Les Classes de Chern Modulo p d'une Représentation Régulière

Bruno Kahn

Received: May 25, 1999

Communicated by Ulf Rehmann

Abstract. Let G be a finite group and ρ a complex linear representation of G. In 1961, Atiyah and Venkov independently defined Chern classes $c_i(\rho)$ with values in the integral or mod p cohomology of G. We consider here the mod p Chern classes of the regular representation r_G of G. Venkov claimed that $c_i(r_G) = 0$ for $i < p^n - p^{n-1}$, where p^n is the highest power of p dividing $|G|$; however his proof is only valid for G elementary abelian. In this note, we show Venkov's assertion is valid for any G. The proof also shows that the $c_i(r_G)$ are p-powers of cohomology classes invariant by $Aut(G)$ as soon as G is a non-abelian p-group.

1991 Mathematics Subject Classification: 20J06, 20C15
Keywords and Phrases: Finite groups, Chern classes, regular representation

Introduction

Soient G un groupe fini et ρ une représentation linéaire complexe de G. La définition des classes de Chern de ρ est généralement attribuée à Atiyah [1, appendice]. Toutefois, ces classes ont également été introduites par B.B. Venkov dans une note contemporaine [16].

Venkov annonce dans cette note un certain nombre de résultats[1]. En particulier, soit r_G la représentation régulière de G. Venkov [16] annonce le théorème suivant:

0.1. Théorème. *Soit p un nombre premier, et soit $\nu = v_p(|G|)$. Alors les classes de Chern $c_i(r_G) \in H^{2i}(G, \mathbb{Z}/p)$ de r_G à coefficients $\mathbb{Z}/p$ sont nulles pour $i < p^\nu$, sauf peut-être si i est de la forme $p^\nu - p^l$ pour un $l < \nu$.*

[1] Certains sont manifestement erronés, comme celui affirmant que les classes de Chern de ρ et son degré déterminent la classe de ρ dans $R(G)$.

Son esquisse de démonstration ne donne malheureusement le résultat annoncé que dans le cas où G est abélien élémentaire. Dans cet article, nous nous proposons de démontrer le théorème annoncé par Venkov. La méthode est inspirée de [7].

Je remercie Don Zagier pour son aide dans la démonstration du lemme 1.3 et le referee pour sa lecture soigneuse du manuscrit.

1. Classes de Chern modulo p d'un fibré vectoriel complexe

Soit E un fibré vectoriel complexe sur un espace topologique X, et soit p un nombre premier. Pour tout $i \geq 0$, on note $c_i(E) \in H^{2i}(X, \mathbb{Z}/p)$ la i-ème classe de Chern modulo p de E.

1.1. Théorème. *Supposons que $c_i(E) = 0$ pour $i \not\equiv 0 \pmod{p-1}$. Si les $c_i(E)$ ne sont pas tous nuls, il existe $\nu > 0$ tel que*

(i) *pour $i < p^\nu - p^{\nu-1}$, $c_i(E) = 0$; $c_{p^\nu - p^{\nu-1}}(E) \neq 0$.*

(ii) *$\mathcal{P}^k c_{p^\nu - p^{\nu-1}}(E) = \binom{p^\nu - p^{\nu-1} - 1}{k} c_{p^\nu - p^{\nu-1} + (p-1)k}(E)$ pour $0 < k < p^{\nu-1}$, où $\mathcal{P}^k$ est la k-ième puissance de Steenrod ($\mathcal{P}^k = Sq^{2k}$ si $p = 2$);*

(iii) *pour $p^\nu - p^{\nu-1} \leq i < p^\nu$, $c_i(E) = 0$ si i n'est pas de la forme $p^\nu - p^r$ $(r < \nu)$.*

Démonstration. Elle procède essentiellement comme dans [7, dém. de la prop. 1.1]. Pour simplifier, notons $c_i = c_i(E)$; soit M le plus petit entier tel qu $c_M \neq 0$. D'après [11, th. 2] (voir aussi [8]), on a

$$\mathcal{P}^k c_i = \binom{i-1}{k} c_{i+(p-1)k} + \sum_{0 \leq l < (p-1)k} c_{i+l} P_l(c)$$

où $P_l(c)$ est un polynôme en les c_j isobare de poids $(p-1)k - l$, donc ne faisant intervenir c_j que pour $j \leq (p-1)k$. On a donc, pour $i < M$:

$$\binom{i-1}{k} c_{i+(p-1)k} = 0 \quad \text{pour} \quad 0 < k < \frac{M}{(p-1)}$$

et pour $i = M$:

$$\mathcal{P}^k c_M = \binom{M-1}{k} c_{M+(p-1)k} \quad \text{pour} \quad 0 < k < \frac{M}{(p-1)}.$$

