JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

MARTIN J. TAYLOR

Résolvandes et espaces homogènes principaux de schémas en groupe

Journal de Théorie des Nombres de Bordeaux, tome 2, n° 2 (1990), p. 255-271

<http://www.numdam.org/item?id=JTNB_1990__2_2_255_0>

Séminaire de Théorie des Nombres,
Bordeaux **2** *(1990), 255–271*

Résolvandes et espaces homogènes principaux de schémas en groupe.

par MARTIN J. TAYLOR

1. Introduction Soit $\mathfrak{O}$ un anneau de Dedekind de caractéristique zéro et soit K son corps de fractions. Nous notons $\mathfrak{X} = Spec(\mathfrak{O})$ et nous désignons par $\mathfrak{g} \in \mathfrak{X}$ le point générique de $\mathfrak{O}$. Une fois pour toutes nous choisissons une clôture algébrique $\overline{K}$ de K ; $\overline{\mathfrak{O}}$ désigne la clôture intégrale de $\mathfrak{O}$ dans $\overline{K}$.

Soient G un groupe fini abélien, A l'algèbre de groupe $K[G]$ et B désigne l'algèbre d'applications $Map(G, K)$. L'élément $\ell \in B$ est défini par la règle

$$\ell(g) = \begin{cases} 1 & \text{si } g = 1 \\ 0 & \text{sinon.} \end{cases} \tag{1}$$

Les algèbres A et B sont duales (au sens de Cartier) via l'accouplement naturel $<,>: A \times B \to K$. Soit $\mathfrak{B}$ un ordre de Hopf de B. (C'est-à-dire un ordre qui est stable par la comultiplication de B.) Alors nous désignons par $\mathfrak{A}$ le $\mathfrak{O}$-dual de $\mathfrak{B}$ par rapport à $<,>$; c'est un ordre de Hopf de A. Nous notons $A^0 = \mathrm{Spec}(\mathfrak{A})$, $B^0 = Spec(\mathfrak{B})$. On sait par la théorie des algèbres de Hopf (voir [S] par exemple) que $\mathfrak{B}$ est un $\mathfrak{A}$-module localement libre de rang un.

Soit C une algèbre galoisienne sur K avec $G = Gal(C/K)$. On dit qu'un $\mathfrak{O}$-ordre $\mathfrak{C}$ de C est une $\mathfrak{A}$-algèbre si $\mathfrak{C}$ est stable par l'action de $\mathfrak{A}$, i.e. $\mathfrak{C}\mathfrak{A} = \mathfrak{C}$. On appelle une telle $\mathfrak{A}$-algèbre $\mathfrak{C}$ un *espace homogène principal de* $\mathfrak{B}$ si il y a un isomorphisme d'anneaux

$$\xi : \mathfrak{C} \underset{\mathfrak{O}}{\otimes} \overline{\mathfrak{O}} \cong \mathfrak{B} \underset{\mathfrak{O}}{\otimes} \overline{\mathfrak{O}} \tag{2}$$

où ξ est de la forme $\xi(c \otimes \lambda)(g) = \tau(c^g)\lambda$ pour tout $g \in G$, pour une K-projection non-triviale $\tau : C \to \overline{K}$. Alors ξ est un homomorphisme de $(\mathfrak{A}, \overline{\mathfrak{O}})$ algèbres où $\mathfrak{A}$ agit sur les facteurs de gauche de (2), et $\overline{\mathfrak{O}}$ agit sur les facteurs de droite de (2).

Manuscrit reçu le 10 octobre 1989, révisé le 23 janvier 1990.

Nous notons l'ensemble de classes d'isomorphismes d'espaces homogènes principaux de $\mathfrak{B}$ par $PH(\mathfrak{B})$,

Remarque : Normalement (voir par exemple [W]) la condition (2) est remplacée par la condition équivalente

$$\mathfrak{C} \underset{\mathfrak{O}}{\otimes} \mathfrak{C} \cong \mathfrak{B} \underset{\mathfrak{O}}{\otimes} \mathfrak{C} . \tag{2'}$$

Il est évident que (2') implique (2). Par contre si (2) est vraie, on sait que $(\mathfrak{C} \otimes \overline{\mathfrak{O}}) \otimes \mathfrak{C} \cong (\mathfrak{B} \otimes \overline{\mathfrak{O}}) \otimes \mathfrak{C}$. Puisque C est une algèbre galoisienne on a l'isomorphisme $C \otimes C \cong B \otimes C$, et (2') en découle puisque $\overline{\mathfrak{O}}$ est fidèlement plat sur $\mathfrak{O}$.

Soit $\delta(G)$ le sous-groupe de $G \times G$ défini par

$$\delta(G) = \{(g, g^{-1}) \mid g \in G\}.$$

Si $\mathfrak{C}'$ est aussi un espace homogène principal de $\mathfrak{B}$, nous notons

$$\mathfrak{C}.\mathfrak{C}' = (\mathfrak{C} \underset{\mathfrak{O}}{\otimes} \mathfrak{C}')^{\delta(G)}.$$

On vérifie aisément que $\mathfrak{C}.\mathfrak{C}'$ est un espace homogène principal, et que $PH(\mathfrak{B})$, munie de cette opération, est un groupe. On sait d'ailleurs que ce groupe est paramétrisé par le groupe de cohomologie $H^1(\mathfrak{X}, B^0)$ (pour la topologie f.p.q.c.).

Nous considérons maintenant brièvement le cas élémentaire où $K = \mathfrak{O}$. Soit $\Omega = Gal(\overline{K}/K)$. Par la théorie de descente galoisienne (voir [Se]) , on sait que

$$\begin{aligned} PH(B) &\cong H^1(\Omega, Aut(B)) = H^1(\Omega, G) \\ &= \mathrm{Hom}(\Omega, G) \end{aligned} \tag{3}$$

Explicitement on associe à $\pi \in \mathrm{Hom}(\Omega, G)$ la G-algèbre $C = (\mathrm{Map}(G, \overline{K}))^{\Omega}$ où Ω opère sur G par π.

