MICHEL ENGUEHARD

Obstructions et p-groupes de classe 3

Astérisque, tome 142-143 (1986), p. 3-48

<http://www.numdam.org/item?id=AST_1986__142-143__3_0>

Société Mathématique de France
Astérisque 142-143 (1986)

OBSTRUCTIONS ET p-GROUPES DE CLASSE 3

Dans une première partie (chapitre I) est exposée ce que l'on peut considérer comme une généralisation de la théorie des obstructions: si G est un groupe, N un sous-groupe normal de G et A un G-module, donner une condition explicite pour qu'un 2-cocycle de N dans A soit restriction d'un 2-cocycle de G dans A. La suite de Serre-Hochschild et la méthode de décalage apportent une certaine réponse. Interviennent les groupes de cohomologie $H^2(G/N,H^1(N,A))$ et $H^3(G/N,A^N)$. La procédure qui suit m'a été signalée par Lluis Puig. Soit B un G-module convenablement choisi (par exemple quotient par A du G-module induit sur A, cf I.(b),1.), et posons $Q = G/N$; on définit deux suites exactes qui se croisent en deux points

$$[\mathfrak{C}_1] \qquad 0 \longrightarrow H^1(Q,B^N) \xrightarrow{\upsilon_1} H^2(G,A) \xrightarrow{res} H^2(N,A)^G \xrightarrow{\upsilon_2} H^2(Q,B^N)$$

$$[\mathfrak{C}_2] \qquad H^1(Q,B^N) \xrightarrow{\upsilon_3} H^1(Q,H^1(N,A)) \xrightarrow{\upsilon_4} H^3(Q,A^N) \xrightarrow{\upsilon_5} H^2(Q,B^N) \xrightarrow{\upsilon_6} H^2(Q,H^1(N,A))$$

Ainsi un élément Θ de $H^2(N,A)^G$ est dans l'image de $H^2(G,A)$ si et seulement si $\upsilon_2(\Theta)$ est nul. Cette condition se décompose en deux

1) $(\upsilon_6 \circ \upsilon_2)(\Theta)$ est nul,

2) si tel est le cas, par $(\upsilon_5)^{-1}$ on obtient dans $H^3(Q,A^N)$ une classe modulo le sous-groupe $\upsilon_4(H^1(Q,H^1(N,A))$ et la seconde condition nécessaire est que cette classe contienne 0.

Au chapitre I, (b) on décrit comment on peut calculer explicitement, en fonction d'un 2-cocycle de N dans A et d'une section de Q dans G, les éléments de $\mathcal{H}^3(Q,A^N)$ et $\mathcal{H}^2(Q,\mathcal{H}^1(N,A))$ ainsi rencontrés. La procédure conduit à utiliser un système de facteurs gauche, et il semble qu'avec un système de facteurs droit les formules soient nécessairement plus compliquées ([1]), sauf lorsque N opère trivialement sur A. Cette dernière hypothèse nous rapproche de la théorie classique des obstructions de Eilenberg et MacLane [2].

Pour préciser ce point, adoptons les notations suivantes:

pour tout groupe X, Aut(X) est le groupe des automorphismes de X, Int_X est le morphisme canonique "automorphismes intérieurs" ($\mathrm{Int}_X : X \longrightarrow \mathrm{Aut}(X)$) et on pose $\mathrm{Out}(X) = \mathrm{Aut}(X)/\mathrm{Int}_X(X)$.

Considérons une extension $\hat{N}$ de N par A et supposons en outre que A soit le centre de $\hat{N}$. Une extension $\hat{G}$ de G par A qui se restreint en $\hat{N}$ définit des extensions de Q par $\hat{N}$ admettant G pour quotient ([2]). Le groupe N est isomorphe à $\mathrm{Int}_{\hat{N}}(\hat{N})$; le groupe $\hat{G}$ opère sur $\hat{N}$ par automorphismes intérieurs, ce qui définit un morphisme de $\hat{G}$ dans $\mathrm{Aut}(\hat{N})$ et un morphisme χ de Q dans $\mathrm{Out}(\hat{N})$. Selon la théorie des obstructions, la donnée de χ définit une structure de Q-module sur A et l'existence d'une extension de Q par $\hat{N}$ induisant précisément χ équivaut à la nullité d'un certain élément $\mathfrak{m}$ de $\mathcal{H}^3(Q,A)$. En fait $\mathfrak{m}$ est déterminé par le sous-groupe $\chi(Q)$ de $\mathrm{Out}(\hat{N})$ et par χ: il existe un élément privilégié $\mathfrak{m}_o$ de $\mathcal{H}^3(\mathrm{Out}(\hat{N}),A)$ dont l'obstruction $\mathfrak{m}$ est la restriction à Q via χ.

([1]) A une section $\sigma: Q \longrightarrow G$ telle que $\sigma(1) = 1$, nous associons
un système de facteurs "gauche" $\varepsilon(s,t) = \sigma(st)^{-1}\sigma(s)\sigma(t)$,
un système de facteurs "droit" $\delta(s,t) = \sigma(s)\sigma(t)\sigma(st)^{-1}$

([2]) Etant donnée une extension $\hat{G}$ de G par A "qui se restreint en $\hat{N}$", l'injection de $\hat{N}$ dans $\hat{G}$ n'est pas nécessairement unique, elle est définie modulo le groupe des automorphismes de $\hat{N}$ qui induisent l'identité sur N et sur A, soit Hom(N,A). A partir d'une classe d'équivalence d'extensions de G par A, on obtient un ensemble de classes d'équivalence d'extensions de Q par $\hat{N}$ sur lequel le groupe Hom(N,A) opère régulièrement.

Si on pose $X = \hat{N}$, si Q est un sous-groupe de $\mathrm{Out}(X)$ et G est l'image inverse de Q dans $\mathrm{Aut}(X)$, la théorie des obstructions donne essentiellement une condition nécessaire et suffisante pour que la suite exacte

$$1 \longrightarrow \mathrm{Int}_X(X) \longrightarrow G \longrightarrow G/\mathrm{Int}_X(X) = Q \longrightarrow 1$$

soit quotient d'une suite

$$1 \longrightarrow X \longrightarrow \hat{G} \longrightarrow Q \longrightarrow 1$$

dans laquelle G opère sur X comme il se doit. Cette condition est que $\mathrm{Res}_Q^{\mathrm{Out}(X)}(\mathfrak{m}_o)$ soit nul. On constate sans peine que la démonstration élémentaire donnée en [5], chapitre IV, se généralise mot pour mot au cas où A est central dans X, mais non nécessairement le centre de X, la suite canonique

$$1 \longrightarrow Z(X) \longrightarrow X \longrightarrow \mathrm{Int}_X(X) \longrightarrow 1$$

étant remplacée par

$$1 \longrightarrow A \longrightarrow X \longrightarrow X/A = N \longrightarrow 1$$

et la suite

$$1 \longrightarrow \mathrm{Int}_X(X) \longrightarrow G \longrightarrow Q \longrightarrow 1$$

remplacée par

$$1 \longrightarrow N \longrightarrow G \longrightarrow G/N = Q \longrightarrow 1$$

à condition de supposer que l'opération de G sur N (par Int_G) est issue d'un morphisme de G dans $\mathrm{Aut}(X)$. On obtient ainsi la proposition 5, chapitre I, (c).

Dans la situation plus générale envisagée ici, on peut tenter d'interprêter $(\upsilon_6 \circ \upsilon_2)$ à l'aide de l'opération éventuelle de $\hat{G}$ sur $\hat{N}$ (chapitre I, (c)). En divisant la suite exacte bien connue

$$1 \longrightarrow \mathcal{Z}^1(N,A) \longrightarrow \mathrm{Aut}(\hat{N})_A \longrightarrow (\mathrm{Aut}(A) \times \mathrm{Aut}(N))_\Theta \longrightarrow 1$$

(où Θ est l'élément de $\mathcal{H}^2(N,A)$ réalisé par $\hat{N}$), par $\mathrm{Int}_{\hat{N}}(A)$, puis par $\mathrm{Int}_{\hat{N}}(\hat{N})$, on obtient les deux suites

$$1 \longrightarrow \mathcal{H}^1(N,A) \longrightarrow \mathrm{Aut}(\hat{N})_A/\mathrm{Int}_{\hat{N}}(A) \longrightarrow \mathcal{A} \longrightarrow 1$$

$$1 \longrightarrow \mathcal{H} \longrightarrow \mathrm{Out}(\hat{N})_A \longrightarrow \mathcal{G} \longrightarrow 1 \quad .$$

Lorsque Θ est fixe par G, G s'envoie dans $\mathcal{A}$ et Q dans $\mathcal{G}$. Si $\hat{G}$ existe, $\hat{G}$ opérant sur $\hat{N}$, les morphismes précédents proviennent de morphismes de G dans $\mathrm{Aut}(\hat{N})_A/\mathrm{Int}_{\hat{N}}(A)$ et de Q dans $\mathrm{Out}(\hat{N})_A$. Ceci est possible si et seulement si un certain élément Ξ

de $\mathcal{H}^2(Q,\mathcal{H})$ est nul. Les suites $[\mathfrak{r}_1]$ et $[\mathfrak{r}_2]$ sont telles que Ξ est une image de $(\upsilon_5 \circ \upsilon_2)(\Theta)$ (chapitre I, proposition 4).

Si Ξ est nul, les divers morphismes η: $Q \longrightarrow \mathrm{Out}(\hat{N})_A$ qui conviennent forment une classe modulo $\mathcal{Z}^1(Q,\mathcal{H})$. Ceci explique que la seconde condition obtenue porte non non sur un élément de $\mathcal{H}^3(Q,A^N)$, mais sur une classe modulo $\upsilon_4(\mathcal{H}^1(Q,\mathcal{H}^1(N,A))$. D'un autre point de vue, selon $[\mathfrak{r}_1]$ les divers éléments de $\mathcal{H}^2(G,A)$ dont Θ est restriction forment une classe modulo $\mathcal{H}^1(Q,B^N)$, et les morphismes η correspondant une classe modulo $\upsilon_3(\mathcal{H}^1(Q,B^N))$. L'application υ_3 n'est pas nécessairement surjective, car υ_4 n'est pas nécessairement nulle.

Dans les chapitres suivants, on n'utilise du chapitre I que la proposition 5. Est résolu le problème suivant: soit p un nombre premier impair; parmi les p-groupes finis de classe 3, classifier ceux qui admettent un groupe cyclique d'automorphismes "le plus gros possible", c'est-à-dire transitif sur les points non nuls de l'espace de Frattini, et en outre irréductible sur les facteurs centraux. Pour p = 3, on obtient entre autres les 3-groupes de Sylow des groupes de Ree, caractérisés par J.G. Thompson [6] et c'est là l'origine du problème posé. Les facteurs centraux étant d'exposant p, les méthodes linéaires, qui ont déjà démontré leur efficacité pour construire certains groupes de classe 2 (par exemple les 2-groupes de Sylow des groupes de Suzuki, [3], [1] et [4],II) s'imposent. Le chapitre II est consacré à quelques résultats utiles dans ce domaine. Au chapitre III, les cobords multiadditifs sont caractérisés par une propriété d'antisymétrie (proposition pour laquelle nous ne disposons pas de référence, démonstration de Lluis Puig). Au chapitre IV on donne quelques résultats partiels concernant les obstructions rencontrés lors de la construction de p-groupes de classe 3 dont les facteurs centraux sont d'exposant p. Les calculs sont menés à leur terme grâce à l'hypothèse portant sur le groupe d'automorphismes du p-groupe considéré.

L'essentiel des chapitres II à IV a été exposé au séminaire sur la théorie des groupes finis à Paris en décembre 1981.

Quelques notations:

Soit X un groupe. Le commutateur de deux éléments x et y de X, noté [x,y], est $xyx^{-1}y^{-1}$. Soit A un X-module. Le k-ième groupe de cohomologie de X dans A, noté $\mathcal{H}^k(X,A)$, est identifié au quotient du groupe des k-cocycles $\mathcal{Z}^k(X,A)$ par le groupe des k-cobords $\mathcal{B}^k(X,A)$, cocycles et cobords étant normalisés, c'est-à-dire de valeur 0 dès que l'une des variables est l'élément neutre 1 de X. L'opération de dérivation sur les fonctions de X^k dans A, notée $d^k(X,A)$, est définie par

$$\begin{aligned}(d^k(X,A)(f))(s_1, \ldots, s_{k+1}) = &\sum_{1 \leqslant m \leqslant k} (-1)^m f(s_1, \ldots, s_m s_{m+1}, \ldots, s_{k+1}) \\ &+ s_1.f(s_1,\ldots,s_{k+1}) + (-1)^{k+1} f(s_1,\ldots,s_m) .\end{aligned}$$

Si $\omega \in \mathcal{Z}^k(X,A)$, on pose

$$\ulcorner\omega\urcorner = \omega + \mathcal{B}^k(X,A) \text{ , donc } \ulcorner\omega\urcorner \in \mathcal{H}^k(X,A) .$$

Etant donnée une suite exacte courte de X-modules, notée $[\mathcal{E}]$, le morphisme cohomologique associé de rang k est noté $\partial^k(X,\mathcal{E})$. Si Y est un sous-groupe de X, l'opération de restriction de X à Y est parfois omise; on écrira donc $\partial^k(Y,\mathcal{E})$ pour $\partial^k(Y,\mathrm{Res}_X^Y(\mathcal{E}))$, etc ...

I. OBSTRUCTIONS.

Soient G un groupe, N un sous-groupe normal de G et A un G-module. On pose $Q = G/N$.

(a) Deux suites exactes.

