TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 148, April 1970

SUR LE RELEVEMENT DES REPRESENTATIONS MODULAIRES D'UN GROUPE FINI

PAR
FRANÇOIS ARIBAUD

Soit A un anneau local de caractéristique 0, d'idéal maximal $\mathfrak{m}$ et de corps résiduel $k=A/\mathfrak{m}$; on supposera que k est de caractéristique $p\neq 0$. Soit G un groupe fini; on appellera *représentation modulaire de* G une représentation de G dans un k-espace vectoriel de dimension finie. Soit V un A-module libre de dimension finie; toute représentation de G dans V définit par passage au quotient modulo $\mathfrak{m}$ une représentation modulaire dont le k-espace vectoriel sous-jacent est $V/\mathfrak{m}V$; on dira que cette représentation modulaire est *la représentation modulaire déduite de la représentation de G dans V par réduction modulo* $\mathfrak{m}$. Mais une représentation modulaire de G n'est pas nécessairement obtenue par réduction modulo $\mathfrak{m}$ à partir d'une représentation de G à coefficients dans A; nous dirons qu'une représentation modulaire ρ de G admet *un relèvement* P si ρ est la représentation déduite de P par réduction modulo $\mathfrak{m}$. Dans ce qui suit nous nous proposons de construire un "système d'obstructions cohomologiques" pour le relèvement d'une représentation modulaire: si ρ est une représentation de G dans un k-espace vectoriel W, on définit par récurrence des "classes caractéristiques", la $s$ième classe étant un élément de $H^2(G, \mathrm{Hom}_k(W, \mathfrak{m}^s/\mathfrak{m}^{s+1}\otimes_k W))$.

Je tiens à remercier M. le Professeur Chevalley pour les indications qu'il m'a données, en particulier sur le rôle joué par certains systèmes de facteurs.

1. Une description du groupe $H^2(G, \mathrm{Hom}(M, N))$, [3].

DEFINITION 1. *Soient R un anneau commutatif unitaire, G un groupe, M et N deux $R[G]$-modules. Un homomorphisme croisé de M dans N est une application $\alpha: G\times G\to \mathrm{Hom}_R(M, N)$ telle que pour tous $s, t, u\in G$ et $m\in M$ on ait*

$$\alpha(s, tu)(m)+s(\alpha(t, u)(m)) = \alpha(st, u)(m)+\alpha(s, t)(um).$$

LEMME 1. *Les notations étant celles de la Définition* 1, *soit a une application de G dans $\mathrm{Hom}_R(M, N)$. L'application δa de $G\times G$ dans $\mathrm{Hom}_R(M, N)$ qui est définie par*

$$\delta a(s, t)(m) = s(a(t)(m))+a(s)(tm)-a(st)(m)$$

est un homomorphisme croisé de M dans N.

Received by the editors October 17, 1968 and, in revised form, July 7, 1969.
Copyright © 1970, American Mathematical Society

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

On a

$$\delta a(s, tu)(m) = s(a(tu)(m)) + a(s)(tum) - a(stu)(m)$$

et

$$s(\delta a(t, u)(m)) = st(a(u)(m)) + s(a(t)(um)) - s(a(tu)(m)),$$

d'où

$$\delta a(s, tu)(m) + s(\delta a(t, u)(m)) = a(s)(tum) + st(a(u)(m)) + s(a(t)(um)) - a(stu)(m).$$

D'autre part

$$\delta a(st, u)(m) = st(a(u)(m)) + a(st)(um) - a(stu)(m)$$

et

$$\delta a(s, t)(um) = s(a(t)(um)) + a(s)(tum) - a(st)(um),$$

d'où

$$\delta a(st, u)(m) + \delta a(s, t)(um) = a(s)(tum) + st(a(u)(m)) + s(a(t)(um)) - a(stu)(m).$$

Finalement

$$\delta a(s, tu)(m) + s(\delta a(t, u)(m)) = \delta a(st, u)(m) + \delta a(s, t)(um). \qquad \text{Q.E.D.}$$

DEFINITION 2. *Soient R un anneau commutatif unitaire, G un groupe, M et N deux $R[G]$-modules. On appelle homomorphisme croisé principal de M dans N un homomorphisme croisé de la forme δa, où a est une application de G dans* $\mathrm{Hom}_R(M, N)$.