Nous revenons maintenant au cas général. Puisque $\overline{\mathfrak{O}}$ est fidèlement plat sur $\mathfrak{O}$, on déduit de (2) que l'application d'extension de scalaires $\otimes_{\mathfrak{O}} K$ est une injection

$$PH(\mathfrak{B}) \to PH(B) \tag{4}$$

Pour un espace homogène principal $\mathfrak{C}$ de $\mathfrak{B}$, nous disons que $\mathfrak{C}$ correspond à $\pi \in Hom(\Omega, G)$, si π est l'image de $\mathfrak{C}$ par la composition des homomorphismes (3) et (4).

Nous avons déjà vu que $\mathfrak{B}$ est localement libre comme $\mathfrak{A}$-module. Donc l'isomorphisme (2) implique que $\mathfrak{C}$ est localement libre sur $\mathfrak{A}$; nous notons $(\mathfrak{C})$ la classe de $\mathfrak{C}$ moins la classe de $\mathfrak{B}$ dans $C\ell(\mathfrak{A})$, le groupe de classes des $\mathfrak{A}$-modules localement libres.

Il est facile de vérifier (voir [W]) que l'application $\mathfrak{C} \to (\mathfrak{C})$ est un homomorphisme de groupes

$$\Psi : PH(\mathfrak{B}) \to C\ell(\mathfrak{A}). \tag{5}$$

Pour $c \in C$ nous écrivons

$$\underline{c} = \sum_{g \in G} c^g g^{-1} \in C[G] \tag{6}$$

On l'appelle la *résolvande* de c. On fait opérer Ω sur C[G] par son action naturelle sur les coefficients. On obtient la formule d'action galoisienne pour $\omega \in \Omega$

$$\begin{aligned} \underline{c}^{\omega} &= \sum c^{g\omega} g^{-1} = \sum c^{g\pi(\omega)} g^{-1} \\ &= \underline{c}\,\pi(\omega) \end{aligned} \tag{7}$$

où π est l'homomorphisme qui correspond à C.

Les deux buts principaux de cet article sont les suivants : on sait depuis longtemps que la théorie des résolvantes et résolvandes est extrêmement bien adaptée à la détermination de la structure galoisienne de nombreux modules arithmétiques ; notre premier but est de démontrer qu'elle est aussi bien adaptée à la théorie des espaces homogènes principaux d'ordres de Hopf. Le deuxième but est d'obtenir une description *algébrique* de Ker ψ ; ainsi nous obtenons une nouvelle démonstration des résultats de Susan Hurley (voir [H]).

Cette deuxième partie répond à une question de Mazur soulevée par les résultats de [ST], où l'on démontre que certains espaces homogènes principaux arithmétiques appartiennent au noyau de ψ. Puisque cette question est la raison principale de cette étude, nous décrivons ce résultat elliptique dans le cadre de cet article. Supposons maintenant que K est un corps de nombres et que E est une courbe elliptique, définie sur K, ayant partout bonne réduction, et à multiplication complexe par $\mathfrak{O}_F$, l'anneau d'entiers

d'un corps quadratique imaginaire F. Pour $\pi \in \mathfrak{O}_F$, $\pi \neq 0$, nous notons G le groupe de points de π division de E et nous supposons que $G \subseteq E(K)$, le groupe de K points de E. Soit $\mathfrak{B}$ l'ordre de Hopf de B tel que $\mathrm{Spec}(\mathfrak{B})$ coïncide avec le $\mathfrak{O}$ schéma en groupe associé à G. La suite de Kummer

$$0 \to G \to E(\overline{K}) \xrightarrow{\pi} E(\overline{K}) \to 0$$

donne une injection

$$\frac{E(K)}{\pi E(K)} \hookrightarrow PH(\mathfrak{B}).$$

En composant avec l'homomorphisme $PH(\mathfrak{B}) \xrightarrow{\psi} C\ell(\mathfrak{A})$ on obtient un homomorphisme

$$\psi' : E(K) \to C\ell(\mathfrak{A}).$$

Dans [ST] on démontre le résultat suivant

THÉORÈME. *Si w_F désigne le nombre de racines de l'unité de F, et si $(\pi, w_F) = 1$; alors le sous groupe $E(K)_{\mathrm{tors}}$ de points d'ordre fini dans $E(K)$ est contenu dans le noyau de ψ'.*

Nous avons maintenant besoin de quelques notations supplémentaires : nous notons

$$\tilde{\mathfrak{A}} = \prod_{\substack{\mathfrak{p} \in \mathfrak{X} \\ \mathfrak{p} \neq \mathfrak{g}}} \mathfrak{A}_{\mathfrak{p}}, \quad \mathbb{A}\mathfrak{A} = \tilde{\mathfrak{A}} \underset{\mathfrak{O}}{\otimes} K$$

c'est-à-dire que $\tilde{\mathfrak{A}}$ est l'anneau d'adèles entiers de $\mathfrak{A}$ et $\mathbb{A}\mathfrak{A}$ est l'anneau d'adèles de $\mathfrak{A}$. Nous notons $U(\mathfrak{A}), U(\tilde{\mathfrak{A}})$ le groupe des unités de $\mathfrak{A}, \tilde{\mathfrak{A}}$ etc. Le groupe $V(\tilde{\mathfrak{A}})$ est défini par

(8)

$$V(\tilde{\mathfrak{A}}) = \left\{ x \in U(\tilde{\mathfrak{A}} \underset{\mathfrak{O}}{\otimes} \overline{\mathfrak{O}}) \mid \exists \pi \in \mathrm{Hom}(\Omega, G) \text{ tel que } x^{\omega} = x\pi(\omega) \ \ \forall \omega \in \Omega \right\}$$

Avec cette notation, nous disons que x correspond à l'homomorphisme π. Evidemment $U(\tilde{\mathfrak{A}}) \subset V(\tilde{\mathfrak{A}})$: c'est le cas où π est l'homomorphisme trivial. Les groupes $V(A)$, $V(\mathbb{A}\mathfrak{A})$ etc sont définis de manière analogue.