Notons $C_i = c_{(p-1)i}$. Sous l'hypothèse du théorème, on a $M = (p-1)m$ pour un m convenable. Les relations ci-dessus donnent alors:

$$\binom{i(p-1)-1}{k} C_{i+k} = 0 \quad \text{pour} \quad 0 < i < m \quad \text{et} \quad 0 < k < m \tag{1}$$

et

$$\mathcal{P}^k C_m = \binom{m(p-1)-1}{k} C_{m+k} \quad \text{pour} \quad 0 < k < m. \tag{2}$$

Prenant en particulier $i = m - k$ dans (1), on obtient:

$$\binom{(m-k)(p-1)-1}{k} \equiv 0 \pmod{p} \quad \text{pour} \quad 0 < k < m. \tag{3}$$

1.2. LEMME. *Tout entier m vérifiant la condition* (3) *est une puissance de p.*

DÉMONSTRATION. Écrivons $m = m_0 p^n$, avec $(m_0, p) = 1$. Supposons $m_0 > 1$. Choisissons $k = p^n$ dans (3). En écrivant dans $\mathbb{F}_p[[t]]$

$$(1+t)^{p^n(m_0-1)(p-1)-1} = (1+t^{p^n})^{(m_0-1)(p-1)}(1-t+t^2-\dots)$$

on voit que le coefficient de t^{p^n} dans $(1+t)^{p^r(m_0-1)(p-1)-1}$ est $(m_0-1)(p-1)+(-1)^{p^n}$. Par hypothèse, on a donc:

$$(m_0-1)(p-1)+(-1)^{p^n} \equiv 0 \pmod p$$

ou encore

$$m_0 \equiv 1+(-1)^{p^n} \equiv 0 \pmod p$$

ce qui contredit l'hypothèse. On a donc $m_0 = 1$ et $m = p^n$. □

Dans le théorème 1.1, (i) résulte du lemme 1.2 et (ii) résulte de (i) et de (2). Pour voir (iii), soit $j \le 2p^n - 2$ tel que $C_j \neq 0$. En vertu de (1), on a alors:

$$\binom{(j-k)(p-1)-1}{k} \equiv 0 \pmod p \quad \text{pour} \quad j - p^n < k < p^n. \tag{4}$$

il suffit donc de prouver:

1.3. LEMME. *Tout $j \in [p^n, p^n + p^{n-1} + \dots + 1]$ vérifiant* (4) *est de la forme $p^n + p^{n-1} + \dots + p^r$.*

DÉMONSTRATION. (Don Zagier) Soit r le plus petit entier tel que $j \le p^n + p^{n-1} + \dots + p^r$. On a donc

$$j = p^n + p^{n-1} + \dots + p^{r+1} + x$$

avec $0 < x \le p^r$.

Supposons $x < p^r$. Choisissons $k = p^{n-1} + p^{n-2} + \dots + p^r$. Alors l'entier $N = (j-k)(p-1) - 1$ vérifie l'inégalité

$$(p^n - p^r)(p-1) < N < p^n(p-1)$$

donc a un développement en base p ayant pour chiffres

chiffre	$p-2$	$p-1$	$p-1$	$\dots$	$p-1$	c	$*$	$\dots$	$*$
place	n	$n-1$	$n-2$	$\dots$	$r+1$	r	$r-1$	$\dots$	0

avec $c > 0$, tandis que k a pour développement en base p

chiffre	0	1	1	$\dots$	1	1	0	$\dots$	0
place	n	$n-1$	$n-2$	$\dots$	$r+1$	r	$r-1$	$\dots$	0

On a donc

$$\binom{(j-k)(p-1)-1}{k}$$
$$\equiv \binom{p-2}{0}\binom{p-1}{1}\binom{p-1}{1}\cdots\binom{p-1}{1}\binom{c}{1}\binom{*}{0}\cdots\binom{*}{0}$$
$$\not\equiv 0 \pmod p$$

ce qui contredit l'hypothèse. □

2. L'INVARIANT ν_p

NOTATION. Soit E un fibré vérifiant la condition du théorème 1.1. L'entier ν de ce théorème est noté $\nu_p(E)$. Si tous les $c_i(E)$ sont nuls, on note $\nu_p(E) = \infty$.