Les homomorphismes croisés principaux de M dans N forment un sous-R-module $P\,\mathrm{hom}_R(G; M, N)$ du R-module $X\,\mathrm{hom}_R(G; M, N)$ des homomorphismes croisés de M dans N. Le R-module quotient

$$X_R(G; M, N) = X\,\mathrm{hom}_R(G; M, N)/P\,\mathrm{hom}_R(G; M, N)$$

sera appelé *le module des classes d'homomorphismes croisés de M dans N.*

Comme M et N sont des G-modules, on peut faire opérer G sur $\mathrm{Hom}_R(M, N)$ en définissant pour tout $g \in G$ et tout $f \in \mathrm{Hom}_R(M, N)$ gf comme l'application, $m \mapsto gf(g^{-1}m)$.

Un système de facteurs de G à valeurs dans $\mathrm{Hom}_R(M, N)$ est une application h de $G \times G$ dans $\mathrm{Hom}_R(M, N)$ telle que pour tous $s, t, u \in G$ on ait

$$sh(t, u) - h(st, u) + h(s, tu) - h(s, t) = 0,$$

i.e. telle que pour tout $m \in M$ on ait dans N

$$s(h(t, u)(s^{-1}m)) - h(st, u)(m) + h(s, tu)(m) - h(s, t)(m) = 0.$$

Considérons alors l'application $h^*\colon G \times G \to \mathrm{Hom}_R(M, N)$ définie par

$$h^*(s, t)(m) = h(s, t)(stm)$$

pour tous $s, t \in G$ et $m \in M$.

PROPOSITION 1. *L'application $h \mapsto h^*$ réalise un isomorphisme du R-module des systèmes de facteurs de G à valeurs dans* $\mathrm{Hom}_R(M, N)$ *sur le R-module des homomorphismes croisés de M dans N. Cet isomorphisme définit un isomorphisme de $H^2(G, \mathrm{Hom}_R(M, N))$ sur $X_R(G; M, N)$.*

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

Soit h un système de facteurs. Pour tous $s, t, u \in G$ et $m \in M$ on a

$$\begin{aligned} h^*(s, tu)(m) &= h(s, tu)(stum) \\ s(h^*(t, u)(m)) = s(h(t, u)(tum)) &= s(h(t, u)(s^{-1}stum)) = sh(t, u)(stum) \\ h^*(st, u)(m) &= h(st, u)(stum) \\ h^*(s, t)(um) &= h(s, t)(stum). \end{aligned}$$

D'où

$$\begin{aligned} h^*(s, tu)(m)+s(h^*(t, u)(m))-h^*(st, u)(m)-h^*(s, t)(um) \\ = h(s, tu)(stum)+sh(t, u)(stum)-h(st, u)(stum)-h(s, t)(stum) \\ = [h(s, tu)+sh(t, u)-h(st, u)-h(s, t)](stum). \end{aligned}$$

Dire que h est un système de facteurs revient à dire que l'application linéaire du second membre est nulle. Par suite h^* satisfait à l'identité de définition des homomorphismes croisés de M dans N.

D'autre part, si α est un homomorphisme croisé de M dans N, le même calcul montre que l'application α' de $G \times G$ dans $\mathrm{Hom}_R(M, N)$ définie par

$$\alpha'(s, t)(m) = \alpha(s, t)(t^{-1}s^{-1}m)$$

est un système de facteurs de G à valeurs dans $\mathrm{Hom}_R(M, N)$. Or il est immédiat que l'application $\alpha \mapsto \alpha'$ est l'application inverse de $h \mapsto h^*$. Comme l'application $h \mapsto h^*$ est R-linéaire, cette application est un isomorphisme R-linéaire du R-module des systèmes ce facteurs sur le R-module des homomorphismes croisés de M dans N.

Soit $h(s, t) = sf(t)+f(s)-f(st)$ un système de facteurs principal de G à valeurs dans $\mathrm{Hom}_R(M, N)$, f étant donc une application de G dans $\mathrm{Hom}_R(M, N)$. On a

$$\begin{aligned} h^*(s, t)(m) &= sf(t)(stm)+f(s)(stm)-f(st)(stm) \\ &= s(f(t)(tm))+f(s)(stm)-f(st)(stm). \end{aligned}$$

Si a est l'application de G dans $\mathrm{Hom}_R(M, N)$ définie par

$$a(s)(m) = f(s)(sm)$$

pour tout $s \in G$ et tout $m \in M$, on a

$$\begin{aligned} h^*(s, t)(m) &= s(a(t)(m))+a(s)(tm)-a(st)(m) \\ &= \delta a(s, t)(m) \end{aligned}$$

dans les notations du Lemme 1.