Si $v \in V(\tilde{\mathfrak{A}})$ et si v correspond à l'homomorphisme $\pi : \Omega \to G$, on écrit $v = \Sigma v_g \ g^{-1}$; alors

$$\Sigma \ v_g g^{-1} \pi(\omega) = v \ \pi(\omega) = v^{\omega} = \Sigma v_g^{\omega} g^{-1}$$

on en conclut que

$$v_{g\pi(\omega)} = v_g^{\omega}. \tag{9}$$

Si π est une surjection, alors il est évident, grâce à (9), que v est une résolvande ; par contre, si π n'est pas une surjection, v n'est pas forcément une résolvande et on l'appelle une *résolvande généralisée*.

Nous terminons ce paragraphe avec la définition du groupe $W(A)$

$$W(A) = V(A) \cap (V(\tilde{\mathfrak{A}})U(\mathbb{A}\mathfrak{A})). \tag{10}$$

Il est clair que $W(A)$ contient $V(\mathfrak{A})U(A)$.

2. Résultats

THÉORÈME 1. *Il y a un isomorphisme naturel*

$$\theta : PH(\mathfrak{B}) \xrightarrow{\sim} \frac{W(A)}{U(A)}$$

et θ induit un isomorphisme

$$Ker\psi \cong \frac{V(\mathfrak{A})U(A)}{U(A)}.$$

Nous signalons que dans le cas où $\mathfrak{O}$ est local et G d'ordre premier, le groupe d'espaces homogènes principaux est déterminé dans [R].

Supposons maintenant que G est cyclique d'ordre n et que K contient μ_n, le groupe de racines de l'unité d'ordre n de $\overline{K}$. Soit χ un caractère fidèle de G et soit f l'idéal de $\mathfrak{O}$ engendré par les éléments $\chi(a)-\epsilon(a)$ pour $a \in \mathfrak{A}$; on appelle f le conducteur de $\mathfrak{A}$. Si $a \in V(\mathfrak{A})$, alors $(\chi(a)-\epsilon(a))\epsilon(a)^{-1} \in f\mathfrak{O}$; donc $\chi(a)^n\epsilon(a)^{-n}$ appartient au groupe $U_f = \mathfrak{O}^* \cap (1+f\mathfrak{O})^n$. Avec ces notations et ces hypothèses on a

THÉORÈME 2. *(a) L'application $a \to \chi(a^n)\epsilon(a^{-n})$ définie sur $V(\mathfrak{A})U(A)$, induit une injection*

$$\alpha_\chi : Ker\psi \hookrightarrow \frac{U_f K^{*n}}{K^{*n}}$$

(b) De plus, si n est premier et si K est un corps de nombres, alors α_χ est un isomorphisme et $U_f = (1+f^n) \cap \mathfrak{O}^*$.

La dernière partie du Théorème 2 est une conséquence immédiate des résultats de Susan Hurley obtenus dans [H] ; nos résolvandes nous donnent

une nouvelle perspective sur son résultat. Dans le cas où $\mathfrak{A}$ est l'ordre maximal (resp. $\mathfrak{O}[G]$) ce résultat est déjà obtenu dans l'article [CS] (resp. [C]).

Pour un idéal $\mathfrak{a}$ de $\mathfrak{O}$, $C\ell_{\mathfrak{a}}(\mathfrak{O})$ désigne le groupe des classes de rayon de conducteur $\mathfrak{a}$, et $C\ell_{\mathfrak{a}}(\mathfrak{O})_n$ est le sous-groupe des éléments qui sont annulés par n. Nous notons

$$\nu : C\ell_{f^n}(\mathfrak{O})_n \to C\ell_f(\mathfrak{O})_n$$

l'homomorphisme induit par la surjection naturelle

$$C\ell_{f^n}(\mathfrak{O}) \to C\ell_f(\mathfrak{O}).$$

Afin de mieux décrire $PH(\mathfrak{B})$ nous définissons le groupe

$$V_f = \{v \in K^* \mid v \in K_{\mathfrak{p}}^{*n}(1 + f^n\mathfrak{O}_{\mathfrak{p}}) \text{ pour tout } \mathfrak{p} \neq \mathfrak{g}\}.$$

Par le lemme 1 du prochain paragraphe, on sait que

$$U_f = (1 + f^p) \cap \mathfrak{O}^*$$

donc il est évident que $U_f \subset V_f$. Avec les hypothèses du Théorème 2(b) on a

THÉORÈME 3.

$$PH(\mathfrak{B}) \cong \frac{V_f}{K^{*n}}$$

et il y a une suite exacte

$$1 \to \frac{U_f K^{*n}}{K^{*n}} \underset{i}{\to} PH(\mathfrak{B}) \xrightarrow{\pi} Im(\nu) \to 1.$$

3. Démonstrations

Nous commençons la démonstration du théorème 1, en définissant l'homomorphisme θ. Comme on l'a déjà vu, pour chaque premier $\mathfrak{p} \in \mathfrak{X}$

$$\mathfrak{C}_{\mathfrak{p}} \cong \mathfrak{B}_{\mathfrak{p}} \cong \mathfrak{A}_{\mathfrak{p}} \text{ en tant que } \mathfrak{A}_{\mathfrak{p}} - \text{module.}$$

Soit $c_{\mathfrak{p}} \in \mathfrak{C}_{\mathfrak{p}}$ un générateur de $\mathfrak{C}_{\mathfrak{p}}$ sur $\mathfrak{A}_{\mathfrak{p}}$. Par [S] on sait que $\mathfrak{B}_{\mathfrak{p}}$ est $\mathfrak{A}_{\mathfrak{p}}$-libre sur $t_{\mathfrak{p}}\ell$ où

$$\mathfrak{B}_{\mathfrak{p}} \cap K_{\mathfrak{p}}\ell = t_{\mathfrak{p}}\ell.\mathfrak{O}_{\mathfrak{p}}$$

Grâce à (2), nous savons que $\xi(c_\mathfrak{p}) = t_\mathfrak{p}\ell v_\mathfrak{p}$ où $v_\mathfrak{p}$ est un élément de $U(\mathfrak{A}_\mathfrak{p} \otimes \mathfrak{O})$. En évaluant en les éléments de G, nous déduisons qu'avec la notation de (2)

$$t_\mathfrak{p} v_\mathfrak{p} = \underline{\xi(c_\mathfrak{p})}(1_G) = \sum \tau(c^g) g^{-1} \text{ et donc } v_\mathfrak{p} \in V(\mathfrak{A}_\mathfrak{p}).$$

Puisque $\ell v_\mathfrak{p}$ et $\ell v_\mathfrak{g}$ sont tous les deux des générateurs de $\xi(C) \otimes_K K_\mathfrak{p}$, sur $A_\mathfrak{p}$, on sait que $v_\mathfrak{g} \in v_\mathfrak{p} U(A_\mathfrak{p})$ pour chaque idéal maximal $\mathfrak{p}$ de $\mathfrak{O}$; de plus $v_\mathfrak{g} v_\mathfrak{p}^{-1}$ appartient à $U(\mathfrak{A}_\mathfrak{p})$ pour presque tout $\mathfrak{p}$; c'est-à-dire $v_\mathfrak{g} \in V(\tilde{\mathfrak{A}})\ U(\mathbb{A}\mathfrak{A})$.