2.1. PROPOSITION. *Soit $f : Y \to X$ un revêtement fini, et soit E un fibré vectoriel complexe sur Y vérifiant les conditions du théorème 1.1. Soit $\nu = \nu_p(E)$; supposons que $\operatorname{rg} E$ soit divisible par p^ν. Alors*

(i) *f_*E vérifie les conditions du théorème 1.1.*
(ii) *On a $\nu_p(f_*E) \geq \nu_p(E)$.*
(iii) *Soit $r = p^\nu - p^{\nu-1}$. Alors*

$$c_r(f_*E) = f_*c_r(E).$$

DÉMONSTRATION. Par un dévissage standard, on se ramène au cas où f est galoisien de degré p. Dans ce cas, on utilise la formule d'Evens-Kahn-Fulton-MacPherson [3], [4, th. 14.2]

$$c(f_*E) = \mathcal{N}(c(E)) + \sum_{i=0}^{n-1}\big((1-\mu^{p-1})^{n-i} - 1\big)\mathcal{N}(c_i(E)) \tag{5}$$

où $n = \operatorname{rg} E$, $\mathcal{N}$ est le transfert multiplicatif d'Evens-Steiner [2], [15] et $\mu = c_1(L)$ avec $f_*\mathbf{1} = \bigoplus_{\mathbf{i=0}}^{\mathbf{p-1}} \mathbf{L}^{\otimes \mathbf{i}}$ ($\mathbf{1}$ est le fibré trivial de rang 1).

Pour voir (i), il suffit de vérifier que $\mathcal{N}(c(E))$ ne fait intervenir que des classes de degré divisible par $p-1$, ce qui résulte de [4, th. 8.1]. D'après [4, cor. 5.7], on a la formule

$$c_i(f_*E) = f_*c_i(E) + c_i(nf_*\mathbf{1}) \quad \text{pour} \quad \mathbf{i} \leq \mathbf{r}.$$

Écrivons $n = n_0p^\nu$. Alors $c(nf_*\mathbf{1}) = (\mathbf{1} - \mu^{\mathbf{p-1}})^{\mathbf{n}} = (\mathbf{1} - \mu^{(\mathbf{p-1})\mathbf{p}^\nu})^{\mathbf{n_0}}$, donc $c_i(nf_*\mathbf{1}) = \mathbf{0}$ pour $i < (p-1)p^\nu$, ce qui démontre (ii) et (iii). □

2.2. PROPOSITION. *Soient p un nombre premier, X un espace topologique et E un fibré sur X vérifiant la condition du théorème 1.1, et tel que $p^{\nu_p(E)} \mid \operatorname{rg}(E)$. Alors*

$$\nu_p(E \boxtimes B(r_{\mathbb{Z}/p})) = \nu_p(E) + 1$$

où $E \boxtimes B(r_{\mathbb{Z}/p})$ est le produit tensoriel externe de E et de $B(r_{\mathbb{Z}/p})$ sur l'espace $X \times B\mathbb{Z}/p$.

Démonstration. On peut écrire

$$r_{\mathbb{Z}/p} = \bigoplus_{\chi \in X(\mathbb{Z}/p)} \chi$$

où $X(\mathbb{Z}/p)$ est le groupe des caractères de $\mathbb{Z}/p$. Choisissons un générateur τ de ce groupe. On a alors

$$c(E \boxtimes B(r_{\mathbb{Z}/p})) = c(E \boxtimes \bigoplus_{i\in\mathbb{Z}/p} B(\tau^i)) = \prod_{i\in\mathbb{Z}/p} c(E \boxtimes B(\tau^i)).$$

Soit $n = \operatorname{rg} E$. On a

$$c(E \boxtimes B(\tau^i)) = \sum_{j=0}^{n} c_j(E) \times (1 + ic_1(\tau))^{n-j}$$

où $\times$ désigne le cross-produit. Les termes de plus bas degré sont

$$(1 + ic_1(\tau))^n + c_r(E)$$

où $r = p^{\nu_p(E)} - p^{\nu_p(E)-1}$. Par hypothèse sur n, les termes apparaissant dans $(1 + ic_1(\tau))^n - 1$ sont tous de degré $> r$. On a donc

$$c(E \boxtimes B(\tau^i)) \equiv 1 + c_r(E) \pmod{\deg r + 1}$$

et

$$c(E \boxtimes B(r_{\mathbb{Z}/p})) \equiv (1 + c_r(E))^p \equiv 1 \pmod{\deg r + 1}.$$