Réciproquement soit $\alpha = \delta a$ un homomorphisme croisé principal de M dans N. Le système de facteurs α' associé est défini par

$$\begin{aligned} \alpha'(s, t)(m) &= \alpha(s, t)(t^{-1}s^{-1}m) = \delta a(s, t)(t^{-1}s^{-1}m) \\ &= s(a(t)(t^{-1}s^{-1}m))+a(s)(s^{-1}m)-a(st)(t^{-1}s^{-1}m). \end{aligned}$$

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

Si l'on pose $f(s)(m)=a(s)(s^{-1}m)$, on a

$$\begin{aligned}\alpha'(s,t)(m) &= s(f(t)(s^{-1}m))+f(s)(m)-f(st)(m)\\ &= sf(t)(m)+f(s)(m)-f(st)(m)\end{aligned}$$

et $\alpha'(s,t)$ est un système de facteurs principal. Par suite l'isomorphisme $h \mapsto h^*$ définit un isomorphisme du sous-module des systèmes de facteurs principaux sur le sous-module des homomorphismes croisés principaux. Par passage au quotient cet isomorphisme définit ensuite un isomorphisme de $H^2(G, \mathrm{Hom}_R(M,N))$ sur $X_R(G; M, N)$. Q.E.D.

2. **Relèvement des représentations modulaires.** Soient toujours R un anneau commutatif unitaire et G un groupe. On désigne par $\mathfrak{a}$ un idéal de carré nul de R, par V un R-module libre de dimension finie et par $\overline{V}$ le $R/\mathfrak{a}$-module libre $V/\mathfrak{a}V$; l'application canonique de V dans $\overline{V}$ sera notée π. Si ρ est une représentation de G dans $\overline{V}$, on peut trouver pour tout $g \in G$ une application R-linéaire $P(g)$ de V dans V telle que le diagramme

$$\begin{array}{ccc} V & \xrightarrow{P(g)} & V \\ \pi\downarrow & & \downarrow\pi \\ \overline{V} & \xrightarrow{\rho(g)} & \overline{V} \end{array}$$

soit commutatif. On dira que *les $P(g)$ forment un système de représentants de ρ dans V.*

Lemme 2. *Chaque $P(g)$ conserve $\mathfrak{a}V$, et la famille des restrictions des $P(g)$ à $\mathfrak{a}V$ est une représentation de G dans $\mathfrak{a}V$. Cette représentation ne dépend pas du choix du système de représentants $P(g)$ de ρ dans V; elle est équivalente au produit tensoriel sur $R/\mathfrak{a}$ de la représentation identique de G dans $\mathfrak{a}$ et de la représentation ρ.*

Comme les $P(g)$ sont R-linéaires, ils conservent $\mathfrak{a}V$. Si $m \in V$ et si $s, t \in G$, on a $\pi(P(s)P(t)(m))=\rho(s)\rho(t)(\pi(m))=\pi(P(st)(m))$, et $P(s)P(t)(m)-P(st)(m) \in \mathfrak{a}V$. Comme les $P(g)$ sont R-linéaires, on a $P(s)P(t)(p)-P(st)(p) \in \mathfrak{a}(\mathfrak{a}V)=\mathfrak{a}^2V=0$, $\mathfrak{a}$ étant de carré nul, pour tout $p \in \mathfrak{a}V$; autrement dit pour tout $p \in \mathfrak{a}V$ et tous $s, t \in G$ on a $P(s)P(t)(p)=P(st)(p)$. Soit $P'(g)$ un deuxième système de représentants de ρ dans V; pour tout $s \in G$ et tout $m \in V$ on a $\pi(P(s)(m))=\pi(P'(s)(m))$ et $P(s)(m)-P'(s)(m) \in \mathfrak{a}V$; par suite, si $p \in \mathfrak{a}V$, $P(s)(p)-P'(s)(p) \in \mathfrak{a}^2V=0$, soit $P(s)(p)=P'(s)(p)$. En particulier il existe un relèvement P' de ρ tel que $P'(e)=\mathrm{id}$; pour tout relèvement P de ρ et pour tout $p \in \mathfrak{a}V$ on a, si e est l'élément neutre de G, $P(e)(p)=P'(e)(p)=p$, ce qui achève de montrer que tout relèvement de ρ définit une représentation de G dans $\mathfrak{a}V$.