Nous définissons $\theta(\mathfrak{C}) = v_\mathfrak{g} U(A)$. Il est facile de vérifier que $\theta(\mathfrak{C})$ est indépendant du choix de générateur $c_\mathfrak{g}$ de C. Si $\mathfrak{C}$(resp$\mathfrak{C}'$) correspond à l'homomorphisme π(resp π') dans $\mathrm{Hom}(\Omega, G)$; alors, grâce à (3) et (4), pour démontrer que θ est un homomorphisme, il suffit de remarquer que $v_\mathfrak{g} v'_\mathfrak{g}$ correspond à l'homomorphisme $\pi\ \pi'$.

Il est clair que $\theta(\mathfrak{C}) = 1 \Leftrightarrow v_\mathfrak{g} \in U(A) \Leftrightarrow \mathfrak{C}$ correspond à l'homomorphisme trivial $\pi = 1$; grâce à (3) et (4), ceci se passe si et seulement si $\mathfrak{C}$ est trivial (i.e. $\mathfrak{C} \cong \mathfrak{B}$). Donc on sait que θ est injectif. Finalement il nous faut démontrer que θ est surjectif ; c'est la partie centrale de la démonstration. Soit $v = \tilde{v}u$, où $\tilde{v} \in V(\tilde{\mathfrak{A}}), u \in U(\mathbb{A}\mathfrak{A})$. Pour chaque idéal maximal $\mathfrak{p}$ nous définissons

$$\mathfrak{C}_\mathfrak{p} = t_\mathfrak{p} \ell \tilde{v}_\mathfrak{p} \mathfrak{A}_\mathfrak{p}$$

où $\tilde{v}_\mathfrak{p}$ désigne la $\mathfrak{p}$-composante de $\tilde{v}$; de même on pose

$$C = \ell v A.$$

Il est évident que tous les $\mathfrak{C}_\mathfrak{p}$ sont $\mathfrak{A}_\mathfrak{p}$-stables ; de plus, puisque $\tilde{v}_\mathfrak{p} \in U(\mathfrak{A}_\mathfrak{p} \otimes \overline{\mathfrak{O}})$ (resp $v \in U(A \otimes \overline{K})$), on déduit que

$$\mathfrak{C}_\mathfrak{p} \otimes \overline{\mathfrak{O}} = t_\mathfrak{p} \ell \tilde{v}_\mathfrak{p} (\mathfrak{A}_\mathfrak{p} \otimes \overline{\mathfrak{O}}) = \mathfrak{B}_\mathfrak{p} \otimes \overline{\mathfrak{O}}$$

$$C \otimes \overline{K} = t_\mathfrak{g} \ell\ v(A \otimes \overline{K}) = B \otimes \overline{K}.$$

Donc, pour démontrer que $\mathfrak{C} = C \cap (\bigcap_\mathfrak{p} \mathfrak{C}_\mathfrak{p})$ est un espace homogène principal, il suffit de démontrer que $\mathfrak{C}$ est un anneau. Pour démontrer cela, nous définissons une nouvelle action de Ω sur $B \otimes \overline{K}$ par la règle

$$[\ell v(a \otimes \lambda)]^\omega = [\ell v(a \otimes \lambda^\omega)]$$

pour $a \in A$, $\lambda \in \overline{K}, \omega \in \Omega$.

Maintenant il nous faut démontrer que cette action respecte la multiplication de $B \otimes \overline{K}$. En utilisant le fait que $v = \tilde{v}u$, $u \in U(\mathfrak{A}\mathfrak{A})$, le même raisonnement montre que $\mathfrak{C}$ est l'anneau de Ω points fixes de $\mathfrak{B} \otimes \overline{\mathfrak{O}}$ muni de cette nouvelle action.

Par linéarité il suffit de démontrer que

$$[\ell v h]^{\omega}[\ell v h']^{\omega} = [\ell v h.\ \ell v h']^{\omega} \tag{11}$$

pour $h, h' \in G$. Nous écrivons $v = \Sigma v_g g^{-1}$, et nous savons par (9) que $v_{g\pi(\omega)} = v_g^{\omega}$. Par définition même de cette action :
$[\ell h v]^{\omega} = \ell v h$, $[\ell h' v]^{\omega} = \ell v h'$. De plus, en évaluant en les éléments G, on a l'identité

$$\ell(\Sigma a_g g^{-1})\ell(\Sigma b_g\ g^{-1}) = \ell(\Sigma a_g b_g g^{-1}) \tag{12}$$

Donc

$$\begin{aligned} [\ell v h]^{\omega}.[\ell v h']^{\omega} &= [\ell v h.\ell v h'] \\ &= [\ell(\Sigma v_{gh} v_{gh'} g^{-1})]. \end{aligned} \tag{13}$$

Ceci détermine le membre de gauche de (11) et aussi démontre que

$$\begin{aligned} [\ell v h.\ell v h']^{\omega} &= [\ell v.(v^{-\omega}\Sigma v_{gh}^{\omega} v_{gh'}^{\omega} g^{-1})] \\ &= [\ell.\pi(\omega)^{-1}(\Sigma v_{gh}^{\omega} v_{gh'}^{\omega} g^{-1})] \\ &= [\ell(\Sigma v_{gh\pi(\omega)^{-1}}^{\omega} v_{gh'\pi(\omega)^{-1}}^{\omega} g^{-1})] \\ \text{par(9)} \quad &= [\ell(\Sigma v_{gh} v_{gh'} g^{-1})] \\ \text{par(13)} \quad &= [\ell v h]^{\omega}[\ell v h']^{\omega}. \end{aligned}$$

□

Ceci achève la démonstration de la première partie du théorème 1.