On considère un plongement (i,C), où C est un G-module, i un monomorphisme de A dans C, les groupes de cohomologie $H^k(G,C)$, $H^k(N,C)$ et $H^k(Q,C^N)$ étant nuls dès que $k \geqslant 1$ (par exemple C relativement injectif, comme le module qui sera choisi en (b)). Posant $B = C/A$, on a une suite exacte

$$[\mathfrak{X}] \qquad 0 \longrightarrow A \xrightarrow{i} C \xrightarrow{p} B \longrightarrow 0 \quad .$$

et, sous ces hypothèses, la

Proposition 1. *Il existe deux suites exactes de groupes abéliens*

$$[\mathfrak{r}_1] \qquad 0 \longrightarrow H^1(Q,B^N) \xrightarrow{\cup_1} H^2(G,A) \xrightarrow{\text{res}} H^2(N,A)^G \xrightarrow{\cup_2} H^2(Q,B^N)$$

$$[\mathfrak{r}_2] \qquad H^1(N,A)^Q \longrightarrow H^2(Q,A^N) \longrightarrow H^1(Q,B^N) \xrightarrow{\cup_3} H^1(Q,H^1(N,A)) \xrightarrow{\cup_4} H^3(Q,A^N)$$
$$\xrightarrow{\cup_5} H^2(Q,B^N) \xrightarrow{\cup_6} H^2(Q,H^1(N,A)) \quad .$$

Démonstration. La suite $[\mathfrak{r}_1]$ se déduit de la suite de Serre-Hochschild relative au G-module B, soit

$$0 \longrightarrow H^1(Q,B^N) \xrightarrow{\text{inf}} H^1(G,B) \xrightarrow{\text{res}} H^1(N,B)^G \xrightarrow{\kappa_B} H^2(Q,B^N)$$

où inf est l'inflation et κ_B la transgression. Puisque $H^1(G,C)$ et $H^2(G,C)$ sont nuls, tout comme $H^1(N,C)$ et $H^2(N,C)$, les morphismes cohomologiques

$$\partial^1(G,\mathfrak{X}) : H^1(G,B) \longrightarrow H^2(G,A)$$

et

$$\partial^1(N,\mathfrak{X}) : H^1(N,B) \longrightarrow H^2(N,A)$$

sont des isomorphismes; le second est aussi un isomorphisme de G-modules, induisant un isomorphisme de $H^1(N,B)^G$ dans $H^2(N,A)^G$.

Pour construire $[\mathfrak{r}_2]$, considérons la suite de cohomologie de la restriction de $[\mathfrak{X}]$ à N. Puisque $H^1(N,C)$ est nul, elle débute par

$$0 \longrightarrow A^N \longrightarrow C^N \longrightarrow B^N \xrightarrow{\rho} H^1(N,A) \longrightarrow 0$$

où $\qquad \rho = \partial^o(N,\mathfrak{X}) \quad .$

Soient les deux suites exactes courtes qui s'en déduisent

$[\mathfrak{U}]$ $\qquad 0 \longrightarrow A^N \longrightarrow C^N \longrightarrow C^N/A^N \longrightarrow 0$

$[\mathfrak{U}_1]$ $\qquad 0 \longrightarrow C^N/A^N \xrightarrow{j} B^N \xrightarrow{\rho} H^1(N,A) \longrightarrow 0 .$

De la suite de cohomologie de la suite exacte de Q-modules $[\mathfrak{U}_1]$, extrayons

$[\mathfrak{c},\mathfrak{U}_1]$
$$H^1(N,A)^Q \longrightarrow H^1(Q,C^N/A^N) \longrightarrow H^1(Q,B^N) \longrightarrow H^1(Q,H^1(N,A)) \longrightarrow H^2(Q,C^N/A^N)$$
$$\longrightarrow H^2(Q,B^N) \longrightarrow H^2(Q,H^1(N,A)) .$$

Puisque $H^1(Q,C^N)$ et $H^2(Q,C^N)$ sont nuls, les morphismes cohomologiques
$$\partial^1(Q,\mathfrak{U}) : H^1(Q,C^N/A^N) \longrightarrow H^2(Q,A^N)$$
$$\partial^2(Q,\mathfrak{U}) : H^2(Q,C^N/A^N) \longrightarrow H^3(Q,A^N)$$
sont des isomorphismes , et on déduit ainsi la suite $[\mathfrak{c}_2]$ de $[\mathfrak{c},\mathfrak{U}_1]$.

Le module C peut être choisi de telle sorte que le morphisme composé $\partial^1(Q,\mathfrak{U})^{-1} \circ \partial^0(Q,\mathfrak{U}_1) : H^1(N,A)^Q \longrightarrow H^2(Q,A^N)$ soit le morphisme de transgression κ_A.

Les deux suites exactes de la proposition 1 se croisent en $H^1(Q,B^N)$ et en $H^2(Q,B^N)$. Un élément Θ de $H^2(N,A)^G$ est dans l'image par restriction de $H^2(G,A)$ si et seulement si son image Λ dans $H^2(Q,B^N)$ par $\upsilon_2 = \kappa_B \circ \partial^1(N,\mathfrak{X})^{-1}$ est nulle, condition qui se décompose en deux

a) $H^2(Q,\rho)(\Lambda)$ est nul (dans $H^2(Q,H^1(N,A))$),

b) ceci étant, il existe $\mathfrak{m} \in H^3(Q,A^N)$ tel que $\Lambda = \upsilon_5(\mathfrak{m}) = H^2(Q,j)(\partial^2(Q,\mathfrak{U})^{-1}(\mathfrak{m}))$ et Λ est nul si et seulement si $\mathfrak{m} \in \upsilon_4(H^1(Q,H^1(N,A))$ (où $\upsilon_4 = \partial^2(Q,\mathfrak{U}) \circ \partial^1(Q,\mathfrak{U}_1)$).

(b) <u>Calcul</u> <u>de</u> Λ <u>et</u> $\mathfrak{m}$.

Soit σ une section de Q dans G; $\sigma(1) = 1$ et $N\sigma(s) = s$ pour tout $s \in Q$. Soit ε (resp. δ) le système de facteurs gauche (resp. droit) associé. Soit enfin β_2 un cocycle de N dans A, élément de Θ, où $\Theta \in H^2(N,A)^G$. On se propose de calculer, en fonction de σ et β_2, des cocycles de classes respectives $H^2(Q,\rho)(\Lambda)$ et $\mathfrak{m}$(avec les notations du paragraphe (a))

On utilisera la notation suivante: si M est un G-module, non nécessairement un Q-module, et f une application de Q^k dans M ($k \in \mathbb{N}$), $d_\sigma^k(Q,M)(f)$ est l'application de Q^{k+1} dans M qui envoie $(s_1,\ldots,s_{k+1})$ sur
$$\sum_{1 \leqslant t \leqslant m} (-1)^t f(s_1,\ldots,s_t s_{t+1},\ldots,s_{k+1}) + \sigma(s_1).f(s_2,\ldots,s_{k+1}) + (-1)^{k+1} f(s_1,\ldots,s_k) .$$

1. La suite $\mathfrak{X}$.

Prenons pour C le "G-module induit défini sur A"; il admet pour support le groupe additif des applications de G dans A et est muni de l'opération

$$(s.h)(t) = h(ts) \qquad (t \in G,\ s \in G,\ h \in C).$$

C'est un G-module relativement injectif, donc un X-module relativement injectif pour tout sous-groupe X de G, et C^N est un G/N-module relativement injectif pour tout sous-groupe normal N de G. Par exemple, si $\eta_1 \in \mathfrak{Z}^1(G,C)$, on a $\eta_1 = d^o(G,C)(h)$, où $h(s) = \eta_1(s)(1)$ $(s \in G)$; de même, si $\eta_2 \in \mathfrak{Z}^2(G,C)$, on a $\eta_2 = d^1(G,C)(h_1)$, avec, pour $s \in G$ et $t \in G$, $h_1(s)(t) = \eta_2(t,s)(1)$. Il est clair que C^N est isomorphe au Q-module induit défini sur A.

Soit i l'injection de A dans C définie par

$$i(a)(s) = s.a \qquad (s \in G,\ a \in A).$$

C'est un G-morphisme et le sous-groupe i(A) de C admet comme supplémentaire l'ensemble des fonctions de G dans A, nulles en 1. En y transportant l'action de G, on voit que C/A est isomorphe au G-module B défini sur ce support par

$$(s.f)(t) = f(ts) - t.f(s) \qquad (t \in G,\ s \in G,\ f\colon G \longrightarrow A,\ f(1) = 0).$$

La projection p de C sur B est telle que

$$p(h)(s) = h(s) - s.h(1) \qquad (s \in G,\ h \in C).$$

2. La suite $\mathfrak{U}_1$.

Si $f \in B^N$, la restriction de f à N est un cocycle , soit β_1, et on a

$$\rho(f) = \partial^o(N,\mathfrak{X})(f) = \ulcorner\beta_1\urcorner.$$

Si $\beta_1 = d^o(N,A)(a)$ (où $a \in A$), alors $f = p(h)$, h étant défini par (si $s \in Q$, $y \in N$) $h(\sigma(s)y) = f(\sigma(s)) - \sigma(s).a$; il en résulte que $f = j(h + i(A^N))$.

3. Morphisme de transgression.

Le morphisme de transgression κ_A lié à l'extension G de Q par N est égal à $\partial^1(Q,\mathfrak{U}) \circ \partial^o(Q,\mathfrak{U}_1)$ (¹)

Soit $\beta_1 \in \mathfrak{Z}^1(N,A)$, de classe stable par G. Cette stabilité équivaut à l'existence d'une application f de G dans A telle que

(1) $$d^o(G,\mathfrak{Z}^1(N,A))(\beta_1) = d^o(N,A) \circ f .$$

(¹) ici intervient la structure de G-module de C.

L'application f n'est évidemment pas unique, mais on peut supposer

(2) f appartient à B^N et f prolonge β_1.

Selon le point 2, une telle application f permet de calculer $\partial^o(Q,\mathfrak{U}_1)(\ulcorner\beta_1\urcorner)$, par la relation $\sigma(s).f - f = p(h(s))$ $(s \in Q,\ h(s) \in C^N)$. L'application h définit alors un élément ξ_1 de $\mathcal{Z}^1(Q,C^N/A^N)$, par

$$\xi_1(s) = h(s) + A^N \qquad (s \in Q)$$

et alors $\ulcorner\xi_1\urcorner = \partial^o(Q,\mathfrak{U}_1)(\ulcorner\beta_1\urcorner)$.

Définissant alors $\mu_2 \in \mathcal{Z}^2(Q,A^N)$ par

$$d^1(Q,C^N)(h) = i \circ \mu_2 ,$$

on a

$$\partial^1(Q,\mathfrak{U})(\ulcorner\xi_1\urcorner) = \ulcorner\mu_2\urcorner.$$

On obtient ainsi, en tenant compte de (1) et (2),

$$h(s)(\sigma(t)y) = f(\sigma(t)\sigma(s)) - \sigma(t).f(\sigma(s)) - f(\sigma(t))$$

$$\mu_2(s,t) = f(\sigma(s)\sigma(t)) - \sigma(s).f(\sigma(t)) - f(\sigma(s)). \qquad (s \in Q,\ t \in Q,\ y \in N) \qquad (3)$$

Notons que si μ_2 est un cobord, dérivé d'une application m_1 de Q dans A^N, alors β_1 est restriction de $\zeta_1 \in \mathcal{Z}^1(G,A)$, où ζ_1 est défini par

$$\zeta_1(\sigma(s)y) = f(\sigma(s)y) + m_1(s) \qquad (s \in Q,\ y \in N).$$

4. <u>De</u> $\mathcal{H}^2(Q,A^N)$ <u>à</u> $\mathcal{H}^1(Q,B^N)$.

Soit $\mu_2 \in \mathcal{Z}^2(Q,A^N)$. Le morphisme $\partial^1(Q,\mathfrak{U})^{-1}$ envoie $\ulcorner\mu_2\urcorner$ sur la classe de ξ_1 $\xi_1 \in \mathcal{Z}^1(Q,C^N/A^N)$, ξ_1 étant défini par $\tilde{\xi}_1 : Q \to C^N$,

$$\tilde{\xi}_1(s)(\sigma(t)y) = \mu_2(t,s) \qquad (s \in Q,\ t \in Q,\ y \in N).$$

Il en résulte que $\mathcal{H}^1(Q,j) \circ \partial^1(Q,\mathfrak{U})^{-1}$ envoie $\ulcorner\mu_2\urcorner$ sur la classe de $\lambda_1 \in \mathcal{Z}^1(Q,B^N)$, où

$$\lambda_1(s)(\sigma(t)y) = \mu_2(t,s) \qquad (s \in Q,\ t \in Q,\ y \in N).$$

5. <u>Exactitude en</u> $\mathcal{H}^1(Q,B^N)$.