Comme $\mathfrak{a}$ est de carré nul, la structure d'idéal de $\mathfrak{a}$ définit une structure de $R/\mathfrak{a}$-module sur $\mathfrak{a}$. On peut remplacer la représentation ρ par une représentation par des matrices carrées (d'ordre n) $(a_i^j(g))$ équivalente. On obtient alors un

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

relèvement de cette représentation en considérant des matrices $(b_i^j(g))$ à coefficients dans A telles que $\pi(b_i^j(g))=a_i^j(g)$. Comme $V=A^n$, $\mathfrak{a}V$ s'identifie au sous-module $\mathfrak{a}^{xn}$ de V des éléments dont toutes les coordonnées appartiennent à $\mathfrak{a}$. Pour un élément $x=(x^i)$ de $\mathfrak{a}^{xn}$ on a

$$P(g)(x) = \left(\sum b_i^j(g)x^i\right).$$

Mais

$$\sum b_i^j(g)x^i = \sum a_i^j(g)x^i$$

la deuxième expression étant calculée au moyen de la structure de $R/\mathfrak{a}$-module de $\mathfrak{a}$. Mais les expressions

$$(x^i) \mapsto \left(\sum a_i^j(g)x^i\right)$$

définissent la représentation de G dans $\mathfrak{a}^{xn}$ produit tensoriel de la représentation identique de G dans $\mathfrak{a}$ et de la représentation $(a_i^j(g))$ de G dans k^n. Q.E.D.

LEMME 3. *Soient $s, t \in G$ et $m \in V$. L'élément*

$$r(s, t; m) = P(s)P(t)(m)-P(st)(m)$$

appartient à $\mathfrak{a}V$ et ne dépend que de la classe de m dans $\overline{V}$. Par passage à $\overline{V}=V/\mathfrak{a}V$ l'application $m \mapsto r(s, t; m)$ définit un homomorphisme croisé α du $(R/\mathfrak{a}, G)$-module $\overline{V}$ dans le $(R/\mathfrak{a}, G)$-module $\mathfrak{a}V$. La classe de α dans le module $X_{R/\mathfrak{a}}(G; \overline{V}, \mathfrak{a}V)$ des classes d'homomorphismes croisés de $\overline{V}$ dans $\mathfrak{a}V$ est indépendante du choix du système de représentants de ρ dans V.

On a déjà montré au cours de la démonstration du Lemme 2 que pour tout $m \in V$ et tous $s, t \in G$ l'élément $r(s, t; m)$ appartient à $\mathfrak{a}V$ et que $r(s, t; m)=0$ si $m \in \mathfrak{a}V$. Comme $r(s, t; m)$ est R-linéaire en m, l'application $m \mapsto r(s, t; m)$ se factorise en une application linéaire de $\overline{V}$ dans $\mathfrak{a}V$ que l'on notera $\alpha(s, t; ?)$. Soient $m \in V$ et $s, t, u \in G$. On a

$$\begin{aligned} r(s, tu; m) &= P(s)P(tu)(m)-P(stu)(m) \\ P(s)r(t, u; m) &= P(s)[P(t)P(u)(m)-P(tu)(m)] \\ &= P(s)P(t)P(u)(m)-P(s)P(tu)(m) \\ r(st, u; m) &= P(st)P(u)(m)-P(stu)(m) \\ r(s, t; P(u)(m)) &= P(s)P(t)P(u)(m)-P(st)P(u)(m) \end{aligned}$$

d'où

$$\begin{aligned} r(s, tu; m)+P(s)r(t, u; m) &= P(s)P(t)P(u)(m)-P(stu)(m) \\ &= r(st, u; m)+r(s, t; P(u)(m)). \end{aligned}$$

Si μ est la classe de m dans $\overline{V}$, la classe de $P(u)(m)$ dans $\overline{V}$ est égale à $\rho(u)\mu$; d'autre part la définition de la représentation de G dans $\mathfrak{a}V$ montre que $P(s)r(t, u; m) = s\alpha(t, u; \mu)$. Finalement on a

$$\alpha(s, tu; \mu)+s\alpha(t, u; \mu) = \alpha(st, u; \mu)+\alpha(s, t; u\mu),$$

et α est un homomorphisme croisé de $\overline{V}$ dans $\mathfrak{a}V$.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

