x_i)) = V^j(\varphi(x_i)) \in \mathcal{L}_K.$$

Choisissant pour tous i,j un relèvement $b_{-j,i}$ de $a_{-j,i}$ dans A', cette relation s'écrit

$$(3.1.3) \quad \forall\, i,\ \forall\, j < m_i,\ \sum_{n=0}^{\infty} p^{-n-1}\ b_{-j-n,i}^{p^n} \in A'.$$

Lemme 3.2. : *Sous les hypothèses précédentes, $G_K(\overline{K})$ s'identifie à l'ensemble des classes de congruence modulo p de familles d'éléments $(b_{-j,i})_{i \in \mathbb{Z}/s,\, 0 \le j \le m_i}$, où les $b_{-j,i}$ sont des entiers d'une extension finie de K et vérifient les relations*

$$(3.2.1) \quad \forall\, i,\ (b_{0,i})^{p^{n_i}} \equiv b_{-m_{i+1},i+1} \mod p,$$

$$(3.2.2) \quad \forall\, i,\ \forall\, j < m_i,\ b_{-j,i} + p^{-1}(b_{-j-1,i})^p \equiv 0 \mod p.$$

Les relations (3.1.2) entraînent les relations (3.2.1). Montrons les relations (3.2.2). D'après (3.1.1), on peut écrire pour $j \ge 1$

$$b_{-j,i}^p = p\, c_{-j,i},$$

avec $c_{-j,i} \in A'$. Donc, pour $n \ge 1$, $p^{-n-1}\, b_{-j-n,i}^{p^n} = p^{p^{n-1}-n-1}\, c_{-j-n,i}^{p^{n-1}}$. Or, si $p \neq 2$, $p^{n-1}-n-1 \ge 0$ si $n \ge 2$, de sorte que dans ce cas, $p^{-n-1}\, b_{-j-n,i}^{p^n}$ est entier pour $n \ge 2$. Les relations (3.1.3) se réduisent alors à

$$\forall\, i,\ \forall\, j < m_i,\ p^{-1}\, b_{-j,i} + p^{-2}\, b_{-j-1,i}^p \in A',$$

c'est-à-dire (3.2.2). Si $p = 2$, on a seulement $2^{n-1}-n-1 \ge 0$ pour $n \ge 3$, et les relations (3.1.3) se réduisent à

$$\forall\, i,\ \forall\, j < m_i,\ p^{-1}\, b_{-j,i} + p^{-2}\, b_{-j-1,i}^p + p^{-3}\, b_{-j-2,i}^{p^2} \in A',$$

soit encore

$$(3.2.3) \quad \forall\, i,\ \forall\, j < m_i,\ b_{-j,i} + p^{-1}\, b_{-j-1,i}^p + p^{-2}\, b_{-j-2,i}^{p^2} \in pA'.$$

Mais pour $p = 2$, G est unipotent par hypothèse, de sorte que V est nilpotent, et, pour tout i, $V^{m_i+1}(y_i) = 0$, c'est-à-dire $a_{-m_i-n,i} = 0$ pour $n \ge 1$. On peut donc supposer $b_{-m_i-n,i} = 0$ pour $n \ge 1$, et on obtient pour $j = m_i - 1$

$$b_{-m_i+1,i} + p^{-1}\, b_{-m_i,i}^p \equiv 0 \mod p.$$

Procédent par récurrence descendante, on suppose (3.2.2) vraie pour j .

Les deux termes étant entiers, on obtient par élévation à la puissance p-ième

$$b_{-j,i}^{p} \equiv (-p)^{-p}\ b_{-j-1,i}^{p^2} \mod p^2,$$

soit

$$p^{-1}\ b_{-j,i}^{p} \equiv -(-p)^{-p-1}\ b_{-j-1,i}^{p^2} \mod p.$$

En substituant dans (3.2.3) pour j-1, on obtient

$$b_{-j+1,i} + (p^{-2}-(-p)^{-p-1})\ b_{-j-1,i}^{p^2} \equiv 0 \mod p,$$

donc $(-p)^{-p-1}((-p)^{p-1}-1)\ b_{-j-1,i}^{p^2}$ est entier, donc $(-p)^{-p-1}\ b_{-j-1,i}^{p^2}$ aussi, et $p^{-2}\ b_{-j-1,i}^{p^2} \in pA'$. Par suite, la congruence (3.2.3) pour j-1 se réduit à la congruence (3.2.2) pour j-1, ce qui établit la récurrence.