Si $\lambda_1 \in \mathcal{Z}^1(Q,B^N)$, on définit $\nu_1 \in \mathcal{Z}^1(Q,\mathcal{H}^1(N,A))$ par une application $\tilde{\nu}_1$ de Q dans $\mathcal{Z}^1(N,A)$:

$$\tilde{\nu}_1(s)(y) = \lambda_1(s)(y) \qquad (s \in Q,\ y \in N)$$

et on a alors

$$\mathcal{H}^1(Q,\rho)(\ulcorner\lambda_1\urcorner) = \ulcorner\nu_1\urcorner .$$

Si $\ulcorner\nu_1\urcorner$ est nul, il existe $\beta_1 \in \mathcal{Z}^1(N,A)$ et $r_1 : Q \to A$ tels que, pour $s \in Q$,

$$\tilde{\nu}_1(s) = \sigma(s).\beta_1 - \beta_1 + d^o(N,A)(r_1(s)).$$

En prolongeant β_1 en une application $f \in B^N$, par la formule

$$f(\sigma(t)y) = \sigma(t).\beta_1(y) \qquad (t \in Q,\ y \in N),$$

on peut exhiber une application $\tilde{\xi}'_1$ de Q dans C^N telle que

$$\lambda_1 - d^o(Q,B^N)(f) = p \circ \tilde{\xi}'_1 .$$

On trouve, pour $s \in Q$, $t \in Q$ et $y \in N$, comme solution en $\tilde{\xi}'_1$,

$$\tilde{\xi}'_1(s)(\sigma(t)y) = -\sigma(ts).\beta_1(\varepsilon(t,s)) - \sigma(t).r_1(s) + \lambda_1(s)(\sigma(t)).$$

La relation

$$d^1(Q,C^N)(\tilde{\xi}'_1) = i \circ \mu_2$$

définit $\mu_2 \in \mathfrak{Z}^2(Q,A^N)$ et il est clair que l'on a alors

$$\ulcorner\lambda_1\urcorner = (\mathcal{H}^1(Q,j) \circ \partial^1(Q,\mathfrak{N})^{-1})(\ulcorner\mu_2\urcorner).$$

Le calcul donne, pour $s \in Q$ et $t \in Q$,

$$\mu_2(s,t) = -(d^1_\sigma(Q,A) \circ r_1)(s,t) - \sigma(st).\beta_1(\varepsilon(s,t)) + \lambda_1(t)(\sigma(s)).$$

6. L'application υ_4.

Soit $\nu_1 \in \mathfrak{Z}^1(Q,\mathcal{H}^1(N,A))$ et supposons ν_1 défini par une application $\tilde{\nu}_1$ de Q dans $\mathfrak{Z}^1(N,A)$ telle qu'il existe $r_2\colon Q^2 \longrightarrow A$ normalisée et vérifiant

(4) $$d^1_\sigma(Q,\mathfrak{Z}^1(N,A))(\tilde{\nu}_1) = d^o(N,A) \circ r_2 .$$

En prolongeant $\tilde{\nu}_1(s)$ en $1_1(s)$ comme en 5, ($1_1(s) \in B^N$), on définit $1_1\colon Q \longrightarrow B^N$, et l'image de $\ulcorner\nu_1\urcorner$ dans $\mathcal{H}^2(Q,C^N/A^N)$ est la classe de ξ_2, où ξ_2 est défini par $\tilde{\xi}_2$,

$$d^1(Q,B^N)(1_1) = j \circ \xi_2 = p \circ \tilde{\xi}_2.$$

On obtient, pour $s \in Q$, $t \in Q$, $u \in Q$ et $y \in N$,

$$\tilde{\xi}_2(t,u)(\sigma(s)y) = \sigma(st).\tilde{\nu}_1(u)(\varepsilon(s,t)) - \sigma(s).r_2(t,u).$$

La relation $d^2(Q,C^N)(\tilde{\xi}_2) = i \circ \mu_3$ définit $\mu_3 \in \mathfrak{Z}^3(Q,A^N)$ et on a alors

$$\partial^2(Q,\mathfrak{N})(\ulcorner\xi_2\urcorner) = \ulcorner\mu_3\urcorner = \upsilon_4(\ulcorner\nu_1\urcorner).$$

On obtient ainsi, si $s \in Q$, $t \in Q$ et $u \in Q$,

(5) $$\mu_3(s,t,u) = -(d^2_\sigma(Q,A)(r_2))(s,t,u) + \sigma(st).\tilde{\nu}_1(u)(\varepsilon(s,t)).$$

Notons que r_2 est défini modulo le groupe des applications normalisées de Q^2 dans A^N, si bien que les diverses solutions en r_2 de (4) conduisent par (5) à toute une classe modulo $\mathfrak{B}^3(Q,A^N)$.

Supposons maintenant que $\ulcorner\mu_3\urcorner$ soit nul; il existe alors une application m_2

de Q^2 dans A^N, normalisée, telle que $\mu_3 = d^2(Q,A^N)(m_2)$. En posant, pour s, t $\in$ Q et y $\in$ N

$$\lambda_1(s)(\sigma(t)y) = \sigma(t).\tilde{\nu}_1(s)(y) + m_2(t,s) + r_2(t,s)$$

on définit un élément λ_1 de $\mathcal{Z}^1(Q,B^N)$, tel que

$$\ulcorner\nu_1\urcorner = \mathcal{H}^1(Q,\rho)(\ulcorner\lambda_1\urcorner).$$

7. L'application υ_5.

Si $\mu_3 \in \mathcal{Z}^3(Q,A^N)$, en posant (pour s $\in$ Q, t $\in$ Q, u $\in$ Q et y $\in$ N)

$$\xi_2'(t,u)(\sigma(s)y) = \mu_3(s,t,u)$$

on définit ξ_2': $Q^2 \longrightarrow C^N$, application qui induit $\xi_2' \in \mathcal{Z}^2(Q,C^N/A^N)$ et on a alors

$$\ulcorner\xi_2'\urcorner = \partial^2(Q,\mathcal{U})^{-1}(\ulcorner\mu_3\urcorner)$$

Soit $\lambda_2' = j \circ \xi_2' = p \circ \xi_2'$; λ_2' est un élément de $\mathcal{Z}^2(Q,B^N)$ et on a

$$\ulcorner\lambda_2'\urcorner = \upsilon_5(\ulcorner\mu_3\urcorner).$$

On obtient selon 1, si s $\in$ Q, t $\in$ Q, u $\in$ Q et y $\in$ N,

$$\lambda_2'(t,u)(\sigma(s)y) = \mu_3(s,t,u)$$

Si, avec les notations de 6, $\ulcorner\mu_3\urcorner = \upsilon_4(\ulcorner\nu_1\urcorner)$ (où $\nu_1 \in \mathcal{Z}^1(Q,\mathcal{H}^1(N,A))$, alors μ_3 vérifie (5), et on a $d^2(Q,C^N)(\xi_2' - \xi_2) = 0$. Selon 1, si x_1 est l'application de Q dans C^N définie par $x_1(s)(\sigma(t)y) = \xi_2'(t,s)(1) - \xi_2(t,s)(1)$ (t $\in$ Q, s $\in$ Q et y $\in$ N) alors $d^1(Q,C^N)(x_1) = \xi_2' - \xi_2$. Il en résulte que

$$\lambda_2' = d^1(Q,B^N)(1_1 + p \circ x_1)$$

avec $$(1_1 + p \circ x_1)(s)(\sigma(t)y) = \sigma(t).\tilde{\nu}_1(s)(y) + r_2(t,s).$$

(s $\in$ Q, t $\in$ Q, y $\in$ N)

8. Calcul de $\partial^1(G,\mathfrak{X})$.

Si $\eta_1 \in \mathcal{Z}^1(G,B)$, soit ζ_2: $G^2 \longrightarrow A$ définie par

$$\zeta_2(s,t) = \eta_1(t)(s) \qquad (s \in Q,\ t \in Q).$$

Alors ζ_2 est un 2-cocycle de G dans A, et on a $\partial^1(G,\mathfrak{X})(\ulcorner\eta_1\urcorner) = \ulcorner\zeta_2\urcorner$. Au total, l'application composée $\partial^1(G,\mathfrak{X}) \circ \inf_{\mathcal{B}} \circ \mathcal{H}^1(Q,j) \circ \partial^1(Q,\mathcal{U})^{-1}$ est évidemment l'inflation $\inf_A$ de $\mathcal{H}^2(Q,A^N)$ dans $\mathcal{H}^2(G,A)$.

9. L'application υ_2.

Le morphisme $\partial^1(N,\mathfrak{X})$ se définit comme $\partial^1(G,\mathfrak{X})$ en 8. Si $\alpha_1 \in \mathcal{Z}^1(N,B)$, on obtient $\beta_2 \in \mathcal{Z}^2(N,A)$ en posant $\beta_2(x,y) = \alpha_1(y)(x)$ (x $\in$ N, y $\in$ N) et on a alors

$$\beta_2 = \partial^1(N,\mathfrak{X})(\ulcorner\alpha_1\urcorner).$$

Inversement, si β_2 est donné, la même égalité définit $\alpha_1(y)$ sur N et on prolonge α_1 en un 1-cocycle de G dans B par un choix arbitraire des $\alpha_1(y)(\sigma(s))$ $(s \in Q)$ en posant par exemple

(6) $$\alpha_1(y)(\sigma(t)x) = \sigma(t).\beta_2(x,y) \qquad (t \in Q,\ x \in N,\ y \in N).$$

La stabilité de $\ulcorner\beta_2\urcorner$ par G se traduit par l'existence d'une application h_1 de G dans l'ensemble des fonctions de N dans A, telle que

(7) $$d^o(G,\mathfrak{Z}^2(N,A))(\beta_2) = d^1(N,A) \circ h_1 .$$

Il est commode de supposer h_1 normalisé, comme f l'est en 3. par les relations (2) et vérifiant les égalités

$$h_1(y)(x) = -\beta_2(x,y) + \beta_2(y,y^{-1}xy) \quad (x \in N,\ y \in N)$$
$$h_1(\sigma(t)y) = \sigma(t).h_1(y) + h_1(\sigma(t)) \quad (t \in Q).$$

La stabilité de $\ulcorner\alpha_1\urcorner$ défini par (6) se traduit alors par l'existence d'une application f_1 de G dans B telle que

$$d^o(G,\mathfrak{Z}^1(N,B))(\alpha_1) = d^o(N,B) \circ f_1 ,$$
$$\left.\begin{array}{l} f_1(y) = \alpha_1(y) \\ f_1(\sigma(t)y) = \sigma(t).f_1(y) + f_1(\sigma(t)). \end{array}\right. \quad (y \in N,\ t \in Q)$$

On constate que ces relations sont satisfaites si, pour $y \in N$, $s \in Q$, $t \in Q$

(8) $$f_1(\sigma(t))(\sigma(s)y) = \sigma(st).\beta_2(\varepsilon(s,t),y^{\sigma(t)}) - \sigma(s).h_1(\sigma(t))(y).$$

Selon 3, l'image de $\ulcorner\alpha_1\urcorner$ par κ_B est la classe de $\lambda_2 \in \mathfrak{Z}^2(Q,B^N)$, où

(9) $$\lambda_2(s,t) = f_1(\sigma(s)\sigma(t)) - \sigma(s).f_1(\sigma(t)) - f_1(\sigma(s)) \quad (s \in Q,\ t \in Q)$$

10. Première condition.

Supposant $\ulcorner\beta_2\urcorner$ dans $\mathcal{H}^2(N,A)^G$, une première condition est que $(\upsilon_6 \circ \upsilon_2)(\ulcorner\beta_2\urcorner)$ soit nul. Selon les notations de 9 et les résultats de 2, en posant

$$\tilde{\nu}_2(s,t)(y) = \lambda_2(s,t)(y) \qquad (s \in Q,\ t \in Q,\ y \in N),$$

on définit une application de Q^2 dans $\mathfrak{Z}^1(N,A)$ qui induit un 2-cocycle ν_2 de Q dans $\mathcal{H}^1(N,A)$; on a alors $\ulcorner\nu_2\urcorner = \mathcal{H}^2(Q,\rho)(\ulcorner\beta_2\urcorner) = \upsilon_6(\ulcorner\lambda_2\urcorner)$. Un calcul montre que

(10) $$\tilde{\nu}_2(s,t) = -h_1(\sigma(s)\sigma(t)) + \sigma(s).h_1(\sigma(t)) + h_1(\sigma(s)) \quad (s \in Q,\ t \in Q)$$

Le cocycle ν_2 est un cobord si et seulement siil existe des applications $\tilde{n}_1$ de Q dans $\mathfrak{Z}^1(N,A)$ et r_2' de Q^2 dans A telles que

(12) $$\tilde{\nu}_2 = d^1_\sigma(Q,\mathcal{Z}^1(N,A))(\tilde{n}_1) + d^o(N,A) \circ r'_2 \ .$$

On peut alors supposer $\tilde{n}_1$ et r'_2 "normalisés" car $\tilde{\nu}_2$ l'est.

11. Seconde condition.

Si (12) est satisfaite, $\ulcorner\lambda_2\urcorner$ appartient à l'image de υ_5. Pour exhiber un 3-cocycle de Q dans A^N représentatif, relevons $\tilde{n}_1$ en une application l'_1 de Q dans B^N par

$$l'_1(s)(\sigma(t)y) = \sigma(t).\tilde{n}_1(s)(y) \quad (s \in Q,\ t \in Q,\ y \in N).$$

Il existe alors $x_2 : Q^2 \longrightarrow C^N$ tel que $p \circ x_2 = \lambda_2 - d^1(Q,B^N)(l'_1)$ et on obtient un 3-cocycle de Q dans A, soit μ_3, par la relation $d^2(Q,C^N)(x_2) = i \circ \mu_3$. Un calcul élémentaire donne, pour $s \in Q$, $t \in Q$, $u \in Q$ et $y \in N$,

$$x_2(t,u)(\sigma(s)y) = (p \circ x_2)(t,u)(\sigma(s)) - \sigma(s).r'_2(t,u)$$

et $$\mu_3(s,t,u) = -(d^2_\sigma(Q,A)(r'_2))(s,t,u) + \lambda_2(t,u)(\sigma(s)) - \sigma(st).\tilde{n}_1(u)(\varepsilon(s,t)).$$

En utilisant (6), (8) et la valeur de λ_2 donnée par (9), on obtient

(13) $$\begin{aligned}\mu_3(s,t,u) = {} & (d^2_\sigma(Q,A)(-r'_2))(s,t,u) + \sigma(st).h_1(\sigma(u))(\varepsilon(s,t)) \\ & - \sigma(st).\tilde{n}_1(u)(\varepsilon(s,t)) \\ & + \sigma(stu).(\beta_2(\varepsilon(s,tu),\varepsilon(t,u)) - \beta_2(\varepsilon(st,u),\varepsilon(s,t)^{\sigma(u)})).\end{aligned}$$

Notons que, grâce à (10), la relation (12) s'écrit aussi

$$d^o(N,A)(r'_2(s,t)) = -h'_1(\sigma(s)\sigma(t)) + h'_1(\sigma(s)) + \sigma(s).h'_1(\sigma(t))$$

où l'on a posé $h'_1(\sigma(s)y) = h_1(\sigma(s)y) - \tilde{n}_1(s)$ $(s \in Q,\ y \in N)$. L'égalité (7) est satisfaite par h'_1 comme par h_1, car $\tilde{n}_1$ est à valeurs dans $\mathcal{Z}^1(N,A)$; $\tilde{\nu}_2$ est alors remplacé par $\tilde{\nu}'_2$, qui est à valeurs dans $\mathcal{B}^1(N,A)$.