On considère maintenant $\mathrm{Ker}\psi$. Par la théorie standard (voir par exemple [F]) on sait que

$$C\ell(\mathfrak{A}) \cong \frac{U(\mathfrak{A}\mathfrak{A})}{U(\tilde{\mathfrak{A}})U(A)} \tag{14}$$

et qu'avec la notation précédente la classe $(\mathfrak{C})$ est représentée par l'élément $v_g \tilde{v}^{-1} \in U(\mathfrak{A}\mathfrak{A})$. Donc $\mathfrak{C} \in Ker\psi \iff v_g \tilde{v}^{-1} \in U(\tilde{\mathfrak{A}})U(A) \iff v_g^{-1} u \in$

$V(\tilde{\mathfrak{A}})$ pour un élément $u \in U(A) \Longleftrightarrow v_g \in V(\mathfrak{A})U(A)$. Ainsi on a démontré que $\mathrm{Ker}\psi$ est isomorphe à $V(\mathfrak{A})U(A)/U(A)$ via θ.

□

Ensuite nous abordons la démonstration du théorème 2. Dorénavant nous supposons que G est d'ordre n et que K contient les racines n-ièmes de l'unité. Nous notons χ un caractère fidèle de G.

Soit $\mathfrak{C}$ un espace homogène principal de $\mathfrak{B}$ qui est isomorphe à $\mathfrak{B}$ en tant que $\mathfrak{A}$−module. Avec la notation du théorème 1 on sait que $\theta(\mathfrak{C}) = vU(A)$ avec $v \in V(\mathfrak{A})$ et $v^\omega = v\pi(\omega)$; d'où on déduit

$$\chi(v)^\omega = \chi(v)\chi(\pi(\omega)). \tag{15}$$

Puisque $\pi(\omega)^n = 1, v^n$ est fixe par Ω ; c'est-à-dire $v^n \in U(\mathfrak{A})$. Il découle de la définition de f que $\chi(v^n)\epsilon(v^n)^{-1} \in U_f$, et donc l'application $vU(A) \to \chi(v)K^*$ induit un homomorphisme

$$\alpha_\chi : \mathrm{Ker}\psi \cong \frac{V(\mathfrak{A})U(A)}{U(A)} \to \frac{U_f^{1/n}K^*}{K^*}.$$

Or, $\alpha_\chi(\mathfrak{C}) = 1 \Longleftrightarrow \chi(v) \in K^*$. Puisque χ est fidèle, ceci a lieu si et seulement si $\pi = 1$. En utilisant (3) et (4) on a démontré que $\alpha_\chi(\mathfrak{C}) = 1$ si et seulement si $\mathfrak{C}$ est trivial.

Finalement nous considérons la deuxième partie du théorème 2, et donc nous supposons maintenant que $n = p$ est un nombre premier.

Soit $u \in U_f^{1/p}$; notons c l'élément de $\overline{K}$

$$c = \frac{1}{p}\sum_{i=0}^{p-1} u^i = \frac{1}{p}.\frac{1-u^p}{1-u}.$$

Dans la suite on suppose $u \notin K^*$; alors u n'est pas une racine p-ième de l'unité, et donc $c \neq 0$.

Nous identifions $G \cong Gal(K(u)/K)$ de telle façon que l'on ait $u^g = u\chi(g)$ pour tout $g \in G$. Afin de démontrer que $u \in \mathrm{Im}(\alpha_\chi)$, il suffit de démontrer que la résolvande $\underline{c} \in V(\mathfrak{A})$, car on sait que

$$\begin{aligned} \chi^j(\underline{c}) &= \frac{1}{p}\sum_i \sum_g u^{ig}\chi^j(g^{-1}) \\ &= \frac{1}{p}\sum_i u^i \sum_g \chi^i(g)\chi^j(g^{-1}) \\ &= u^j \end{aligned} \tag{16}$$

pour $0 \leq j < p$.

Par définition $\underline{c}$ est une résolvande et, grâce à (16), on sait que $\underline{c}$ est une unité dans n'importe quel ordre de $K[G]$ qui la contient. On est donc ramené à démontrer

$$\underline{c} \in \mathfrak{A} \otimes \overline{\mathfrak{O}}. \tag{17}$$

Ainsi on se ramène tout de suite au cas local où K est une extension finie de $\mathbb{Q}_p$. Ceci nous permet d'utiliser le théorème de Tate-Oort de [TO] sur la classification de schémas en groupe de rang p.

Notons $\mathbb{F}_p$ le corps à p éléments et identifions $\mathbb{F}_p^*$ et $\mathrm{Aut}(G)$ de la façon naturelle. Soit $\alpha : \mathbb{F}_p^* \to K^*$ le caractère de Teichmüller ; c'est-à-dire

$$\varphi(a \bmod(p)) \equiv a \bmod p\mathfrak{O}.$$

Pour chaque entier $1 \leq i \leq p-1, e_i$ désigne l'idempotent associé à φ^i

$$e_i = \frac{1}{p-1} \sum_{a \in \mathbb{F}_p^*} \varphi^{-i}(a) a.$$

Une fois pour toutes nous choisissons un générateur g de G, et on définit $x_i = ge_i$. Tate et Oort montrent que

$$x_1^i = w_i x_i \text{ où } w_i \mathfrak{O} = i\mathfrak{O} \ (1 \leq i \leq p).$$

De plus ils montrent qu'il existe $b' \in \mathfrak{O}$ tel que $b = b'^{(p-1)}$ divise w_p (dans $\mathfrak{O}$) et que

$$\mathfrak{A} = \mathfrak{O}[x_1/a'] \tag{18}$$

où a' est une racine $p-1$-ième de $w_p b^{-1}$. On a la description équivalente de $\mathfrak{A}$

$$\mathfrak{A} \cong \frac{\mathfrak{O}[y]}{(y^p - by)}$$

pour un indéterminé y. Grâce à (18) on sait que

$$\mathfrak{A} = \mathfrak{O} + \sum_{i=1}^{p-1} \left(\frac{x_1}{a'}\right)^i \mathfrak{O}.$$

d'où l'on déduit que, pour démontrer (17), il suffit de vérifier que

$$(19)\qquad \left.\begin{aligned} &\underline{c}e_i \in \frac{1}{a'^i}\overline{\mathfrak{O}}[G] \quad 1 \le i < p-1 \\ &\underline{c}e_{p-1} \in \overline{\mathfrak{O}} + \frac{1}{a}\sum_{g\in G}(g-1). \end{aligned}\right\}$$