Soit $P'(g)$ un deuxième système de représentants de ρ dans V et posons $v(t; m) = P'(t)(m) - P(t)(m)$ pour $t \in G$ et $m \in M$. On a vu au cours de la démonstration du Lemme 2 que $v(t; m) \in \mathfrak{a}V$ et que $v(t; m) = 0$ si $m \in \mathfrak{a}V$. Pour tout $t \in G$ l'application qui à m associe $v(t; m)$ est R-linéaire et elle se factorise par une application de $\overline{V}$ dans $\mathfrak{a}V$ que l'on notera $a(t; ?)$. Si $r'(s, t; m) = P'(s)P'(t)(m) - P'(st)(m)$ on a

$$\begin{aligned} r'(s, t; m) &= P'(s)[P(t)(m) + v(t; m)] - P(st)(m) - v(st; m) \\ &= P(s)P(t)(m) + P(s)v(t; m) + v(s; P(t)(m)) + v(s; v(t; m)) \\ &\quad - P(st)(m) - v(st; m). \end{aligned}$$

Or $P(s)P(t)(m) - P(st)(m) = r(s, t; m)$; si μ est la classe de m dans $\overline{V}$, $P(s)v(t; m) = sa(t; \mu)$ et $v(s; P(t)(m)) = a(s; t\mu)$; d'autre part, comme $v(t; m) \in \mathfrak{a}V$, $v(s; v(t; m)) = 0$. Finalement, si β est l'homomorphisme croisé associé à r', on a

$$\begin{aligned} \beta(s, t; \mu) &= \alpha(s, t; \mu) + sa(t; \mu) + a(s; t\mu) - a(st; \mu) \\ &= \alpha(s, t; \mu) + \delta a(s, t; \mu). \end{aligned}$$ Q.E.D.

D'après la Proposition 1 du paragraphe 1 on peut identifier canoniquement $X_{R/\mathfrak{a}}(G; \overline{V}, \mathfrak{a}V)$ à $H^2(G, \mathrm{Hom}_{R/\mathfrak{a}}(\overline{V}, \mathfrak{a}V))$.

DEFINITION 3. *Les notations étant celles du Lemme* 3, *l'élément de*

$$H^2(G, \mathrm{Hom}_{R/\mathfrak{a}}(\overline{V}, \mathfrak{a}V))$$

image de la classe de α *dans* $X_{R/\mathfrak{a}}(G; \overline{V}, \mathfrak{a}V)$ *par l'isomorphisme canonique est appelé la classe caractéristique de la représentation* ρ *de* G *dans* $\overline{V}$.

On dira qu'*une représentation* ρ *de* G *dans* $\overline{V}$ *admet un relèvement* s'il existe un système de représentants $P(g)$ de ρ dans V tel que $g \mapsto P(g)$ soit une représentation de G dans V.

LEMME 4. *Soient* L *un anneau,* $\mathfrak{n}$ *un idéal bilatère de* L *contenu dans le radical de* L, V *un* L*-module libre de dimension finie et* e *un projecteur de* V. *On suppose que*

$$e \otimes 1 \colon V/\mathfrak{n}V = V \otimes_L L/\mathfrak{n} \to V \otimes_L L/\mathfrak{n} = V/\mathfrak{n}V$$

est le projecteur identique. Alors e *est le projecteur identique.*

Comme e est un projecteur on a

$$0 = \mathrm{Im}\,((1-e) \otimes 1) = \mathrm{Im}\,(1-e) \otimes_L L/\mathfrak{n}.$$

Comme $\mathfrak{n}$ est contenu dans le radical, on a d'après le lemme de Nakayama $\mathrm{Im}\,(1-e) = 0$. Par suite $x - e(x) = 0$ pour tout $x \in V$, i.e. $x = e(x)$. Q.E.D.