La seconde condition nécessaire pour que $\ulcorner\beta_2\urcorner$ soit restriction depuis $\mathcal{H}^2(G,A)$ est que $\ulcorner\mu_3\urcorner$ soit dans l'image de υ_4; cette application a été calculée en 6; il faut qu'il existe $\tilde{\nu}_1$ et r_2 telles que (4) et (5) soient vraies. Compte-tenu de (13) la relation (5) s'écrit finalement

$$\begin{aligned}& d^2_\sigma(Q,A)(r_2 - r'_2)(s,t,u) + \sigma(st).(h_1(\sigma(u)) - \tilde{n}_1(u) - \tilde{\nu}_1(u))(\varepsilon(s,t)) \\ & + \sigma(stu).(\beta_2(\varepsilon(s,tu),\varepsilon(t,u)) - \beta_2(\varepsilon(st,u),\varepsilon(s,t)^{\sigma(u)})) = 0\end{aligned}$$

Là encore, l'égalité (7) est vérifiée si on remplace h_1 par h''_1, avec, pour $s \in Q$ $h''_1(\sigma(s)) = h_1(\sigma(s)) - \tilde{n}_1(s) - \tilde{\nu}_1(s)$. Celà conduit à supposer $\tilde{\nu}_1$ nul et r_2 à valeurs dans A^N.

12. Image inverse dans $\mathcal{H}^2(G,A)$.

Selon le calcul du morphisme de transgression fait en 3 (appliqué ici à B), si L est une application de Q dans B^N et $\lambda_2 = d^1(Q,B^N)(L)$, alors $(f_1 + L)$ est un élément de $\mathcal{Z}^1(G,B)$ qui prolonge α_1, et donc β_2 est prolongé par $\zeta_2 \in \mathcal{Z}^2(G,A)$, où

$$\zeta_2(u,v) = (f_1 + L)(v)(u) \qquad (u \in G,\ v \in G).$$

D'après (5), 6 et 11, on a

$$d^2(Q,C^N)(\tilde{\xi}_2) = i \circ \mu_3 = d^2(Q,C^N)(x_2)$$

donc
$$d^2(Q,C^N)(x_2 - \tilde{\xi}_2) = 0\ .$$

Comme on l'a remarqué en 1, on a alors

$$x_2 - \tilde{\xi}_2 = d^1(Q,C^N)(x_1), \quad x_1 : Q \longrightarrow C^N$$

avec
$$\begin{aligned} x_1(s)(\sigma(t)y) &= x_2(t,s)(1) - \tilde{\xi}_2(t,s)(1) \\ &= - r_2'(t,s) + r_2(t,s) \quad (t \in Q,\ s \in Q,\ y \in N). \end{aligned}$$

Il en résulte que

$$\begin{aligned} \lambda_2 &= p \circ x_2 + d^1(Q,B^N)(1_1') \\ &= p \circ (x_2 - \tilde{\xi}_2) + p \circ \tilde{\xi}_2 + d^1(Q,B^N)(1_1') \\ &= d^1(Q,B^N)(p \circ x_1 + 1_1 + 1_1'). \end{aligned}$$

On obtient donc une solution en L:

$$\begin{aligned} L(s)(\sigma(t)y) = r_2(t,s) - r_2'(t,s) + \sigma(t).\tilde{\nu}_1(s)(y) + \sigma(t).\tilde{n}_1(s)(y) \\ + \lambda_1(s)(\sigma(t)y) \end{aligned}$$

où $s \in Q$, $t \in Q$, $y \in N$ et λ_1 parcourt $\mathcal{Z}^1(Q,B^N)$.

Des relations (6), (7) et (8) on déduit

$$f_1(\sigma(s)x)(\sigma(t)y) = \sigma(ts).\beta_2(\varepsilon(t,s),y^{\sigma(s)}) + \sigma(t)\sigma(s).\beta_2(y^{\sigma(s)},x) - \sigma(t).h_1(\sigma(s))(y)$$

ce qui conduit à

$$\begin{aligned} \zeta_2(\sigma(t)y,\sigma(s)x) = \sigma(ts).\beta_2(\varepsilon(t,s),(y^{\sigma(s)})x) + \sigma(t).(\sigma(s).\beta_2(y^{\sigma(s)},x) - h_1(\sigma(s))(y) \\ + \tilde{\nu}_1(s)(y) + \tilde{n}_1(s)(y) + \lambda_1(s)(\sigma(t)y)) + (r_2 - r_2')(t,s)\ . \end{aligned}$$

Le paramètre λ_1 correspond à l'égalité

$$\upsilon_1(\mathcal{H}^1(Q,B^N)) = \mathrm{Ker}(\mathrm{res}\colon \mathcal{H}^2(G,A) \longrightarrow \mathcal{H}^2(N,A)^G)$$

En résumé des calculs qui précèdent, on obtient la proposition suivante, où on a posé $h = h_1''$ et $r_2' = m$.

Proposition 2. *Soit* $\beta \in \mathcal{Z}^2(N,A)$. *Pour que* β *soit restriction d'un élément de* $\mathcal{Z}^2(G,A)$, *il faut et il suffit qu'il existe*

$$h: G \longrightarrow \mathcal{F}(N,A) \quad \text{et} \quad m: Q^2 \longrightarrow A$$

tels que

$$(a)\quad d^o(G,A)(\beta) = d^1(N,A) \circ h$$

$$(b)\quad h(\sigma(s)y) = h(\sigma(s)) + \sigma(s).h(y) \qquad (s \in Q,\ y \in N)$$

$$h(y)(x) = \beta(y,y^{-1}xy) - \beta(x,y) \qquad (x \in N,\ y \in N)$$

$$(c)\quad \text{si} \quad \nu(s,t) = -\,h(\sigma(s)\sigma(t)) + \sigma(s).h(\sigma(t)) + h(\sigma(s)) \quad (s,\ t \in Q)$$

alors $\nu = d^o(N,A) \circ m.$

(d) si, pour $(s,t,u) \in Q^3$, *on pose*

$$\mu(s,t,u) = \sigma(stu).(\beta(\varepsilon(s,tu),\varepsilon(t,u)) - \beta(\varepsilon(st,u),\varepsilon(s,t)^{\sigma(u)})) + \sigma(st).h(\sigma(u))(\varepsilon(s,t)) - d^2_\sigma(Q,A)(m)(s,t,u)$$

alors μ *est nulle.*

La condition (a) exprime que $\ulcorner\beta\urcorner$ *est stable par* G. *La condition (b) est alors réalisable. Sous les conditions (a) et (b),* ν *définit un élément de* $\mathcal{H}^2(Q,\mathcal{H}^1(N,A))$ *Sous les conditions (a), (b) et (c), l'application* μ *est un 3-cocycle de* Q *dans* A^N. *Si (d) est réalisée, elle suppose* h *et* m *convenablement choisis parmi les solutions de (a), (b) et (c).*

Les éléments de $\mathcal{H}^2(G,A)$ *dont* $\ulcorner\beta\urcorner$ *est restriction sont les classes des 2-cocycles* ζ *tels que*

$$\zeta(\sigma(t)y,\sigma(s)x) = \sigma(ts).\beta(\varepsilon(t,s),(y^{\sigma(s)})x) + \sigma(t).(\sigma(s).\beta(y^{\sigma(s)},x) - h(\sigma(s))(y)) - m(t,s) + \lambda(s)(\sigma(t)y)$$

où λ *parcourt* $\mathcal{Z}^1(Q,B^N)$, $x \in N$, $y \in N$, $s \in Q$, $t \in Q$.

Redressement. Le choix, imposé par la définition de B, d'un système de facteurs gauche ε pour G entraîne que

$$\zeta(\sigma(t),x) = 0 \quad \text{si } t \in Q,\ \ x \in N\ ,$$

dans la proposition 2. L'extension de G par A s'écrit donc sur A x Q x N, avec en particulier $(a,0,0)(0,s,0)(0,0,y) = (a,s,y)$ si $(a,s,y) \in A \times Q \times N$.

Il est plus satisfaisant, surtout si N est abélien (et donc G défini par un élément de $\mathcal{H}^2(Q,N)$, ou un 2-cocycle de Q dans N), de prendre comme support A x N x Q, en utilisant un système de facteurs droit. Le redressement peut s'opérer ainsi

Pour tout groupe X et tout X-module M, on peut définir sur $\mathcal{F}(X^k,M)$ une transformation involutive qui stabilise $\mathcal{B}^k(X,M)$ et $\mathcal{Z}^k(X,M)$, induisant l'identité sur $\mathcal{H}^k(X,M)$; à $\varphi\colon X^k \longrightarrow M$, on associe φ^* définie par

$$\varphi^*(s_1, \ldots, s_k) = \varepsilon s_1 s_2 \ldots s_k.\varphi(s_k^{-1}, \ldots, s_1^{-1})$$

avec $\varepsilon = 1$ si k est congru à 0 ou 3 modulo 4, et $\varepsilon = -1$ sinon. Cette transformation commute à la dérivation. Il lui correspond sur les sections la transformation notée également $(\sigma \longrightarrow \sigma^*)$, où $\sigma\colon Q \longrightarrow G$, et $\sigma^*(t) = \sigma(t^{-1})^{-1}$ $(t \in Q)$. Si δ^* est le système de facteurs droit associé à σ^*, on a alors

$$\delta^*(s,t) = \varepsilon(t^{-1},s^{-1}) \qquad (s \in Q,\ t \in Q).$$

On posera donc

$$\beta_2^*(x,y) = -\,xy.\beta_2(y^{-1},x^{-1})$$

et la relation (7) se transforme en

$$d^o(G,\mathcal{Z}^2(N,A))(\beta_2^*) = d^1(N,A) \circ h' \quad \text{où} \quad h'(g) = (h_1^*(g))^*.$$

De même, posons

$$\mu_3^*(s,t,u) = \sigma^*(s)\sigma^*(t)\sigma^*(u).\mu_3(u^{-1},t^{-1},s^{-1}) ,$$

$$\tilde{n}_1^*(s) = -\,\sigma^*(s).\tilde{n}_1(s^{-1}),$$

$$\tilde{\nu}_1^*(s) = -\,\sigma^*(s).\tilde{\nu}_1(s^{-1}).$$

Les relations (5) et (10) ne changent pas de forme, par contre la formule (13) est moins simple si $A \neq A^N$. Dans cette dernière hypothèse, on a les simplifications préalables résultant de $\mathcal{Z}^1(N,A) = \mathrm{Hom}(N,A) = \mathcal{H}^1(N,A)$, on peut donc supposer que r_2' est nul, et on obtient l'énoncé suivant

<u>Proposition</u> 3. <u>*Supposons*</u> $A = A^N$. <u>*Soit*</u> $\beta \in \mathcal{Z}^2(N,A)$. <u>*Pour que*</u> β <u>*soit restriction d'un élément de*</u> $\mathcal{Z}^2(G,A)$, <u>*il faut et il suffit qu'il existe*</u> $h\colon G \longrightarrow \mathcal{F}(N,A)$ <u>*tel que*</u>

(a) $d^o(G,A)(\beta) = d^1(N,A) \circ h$

(b) $h(y\sigma(s)) = h(y) + y.h(\sigma(s)) \qquad (y \in N,\ s \in Q)$

$h(y)(x) = \beta(y,y^{-1}xy) - \beta(x,y) \qquad (x \in N,\ y \in N)$

(c) <u>*quels que soient*</u> s, t, u $\in$ Q,

$-h(\sigma(s)\sigma(t)) + \sigma(s).h(\sigma(t)) + h(\sigma(s)) = 0$

(d) <u>*Soit*</u> $\mu\colon Q^3 \longrightarrow A$, <u>*défini par*</u>

$$\mu(s,t,u) = \beta({}^{\sigma(s)}\delta(t,u),\delta(s,tu)) - \beta(\delta(s,t),\delta(st,u)) + h(\sigma(s))({}^{\sigma(s)}\delta(t,u))$$

Alors μ *est un cobord de* Q^3 *dans* A.

Les éléments de $H^2(G,A)$ *dont* $\ulcorner\beta\urcorner$ *est restriction sont les classes des 2-cocycles* ζ *tels que*

$$\zeta(x\sigma(s),y\sigma(t)) = \beta(x({}^{\sigma(s)}y),\delta(s,t)) + \beta(x,{}^{\sigma(s)}y) + h(\sigma(s))({}^{\sigma(s)}y) - m(s,t)$$
$$+ \theta(x\sigma(s),y\sigma(t))$$

où $\mu = d^2(Q,A)(m)$

$\theta \in Z^2(G,A)$ et $\theta(yg',g) = \theta(g',g)$ *quels que soient* $g', g \in G$, $y \in N$

(c) Opérations sur $\hat{N}$.