Puisque $x_1^p = w_p x_1$, on déduit facilement que

$$(20)\qquad \chi(x_1)\mathfrak{O} = (1-\zeta)\mathfrak{O}, \quad \text{où } \zeta = \chi(g).$$

De la description explicite de $\mathfrak{A}$ (18), on peut conclure que le conducteur f est

$$f = (1-\zeta)a'^{-1}\mathfrak{O} = b'\mathfrak{O}.$$

Le résultat suivant est valable dans le cas global comme dans le cas local.

LEMME 1. *Pour $f \supseteq (1-\zeta)\mathfrak{O}$ on a l'égalité $U_f = (1+f^p)\cap \mathfrak{O}^*$.*

DÉMONSTRATION. Soit $\delta \in f\overline{\mathfrak{O}}$. Alors, par la formule binôme $(1+\delta)^p \in 1 + f^p\overline{\mathfrak{O}}$, ce qui démontre l'inclusion $U_f \subset (1+f^p)\cap\mathfrak{O}^*$.

Réciproquement supposons que $1+\eta \in \overline{\mathfrak{O}}^*$ est tel que $(1+\eta)^p \in 1+f^p$; il nous faut démontrer $\eta \in f\overline{\mathfrak{O}}$. Encore une fois nous pouvons nous placer dans la situation locale. Nous notons v la valuation additive de $\mathfrak{O}$. Supposons que $v(1-\zeta) = b, v(f) = a$; donc par hypothèse $a \le b$. On peut en fait supposer que $a > 0$; donc $c = v(\eta) > 0$ et $v(\sum_{i=1}^{p-1}\binom{p}{i}\eta^i) = v(p\eta)$. Puisque $v((1+\eta)^p - 1) \ge pa$, on sait que

soit $v(p\eta) > v(\eta^p)$, d'où $pa \le v(\eta^p)$ et donc $v(\eta) \ge a$,

soit $v(\eta^p) \ge v(p\eta)$, d'où $(p-1)v(\eta) \ge v(p) = (p-1)b \ge (p-1)a$. □

Supposons que $u^p \in U_f$; alors on peut écrire u de la forme $u = 1+\beta$, avec $\beta \in b'\overline{\mathfrak{O}}$. Avant de démontrer (19), nous démontrons

PROPOSITION.

(a) $\displaystyle\sum_{k=0}^{p-1} u^k \in b\overline{\mathfrak{O}}$

(b) *pour* $1 \le j \le p-1$, $\displaystyle\sum_{k=1}^{p-1} u^k\varphi^{-j}(k) \in b'^j\overline{\mathfrak{O}}$.

Il est intéressant de remarquer que la démonstration du résultat (b) remonte à la détermination algébrique par Kronecker des sommes de Gauss.

DÉMONSTRATION. Traitons d'abord la partie (a). Puisque $b' | (1-\zeta)$, nous savons que

$$\sum_{k=0}^{p-1} u^k = \frac{1-u^p}{1-u} = \frac{1-(1+\beta)^p}{-\beta} \in \beta^{p-1}\overline{\mathfrak{O}} \subseteq b\overline{\mathfrak{O}}.$$

Considérons maintenant (b). De la définition du caractère φ on déduit la congruence mod $p\overline{\mathfrak{O}}$

$$\sum_{k=1}^{p-1} u^k \varphi^{-j}(k) \equiv \sum_{1}^{p-1} u^k k^{p-1-j} \equiv \sum_{1}^{p-1} (1+\beta)^k k^{p-1-j}$$
$$\equiv \sum_{k=1}^{p-1} \sum_{n=0}^{k} \binom{k}{n} \beta^n k^{p-1-j}.$$

Nous notons $P_n(x)$ le polynôme $\frac{x(x-1)\ldots(x-n-1)}{n!}$, et nous remarquons que $P_n(m) = 0$ pour $0 \leq m \leq n$. Donc

$$\sum_{k=1}^{p-1} u^k \varphi^{-j}(k) \equiv \sum_{k=1}^{p-1} \sum_{n=0}^{p-1} P_n(k) \beta^n k^{p-1-j}$$
$$\equiv \sum_{n=0}^{p-1} \beta^n \sum_{k=1}^{p-1} P_n(k) k^{p-1-j} \tag{21}$$

Puisque $P_n(x)$ est de degré n, il est clair que (pour n croissant) la somme

$$\sum_{1}^{p-1} P_n(k) k^{p-1-j} \bmod p\overline{\mathfrak{O}}$$

est non nulle pour la première fois lorsque $n = j$. Ceci démontre que le membre de gauche de (21) est divisible par b'^j. □

Il est maintenant facile de terminer la démonstration de (19) à l'aide de la proposition.

Parce que

$$\underline{c} = \sum_{m=0}^{p-1} c^{g^m} g^{-m} = (\sum_{m} c^{g^m}) + (\sum_{m} c^{g^m}(g^{-m}-1))$$
$$= 1 + \sum_{m=0}^{p-1} c^{g^m}(g^{-m}-1),$$

nous sommes amenés à considérer

$$\sum_{m=0}^{p-1} c^{g^m}(g^{-m}-1)e_j = \sum_{m=0}^{p-1}\sum_{n=1}^{p-1} \tfrac{1}{p-1}.c^{g^m}(g^{-mn}-1)\varphi^{-j}(n)$$

$$= \tfrac{1}{p(p-1)} \sum_{k=0}^{p-1}\sum_{m=0}^{p-1}\sum_{n=1}^{p-1} u^{k.g^m}(g^{-mn}-1)\varphi^{-j}(n).$$