Réciproquement, si on se donne une famille $(b_{-j,i})$ vérifiant (3.2.1) et (3.2.2), on prend pour $a_{-j,i}$ la réduction modulo p de $b_{-j,i}$ si $j \leq m_i$, et 0 si $j > m_i$, sauf dans le cas où G est de type multiplicatif, où l'on pose $a_{-j,1} = a_{-j',1}$, où j' est le reste de la division de j par r.
On vérifie alors sans difficulté les relations (3.1.1) à (3.1.3).

Lemme 3.3 : *Soit* $(b_{-j,i})_{i \in \mathbb{Z}/s, 0 \leq j \leq m_i}$ *une famille d'éléments de* A' *vérifiant* (3.2.1) *et* (3.2.2). *Supposons qu'il existe des indices* (i,j) *et* (i',j') *et des entiers* α,β, *tels que*

$$(-p)^{-\beta}\ b_{-j,i}^{p^\alpha} \equiv b_{-j',i'} \mod p.$$

Alors

a) *Si* $j' \neq 0$, *les* $b_{-j,i}$ *vérifient la congruence*

$$(-p)^{-p\beta-1}\ b_{-j,i}^{p^{\alpha+1}} \equiv b_{-j'+1,i'} \mod p.$$

b) *Si* $j'=0$, *les* $b_{-j,i}$ *vérifient la congruence*

$$(-p)^{-p^{n_{i'}}\beta}\ b_{-j',i}^{p^{\alpha+n_{i'}}} \equiv b_{m_{i'+1},i'+1} \mod p.$$

a) Elevant la congruence à la puissance p, on obtient

$$(-p)^{-p\beta}\ b_{-j,i}^{p^{\alpha+1}} \equiv b_{-j',i'}^{p} \mod p^2,$$

d'où

$$(-p)^{-p\beta-1}\ b_{-j,i}^{p^{\alpha+1}} \equiv (-p)^{-1}\ b_{-j',i'}^{p} \equiv b_{-j'+1,i'} \mod p$$

d'après (3.2.2).

b) La congruence donnée entraîne

$$(-p)^{-p^{n_{i'}}\beta}\ b_{-j,i}^{p^{\alpha+n_{i'}}} \equiv b_{0,i'}^{p^{n_{i'}}} \equiv b_{m_{i'+1},i'+1} \mod p$$

d'après (3.2.1).

Lemme 3.4 : *Soit* $(b_{-j,i})_{i\in\mathbb{Z}/s,0\le j\le m_i}$ *une famille d'éléments de* A' *vérifiant* (3.2.1) *et* (3.2.2). *Pour tout* (i,j), *posons*

$$\mu_{i,j} = \sum_{n=1}^{j} p^{r-n} + \sum_{n=j+n_i}^{j+n_i+m_{i+1}} p^{r-n} + \sum_{n=j+n_i+m_{i+1}+n_{i+1}}^{j+n_i+m_{i+1}+n_{i+1}+m_{i+2}} p^{r-n} + \ldots + \sum_{n=r-m_i+j+1}^{r} p^{r-n}.$$

Alors $b_{-j,i}$ *vérifie la congruence*

$$b_{-j,i}^{p^r} \equiv (-p)^{\mu_{i,j}}\ b_{-j,i} \mod p^{\mu_{i,j}+1}.$$

Il suffit de partir de la relation (3.2.2) si $j \neq 0$ (resp. (3.2.1) si $j = 0$), et d'appliquer le lemme précédent jusqu'à ce qu'on obtienne $(i',j') = (i,j)$.

Fixons (i,j), et posons $\mu = \mu_{i,j}$.

Lemme 3.5 : *Soit* $x \in A'$ *tel que* $x^q \equiv (-p)^{\mu}x \mod p^{\mu+1}$. *Alors il existe un unique* $x' \in \overline{A}$ *tel que* $x'^q = (-p)^{\mu}x'$ *et* $x' \equiv x \mod p$ ($\overline{A}$ *désignant l'anneau des entiers d'une clôture algébrique* $\overline{K}$ *de* K).