Proposition 4. *Soient* $\Theta \in H^2(N,A)^G$ *et* $\hat{N}$ *une extension de* N *par* A *réalisant* Θ. *Il existe des suites exactes naturelles et des morphismes de suites exactes*

$$\begin{array}{ll}
[\mathfrak{Aut}] & 1 \to Z^1(N,A) \to \mathrm{Aut}(\hat{N})_A \to \mathfrak{B} \to 1 \\
[\overline{\mathfrak{Aut}}] & 1 \to H^1(N,A) \to \mathrm{Aut}(\hat{N})_A/\mathrm{Int}_{\hat{N}}(A) \to \mathfrak{B} \to 1 \\
 & \quad\ \ {\scriptstyle\pi}\downarrow \\
[\mathfrak{Out}] & 1 \to \mathfrak{C} \to \mathrm{Out}(\hat{N})_A \to \mathfrak{A} \to 1 \\
 & [\mathfrak{Aut}] \to [\overline{\mathfrak{Aut}}] \to [\mathfrak{Out}]
\end{array}$$

où $\mathfrak{B}$ *est un sous-groupe de* $\mathrm{Aut}(A) \times \mathrm{Aut}(N)$, $\mathfrak{C}$ *un quotient de* $H^1(N,A)$, $\mathfrak{A}$ *un quotient de* $\mathfrak{B}$.

Soit $\Delta \in H^2(\mathfrak{A},\mathfrak{C})$ *la classe de* $[\mathfrak{Out}]$. *L'opération de* G *sur* N *et sur* A *définit un morphisme* $\chi\colon Q \to \mathfrak{A}$, *et on a.*

$$H^2(\chi,\mathfrak{C})(\Delta) = (H^2(Q,\pi) \circ \upsilon_6 \circ \upsilon_2)(\Theta)$$

(les applications υ_2 *et* υ_6 *sont celles qui ont été exhibées au cours de la démonstration de la proposition 1)*

Démonstration: La définition de $[\mathfrak{Aut}]$ va de soi; tout automorphisme de $\hat{N}$ qui stabilise A induit un automorphisme ψ de N et se restreint en un automorphisme ϕ de A, liés par la condition

(1) $\qquad \phi(x.a) = \psi(x).\phi(a) \qquad ((a,x) \in A \times N)$

On obtient ainsi un morphisme τ de $\mathrm{Aut}(N)_A$ dans $\mathrm{Aut}(A) \times \mathrm{Aut}(N)$. Le groupe des couples (ϕ,ψ) vérifiant (1) opère sur $H^2(N,A)$ ((ϕ,ψ) opère par $H^2(\psi^{-1},A) \circ H^2(N,\phi)$) et sur $Z^2(N,A)$. L'image $\mathfrak{B}$ de τ est l'ensemble des (ϕ,ψ) qui satisfont (1) et stabilisent Θ.

Le noyau de τ, groupe des automorphismes de $\hat{N}$ qui opèrent trivialement sur A et sur N, est isomorphe à $\mathcal{Z}^1(N,A)$. Concrètement, si N est défini sur A x N par le 2-cocycle β_2, et $(\phi,\psi) \in \mathrm{Aut}(A) \times \mathrm{Aut}(N)$, la transformation

$$(a,x) \longrightarrow (\phi(a) + h(\psi(x)),\psi(x)) \quad ((a,x) \in A \times N)$$

est un automorphisme de $\hat{N}$ si et seulement si on a (1) et

$$(2) \qquad (\phi,\psi).\beta_2 - \beta_2 = d^1(N,A)(h)$$

En particulier, si $\beta_1 \in \mathcal{Z}^1(N,A)$, l'application $((a,x) \longrightarrow (a + \beta_1(x),x))$ est un automorphisme de $\hat{N}$. Les automorphismes intérieurs de $\hat{N}$ selon les éléments de A correspondent de cette façon aux 1-cobords de N dans A. La suite $[\mathfrak{Aut}]$ admet ainsi comme quotient la suite $[\overline{\mathfrak{Aut}}]$.

Si un groupe Y opère sur N et A en fixant la structure de N-module de A, il opère sur $\mathcal{H}^2(N,A)$ et, s'il fixe Θ, Y a une image dans $\mathcal{B}$. L'élément de $\mathcal{H}^2(Y,\mathcal{H}^1(N,A))$ ainsi défini se calcule facilement:

soit, pour tout $g \in Y$, $h(g)$ une application de N dans A telle que

$$g.\beta_2 - \beta_2 = d^1(N,A)(h(g)).$$

Alors h définit un relèvement $\Sigma : Y \longrightarrow \mathrm{Aut}(\hat{N})_A$, par

$$\Sigma(g)(a,x) = (g.a + h(g)(g.x),g.x) \quad ((a,x) \in A \times N)$$

Si $s, t \in Y$, $\Sigma(s)\Sigma(t)\Sigma(st)^{-1}$, étant dans le noyau de τ, définit $\beta_1(s,t) \in \mathcal{Z}^1(N,A)$ et $\beta_1 = d^1(Y,\mathcal{F}(N,A))(h)$; avec $Y = \mathcal{B}$, on obtient l'élément de $\mathcal{H}^2(\mathcal{B},\mathcal{Z}^1(N,A))$ cherché.

Si Y = G, extension de Q par N, comme on le suppose dans ce chapitre, G opérant sur N par Int_G, en divisant $[\mathfrak{Aut}]$ par $\mathrm{Int}_{\hat{N}}(\hat{N})$ et G par N, on obtient la suite exacte $[\mathfrak{Out}]$ et un morphisme χ: $Q \longrightarrow \mathcal{A}$. D'où $\Delta \in \mathcal{H}^2(\mathcal{A},\mathcal{L})$ et $\mathcal{H}^2(\chi,\mathcal{L})(\Delta) \in \mathcal{H}^2(Q,\mathcal{L})$.

Il est clair maintenant que l'élément de $\mathcal{H}^2(Q,\mathcal{L})$ ainsi défini est image par $\mathcal{H}^2(Q,\pi)$ de $(\upsilon_6 \circ \upsilon_2)(\Theta)$ calculé dans la démonstration de la proposition 1 (cf (10)) (une première publication - mai 83 - contenait un énoncé inexact sur ce sujet)

<u>Opérations</u> <u>de</u> G.

L'existence d'une extension de G par A contenant $\hat{N}$ suppose l'existence d'un relèvement de G dans le groupe $\mathrm{Aut}(\hat{N})_A/\mathrm{Int}_{\hat{N}}(A)$. Si ζ_2 étend β_2, comme dans la proposition 2, soit $\hat{G}$ construit sur A x G par ζ_2. On voit que $\mathrm{Int}_{\hat{G}}((0,g))$ est défini par $h': G \longrightarrow \mathcal{F}(G,A)$, si, pour $g \in G$, $s \in G$ et $a \in A$,

$$(0,g)(a,s)(0,g)^{-1} = (g.a + h'(g)(gsg^{-1}), gsg^{-1});$$

On obtient $h'(g)(s) = -\zeta_2(s,g) + \zeta_2(g,g^{-1}sg)$, et h' définit un 1-cocycle de G dans $\mathcal{F}(G,A)/\mathcal{B}^1(G,A)$ (on a $d^1(G,\mathcal{F}(G,A))(h') = -d^0(G,A) \circ \zeta_2$). Appliqué à N à la place de G, ce résultat conduit aux conditions imposées à h_1 en (b) de la proposition 2. Dans les hypothèses et notations de la proposition 2, le relèvement de G dans $\mathrm{Aut}(\hat{N})_A/\mathrm{Int}_{\hat{N}}(A)$ est défini de façon analogue par $h'': G \longrightarrow \mathcal{F}(N,A)$ avec par exemple

(3) $$h''(\sigma(s))(y) = h(\sigma(s))(y) - \lambda(s)(y) \quad \text{où } \lambda \in \mathcal{Z}^1(Q,B^N).$$

Or, selon un résultat classique, étant donné le morphisme initial de G dans $\mathcal{B}$, les divers relèvements possibles de G dans $\mathrm{Aut}(\hat{N})_A/\mathrm{Int}_{\hat{N}}(A)$ forment une orbite régulière selon $\mathcal{Z}^1(G,\mathcal{H}^1(N,A))$. Mais $\hat{N}$ étant donné, le relèvement de N est imposé (par $\mathrm{Int}_{\hat{N}}$), et les divers relèvements de G a priori acceptables coïncident sur N. Ils forment donc une orbite régulière selon le noyau de la restriction qui envoie $\mathcal{Z}^1(G,\mathcal{H}^1(N,A))$ dans $\mathcal{Z}^1(N,\mathcal{H}^1(N,A))$, c'est-à-dire selon $\mathcal{Z}^1(Q,\mathcal{H}^1(N,A))$. En considérant comme équivalents des relèvements qui diffèrent par un automorphisme intérieur selon un élément de $\mathcal{H}^1(N,A)$ lui-même, on obtient un ensemble T, qui est lui-même une orbite régulière selon $H^1(Q,\mathcal{H}^1(N,A))$. La formule (3) montre que les diverses opérations de G sur $\hat{N}$ obtenues dans les extensions possibles ζ_2 de β_2 définissent un sous-ensemble de T, sous-ensemble qui est une orbite selon $\upsilon_3(H^1(Q,B^N))$, soit $\mathrm{Ker}(\upsilon_4)$.

Si on envisage de la même façon les morphismes de Q dans $\mathrm{Out}(\hat{N})$ qui relèvent χ, ils forment - s'il en existe - à équivalence convenable près, une orbite régulière selon $H^1(Q,\mathcal{L})$, et il suffit pour qu'il en existe que $H^2(\mathcal{L},\chi)(\Delta) = 0$, ce qui qui est une conséquence de la condition $(\upsilon_6 \circ \upsilon_2)(\Theta) = 0$. Mais les relèvements obtenus par prolongement de β_2 forment une orbite selon $H^1(Q,\pi)(\mathrm{Im}(\upsilon_3))$.

L'application υ_3 n'est pas nécessairement surjective, car υ_4 n'est pas nécessairement nulle. Supposons par exemple comme au chapitre IV que G opère trivialement sur A, et que N est central dans G. Si N et Q sont des p-groupes abéliens élémentaires pour un premier p impair, et si G est d'exposant p, G est défini comme extension de Q par N, par une fonction alternée Φ de Q x Q dans N (cf chap.II) Soit alors $h \in \mathrm{Hom}(Q,\mathrm{Hom}(N,A)) = H^1(Q,H^1(N,A))$. On a $\upsilon_4(h) = \ulcorner\mu\urcorner$, où $\mu(s,t,u) = h(s)(\Phi(t,u))/2$. Le 3-cocycle μ est triadditif et ce n'est un cobord que si son antisymétrisé est nul (proposition du chapitre III).

De l'analyse précédente, nous retiendrons la proposition suivante, où $A = A^N$ et l'opération de G dans $\hat{N}$ est imposée. Alors, dans les notations de la proposition 3, θ est astreint à parcourir $Z^2(Q,A)$, ce qui permet l'énoncé

Proposition 5. *Supposons que* N *opère trivialement sur* A *et soient* $\hat{N}$ *une extension de* N *par* A *définie sur* A x N *par* $\beta \in Z^2(N,A)$ *et une opération de* G *sur* $\hat{N}$ *, cohérente avec l'opération de* N *sur* A, *et définie par* $h_o : G \longrightarrow \mathcal{F}(N,A)$, h_o *satisfaisant à la condition (b) de la proposition 4; on a donc*

$$g.(a,x) = (g.a + h_o(g)(gxg^{-1}),gxg^{-1}) \quad (a,x,g) \in A \times N \times G$$

Il existe une extension $\hat{G}$ *de* G *par* A *qui se restreint en* $\hat{N}$ *et où* G *opère sur* $\hat{N}$ *comme ci-dessus si et seulement si le 3-cocycle* μ *de* Q *dans* A *défini par*

$$\mu(s,t,u) = \beta({}^{\sigma(s)}\delta(t,u),\delta(s,tu)) - \beta(\delta(s,t),\delta(st,u)) + h_o(\sigma(s))({}^{\sigma(s)}\delta(t,u))$$

est un cobord.

Les extensions solutions sont réalisées par les 2-cocycles ζ *de* G *dans* A *de la forme*

$$\zeta(x\sigma(s)\ ,\ y\sigma(t)) = \beta(x({}^{\sigma(s)}y),\delta(s,t)) + \beta(x,{}^{\sigma(s)}y) + h_o(\sigma(s))({}^{\sigma(s)}y) - m(s,t)$$

où $\mu = d^2(Q,A)(m)$.

On voit que sur l'ensemble des extensions de G par A qui sont solutions n'opère pas $H^1(Q,B^N)$, mais l'image de $H^2(Q,A)$ dans $H^1(Q,B^N)$ (noyau de υ_3). C'est finalement l'image par inflation de $H^2(Q,A)$ dans $H^2(G,A)$ qui opère régulièrement sur les solutions dans $H^2(G,A)$. D'autre part on démontrerait facilement que sur les classes d'équivalence d'extensions de Q par $\hat{N}$ obtenues dans la proposition 5, opère régulièrement $H^2(Q,A)$. L'équivalence entre extensions de Q par $\hat{N}$ n'est pas l'équivalence entre extensions de G par A. L'opération de G sur N et sur A étant fixée, à une classe d'extensions de G par A correspond un ensemble de classes d'extensions de Q par $\hat{N}$, orbite selon le groupe des automorphismes de $\hat{N}$ stables par G et induisant l'identité sur N et sur A; on a vu que ce dernier groupe est canoniquement isomorphe à $\mathcal{Z}^1(N,A)^G = \mathrm{Hom}(N,A)^G = \mathcal{H}^1(N,A)^Q$. Il s'envoie effectivement dans $\mathcal{H}^2(Q,A)$, par le morphisme de transgression, et le conoyau est isomorphe à l'image par inflation de $\mathcal{H}^2(Q,A)$ dans $\mathcal{H}^2(G,A)$ (exactitude de la suite de Serre-Hochschild).