Il reste à voir que $c_{p^{\nu+1}-p^\nu}(E\boxtimes B(r_{\mathbb{Z}/p})) \neq 0$; pour cela, il suffit de vérifier que le coefficient numérique de $c_{(p-1)p^{\nu-1}}(E) \boxtimes c_1(\tau)^{(p-1)^2p^{\nu-1}}$ dans sa décomposition de Künneth est $\neq 0$. Or

$$\begin{aligned}
c(E \boxtimes B(r_{\mathbb{Z}/p})) &\equiv \prod_{i=0}^{p-1} \big((1 + ic_1(\tau))^n + c_r(E) \times (1 + ic_1(\tau))^{n-r}\big) \\
&\equiv \prod_{i=0}^{p-1} (1 + ic_1(\tau))^n \prod_{i=0}^{p-1} \big(1 + c_r(E) \times (1 + ic_1(\tau))^{-r}\big) \\
&\equiv (1 - c_1(\tau)^{p-1})^n \big(1 + c_r(E) \times \sum_{i=0}^{p-1} (1 + ic_1(\tau))^{-r}\big)
\end{aligned}$$

$$\equiv (1 - c_1(\tau)^{p^{\nu+1}-p^\nu})^{n_0} \big(1 + c_r(E) \times \sum_{i=0}^{p-1} (1 + ic_1(\tau)^{p^{\nu-1}})^{-p+1}\big) \pmod{c_r(E)^2}$$

où on a posé $n = n_0 p^\nu$. Le terme cherché est donc

$$\begin{aligned}
&\sum_{i=0}^{p-1} \binom{-p+1}{(p-1)^2} i^{(p-1)^2} c_{(p-1)p^{\nu-1}}(E) \times c_1(\tau)^{(p-1)^2p^{\nu-1}} \\
&\qquad = -\binom{-p+1}{(p-1)^2} c_{(p-1)p^{\nu-1}}(E) \times c_1(\tau)^{(p-1)^2p^{\nu-1}}
\end{aligned}$$

et on veut voir que $\binom{-p+1}{(p-1)^2} \not\equiv 0 \pmod p$. En écrivant

$$(1+t)^{-p+1} = (1+t^p)^{-1}(1+t) = \sum (-1)^i t^{pi}(1+t) \in \mathbb{F}_p[[t]]$$

on voit que

$$\binom{-p+1}{(p-1)^2} \equiv -1 \pmod p.$$

□

2.3. REMARQUE. Comme dans [7], définissons pour tout $n \geq 0$

$$I^{(n)}(X) = \{[E] \in K(X) \mid c_i(E) = 0 \text{ pour } i \not\equiv 0 \pmod{p-1},$$
$$\nu_p(E) \geq n \text{ et } \operatorname{rg} E \equiv 0 \pmod{p^n}\}.$$

On vérifie facilement (par le principe de scindage, par exemple) que $I^{(n)}(X)$ est un *idéal* de $K(X)$, stable par image réciproque. La proposition 2.1 montre que $I^{(n)}(X)$ se conserve également par image directe pour un revêtement fini. Comme dans [7], on peut demander:

QUESTION. Est-il vrai que $I^{(m)}(X)I^{(n)}(X) \subset I^{(m+n)}(X)$ pour tous m, n, X?

Il est facile de voir, encore par le principe de scindage, que la réponse est oui pour $m = 1$.

3. REPRÉSENTATIONS RATIONNELLES

Soient G un groupe et $\rho : G \to GL_n(\mathbb{C})$ une représentation de dimension finie de G. La construction de Borel associe à ρ un fibré vectoriel $B\rho$ sur l'espace classifiant BG de G. Les classes de Chern de $B\rho$ sont par définition les classes de Chern de ρ; on les note $c_i(\rho)$.

Supposons ρ définie sur $\mathbb{Q}$. Alors la condition du théorème 1.1 est vérifiée pour tout p [5]; l'invariant $\nu_p(B\rho) =: \nu_p(\rho)$ est donc défini.

Supposons G fini, et prenons $\rho = r_G$, représentation régulière de G. Alors ρ est évidemment définie sur $\mathbb{Q}$. L'entier $\nu_p(r_G)$ est noté $\nu_p(G)$.