Posons $P(X) = X^q - (-p)^{\mu}X$. Par hypothèse, $P(x) = a$, avec $v(a) \geq \mu+1$, où v est la valuation p-adique normalisée par $v(p) = 1$. Si $x' = x+py$, il faut montrer qu'il existe un unique $y \in \overline{A}$ tel que $P(x+py) = 0$. Le développement de Taylor de $P(x+py)$ donne

$$P(x+py) = \sum_{i=0}^{q} (py)^i\ (i!)^{-1}\ P^{(i)}(x),$$

de sorte que y doit être racine du polynôme unitaire

$$Q(y) = \sum_{i=o}^{q} (p^{q-i}.i!)^{-1} P^{(i)}(x)\, y^i = \sum_{i=o}^{q} \alpha_{q-i}\, y^i.$$

Tout d'abord, le terme constant α_q est $p^{-q} P(x) = p^{-q}a$, d'où $v(\alpha_q)=v(a)-q$, donc

$$v(\alpha_q) \geq -q+\mu+1.$$

Le terme α_{q-1} est $q^{-q+1} P'(x)$, et $P'(x) = q\, x^{q-1} - (-p)^{\mu}$.

Comme $x^q - (-p)^{\mu}x - a = 0$, $v(x) \geq (q-1)^{-1}\mu$, d'où $v(x^{q-1}) \geq \mu$, et $v(P'(x)) = \mu$. Donc

$$v(\alpha_{q-1}) = -q+\mu+1,$$

et

$$v(\alpha_{q-1}) \leq v(\alpha_q).$$

Observons que μ est une somme de puissances de p, toutes distinctes et d'exposant strictement inférieur à r, de sorte que $\mu < q=p^r$; si $p=2$, G est unipotent, donc $m_i < r$, et μ est somme d'au plus r-1 puissances de p, si bien qu'on a pour tout p l'inégalité $\mu+1 < q$, d'où

$$v(\alpha_{q-1}) < 0.$$

Enfin, pour $i \geq 2$,

$$\begin{aligned} v(\alpha_{q-i}) &= v((p^{q-i}.i!)^{-1} P^{(i)}(x)) \\ &= v(p^{-q+i}(i!)^{-1}(q)!(q-i)!^{-1} x^{q-i}) \\ &= -q+i+v(\binom{q}{i}) + (q-i)v(x) \\ &\geq v(\binom{q}{i}) - q+i+(q-i)(q-1)^{-1}\mu \\ &\geq v(\binom{q}{i})-q+q(q-1)^{-1}\mu+(q-1)^{-1}(q-1-\mu)i. \end{aligned}$$

Or $v(\binom{q}{i}) \geq 1$, $q(q-1)^{-1}\,\mu > \mu$, $q-1-\mu > 0$, de sorte que

$$\forall\ i \geq 2 \qquad v(\alpha_{q-i}) > v(\alpha_{q-1}).$$

Le polygône de Newton de Q montre alors que Q possède une unique racine entière.

3.6. Rappelons (cf. [7]) qu'on définit un caractère

$$\theta_{q-1} : \mathcal{G} = \mathrm{Gal}(\overline{K}/K) \longrightarrow \mu_{q-1}(K) = \mu_{q-1}(A)$$

en choisissant $\zeta \in \overline{K}$ tel que $\zeta^{q-1} = p$, et en posant, pour $g \in \mathcal{G}$,

$$g(\zeta) = \theta_{q-1}(g).\zeta.$$

On notera $\overline{\theta}_{q-1}$ le composé de θ_{q-1} et de l'isomorphisme $\mu_{q-1}(A) \xrightarrow{\sim} \mu_{q-1}(k)$. Pour tout caractère fondamental $\chi_i : \mathbb{F}_q^* \xrightarrow{\sim} \mu_{q-1}(k)$, on notera $\psi_i : \mu_{q-1}(k) \longrightarrow \mathbb{F}_q^*$ son inverse ; on a donc

$$\psi_i^r = \psi_{i-1}.$$

<u>Proposition 3.7</u> : *Soit* $(y_i)_{i \in \mathbb{Z}/s}$ *une famille d'éléments de* $\mathcal{E}\mathcal{W}_K$ *vérifiant les conditions* (3.1.1) *à* (3.1.3). *Alors, pour tout* $g \in \mathcal{G}$,

$$g(y_i) = \theta_{q-1}(g)^{\mu_{i,o}} . y_i .$$

Montrons d'abord que pour tout i, et tout $j \leq m_i$,

$$(3.7.1) \qquad g(a_{-j,i}) = \overline{\theta}_{q-1}(g)^{\mu_{i,j}} . a_{-j,i} .$$