En substituant $r = mn$ (dans $\mathbb{F}_p^*$) et en tenant compte de la relation $u^g = u\zeta$, on a l'égalité

$$(22) \qquad \sum_{m=0}^{p-1} c^{g^m}(g^{-m}-1)e_j$$

$$= \frac{1}{p(p-1)} \sum_{k=0}^{p-1} \sum_{m,r\in\mathbb{F}_p^*} u^k \zeta^{mk} \varphi^{-j}(rm^{-1})(g^{-r}-1)$$

Premier cas : $j = p-1$. On obtient

$$\tfrac{1}{p(p-1)} \sum_{k=0}^{p-1} u^k \left(\textstyle\sum_{m=1}^{p-1} \zeta^{mk}\right) \cdot \left(\sum_{r=1}^{p-1}(g^{-r}-1)\right)$$

$$= \tfrac{1}{p(p-1)} \left(p-1-\sum_{k=1}^{p-1} u^k\right) \left(\sum_{r=1}^{p-1}(g^{-r}-1)\right)$$

$$= \tfrac{1}{p(p-1)} \left(p-\sum_{k=0}^{p-1} u^k\right) \left(\sum_{r=1}^{p-1}(g^{-r}-1)\right)$$

et ce cas de (19) découle de la partie (a) de la proposition et de l'égalité $\mathfrak{D}ab = p\mathfrak{D}$.

Deuxième cas : $1 \leq i < p-1$. Cette fois-ci nous avons l'égalité

$$\sum_{0}^{p-1} c^{g^m}(g^{-m}-1)e_j = \frac{1}{p(p-1)} \sum_{r=1}^{p-1}(g^{-r}-1)\left[\sum_{k=0}^{p-1} u^k \sum_{m=1}^{p-1} \zeta^{mk}\varphi^{-j}(rm^{-1})\right]$$

$$= \frac{1}{p(p-1)} \sum_{r=1}^{p-1} \varphi^{-j}(r)(g^{-r}-1)\left[\sum_{k=1}^{p-1} u^k \varphi^{-j}(k) \sum_{m=1}^{p-1} \zeta^m \varphi^j(m)\right]$$

On en déduit qu'il suffit de vérifier que

$$\frac{1}{p}\left(\sum_{k=1}^{p-1} u^k \varphi^{-j}(k)\right)\left(\sum_{m=1}^{p-1} \zeta^m \varphi^j(m)\right) \in a'^{-j}\overline{\mathfrak{D}}$$

Grâce à la proposition, avec $u = \zeta$,

$$\sum_{1}^{p-1} \zeta^m \varphi^j(m) \in (1-\zeta)^{p-1-j}\mathfrak{O}.$$

En utilisant la partie (b) de la proposition encore une fois, nous pouvons enfin déduire que

$$\frac{1}{p}\left(\sum_{k=1}^{p-1} u^k \varphi^{-j}(k)\right)\left(\sum_{m=1}^{p-1} \zeta^m \varphi^j(m)\right) \in b'^j(1-\zeta)^{-j}\overline{\mathfrak{O}}$$
$$= a'^{-j}\overline{\mathfrak{O}} \qquad \square$$

Il reste à démontrer le théorème 3. Nous gardons toutes les notations précédentes, et nous étendons l'isomorphisme α_χ du théorème 2 à

$$\beta_\chi : PH(\mathfrak{B}) \to \frac{V_f}{K^{*p}}$$

par le composé

$$PH(\mathfrak{B}) \cong \frac{W(A)}{U(A)} \xrightarrow{\theta} \frac{V_f}{K^{*p}}$$

où θ est induit par l'application $w \longmapsto \chi(w)^p$. Le raisonnement déjà utilisé pour montrer que α_χ est injectif démontre que θ, et donc β_χ, est aussi injectif.

Nous voulons maintenant démontrer que β_χ est surjectif. Soit $v \in V_f$, et désormais nous excluons le cas trivial $v \in K^{*p}$. Pour un idéal maximal $\mathfrak{p}$ de $\mathfrak{O}$, on sait, par définition même, que v s'écrit de la forme

$$v = x_\mathfrak{p}^p u_\mathfrak{p} \text{ pour } x_\mathfrak{p} \in K_\mathfrak{p}^*,\ u_\mathfrak{p} \in (1 + f^p\mathfrak{O}_\mathfrak{p})$$

et donc on peut toujours choisir $x_\mathfrak{p} = 1$ pour presque tous les premiers $\mathfrak{p}$. Nous posons

$$z = \frac{1}{p}\sum_{0}^{p-1} v^{i/p} \qquad c_\mathfrak{p} = \frac{1}{p}\sum_{0}^{p-1} u_\mathfrak{p}^{1/p}.$$

Afin de démontrer la surjectivité de β_χ, il suffit de démontrer que la résolvande $\underline{z} \in W(A)$. Pour $0 \leq i \leq p-1$, nous notons $e(i)$ l'idempotent de A associé

au caractère χ^i. Alors

$$\begin{aligned}\underline{z} &= \frac{1}{p}\sum_g \left(\sum_i v^{i/p}\right)^g g^{-1} = \sum_i v^{i/p} e(i) \\ &= \sum_i x_{\mathfrak{p}}^i u_{\mathfrak{p}}^{i/p} e(i) \\ &= \left(\sum_i x_{\mathfrak{p}}^i e(i)\right)\left(\sum_i u_{\mathfrak{p}}^{i/p} e(i)\right) \\ &= \left(\sum_i x_{\mathfrak{p}}^i e(i)\right)\underline{c}_{\mathfrak{p}}.\end{aligned}$$

Or, dans la démonstration du théorème 2 on a déjà vu que $\underline{c}_{\mathfrak{p}} \in V(\mathfrak{A}_{\mathfrak{p}})$, et il est clair que $\Sigma\, x_{\mathfrak{p}}^i e(i) \in A_{\mathfrak{p}}^*$; donc $z \in W(A)$.