Voici quelques propriétés de l'invariant $\nu_p(G)$:

3.1. PROPOSITION. *Soient G un groupe fini, p un nombre premier et H un sous-groupe de G. Alors*
a) On a $\nu_p(H) \leq \nu_p(G)$ et $c_{p^{\nu_p(H)}-p^{\nu_p(H)-1}}(r_G) = \operatorname{Cor}_H^G c_{p^{\nu_p(H)}-p^{\nu_p(H)-1}}(r_H)$.
b) Supposons que H soit un p-sous-groupe de Sylow de G. Alors on a $\nu_p(H) = \nu_p(G)$.

DÉMONSTRATION. a) résulte de la proposition 2.1. Pour voir b), on écrit

$$\operatorname{Res}_H^G r_G = (G:H) r_H$$

donc

$$\mathrm{Res}_H^G\, c(r_G) = c((G:H)r_H) = c(r_H)^{(G:H)}.$$

Comme $(G:H)$ est premier à p, on a $\nu_p((G:H)r_H) = \nu_p(r_H)$. Par ailleurs, l'homomorphisme de restriction

$$\mathrm{Res} : H^*(G, \mathbb{Z}/p) \to H^*(H, \mathbb{Z}/p)$$

est injectif. Il en résulte que $\nu_p(r_G) = \nu_p((G:H)r_H)$. □

3.2. Proposition. *Soit G un groupe fini. Alors $\nu_p(G \times \mathbb{Z}/p) = \nu_p(G) + 1$.*

Cela résulte de la proposition 2.2. □

3.3. Proposition. *Pour tout groupe fini G, on a $\nu_p(G) \leq v_p(|G|)$.*

Démonstration. Soit $r = p^{v_p(|G|)} - p^{v_p(|G|)-1}$: on va montrer que $c_r(r_G) \neq 0$. D'après la proposition 3.1, on peut supposer que G est un p-groupe. Soit E un sous-groupe d'ordre p de G. On a

$$\mathrm{Res}_E^G\, c(r_G) = c(\mathrm{Res}_E^G\, r_G) = c((G:E)r_E) = c(r_E)^{(G:E)}$$

On a $c(r_E) = 1 - c_1(\rho)^{p-1}$, où ρ est un caractère non trivial de E. On sait que $c_1(\rho)$ n'est pas nilpotent dans $H^*(E, \mathbb{Z}/p)$; par conséquent, $c_{p-1}(r_E)^{(G:E)} \neq 0$. Mais

$$c(r_E)^{(G:E)} = (1 + c_{p-1}(E) + \dots)^{(G:E)} = 1 + c_{p-1}(E)^{(G:E)} + \dots$$

puisque $(G:E)$ est une puissance de p. On en conclut que

$$\mathrm{Res}_E^G\, c_r(r_G) = c_{p-1}(E)^{(G:E)} \neq 0.$$

□

Vu le théorème 1.1, l'assertion de Venkov se reformule ainsi:

3.4. Assertion. (Venkov) *Pour tout groupe fini G et tout nombre premier p, on a $\nu_p(G) = v_p(|G|)$.*

La proposition 3.2 implique:

3.5. Proposition. [16] *L'assertion de Venkov est vraie pour un p-groupe abélien élémentaire.* □

4. Groupes d'ordre p^2 et p^3

4.1. Proposition. *L'assertion de Venkov est vraie pour $G = \mathbb{Z}/p^2$.*

Démonstration. On écrit $r_G = \bigoplus_{\chi \in X(G)} \chi$. Choisissant un générateur τ de $X(G)$, on obtient

$$c(r_G) = \prod_{i=0}^{p^2-1}(1 + ic_1(\tau)) = \prod_{i=0}^{p-1}(1 + ic_1(\tau))^p = (1 - c_1(\tau)^{p-1})^p = 1 - c_1(\tau)^{p^2-p}.$$

□

4.2. Proposition. *Supposons p impair. L'assertion de Venkov est vraie pour le groupe non abélien G d'ordre p^3 et d'exposant p.*

Démonstration. En effet, G est produit semi-direct de C et H pour tout sous-groupe H d'indice p de G et tout C engendré par un $g \notin H$. Par la proposition 3.5, $\nu_p(H) = 2$. On a

$$r_H = (r_{G/C})_{|H}$$

où $r_{G/C}$ est la représentation de permutation de G sur G/C, d'où

$$\mathrm{Cor}_H^G c_{p^2-p}(r_H) = \mathrm{Cor}_H^G \mathrm{Res}_H^G c_{p^2-p}(r_{G/C}) = 0.$$

D'après la proposition 3.1 a), on a donc $\nu_p(G) > 2$. D'autre part, $\nu_p(G) \leq 3$ d'après la proposition 3.3. On en conclut que $\nu_p(G) = 3$, comme souhaité. □