D'après 3.5, il existe une unique racine ξ de l'équation $X^q - (-p)^{\mu_{i,j}} X = 0$ dont la réduction modulo p est $a_{-j,i}$. Si $\xi \neq 0$, ξ est de la forme $u\zeta^{\mu_{i,j}}$, où u est une racine (q-1)-ième de $(-1)^{\mu_{i,j}}$ Comme k est algébriquement clos, $u \in W$, donc est invariant par $\mathcal{G}$, d'où l'assertion.

Observons alors que pour tout $j \leq r$

$$p^j \mu_{i,j} = \mu_{i,o} + \sum_{n=o}^{j-1} (p^{r+n} - p^n) = \mu_{i,o} + (p^r - 1) \left(\sum_{n=o}^{j-1} p^n \right).$$

Comme $(\theta_{q-1})^{q-1} = 1$, on en déduit que $(\theta_{q-1})^{\mu_{i,o}} = (\theta_{q-1})^{p^j \mu_{i,j}}$, d'où

$$(\overline{\theta}_{q-1})^{\mu_{i,j}} = (\overline{\theta}_{q-1})^{\mu_{i,o}/p^j} .$$

La relation (3.7.1) s'écrit donc

$$(3.7.2) \quad \forall\, i, \ \forall\, j \leq m_i, \ g(a_{-j,i}) = \overline{\theta}_{q-1}(g)^{\mu_{i,o}/p^j} . a_{-j,i} .$$

Si $j > m_i$, $a_{-j,i} = 0$, sauf dans le cas où G est de type multiplicatif, où $a_{-j,i} = a_{-j',i}$, j' étant le reste de la division de j par r ; comme $(\theta_{q-1})^q = \theta_{q-1}$, le relation (3.7.2) est donc vraie pour tout j'.

On obtient alors

$$g(y_i) = g((a_{-j,i})) = (\overline{\theta}_{q-1}(g)^{\mu_{i,o}/p^j} . a_{-j,i})$$

$$= \theta_{q-1}(g)^{\mu_{i,o}} . (a_{-j,i}) ,$$

car $\theta_{q-1}(g)$ est le vecteur $(\overline{\theta}_{q-1}(g), 0, \ldots, 0, \ldots)$ de W(k).

Théorème 3.8 : *Avec les notations de 3.6, l'action de* $\mathcal{G}$ *sur le* $\mathbb{F}_q$*-vectoriel de rang 1* $G_K(\overline{K})$ *se fait par le caractère* $\psi \circ \overline{\theta}_{q-1} : \mathcal{G} \longrightarrow \mathbb{F}_q^*$, *où* $\psi : \mu_{q-1}(k) \longrightarrow \mathbb{F}_q$ *est donné par*

$$\psi = \psi_{i_1} \circ \ldots \circ \psi_{i_d} ,$$

les indices $i_1, \ldots, i_d$ *étant ceux pour lesquels* $L_{\chi_i} \neq 0$.

En particulier, les exposants des caractères fondamentaux sont égaux à 0 ou 1 (cf. [6], th. 3.4.3).

Reprenant les notations de 3.1, la proposition précédente montre que pour $g \in \mathcal{G}$, $\varphi \in G_k(\overline{K})$,

$$\forall\, i \in \mathbb{Z}/s,\ g(\varphi(x_i)) = \theta_{q-1}(g)^{\mu_{i,o}}\ \varphi(x_i) = \varphi(\overline{\theta}_{q-1}(g)^{\mu_{i,o}}\, x_i).$$