PROPOSITION 2. *Soient* R *un anneau commutatif,* $\mathfrak{a}$ *un idéal de carré nul de* R *contenu dans le radical de* R, V *un* R*-module libre de dimension finie et* G *un groupe. Pour qu'une représentation* ρ *de* G *dans* $\overline{V} = V/\mathfrak{a}V$ *admette un relèvement, il faut et il suffit que la classe caractéristique de* ρ *soit nulle.*

La condition est nécessaire: si $P(g)$ est un système de représentants tel que $g \mapsto P(g)$ soit une représentation de G, on a pour tout $m \in V$ et tous $s, t \in G$, $r(s, t; m) = P(s)P(t)(m) - P(st)(m) = 0$.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

La condition est suffisante: soit ρ une représentation de G dans $\overline{V}$ dont la classe caractéristique est nulle; on choisira un système $P(g)$ de représentants de ρ dans V et on posera, pour tout $m \in V$ et tous $s, t \in G$, $r(s, t; m) = P(s)P(t)(m) - P(st)(m)$. Par hypothèse il existe pour tout $t \in G$ une application R-linéaire $\mu \mapsto a(t; \mu)$ de $\overline{V}$ dans $\mathfrak{a}V$ telle que, si α est l'homomorphisme croisé de $\overline{V}$ dans $\mathfrak{a}V$ associé à $r(s, t; m)$, $\alpha(s, t; \mu) = \delta a(s, t; \mu)$ pour tout $\mu \in \overline{V}$ et tous $s, t \in G$. Soit $v(t; ?)$ l'application R-linéaire de V dans $\mathfrak{a}V$ définie par $v(t; m) = a(t; \pi(m))$, où π est l'application canonique de V sur $\overline{V}$; comme $r(s, t; m) = \alpha(s, t; \pi(m))$ on a

$$r(s, t; m) = sv(t; m) + v(s; P(t)(m)) - v(st; m) \tag{1}$$

pour tout $m \in V$ et tous $s, t \in G$. Posons $P'(g)(m) = P(g)(m) - v(g; m)$; on a (cf. la démonstration du Lemme 3)

$$\begin{aligned} P(s)P(t)(m) - P(st)(m) = {} & P'(s)P'(t)(m) - P'(st)(m) + P'(s)(v(t; m)) \\ & + v(s; P'(t)(m)) + v(s; v(t; m)) - v(st; m). \end{aligned}$$

D'après le Lemme 2, P et P' définissent la même représentation de G dans $\mathfrak{a}V$; on a ainsi $P'(s)(v(t; m)) = sv(t; m)$. Comme $v(t; m) \in \mathfrak{a}V$, $v(s; v(t; m)) = 0$. D'autre part $v(s; P'(t)(m)) = a(s; t\pi(m)) = v(s; P(t)(m))$. Finalement, d'après (1), $P(s)P(t)(m) - P(st)(m) = P'(s)P'(t)(m) - P'(st)(m) + P(s)P(t)(m) - P(st)(m)$, et $P'(s)P'(t)(m) = P'(st)(m)$ quels que soient $m \in V$ et $s, t \in G$. En particulier si e est l'identité de G, $P'(e)$ est un projecteur de V. Comme dans $V/\mathfrak{a}V$ on a $P'(e) \otimes 1 = \rho(e) = \mathrm{id}$, le Lemme 4 montre que $P'(e) = \mathrm{id}$. La famille des $P'(g)$ est donc un relèvement de ρ. Q.E.D.

Soient A un anneau local séparé complet de caractéristique 0, d'idéal maximal $\mathfrak{m}$ et de corps résiduel k; on supposera que k est de caractéristique $p \neq 0$. Soient V un A-module libre de dimension finie et $\overline{V}$ le k-espace vectoriel $V/\mathfrak{m}V$; on désignera par $\pi_{m,n}$ $(m \geqq n)$ l'application canonique de $V/\mathfrak{m}^m V$ sur $V/\mathfrak{m}^n V$; comme A est séparé complet, V est la limite projective du système $(V/\mathfrak{m}^n V, \pi_{m,n})$. Le lemme suivant ne fait que traduire les propriétés fonctorielles de la limite projective:

LEMME 5. *Soit ρ une représentation de G dans $\overline{V}$. On suppose qu'il existe une suite ρ_q de représentations de G dans les $A/\mathfrak{m}^q$-modules $V/\mathfrak{m}^q V$ telle que ρ_q soit un relèvement de ρ_{q-1}*

$$\begin{array}{ccc} V/\mathfrak{m}^q V & \xrightarrow{\rho_q(g)} & V/\mathfrak{m}^q V \\ \Big\downarrow{\scriptstyle \pi_{q,q-1}} & & \Big\downarrow{\scriptstyle \pi_{q,q-1}} \\ V/\mathfrak{m}^{q-1} V & \xrightarrow{\rho_{q-1}(g)} & V/\mathfrak{m}^{q-1} V. \end{array}$$

Alors ρ admet un relèvement dans V.