Lorsqu'une opération cohérente de G sur $\hat{N}$ est imposée, l'existence d'une extension de G par A qui se restreint en $\hat{N}$ équivaut à l'existence d'une extension de Q par $\hat{N}$. La proposition 5 répond donc au problème classique des obstructions et peut se démontrer comme le théorème 8.7 dans [5], chapitre III. Supposons que A soit le centre de $\hat{N}$, groupe que nous notons provisoirement X; supposons également que $G = G_o = \mathrm{Aut}(X)$, et $Q = Q_o = \mathrm{Out}(X)$. La proposition 5 définit un élément $\mathfrak{m}_o$ de $\mathcal{H}^3(\mathrm{Out}(X),Z(X))$, $\mathfrak{m}_o = \ulcorner\mu_o\urcorner$, notations évidentes. On vérifie que μ_o peut être défini comme suit

soient $\sigma_o\colon \mathrm{Out}(X) \longrightarrow \mathrm{Aut}(X)$

$\tau_o\colon N = X/Z(X) \longrightarrow X$

des sections, la première définissant un système de facteurs droit δ_o, la seconde définissant $\beta_2 \in \mathcal{Z}^2(N,Z(X))$, et posons

$$\rho(s,t) = \tau_o(\delta_o(s,t)) \qquad \text{pour } s \in Q_o \text{ et } t \in Q_o;$$

on a

$$\mu_o(s,t,u)\rho(s,t)\rho(st,u) = (\sigma_o(s)(\rho(t,u)))\rho(s,tu).$$

Si, A étant toujours le centre de $X = \hat{N}$, est seulement donné un morphisme $\chi\colon Q \longrightarrow \mathrm{Out}(X)$, on peut définir G, extension de Q par $N = X/Z(X)$ en déplaçant par χ la suite standard

$$1 \longrightarrow \mathrm{Int}(X) = N \longrightarrow \mathrm{Aut}(X) \longrightarrow \mathrm{Out}(X) \longrightarrow 1$$

Chercher une extension de Q par X qui induise χ, c'est chercher une extension de G par Z(X) dont la restriction à N est X, considéré comme extension de N par Z(X). Selon la proposition 5, une telle extension existe si et seulement si $\mathfrak{m}$ est nul, où $\mathfrak{m} = \mathcal{H}^3(\chi,Z(X))(\mathfrak{m}_o)$; c'est le th.8.7 rappelé plus haut.

II. EXTENSIONS DE GROUPES ABÉLIENS ÉLÉMENTAIRES ET p-GROUPES DE CLASSE 2.

Dans ce chapitre et les suivants, p est un nombre premier.

Si X, Y et Z sont des groupes abéliens notés additivement, une fonction

$$f: Z \times Y \longrightarrow X$$

sera dite biadditive si, pour tout $s \in Z$ et tout $t \in Y$ les applications $(t \longrightarrow f(s,t))$ et $(s \longrightarrow f(s,t))$ sont des morphismes de groupes; f sera dite alternée si en outre $Z = Y$, f est biadditive et $f(s,s) = 0$ pour tout $s \in Y$.

On désignera par Alt(Y,X) le groupe additif des fonctions alternées de Y^2 dans X. Si U est un groupe, on désigne par $\Omega_1(U)$ le sous-groupe de U engendré par ses éléments d'ordre p.

Les deux énoncés qui suivent sont rappelés sans démonstration.

Proposition 1. *Soient* X *et* Y *deux groupes abéliens notés additivement et*

[E] $$0 \longrightarrow X \xrightarrow{i} E \longrightarrow Y \longrightarrow 0$$

une extension centrale de Y *par* X. *Soit* σ *une section de* [E], γ *le 2-cocycle associé et*

$$\phi: Y \times Y \longrightarrow X$$

définie par

$$i(\phi(s,t)) = [\sigma(s),\sigma(t)] \qquad (s \in Y,\ t \in Y)$$

On a $$\phi(s,t) = \gamma(s,t) - \gamma(t,s).$$

La fonction ϕ *est alternée de* Y *dans* X, *indépendante de la section* σ *choisie. L'extension est abélienne si et seulement si* ϕ *est nulle. On obtient ainsi une suite exacte*

$$0 \longrightarrow \mathrm{Ext}(Y,X) \longrightarrow H^2(Y,X) \longrightarrow \mathrm{Alt}(Y,X) \longrightarrow 0$$

(cette suite exacte est bien connue, en particulier si on identifie Alt(Y,X) à $\mathrm{Hom}(\Lambda^2(Y),X)$)

Si 2 est inversible dans X, la suite exacte précédente est naturellement scindée; le 2-cocycle γ se décompose en $\gamma = \gamma_0 + \gamma_1$, avec

$$\gamma_o(s,t) = (\gamma(s,t) + \gamma(t,s))/2 \quad \text{et} \quad \gamma_1(s,t) = \phi(s,t)/2.$$

L'extension abélienne de Y par X dont γ_o est un 2-cocycle sera dite "extension abélienne projetée de [E]".

Proposition 2. *Hypothèses et notations de la proposition 1. Soit*

$$u: \Omega_1(Y) \longrightarrow X/pX$$

définie par

$$\sigma(s)^p = i(v(s)) \quad \textit{et} \quad u(s) = v(s) + pX \quad (s \in \Omega_1(Y),\ v(s) \in X).$$

Si p *est impair ou si l'extension est abélienne,* u *est un morphisme de groupes indépendant de* σ. *Si* Y *est somme directe de groupes cycliques et l'un des deux groupes* X, Y *d'exposant* p, Ext(Y,X) *est ainsi naturellement isomorphe à* $\mathrm{Hom}(\Omega_1(Y), X/pX)$.

(si p = 2 et l'extension est non abélienne, u est une application de type quadratique associée à la fonction ϕ introduite dans la proposition 1)

Proposition 3. *Hypothèses et notations des propositions 1 et 2. Supposons* X *et* Y p-*groupes abéliens élémentaires (*p *impair). Soient* f *un automorphisme de* X *et* g *un automorphisme de* Y. *Il existe un automorphisme* h *de* E *qui stabilise* i(X) *et induit* f *sur* X, g *sur* Y, *si et seulement si*

$$\phi \circ (g \times g) = f \circ \phi \quad \textit{et} \quad u \circ g = f \circ u.$$

Notons que lorsque f et g sont fixés et convenables, les automorphismes de E qui induisent f sur X et g sur Y forment une classe modulo le groupe des automorphismes de E triviaux sur X et sur Y, soit Hom(Y,X) (cf la proposition 4 du chapitre I)

Proposition 4. *Soit* H *un groupe abélien opérant fidèlement et irréductiblement sur* G, p-*groupe abélien élémentaire. Alors* H *est cyclique et d'ordre premier à* p. *Il existe un corps fini* $\mathbb{K}$ *de caractéristique* p, *ordre* q, *et deux applications* ν *et* ρ *telles que*

(a) ν *est un isomorphisme de* G *sur le groupe additif de* $\mathbb{K}$,

(b) ρ *est un monomorphisme de* H *dans le groupe multiplicatif* $K^\times$ *de* $\mathbb{K}$,

(c) *pour tout* $(x,s) \in H \times G$, *on a*

$$\nu(x.s) = \rho(x)\nu(s),$$

(d) *le corps* $\mathbb{K}$ *est engendré sur le corps premier par* $\rho(H)$ *et* q *est la plus* *petite puissance de* p *telle que l'ordre de* H *divise* (q - 1).

Inversement, deux monomorphismes ρ_1 *et* ρ_2 *de* H *dans* $K^\times$ *définissent des* $\mathbb{F}_p H$-*modules isomorphes si et seulement si il existe un automorphisme* σ *de* $\mathbb{K}$ *tel que*

$$\sigma \circ \rho_1 = \rho_2 .$$

Notations: si τ et ν sont des applications d'un ensemble E à valeurs dans un corps $\mathbb{K}$, on pose $(\tau.\nu): E \times E \to \mathbb{K}$ $\quad (\tau.\nu)(x,y) = \tau(x)\nu(y)$,

$$(\tau * \nu): E \times E \to \mathbb{K} \qquad (\tau*\nu) = (\tau.\nu) - (\tau.\nu).$$

La proposition suivante se déduit de l'indépendance linéaire des automorphismes d'un corps, elle pourrait s'énoncer pour une extension galoisienne finie.

Proposition 5. *Soient* $\mathbb{K}$ *un corps fini de caractéristique* p, $\mathfrak{G}$ *son groupe d'automorphismes et* K *son groupe additif, également espace sur le corps premier.*

(a) $\{\tau\}_{\tau \in \mathfrak{G}}$ *est une base sur* $\mathbb{K}$ *de* End(K),

(b) $\{(\tau.\nu)\}_{(\tau,\nu)\in\mathfrak{G}^2}$ *est une base sur* $\mathbb{K}$ *de l'espace des applications biadditives de* K^2 *dans* K,

(c) $\{(\tau*\nu)\}_{\tau,\nu\in\mathfrak{G},\tau\neq\nu}$ *est une base sur* $\mathbb{K}$ *de* Alt(K,K),

(d) si $p \neq 2$, *soient* $\tau, \nu \in \mathfrak{G}$; *la fonction quadratique* f *de* K *dans* K *telle que* $f(x) = \tau(x)\nu(x)$ $(x \in K)$ *détermine* $\{\tau,\nu\}$,

(e) si $p \neq 2$, *soient* $\tau, \nu, \kappa \in \mathfrak{G}$; *la fonction cubique* c *définie par* $c(x) = \tau(x)\nu(x)\kappa(x)$ $(x \in K)$ *détermine* $\{\tau,\nu,\kappa\}$.

Par commodité, nous noterons en exposant à droite les éléments de $\mathfrak{G}$, et plus généralement les applications de K dans K qui, fixant 0, induisent des endomorphismes du groupe multiplicatif $K^\times$ de $\mathbb{K}$.

Les groupes $U(\sigma)$ et $U_o(\sigma_o)$.

Soient toujours $\mathbb{K}$, K, $K^\times$, q et $\mathfrak{G}$ comme dans les propositions 3 et 4. Si q est un carré, $q = q_o^2$, soit $\mathbb{K}_o$ le corps de Galois d'ordre q_o, sous-corps de $\mathbb{K}$, $\sigma_o \in \mathfrak{G}$ tel que $\mathrm{Gal}(\mathbb{K}/\mathbb{K}_o) = \{1,\sigma_o\}$ et choisissons $a_o \in \mathbb{K}$ non nul, de trace nulle $a_o + a_o^{\sigma_o} = 0$ (a_o est défini modulo un élément de $(K_o)^\times$).

Soit $\sigma \in \mathfrak{G}$. Selon les propositions 1 et 2, la fonction alternée $(1*\sigma)$ définit un groupe extension de K par K, exposant p et ordre q^2, de classe 2 si $\sigma \neq 1$, groupe qui sera noté $U(\sigma)$. Une présentation standard en est

$U(\sigma)$ est de support $K \times K$, avec pour produit

$$(\alpha,\beta)(\lambda,\delta) = (\alpha + \lambda + \beta\delta^{\sigma},\beta + \delta)$$

et $K^{\times}$ opère sur $U(\sigma)$ selon la formule

$$x.(\alpha,\beta) = (x^{1+\sigma}\alpha,x\beta).$$

De même la fonction alternée $2a_o(1*\sigma_o)$ prend ses valeurs dans $\mathbb{K}_o$ et définit donc une extension de K par K_o, soit un groupe d'exposant p, ordre $q_o^{\,3}$, classe 2, sur lequel opère également $K^{\times}$; notons-le $U_o(\sigma_o)$

$U_o(\sigma_o)$ est de support $K_o \times K$, avec pour produit

$$(\alpha,\beta)(\lambda,\delta) = (\alpha + \lambda + a_o(\beta\delta^{\sigma_o} - \beta^{\sigma_o}\delta),\beta + \delta)$$

et $$x.(\alpha,\beta) = (x^{1+\sigma}\,\alpha,x\beta) \qquad (x \in K^{\times}).$$

Les groupes $U(\sigma)$ et $U_o(\sigma_o)$ sont caractérisés par la proposition suivante

<u>Proposition</u> 6. ($p \neq 2$)<u>*Soit*</u> U <u>*un*</u> p-<u>*groupe de classe*</u> 2 <u>*admettant un groupe cyclique d'automorphismes*</u> H <u>*d'ordre*</u> $(q - 1)$ <u>*opérant irréductiblement sur chacun des facteurs de la suite centrale descendante de*</u> U. <u>*Alors*</u> U <u>*est d'exposant*</u> p <u>*et*</u>

<u>*ou bien il existe*</u> $\sigma \in (\mathfrak{G} - \{1,\sigma_o\})$ <u>*tel que le produit semi-direct*</u> U.H <u>*soit isomorphe à*</u> $U(\sigma).K^{\times}$,

<u>*ou bien*</u> q <u>*est un carré*</u> $q_o^{\,2}$ <u>*et*</u> U.H <u>*est isomorphe à*</u> $U_o(\sigma_o).K^{\times}$.

(q est supposé égal à l'ordre d'un corps fini $\mathbb{K}$ dont $\mathfrak{G}$ est le groupe d'automorphismes)

<u>Démonstration</u>.