4.3. Proposition. *Soit G un p-groupe tel que tout sous-groupe propre de G soit abélien élémentaire. Alors*

- *soit G est abélien élémentaire;*
- *soit G est cyclique d'ordre p^2;*
- *soit p est impair est G est d'ordre p^3 et d'exposant p.*

Démonstration. Supposons que G ne soit pas abélien élémentaire. S'il est cyclique, il est nécessairement d'ordre p^2. Si G n'est pas cyclique, tout élément de G est contenu dans un sous-groupe propre de G, donc est d'ordre $\leq p$. Par conséquent, G est d'exposant p. Si $p = 2$, c'est impossible, car G serait alors abélien élémentaire.
Supposons donc $p > 2$. Comme G n'est pas cyclique, on a $(G : [G,G]) > p$; comme $[G,G]$ est distingué dans G, pour tout $g \in G$ le sous-groupe engendré par g et $[G,G]$ est propre, ce qui implique par hypothèse que $[G,G]$ est *central.* On en déduit une application bilinéaire alternée

$$[,] : G/[G,G] \times G/[G,G] \to [G,G]$$

dont l'image engendre $[G,G]$. La conclusion résulte alors du lemme suivant:

4.4. Lemme. *Soit $[,] : V \times V \to W$ une application bilinéaire alternée, où V, W sont des $\mathbb{F}_p$-espaces vectoriels. Supposons que $[,] \neq 0$, que l'image de $[,]$ engendre W et que, pour tout hyperplan H de V, $[,]_{|H} = 0$. Alors* $\dim V = 2$ *et* $\dim W = 1$.

En effet, choisissons un hyperplan H de V et soit $e \in V \setminus H$. Soit $K \subset H$ un hyperplan de H. Alors $< e, K >$ est un hyperplan de V; il en résulte que $[e, K] = 0$ et donc que $[V, K] = 0$. Mais alors on a $\dim H = 1$: sinon, tout élément de H serait contenu dans un de ses hyperplans, et on aurait $[V, H] = 0$, d'où $[V, V] = 0$ puisque $[,]$ est alternée. □

5. Démonstration de l'assertion de Venkov

5.1. Lemme. *Soient G un p-groupe, H un sous-groupe de G d'indice p et $a \in H^*(H, \mathbb{Z}/p)$ une classe de cohomologie invariante sous l'action de G/H.*

Alors

$$\operatorname{Cor}_H^G a^p = 0.$$

Démonstration. On a

$$Res_H^G \mathcal{N}(a) = \prod_{\sigma \in G/H} \sigma a = a^p$$

d'où

$$\operatorname{Cor}_H^G a^p = \operatorname{Cor}_H^G \operatorname{Res}_H^G \mathcal{N}(a) = 0.$$

□

(Autre démonstration: $(\operatorname{Cor} a)^2 = \operatorname{Cor}(a \cdot \operatorname{Res} \operatorname{Cor} a) = 0$, d'où $(\operatorname{Cor} a)^p = \operatorname{Cor}(a^p) = 0$.)

5.2. Lemme clé. *Soit G un p-groupe non abélien élémentaire. Supposons que l'assertion de Venkov soit vraie pour G. Alors $c(r_G) = a^p$, où $a \in H^*(G, \mathbb{Z}/p)$ est invariant sous l'action des automorphismes de G.*

Démonstration. Soit $\Phi(G)$ le sous-groupe de Frattini de G. On peut écrire

$$r_G = r_{G/\Phi(G)} \oplus \rho$$

avec

$$\rho = \rho' \oplus p\rho''$$

où $r_{G/\Phi(G)}$ est la somme des caractères abéliens d'ordre p de G, ρ' est la somme de ses caractères abéliens d'ordre $> p$ et $p\rho''$ est la somme de ses autres caractères irréductibles, avec leur multiplicité. (Rappelons qu'un caractère irréductible intervient dans r_G avec une multiplicité égale à son degré; comme G est un p-groupe, ce degré est une puissance de p. Cf. par exemple [13, p. 30, cor. 1 et p. 68, cor. 2].)