La définition de l'homomorphisme π utilisé dans l'énoncé du théorème 3 dépend du résultat suivant

LEMME 2. *Pour $v \in V_f$, il existe un idéal $\mathfrak{a}$ de $\mathfrak{O}$ tel que $v^{1/p}\overline{\mathfrak{O}} = \mathfrak{a}\overline{\mathfrak{O}}$.*

DÉMONSTRATION. On se ramène tout de suite au cas local et l'on suppose que v correspond par β_χ à $\mathfrak{C} \in PH(\mathfrak{B})$. Par la théorie standard (voir [S]) on sait qu'il existe $t \in \mathfrak{O}$ tel que $\mathfrak{B} = \ell t.\mathfrak{A}$. Donc, si $\mathfrak{C} = y\mathfrak{A}$, alors pour (2) on sait que $y = \ell t.a$ pour $a \in (\mathfrak{A} \otimes \overline{\mathfrak{O}})^*$. En considérant les résolvandes et en appliquant le caractère χ, on conclut que $\chi(\underline{y}) = tu$ pour $u \in \overline{\mathfrak{O}}^*$. Mais par la construction même de $v, v^{1/p} = \chi(\underline{y})x$ par $x \in K^*$. Ceci démontre que $v^{1/p}\overline{\mathfrak{O}} = x\chi(\underline{y})\overline{\mathfrak{O}} = xt\overline{\mathfrak{O}}$. □

Pour un élément $v \in V_f$, on sait par le théorème d'approximation faible que l'on peut toujours choisir $v' \in V_{f'}$ dans la même classe de V_f/K^{*^p} tel que $v \in 1 + f^p\mathfrak{O}_{\mathfrak{p}}$ pour tout $\mathfrak{p}|f$. Dans la suite nous supposerons que tous les représentants choisis, des classes de V_f/K^{*^p}, satisfont cette condition. L'homomorphisme $\pi : PH(\mathfrak{B}) \to \mathrm{Im}(\nu)$ est défini comme suit : pour $\mathfrak{C} \in PH(\mathfrak{B})$ on choisit $v \in \beta_\chi(\underline{\mathfrak{C}})$, et puis $\pi(\mathfrak{C})$ est la classe dans $C\ell_f(\mathfrak{O})$ de l'idéal $\mathfrak{a}$ de $\mathfrak{O}$ tel que $v^{1/p} = \mathfrak{a}\mathfrak{O}$. Puisque $\mathfrak{a}^p = v\mathfrak{O}$ et $v \in 1+f^p\mathfrak{O}_{\mathfrak{p}}$ pour $\mathfrak{p}|f$, il est évident que la classe de $\mathfrak{a}^p$ est triviale dans $C\ell_{f^p}(\mathfrak{O})$. De plus, si v' est un autre représentant de $\beta_\chi(\mathfrak{C})$, alors $v' = v\lambda$ pour $\lambda \in K^{*^p}$ et $\lambda \in (1+f^p\mathfrak{O}_{\mathfrak{p}})$ pour tout $\mathfrak{p}|f$; grâce au lemme 1 on sait que $\lambda^{1/p} \in (1+f\mathfrak{O}_{\mathfrak{p}})$ pour tout $p|f$ et donc la classe de $\mathfrak{a}$ dans $C\ell_f(\mathfrak{O})$ ne change pas.

Il nous reste à démontrer que la suite est exacte.

$\mathrm{Im}(i) \subset \mathrm{Ker}(\pi)$: Si $u \in U_f$, alors $\pi(uK^{*p}) =$ classe $(\mathfrak{a})$ où $u^{1/p}\overline{\mathfrak{O}} = \mathfrak{a}\overline{\mathfrak{O}}$. C'est-à-dire $\mathfrak{a} = \mathfrak{O}$, et donc $\pi(uK^{*p})$ est la classe triviale.

$\mathrm{Ker}(\pi) \subset \mathrm{Im}(i)$: Supposons que l'élément $v \in V_f$ est tel que $\pi(vK^{*p}) = \underline{1}$. Ceci implique qu'il existe $x \in K^*$ avec $x \equiv 1 \bmod f$ tel que $v^{1/p}x.\overline{\mathfrak{O}} = \overline{\mathfrak{O}}$; donc $vx^pK^{*p} \subset U_fK^{*p}$.

ν est surjectif : Supposons que l'idéal $\mathfrak{a}$ est premier avec p et qu'il représente une classe de $\mathrm{Im}(\nu)$. Par définition même $\mathfrak{a}^p = v\mathfrak{O}$ pour $v \in K^*$ tel que $v \equiv 1 \bmod f^p$. Alors $v^{1/p} \equiv 1 \bmod f\overline{\mathfrak{O}}$ (voir le lemme 1). Puisque toutes les K-valuations de v sont divisibles par p, on déduit que $v \in V_f$ et de plus $\pi(v) = \mathfrak{a}$, parce que $\mathfrak{a}\overline{\mathfrak{O}} = v^{1/p}\overline{\mathfrak{O}}$. □

BIBLIOGRAPHIE

[C] L. N. CHILDS, *The group of unramified Kummer extensions of prime degree*, Proc. L.M.S. **35(3)** (1977), 407-422.

[CS] S. CHASE and M. SWEEDLER,, *Hopf algebras and Galois theory*, SLN **97**. Springer-Verlag, New-York, Berlin (1969).

[F] A. FRÖHLICH, *Galois module structure of algebraic integers*, Springer Ergebnisse **3**. Folge, Band **1**, (1983).

[H] S. HURLEY, *Galois objects with normal bases for free Hopf algebras of prime degree*, J. of Algebra **109**, (1987), 292-318.

[R] L. ROBERTS, *On the flat cohomology of finite groupe schemes*, Harvard thesis (1968).

[Se] J.-P. SERRE, *Cohomologie galoisienne*, Lecture Notes in Mathematics N°5, Springer Verlag (1966).

[ST] A. SRIVASTAV and M.J. TAYLOR, *Elliptic curves with complex multiplication and Galois module structure*, Invent. Math. **99** (1990), 165–184.

[S] M. SWEEDLER, *Hopf Algebras*, Benjamin, New-York, (1969).

[TO] J. TATE and F. OORT, *Group schemes of prime order*, Ann. Scient. Ec. Norm. Sup. **4e série, tome 3** (1970), 1-21.

[W] W.C. WATERHOUSE *Principal homogeneous spaces and group scheme extensions*, Trans. Amer. Math. Soc. **153** (1971), 181-189.

Department of Mathematics
UMIST, P.O. Box 88
Manchester M60 1QD
U.K.