Puisque U est de classe 2 et les facteurs $U/[U,U]$ et $[U,U]$ sont supposés H-irréductibles, ce sont des groupes abéliens élémentaires et on a

$$Z(U) = [U,U] = \Phi(U) \text{ (groupe de Frattini).}$$

Si un p'-automorphisme de U opère trivialement sur son espace de Frattini, c'est l'identité; donc H opère fidèlement sur $U/\Phi(U)$. Selon la proposition 4, $U/\Phi(U)$ est isomorphe à K, H y opérant comme $K^{\times}$; il résulte aussi de l'assertion (d) de la proposition 4 que $Z(U)$ est isomorphe au groupe additif K_1 d'un sous-corps $\mathbb{K}_1$ de $\mathbb{K}$. L'extension de K par K_1 ainsi obtenue est définie par une fonction alternée ϕ de K dans K (à valeurs dans K_1) et un morphisme de K dans K_1 (proposition 1). Puisque H opère sur Z(U), cette opération est définie par un morphisme multiplicatif de $K^{\times}$ dans $K_1^{\times}$, soit ρ. Selon la proposition 3, on doit avoir

$$\phi(xa,xb) = \rho(x)\phi(a,b) \qquad (a,\ b,\ x \in \mathbb{K}).$$

En utilisant l'assertion c) de la proposition 5, on voit que si la composante de ϕ sur $(\tau*\nu)$ est non nulle on a $\rho(x) = \tau(x)\nu(x)$ pour tout $x \in \mathbb{K}$; selon l'assertion d) de la proposition 5, ρ détermine $\{\tau,\nu\}$ et $\phi = a(\tau*\nu)$, où $a \in K$. Mais ϕ étant à valeurs dans K_1, pour tout $\psi \in \mathrm{Gal}(\mathbb{K}/\mathbb{K}_1)$, on a $\psi \circ \phi = \phi$, soit $a^{\psi}(\psi\tau*\psi\nu) = a(\tau*\nu)$

Cette dernière égalité implique que

ou bien ψ est l'identité

ou bien ψ est d'ordre 2, et $\tau = \nu\psi$ et $\nu = \tau\psi$.

Il en résulte que $\mathbb{K}_1$ est soit égal à $\mathbb{K}$, soit égal à $\mathbb{K}_o$ (q étant alors un carré). En outre, si $\mathbb{K}_1 = \mathbb{K}_o$, a est de trace nulle.

Il est toujours possible de modifier les présentations de Z(U) et de U/Z(U) par l'intermédiaire de transformations de K et de K_1, pour obtenir les groupes $U(\sigma)$ ou $U_o(\sigma_o)$:

si $K_1 = K$, en transformant Z(U) par a^{-1} et U/Z(U) par τ, on obtient $\phi = (1*\sigma)$, avec $\sigma = \tau^{-1}\nu$;

si $K_1 = K_o$, soit τ_o la restriction de τ à K_o, il existe $b \in K_o$ tel que $b^{-1}a = 2a_o$ et en transformant U/Z(U) par τ et Z(U) par b^{-1}, on obtient $\phi = 2a_o(1*\sigma_o)$.

Selon la proposition 3, le morphisme u de K dans K_1 correspondant à l'élévation à la puissance p-ième doit commuter à l'action de H, ce qui s'écrit, pour $x \in K$, $u(xa) = x^{1+\sigma}u(a)$ (éventuellement $\sigma = \sigma_o$). En utilisant l'assertion (d) de la proposition 4, on voit que si u admet une composante non nulle sur $\sigma' \in \mathfrak{G}$, on a $x^{\sigma'} = x^{1+\sigma}$ quel que soit $x \in K$, ce qui est absurde car $(1 + \sigma)$ n'est pas additif (seul le cas $\sigma = 1$ et $p = 2$ fait exception). Ainsi u est nul et U est d'exposant p.

Corollaire. *Hypothèses et notations de la proposition 6.*

(a) Si H' *est un groupe d'automorphismes de* U *satisfaisant aux mêmes hypothèses que* H, H *et* H' *sont conjugués dans* AUT(U).

(b) Les groupes $U(\sigma)$ *et* $U(\tau)$ *sont isomorphes si et seulement si*

$$\tau \in \{\sigma,\sigma^{-1}\}.$$

L'assertion (a) résulte immédiatement de la proposition, puisque les produits semi-directs U.H et U.H' sont isomorphes.

Si $U(\sigma)$ et $U(\tau)$ sont isomorphes, d'après (a) il existe un isomorphisme qui envoie $U(\sigma).K^{\times}$ sur $U(\tau).K^{\times}$; il existe donc des isomorphismes f et g de K dans K tels que

$$(1*\tau) \circ (g \times g) = f \circ (1*\sigma)$$

(condition nécessaire et suffisante pour que $U(\sigma)$ et $U(\tau)$ soient isomorphes), mais il existe aussi un automorphisme h de $K^{\times}$ tel que

$$g(xa) = h(x)g(a) \qquad (x \in K^{\times},\ a \in K).$$

Selon cette dernière égalité, $h = g/g(1)$ est à la fois multiplicative et additive, c'est donc un automorphisme de $\mathbb{K}$ (cf la dernière assertion de la proposition 4). La première égalité s'écrit

$$g(1)^{1+\sigma}(h*h\tau) = f \circ (1*\sigma).$$

En décomposant f sur la base $\mathfrak{G}$ de End(K), on voit que f est de la forme $f = a\nu$, où $\nu \in \mathfrak{G}$, avec $g(1)^{1+\tau}(h*h\tau) = a(\nu*\nu\sigma)$, d'où $\tau \in \{\sigma, \sigma^{-1}\}$.

Inversement, $U(\sigma)$ et $U(\sigma^{-1})$ sont isomorphes via $g = \sigma^{-1}$ et $f = -1$.

La première assertion de ce corollaire est renforcée par le résultat plus précis que voici

Proposition 7. *Supposons σ d'ordre au moins 5. Le groupe d'automorphismes de* $U(\sigma)$ *est extension du produit semi-direct* $K^{\times}.\mathfrak{G}$ *par* Hom(K,K).

Démonstration. Tout automorphisme de $U(\sigma)$ induit un automorphisme du centre $Z(U(\sigma))$ et un automorphisme de l'espace de Frattini, le quotient $U/Z(U)$. Réciproquement, si f et g sont des automorphismes de K, le couple (f,g) est induit par un automorphisme de $U(\sigma)$ si et seulement si (proposition 3)

(I) $$f \circ (1*\sigma) = (1*\sigma) \circ (g \times g).$$

Un automorphisme u de $U(\sigma)$ trivial sur le centre et sur l'espace de Frattini de $U(\sigma)$ est déterminé par un homomorphisme v de K dans K (cf la proposition 4 du chapitre I). On obtient ainsi un groupe isomorphe à Hom(K,K), normal dans $\mathrm{Aut}(U(\sigma))$ et sur lequel un couple (f,g) satisfaisant (I) opère par

$$v^{(f,g)} = f^{-1} \circ v \circ g.$$

La proposition 7 se déduit donc du

Lemme 1. *Soit* $\sigma \in \mathfrak{G}$, *d'ordre au moins 5. Soient* f *et* g *des endomorphismes non nuls de* K. *La relation* (I) *est vraie si et seulement si il existe* $a \in \mathbb{K}$ *et* $\nu \in \mathfrak{G}$ *tels que*

$$g = a\nu \quad \text{et} \quad f = a^{1+\sigma}\nu.$$

Pour démontrer ce lemme, décomposons f et g sur la base $\mathfrak{G}$ de Hom(K,K) et supposons (I) vraie. Soit $a(\tau)$ (resp. $b(\tau)$) la composante de f (resp. de g) sur $\tau \in \mathfrak{G}$.

On a
$$f \circ (1*\sigma) = \sum_\tau a(\tau)(\tau*\tau\sigma) \qquad (\tau \in \mathfrak{G})$$
et
$$(1*\sigma) \circ (g \times g) = \sum_{\tau,\nu} b(\tau)b(\nu)^\sigma(\tau*\nu\sigma) \qquad (\tau,\nu \in \mathfrak{G}),$$
d'où il résulte que si τ est distinct de ν et de $\nu\sigma^2$,

$$b(\tau)b(\nu)^\sigma - b(\nu\sigma)b(\nu\sigma^{-1})^\sigma = 0.$$

(cette relation étant d'ailleurs vide si $\tau = \nu\sigma$)

tandis que

$$b(\tau)^{1+\sigma} - b(\tau\sigma)b(\tau\sigma^{-1})^\sigma = a(\tau).$$

Pour établir cette dernière relation, on a utilisé le fait que σ^2 n'est pas l'identité, si bien que $(\tau*\tau\sigma)$ détermine τ. Elle montre que g détermine f; l'application biadditive $(1*\sigma)$ est donc surjective, et, en conséquence, si g est bijective, f est bijective (assertion évidemment fausse si $\sigma = 1$ ou $\sigma = \sigma_o$).

Supposons par contradiction l'existence de τ et ν tels que

$$b(\tau)b(\nu) \neq 0 \text{ et } \tau \neq \nu,\ \nu\sigma^2.$$

On déduit des premières relations que si en outre $\tau\nu^{-1} \notin \langle\sigma\rangle$, il existe $\alpha \in \mathbb{K}$, de norme 1 relativement à $\langle\sigma\rangle$ tel que

$$b(\nu\sigma^j) = \alpha^{1+\sigma+\dots+\sigma^{j-1}} b(\nu)^{\sigma^j}.$$

En utilisant l'hypothèse selon laquelle σ n'est pas d'ordre 2, 3 ou 4, on obtient la même conclusion dès que $\tau\nu^{-1} \notin \{1,\sigma^2\}$. On a alors

$$b(\nu)^{1+\sigma} - b(\nu\sigma)b(\nu\sigma^{-1})^\sigma = 0.$$

Ainsi, si σ est d'ordre au moins 5 et si g admet au moins deux coefficients non nuls, f est nulle, ce qui démontre le lemme, f se déduisant de g.

Les groupes d'automorphismes de $U(\sigma)$ et de $U_o(\sigma_o)$, quand σ est d'ordre 3 ou 4, se calculent grâce aux lemmes suivants, qui peuvent se démontrer par les mêmes méthodes que le lemme 1. On y note $N(x)$ la norme de x relativement à $\langle\sigma\rangle$ $(x \in \mathbb{K})$.

Lemme 2. *Les solutions* $(f,g) \in \mathrm{Hom}(K,K)^2$ *de la condition*

$$f \circ (1*\sigma) = (1*\sigma) \circ (g \times g) \ , \ f \neq 0$$

sont

(a) Si σ *est d'ordre 3,* g *de la forme*

$$g = a\nu + b\nu\sigma + c\nu\sigma^2 \qquad (a,\ b,\ c \in \mathbb{K},\ \nu \in \mathfrak{G})$$

et f *s'en déduisant;* g *est inversible si et seulement si*

$$N(a) + N(b) + N(c) \neq \mathrm{Tr}(ab^{\sigma}c^{\sigma^2}).$$

(c) Si σ *est d'ordre 4,* g *est de l'une des deux formes*

$$g = a\nu + b\nu\sigma + \alpha a\nu\sigma^2 + \alpha^{\sigma}b\nu\sigma^3, \text{ où } a,\ b \in \mathbb{K} \text{ et } \alpha^{1+\sigma^2} = 1,\ \nu \in \mathfrak{G}.$$

$$g = a\nu + b\nu\sigma^2, \text{ où } a,\ b \in \mathbb{K} \text{ et } \nu \in \mathfrak{G}.$$

f *se déduisant de* g.

L'endomorphisme g *n'est inversible que dans le dernier cas et sous la condition*

$$N(a) + N(b) \neq a^{1+\sigma^2}.b^{\sigma+\sigma^3} + a^{\sigma+\sigma^3}.b^{1+\sigma^2}.$$

Lemme 3. *Soit* $(f,g) \in \mathrm{End}(K_o) \times \mathrm{End}(K)$ *tel que*

$$f \neq 0,\ f \circ \Phi = \Phi \circ (g \times g),\ \text{où } \Phi = 2a_o(1*\sigma_o).$$

Alors g *est de la forme*

$$g = a\tau + b\tau\sigma_o \ , \text{ où } a,\ b \in \mathbb{K} \text{ et } \tau \in \mathfrak{G},$$

f *se déduit de* g *et* g *est inversible si et seulement si*

$$a^{1+\sigma_o} \neq b^{1+\sigma_o}.$$

III. COBORDS MULTIADDITIFS.

Proposition. *Soient* A *un groupe abélien de type fini et* Z *un groupe abélien sur lequel* A *opère trivialement. Supposons* 2 *inversible dans* Z. *Toute fonction multi-additive de* A^n *dans* Z *est un* n-*cocycle, et c'est un* n-*cobord si et seulement si son antisymétrisée selon le groupe symétrique de degré* n *est nulle.*

Que toute fonction multiadditive soit un cocycle se vérifie aisément.

Si f est une application de A^n dans Z et σ un élément du groupe symétrique S_n, nous posons

$$(\sigma^{-1}.f)(s_1,\ldots,s_n) = f(s_{\sigma(1)},\ldots s_{\sigma(n)}).$$

Ainsi le groupe symétrique opère sur le groupe des fonctions de A^n dans Z, et il stabilise le sous-groupe des applications multiadditives, lequel sera noté V.Soit Π l'opérateur d'antisymétrisation:

$$\Pi.f = \sum_{\sigma \in S_n} \varepsilon(\sigma)(\sigma.f) \qquad (\varepsilon(\sigma) \text{ est la signature de } \sigma).$$

Il est clair que pour tout $\sigma \in S_n$, d'ordre k, considéré comme un endomorphisme de V, ou de $\mathcal{F}(A^n,Z)$ on a

$$\mathrm{Im}(1 - \varepsilon(\sigma)\sigma) \subset \mathrm{Ker}(1 + \varepsilon(\sigma)\sigma + \ldots + (\varepsilon(\sigma)\sigma)^{k-1}) \subset \mathrm{Ker}\,\Pi,$$

la dernière inclusion résultant de la factorisation

$$\Pi = (\sum_{\eta \in S_n/\langle\sigma\rangle} \varepsilon(\eta)\eta)(1 + \varepsilon(\sigma)\sigma + \ldots + (\varepsilon(\sigma)\sigma)^{k-1}).$$

On constate ainsi que tout cobord (multiadditif ou non) est annulé par Π. En effet, si $g \in \mathcal{F}(A^{n-1},Z)$, l'application $((s_i) \longrightarrow g(s_1,\ldots,s_{j-1}+s_j,\ldots,s_n))$ est annulée par $(1 - (j-1,j))$, tandis que $((s_i) \longrightarrow g(s_1,\ldots,s_{n-1}))$ est la transformée par le cycle $(1,2,\ldots,n)$ de l'application $((s_i) \longrightarrow g(s_2,\ldots,s_n))$.