Rappelons que $\mathbb{F}_q$ agit sur $x_i = e_{\alpha_i}$ par le caractère fondamental χ_{α_i}. Ecrivant

$$\overline{\theta}_{q-1}(g)^{\mu_{i,o}} = \chi_{\alpha_i} \circ \psi_{\alpha_i}(\overline{\theta}_{q-1}(g)^{\mu_{i,o}}) = \chi_{\alpha_i}(\psi_{\alpha_i}^{\mu_{i,o}} \circ \overline{\theta}_{q-1}(g)) ,$$

on obtient, en notant $(g, \varphi) \longrightarrow g.\varphi$ l'action de $\mathcal{G}$ sur $G_K(\overline{K})$, et $(\lambda, \varphi) \longmapsto [\lambda]\varphi$ celle de $\mathbb{F}_q$,

$$\begin{aligned}(g.\varphi)(x_i) = g(\varphi(x_i)) &= \varphi(\chi_{\alpha_i}(\psi_{\alpha_i}^{\mu_{i,o}} \circ \overline{\theta}_{q-1}(g)).x_i) \\ &= \varphi([\psi_{\alpha_i}^{\mu_{i,o}} \circ \overline{\theta}_{q-1}(g)]\ (x_i)) \\ &= ([\psi_{\alpha_i}^{\mu_{i,o}} \circ \overline{\theta}_{q-1}(g)]\ \varphi)\ (x_i).\end{aligned}$$

Or

$$\mu_{i,o} = \sum_{n=n_i+1}^{n_i+m_{i+1}} p^{r-n} + \ldots + \sum_{n=r-m_i+1}^{r} p^{r-n},$$

d'où

$$\begin{aligned}\psi_{\alpha_i}^{\mu_{i,o}} &= \Big(\prod_{n=n_i+1}^{n_i+m_{i+1}} \psi_{\alpha_i}^{p^{r-n}}\Big) \times \ldots \times \Big(\prod_{n=r-m_i+1}^{r} \psi_{\alpha_i}^{p^{r-n}}\Big) . \\ &= \Big(\prod_{n=n_i+1}^{n_i+m_{i+1}} \psi_{\alpha_i+n}\Big) \times \ldots \times \Big(\prod_{n=r-m_i+1}^{r} \psi_{\alpha_i+n}\Big) .\end{aligned}$$

D'après 2.8, ii), les indices $\alpha_i+n_i+1,\ldots,\alpha_i+n_i+m_{i+1} = \alpha_{i+1},\ldots,$ $\alpha_i-m_i+1,\ldots,\alpha_i$ sont précisément les indices $i_1,\ldots,i_d$ tels que $L_{\chi_i} \neq 0$. Posant $\Psi = \Psi_{i_1},\ldots,\Psi_{i_d}$, on obtient donc

$$\forall\, g \in G,\ \forall\, \varphi \in G_K(\overline{K}),\ \forall\, i \in \mathbb{Z}/s,\ (g.\varphi)(x_i) = \left([\Psi\circ\overline{\Theta}_{q-1}(g)].\varphi\right)(x_i).$$

Les x_i engendrant M comme D_k-module, $g.\varphi = [\Psi\circ\overline{\Theta}_{q-1}(g)]\varphi$, et $\mathcal{G}$ agit par le caractère $\Psi\circ\overline{\Theta}_{q-1}$.

BIBLIOGRAPHIE

[1] P. BERTHELOT : Cohomologie cristalline des schémas de caractéristique $p > 0$, Lecture Notes in Math., 407, Springer-Verlag.

[2] J.M. FONTAINE : Sur la construction du module de Dieudonné d'un groupe formel, C.R. Acad. Sc. Paris, t. 280, série A, p. 1273 (21 mai 1975).

[3] J.M. FONTAINE : Groupes p-divisibles sur les vecteurs de Witt, C.R. Acad. Sc. Paris, t. 280, série A, p. 1353 (26 mai 1975).

[4] J.M. FONTAINE : Groupes finis commutatifs sur les vecteurs de Witt, C.R. Acad. Sc. Paris, t. 280, série A, p. 1423 (2 juin 1975).

[5] A. GROTHENDIECK : Groupes de Barsotti-Tate et cristaux, Actes Congrès Intern. Math., 1970, t. 1, p. 431-436.

[6] M. RAYNAUD : Schémas en groupes de type $(p,\ldots,p)$, Bull. Soc. Math. France, 102, p. 241-280, (1974).

[7] J.P. SERRE : Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Inv. Math, 15, 259-331, (1972).