La famille des $\rho_q(g)$, pour $g \in G$ fixé, définit un endomorphisme du système projectif $(V/\mathfrak{m}^n V, \pi_{m,n})$. Il lui correspond donc un endomorphisme $P(g)$ de la

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

limite projective V du système, et $g \mapsto P(g)$ est une représentation de G dans V en vertu du caractère fonctoriel de la limite projective. Q.E.D.

Le Lemme 5 ramène la construction d'un relèvement d'une représentation de G dans $\overline{V}$ en une représentation de G dans V à une succession de constructions de relèvements de $V/\mathfrak{m}^{q-1}V$ à $V/\mathfrak{m}^qV$. Comme l'idéal $\mathfrak{m}^{q-1}/\mathfrak{m}^q$ de $A/\mathfrak{m}^q$ est de carré nul, on peut utiliser les constructions du début du paragraphe pour effectuer ces relèvements. En particulier la donnée d'une représentation de G dans $V/\mathfrak{m}^qV$ définit une représentation de G dans $\overline{V}_q = \mathfrak{m}^qV/\mathfrak{m}^{q+1}V$; cette représentation s'obtient en faisant le produit tensoriel sur $A/\mathfrak{m}^{q+1}$ de la représentation triviale de G dans $\mathfrak{m}^q/\mathfrak{m}^{q+1}$ et de la représentation donnée ρ_q de G dans $V/\mathfrak{m}^qV$; cette représentation n'est donc autre que le produit tensoriel sur le corps résiduel $k = A/\mathfrak{m}$ de la représentation triviale de G dans $\mathfrak{m}^q/\mathfrak{m}^{q+1}$ et de la représentation ρ de G dans $\overline{V} = V/\mathfrak{m}V$ déduite de ρ_q par réduction modulo $\mathfrak{m}$. Toute application A-linéaire de $V/\mathfrak{m}^qV$ dans $\mathfrak{m}^qV/\mathfrak{m}^{q+1}V$ s'annule sur $\mathfrak{m}V/\mathfrak{m}^qV$ et définit par passage au quotient une application k-linéaire de $\overline{V} = V/\mathfrak{m}V$ dans $\overline{V}_q = \mathfrak{m}^qV/\mathfrak{m}^{q+1}V$; on a ainsi un isomorphisme de (k, G)-modules de $\mathrm{Hom}_A(V/\mathfrak{m}^qV, \overline{V}_q)$ sur

$$\mathrm{Hom}_k(\overline{V}, \overline{V}) \otimes_k \mathfrak{m}^q/\mathfrak{m}^{q+1}.$$

Si ρ est une représentation de G dans le k-espace vectoriel $\overline{V} = V/\mathfrak{m}V$ qui admet un relèvement ρ_q dans le $A/\mathfrak{m}^q$-module libre $V/\mathfrak{m}^qV$, l'obstruction au relèvement de ρ_q au $A/\mathfrak{m}^{q+1}$-module libre $V/\mathfrak{m}^{q+1}V$ est un élément de

$$H^2(G, \mathrm{Hom}_k(\overline{V}, \overline{V}) \otimes_k \mathfrak{m}^q/\mathfrak{m}^{q+1}),$$

la structure de G-module de $\mathrm{Hom}_k(\overline{V}, \overline{V})$ *étant définie à partir de la représentation ρ.*

Supposons maintenant que le groupe G soit fini. Soit G_p un p-sous-groupe de Sylow de G, où p est la caractéristique du corps résiduel $k = A/\mathfrak{m}$ de A. Si ρ est une représentation de G dans un A-module M, on dira que la représentation σ de G_p dans M définie par $\sigma(g) = \rho(g)$ pour tout $g \in G_p$ est *la restriction de ρ à G_p.*

PROPOSITION 3. *On conserve les notations de l'alinéa précédent. Pour qu'une représentation de G dans $V/\mathfrak{m}^qV$ admette un relèvement dans $V/\mathfrak{m}^{q+1}V$, il faut et il suffit que la représentation de G_p dans $V/\mathfrak{m}^qV$ obtenue par restriction admette un relèvement dans $V/\mathfrak{m}^{q+1}V$.*