La représentation ρ'' est évidemment invariante par automorphismes de G; il en est donc de même de $c(\rho'')$. Si χ est un caractère abélien d'ordre $p^r > p$, il en est de même de χ^i pour tout i premier à p. On a

$$c(\chi^i) = 1 + ic_1(\chi)$$

donc

$$c\Big(\bigoplus_{i \in (\mathbb{Z}/p^r)^*} \chi^i\Big) = \prod_{i \in (\mathbb{Z}/p^r)^*} (1 + ic_1(\chi)) = (1 - c_1(\chi)^{p-1})^{p^{r-1}}.$$

Soit σ un automorphisme de G. Alors σ permute les caractères abéliens d'ordre p^r ainsi que les orbites $[\chi] = \{\chi^i \mid i \in (\mathbb{Z}/p^r)^*\}$ de l'action de $(\mathbb{Z}/p^r)^*$ sur ces caractères. Par conséquent, pour tout $r > 1$, $Aut(G)$ laisse invariante la classe de cohomologie

$$\prod_{[\chi]} (1 - c_1(\chi)^{p-1})$$

où $[\chi]$ décrit les orbites ci-dessus. On en déduit que $c(\rho')$, et donc $c(\rho)$, est de la forme b^p, où b est invariant sous l'action de $Aut(G)$.

Soient $\nu = v_p(|G|)$ et $d = v_p((G : \Phi(G)))$. Par hypothèse, on a $d < \nu$. Par conséquent, $p^d - 1 < p^\nu - p^{\nu-1}$. Il en résulte que

$$c_i(r_{G/\Phi(G)}) = 0 \quad \text{pour} \quad i \geq p^\nu - p^{\nu-1}.$$

D'autre part, on a par hypothèse

$$c(r_{G/\Phi(G)}) = c(r_G)c(\rho)^{-1} = (1 + c_{p^\nu - p^{\nu-1}}(r_G) + \dots)c(\rho)^{-1}.$$

On en déduit que les $c_i(r_{G/\Phi(G)})$ sont des polynômes en les $c_i(\rho)$ (plus précisément, on a $c_i(r_{G/\Phi(G)}) = -c_i(\rho)$ puisque les seules classes de Chern éventuellement $\neq 0$ de $r_{G/\Phi(G)}$ sont celles de degré $\geq p^d - p^{d-1}$ d'après la proposition 3.5). La conclusion du lemme clé en résulte (avec une formule explicite pour a si besoin est). □

5.3. THÉORÈME. *L'assertion de Venkov est vraie.*

DÉMONSTRATION. D'après la proposition 3.1 b), il suffit de la démontrer pour tout p-groupe G. On raisonne par récurrence sur $|G|$. Si G est abélien élémentaire, le théorème résulte de la proposition 3.5. De même, si G est cyclique d'ordre p^2 ou non abélien d'ordre p^3 et d'exposant p, il résulte des propositions 4.1 et 4.2.
Supposons maintenant que G ne soit pas de l'un des types ci-dessus. D'après la proposition 4.3, G contient un sous-groupe H d'indice p qui n'est pas abélien élémentaire. Soit $\nu = v_p(|G|)$. Par hypothèse de récurrence, on a $\nu_p(H) = \nu - 1$; d'autre part, d'après le lemme-clé, on a

$$c_{p^{\nu-1} - p^{\nu-2}}(r_H) = a^p$$

où a est invariant sous l'action de $Aut(H)$. En appliquant le lemme 5.1, on en déduit que $\mathrm{Cor}_H^G\, c_{p^{\nu-1} - p^{\nu-2}}(r_H) = 0$. On conclut comme dans la démonstration de la proposition 4.2. □

5.4. COROLLAIRE. (O. Kroll [9]) *Soit G un p-groupe qui n'est pas abélien élémentaire. Alors on a*

$$\prod_{\chi \in H^1(G, \mathbb{Z}/p) - \{0\}} \beta\chi = 0$$

où β est le Bockstein modulo p.

DÉMONSTRATION. Les arguments du lemme clé montrent que $c(r_{G/\Phi(G)})$ est une puissance p-ième; en particulier, $c_{p^d - 1}(r_{G/\Phi(G)}) = 0$, où $p^d = (G : \Phi(G))$, ce qui est équivalent à l'énoncé du corollaire. □

5.5. REMARQUES.

1. Le corollaire 5.4 a été amélioré par Serre [14]: on a $\prod \beta\chi = 0$, où χ décrit un système de représentants de l'espace projectif sur le $\mathbb{F}_p$-espace vectoriel $H^1(G, \mathbb{Z}/p)$. (Voir aussi [10].)

2. Soit $n = v_p(|G|)$, et soit $r = r_p(G)$ le maximum des rangs des p-sous-groupes abéliens élémentaires de G. En se restreignant à de tels sous-groupes, on voit facilement que les classes

$$c_{p^n - p^{n-1}}(r_G), \ldots, c_{p^n - p^{n-r}}(r_G)$$

sont non nilpotentes et algébriquement indépendantes sur $\mathbb{F}_p$. Par un théorème de Quillen [12, th. 7.1], les autres classes de Chern de r_G sont nilpotentes. D'après un autre théorème de Quillen (*loc. cit.*, cor. 2.4), l'algèbre de cohomologie $H^*(G, \mathbb{Z}/p)$ est un module de type fini sur sa sous-algèbre engendrée par les $c_i(r_G)$; c'est donc un module de type fini sur la sous algèbre engendrée par les $c_{p^n - p^k}(r_G)$ pour $k \in [n-r, n-1]$. Notons que $Aut(G)$ opère trivialement sur cette sous-algèbre. Par ailleurs, le lemme clé 5.2 montre que, si G n'est pas abélien élémentaire, les $c_{p^n - p^k}(r_G)$ sont puissances p-ièmes d'éléments également invariants par $Aut(G)$.
3. Le théorème 5.3 est à comparer avec les résultats obtenus dans [7] pour les classes de Stiefel-Whitney de r_G. Un entier $\nu(\rho)$ analogue à $\nu_p(\rho)$ y est défini pour toute représentation réelle ρ d'un groupe G. Si G est fini, on montre que

$$r_2(G) \leq \nu(r_G) \leq v_2(|G|)$$

où $r_2(G)$ est comme dans la remarque précédente. En général, on a $\nu(r_G) < v_2(|G|)$, par exemple pour $G = \mathbb{Z}/4$. Toutefois, on montre que $\nu(2r_G) = v_2(|G|) + 1$ pour tout groupe fini G.

Références

[1] M.F. Atiyah *Characters and cohomology of finite groups*, Publ. Math. I.H.É.S. 9 (1961), 23–64.

[2] L. Evens *A generalization of the transfer map in the cohomology of groups*, AMS Trans. 108 (1963), 54–65.

[3] L. Evens, D.S. Kahn *An integral Riemann-Roch formula for induced representations of finite groups*, AMS Trans. 245 (1978), 309–330.

[4] W. Fulton, R. MacPherson *Characteristic classes of direct image bundles for covering maps*, Ann. of Math. 125 (1987), 1–92.

[5] A. Grothendieck *Classes de Chern et représentations linéaires des groupes discrets*, *in* Dix exposés sur la cohomologie des schémas, North Holland, 1965.

[6] B. Kahn *Classes de Stiefel-Whitney de formes quadratiques et de représentations galoisiennes réelles*, Invent. Math. 78 (1984), 223–256.

[7] B. Kahn *The total Stiefel-Whitney class of a regular representation*, J. Alg. 144 (1991), 214–247.

[8] S. Mukohda, S. Sawaki *On the $b_p^{k,j}$ coefficient of a certain symmetric function*, J. Fac. Sci. Niigata Univ. 1 (1954), 1–6.

[9] O. Kroll *A representation-theoretical proof of a theorem of Serre*, Aarhus Univ. Preprint Series 33 (1986).

[10] T. Okuyama, H. Sasaki *Evens' norm and Serre's theorem on the cohomology algebra of a p-group*, Arch. Math. (Basel) 54 (1990), 331–339.

[11] F.P. Peterson *A* mod *p Wu formula*. Bol. Soc. Mat. Mexicana 20 (1975), 56–58.

[12] D. Quillen *The spectrum of an equivariant cohomology ring, I, II,* Ann. of Math. 94 (1971), 549–572, 573–602.

[13] J.-P. Serre Représentations linéaires des groupes finis, Hermann, Paris, 1970.

[14] J.-P. Serre *Une relation dans la cohomologie des p-groupes*, C. R. Acad. Sci., Paris, 304 (1987), 587–590.

[15] R. Steiner *Multiplicative transfers in ordinary cohomology*, Proc. Edinburgh Math. Soc. 25 (1982), 113–131.

[16] B.B. Venkov *Classes caractéristiques pour les groupes finis* (en russe), Dokl. Akad. Nauk SSSR 137 (1961), 1274–1277. Traduction anglaise: Sov. Math. Dokl. 2 (1961), 445–447.

Bruno Kahn
Institut de Mathématiques
de Jussieu
Université Paris 7
Case 7012
75251 Paris Cedex 05
France
kahn@math.jussieu.fr