La condition est évidemment nécessaire. Soit ρ_q une représentation de G dans $V/\mathfrak{m}^qV$ et soit $P_{q+1}(g)$ un système de représentants de ρ_q dans $V/\mathfrak{m}^{q+1}V$. Les $P_{q+1}(g)$, $g \in G_p$, forment un système de représentants de la restriction de ρ_q à G_p. Il en résulte que la classe caractéristique de la restriction de ρ_q à G_p est l'image par l'homomorphisme canonique

$$\mathrm{Res}_p : H^2(G, \mathrm{Hom}_k(\overline{V}, \overline{V}) \otimes_k \mathfrak{m}^q/\mathfrak{m}^{q+1}) \to H^2(G_p, \mathrm{Hom}_k(\overline{V}, \overline{V}) \otimes_k \mathfrak{m}^q/\mathfrak{m}^{q+1})$$

de la classe caractéristique de ρ_q. Comme $\mathrm{Hom}_k(\overline{V}, \overline{V}) \otimes \mathfrak{m}^q/\mathfrak{m}^{q+1}$ est annulé par p, il résulte d'un théorème classique sur la cohomologie des groupes (cf. par

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

exemple [2, Chapitre IX, §2, Théorème 4]) que Res_p est injectif. Si la restriction de ρ_q à G_p admet un relèvement, sa classe caractéristique est nulle; par suite la classe caractéristique de ρ_q est nulle et, d'après la Proposition 2, ρ_q admet un relèvement dans $V/\mathfrak{m}^{q+1}V$. Q.E.D.

COROLLAIRE 1. *Soit ρ une représentation de G dans $V/\mathfrak{m}V$. On suppose que le G_p-module obtenu par restriction de ρ à G_p est induit. La représentation ρ admet un relèvement à V.*

D'après le Lemme 5 il suffit de montrer que tout relèvement ρ_q de ρ à $V/\mathfrak{m}^qV$ admet un relèvement à $V/\mathfrak{m}^{q+1}V$; d'après la proposition précédente il suffit de montrer que la restriction σ_q de ρ_q à G_p admet un tel relèvement. La classe caractéristique de σ_q est un élément de $H^2(G_p, \mathrm{Hom}_k(\overline{V}, \overline{V}) \otimes_k \mathfrak{m}^q/\mathfrak{m}^{q+1})$. Comme $\overline{V}$ est un G_p-module induit, la Proposition 1 du §3 du Chapitre IX de [2] montre que le G_p-module $\mathrm{Hom}_k(\overline{V}, \overline{V}) \otimes \mathfrak{m}^q/\mathfrak{m}^{q+1}$ est induit; le groupe de cohomologie correspondant est donc nul. Comme la classe caractéristique de σ_q est ainsi nulle, σ_q admet un relèvement. Q.E.D.

COROLLAIRE 2. *Supposons que p ne divise pas l'ordre de G. Toute représentation de G dans $V/\mathfrak{m}V$ admet un relèvement à V.*

Comme G_p est réduit à l'élément neutre, le G_p-module $V/\mathfrak{m}V$ est induit. Q.E.D.

COROLLAIRE 3. *Soit ρ une représentation de G dans $V/\mathfrak{m}V$ qui fait de $V/\mathfrak{m}V$ un $k[G]$-module indécomposable principal. La représentation ρ admet un relèvement dans V.*

(Cet énoncé est une variante du classique "relèvement des idempotents".)

D'après un théorème de Green (cf. [1, §65, Théorème 65-16]) le $k[G_p]$-module $V/\mathfrak{m}V$ obtenu par restriction est libre. Le corollaire est donc une conséquence du Corollaire 1. Q.E.D.

REFERENCES

1. C. Curtis et I. Reiner, *Representation theory of finite groups and associative algebras*, Pure and Appl. Math., Vol. 11, Interscience, New York, 1962. MR **26** #2519.

2. J.-P. Serre, *Corps locaux*, Actualités Sci. Indust., no. 1296, Hermann, Paris, 1962. MR 27 #133.

3. S. Takahashi, *Arithmetic of group representations*, Tôhoku Math. J. **11** (1959), 216–246. MR **22** #733.

UNIVERSITÉ DE CLERMONT-FERRAND,
CLERMONT-FERRAND, FRANCE

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use