Nous allons démontrer successivement, S_n et Π opérant sur V,

(I) $\mathrm{Ker}\,\Pi$ est engendré par la réunion des $\mathrm{Ker}(1 - \tau)$ (τ transposition);

(II) Si $\Sigma \subset S_n$ et Σ engendre S_n, $\mathrm{Ker}\,\Pi$ est engendré par la réunion des $\mathrm{Im}(1 - \varepsilon(\sigma)\sigma)$ ($\sigma \in \Sigma$);

(III) Pour $1 \leqslant j \leqslant n-1$, $(1 + (j,j+1))(V) \subset \mathcal{B}^n(A,Z)$.

L'hypothèse selon laquelle la multiplication par 2 est une bijection sur Z n'est utilisée que pour démontrer (II).

(I) Décomposons A en somme directe de groupes cycliques C_i $(i \in I)$. Pour toute application f de $\{1,..,n\}$ dans I, soit V_f le groupe des applications multiadditives de $C_{f(1)} \times \ldots \times C_{f(n)}$ dans Z. Ainsi V est somme directe des V_f.

Si f n'est pas injective, soient j et k distincts tels que $f(j) = f(k)$. Si u appartient à la composante V_f de V, comme $C_{f(j)} = C_{f(k)}$ est cyclique et u est multiadditif, on a $(j,k).u = u$. Ainsi V_f est tout entier contenu dans le noyau de $(1 - (j,k))$, a fortiori dans le noyau de Π.

Supposons maintenant f injective, et soit J son image. Le groupe S_n permute régulièrement l'ensemble des applications injectives d'image J, et opère de même sur les composants correspondant de V, par

$$\sigma(V_f) = V_{(f \circ \sigma^{-1})} \qquad (\sigma \in S_n)\ .$$

Il stabilise donc

$$V_J = \sum_{\mathrm{Im}(f') = J} V_{f'}\ .$$

Il est clair que

$$\mathrm{Ker}\,\Pi \cap V_f = \{0\}.$$

Soit K_J le groupe engendré par la réunion des $(1 - \varepsilon(\sigma)\sigma)(V_f)$ $(\sigma \in S_n)$; c'est un supplémentaire de V_f dans V_J. En effet, si $u_\sigma \in \sigma(V_f)$, il existe $u^{(\sigma)} \in V_f$ tel que $u_\sigma = \varepsilon(\sigma)\sigma.u^{(\sigma)}$, et on a alors

$$\sum_{\sigma \in S_n} u_\sigma = \Big(\sum_{\sigma \in S_n} u^{(\sigma)}\Big) - \sum_{\sigma \in S_n} (1 - \varepsilon(\sigma)\sigma).u^{(\sigma)}\ .$$

Les sous-groupes engendrant K_J étant annulés par Π, on en conclut que

$$K_J = \mathrm{Ker}\,\Pi \cap V_J\ .$$

Au total $\mathrm{Ker}\,\Pi$ est engendré par les groupes $\mathrm{Ker}(1 - \tau)$ (τ transposition) et $\mathrm{Im}(1 - \varepsilon(\sigma)\sigma)$ $(\sigma \in S_n)$. Mais les transpositions engendrent S_n, et si $\sigma = \sigma_1\sigma_2$,

$$1 - \varepsilon(\sigma)\sigma = 1 - \varepsilon(\sigma_2)\sigma_2 + (1 - \varepsilon(\sigma_1)\sigma_1)\varepsilon(\sigma_2)\sigma_2.$$

En outre, si τ est une transposition, $\mathrm{Ker}(1 - \tau)$ contient $\mathrm{Im}(1 + \tau)$.On en déduit (I).

(II) Si 2 est inversible dans Z, pour toute involution τ de S_n, on a

$$\mathrm{Ker}(1 - \tau) = \mathrm{Im}(1 + \tau).$$

Selon (I), $\mathrm{Ker}\,\Pi$ est engendré par les sous-groupes $\mathrm{Im}(1 + \tau)$ (τ transposition)

Selon la démonstration de (I) , on obtient également $\mathrm{Ker}\,\Pi$ par génération en considérant les sous-groupes $\mathrm{Im}(1 - \varepsilon(\sigma)\sigma)$ $\sigma \in \Sigma$, dès lors que Σ engendre S_n.

(III) Soit $u \in V$. Posons $v = (1 + (j,j+1)).u$, et soit $g \in \mathcal{F}(A^{n-1},Z)$ définie par

$$g(s_1,\ldots,s_{n-1}) = g(s_1,\ldots,s_j,s_j,s_{j+1},\ldots,s_{n-1}).$$

On constate que

$$d^{n-1}(A,Z)(g) = (-1)^j v,$$

ce qui démontre l'assertion (III).

La dernière assertion de la proposition se déduit de (II) et (III) puisque les transpositions $(j,j+1)$ $(j = 1,\ldots,n-1)$ engendrent S_n.

L'inversibilité de 2 dans Z est nécessaire. Si par exemple Z est un groupe d'exposant 2, le noyau de Π dans V est le groupe des applications multiadditives et symétriques de A^n dans Z. Si $n = 2$, ces 2-cocycles définissent des extensions abéliennes (non nécessairement scindées) de A par Z. Une application biadditive est un 2-cobord si et seulement si elle est alternée. Donc, si $2Z = \{0\}$, le groupe des 2-cobords additifs de A dans Z est l'image de $(1 + \tau)$ (τ transposition).

La proposition précédente sera utilisée pour $n = 3$. On a alors, selon (II)

$$\mathrm{Ker}\,\Pi = (1 - (1,3,2))(V) + (1 + (2,3))(V).$$

Si H est une fonction triadditive dont l'antisymétrisée est nulle, il existe F et G triadditives telles que

$$H(s,t,u) = F(s,t,u) - F(t,u,s) + G(s,t,u) + G(s,u,t) \quad ((s,t,u) \in A^3).$$

Alors H est dérivée de h, où

$$h(s,t) = F(s,t,t) + F(s,t,s) + G(s,t,t) \qquad ((s,t) \in A^2).$$

On a aussi $\quad \mathrm{Ker}\,\Pi \cap \mathrm{Ker}(1 + (2,3)) = (1 - (2,3))(1 - (1,3,2))(V).$

Par conséquent, une fonction H triadditive de A^3 dans Z, alternée en les deux dernières variables est un 3-cobord si et seulement si

$$H(s,t,u) + H(t,u,s) + H(u,s,t) = 0 \text{ quel que soit } (s,t,u) \in A^3.$$

Il exste alors une fonction triadditive F de A^3 dans Z telle que

$$H(s,t,u) = F(s,t,u) - F(s,u,t) - F(t,u,s) + F(u,t,s), \quad ((s,t,u) \in A^3),$$

et H est la dérivée de h, où

$$h(s,t) = F(s,t,s) - F(s,s,t) - F(t,s,s) - F(t,s,t) \qquad ((s,t) \in A^2).$$

IV. SUR CERTAINS p-GROUPES DE CLASSE 3.

On désigne par p un nombre premier impair.

Soient U un p-groupe, X et D deux sous-groupes normaux de U, D contenant X, tels que les facteurs X, D/X et U/D soient centraux. La reconstruction de U depuis ces facteurs peut se faire par étapes: construction des groupes de classe au plus 2, D comme extension de Y = D/X par X, et E = U/X comme extension de Z = U/D par Y, puis opération de E sur D, enfin recollement, la proposition 5 fournissant un critère de recollement. On peut espérer que lorsque X, Y et Z sont élémentaires, les méthodes linéaires exposées au chapitre II permettront de donner des conditions simples, de type linéaire, pour que l'obstruction (élément de $\mathcal{H}^3(Z,X)$) soit nulle. Ce but n'est atteint que sous certaines hypothèses supplémentaires, soit que E soit abélien (proposition 2 et corollaire), soit que le dérivé de U soit d'exposant p (proposition 4). Dans le cas général, on est ramené au même problème, D étant remplacé par sa projection abélienne D_o, et l'opération de E sur D_o convenablement définie.

Une notation: Si $f \in \mathcal{F}(U \times V,W)$, on note

$$f_V : V \longrightarrow \mathcal{F}(U,W) \qquad \text{et} \qquad {}_Uf : U \longrightarrow \mathcal{F}(V,W)$$

les applications qui s'en déduisent naturellement, étant entendu que si U et W sont des groupes et f un morphisme en la première variable, f_V est à valeurs dans Hom(U,W), etc...

Constantes: X, Y et Z sont des groupes abéliens, noté additivement. Sont données deux extensions centrales

$$0 \longrightarrow Y \xrightarrow{i} E \xrightarrow{\pi} Z \longrightarrow 0$$

$$0 \longrightarrow X \xrightarrow{i'} D \xrightarrow{\pi'} Y \longrightarrow 0$$

de classes respectives $\Gamma \in \mathcal{H}^2(Z,Y)$ et $\Theta \in \mathcal{H}^2(Y,X)$.

Soient des sections $\sigma_E : Z \longrightarrow E$ et $\sigma_D : Y \longrightarrow D$; elles définissent des cocycles $\gamma \in \Gamma$ et $\beta \in \Theta$. On désigne par ϕ et ψ les images respectives de Γ et Θ dans

$\mathcal{A}lt(Z,Y)$ et $Alt(Y,X)$(proposition 1 du chapitre II). Le symbole $d^1(M,N)$, où M opère trivialement sur N, sera simplifié en "d", pour tous M, N.

Lemme 1. *Soient* C *un groupe abélien et* $f \in Hom(Y,C)$. *Il existe un morphisme* F *de* E *dans* C *qui prolonge* f *si et seulement si* $\mathcal{H}^2(Z,f)(\Gamma)$ *est nul. Alors* $\tilde{F}$ *est définie par l'application* $(F \circ \sigma_E)$ *qui doit vérifier*

$$d(F \circ \sigma_E) = f \circ \gamma.$$

La première assertion exprime l'exactitude de la suite

$$Hom(E,C) \longrightarrow Hom(Y,C) \longrightarrow \mathcal{H}^2(Z,C),$$

où la dernière flèche est le morphisme de transgression $(f \longrightarrow \mathcal{H}^2(Z,f)(\Gamma))$. En posant $\zeta = F \circ \sigma_E$, on aura, pour un éventuel prolongement F de f,

$$F(i(y)\sigma_E(s)) = f(y) + \zeta(s) \qquad (y \in Y,\ s \in Z)$$

et F est un morphisme si et seulement si

$$\zeta(s) + \zeta(t) = f(\gamma(s,t)) + \zeta(s + t) \quad (s \in Z,\ t \in Z).$$

Corollaire. *Une opération de* E *sur* D, *triviale sur* X *et sur* Y, *et prolongeant l'action de* Y *sur* D *n'existe que si et seulement si*

(1) $$\mathcal{H}^2(Z,{}_Y\psi)(\Gamma) = 0.$$

Une telle opération est définie par une application ζ *de* Z *dans* $Hom(Y,X)$ *telle que*

(2) $$d\zeta = {}_Y\psi \circ \gamma,$$

où, si $(y,s) \in Y \times Z$, $\sigma_E(s).\sigma_D(y) = i'(\zeta(s)(y))\sigma_D(y)$.

En effet, selon I,(c), une opération de E sur D est définie par un morphisme F de E dans $Hom(Y,X)$; la restriction de F à Y est donnée par

$$\sigma_D(y')(x,y)\sigma_D(y')^{-1} = i'(F(i(y'))(y))(x,y) \quad (x \in X,\ y,\ y' \in Y)$$

soit $$F(i(y'))(y) = \psi(y',y)$$

ou $$F \circ i = {}_Y\psi.$$

Le lemme 1 permet de conclure. La condition (1) du corollaire est d'ailleurs une version triviale de l'interprétation de $(\upsilon_6 \circ \upsilon_2)$ (I, proposition 4).

Proposition 1. *Soit* ζ: $Z \longrightarrow Hom(Y,X)$ *telle que* (2) *et soit* μ *l'application de* Z^3 *dans* X *définie par*

(3) $$\mu(s,t,u) = \zeta(s)(\gamma(t,u)) + \beta(\gamma(t,u),\gamma(s,t+u)) - \beta(\gamma(s,t),\gamma(s+t,u)).$$

C'est un 3-cocycle de Z *dans* X *(avec action triviale).*

Il existe une extension de Z *par* D *qui se restreint en* Γ *modulo* X *et qui induit sur* D *l'action définie par* ζ *(selon le corollaire du lemme 1) si et seulement si* $\ulcorner\mu\urcorner$ *est nul. Si* $\mu = -d^2(Z,X)(\omega)$, *une telle extension est réalisée sur* $X \times Y \times Z$ *par la loi*

$$(x,y,z)(x',y',z') = (x+x'+\beta(y,y')+\zeta(z)(y')+\omega(z,z')+\beta(y+y',\gamma(z,z')) ,\quad y+y'+\gamma(z,z') ,\ z+z').$$

Cette proposition est une réécriture de la proposition 5 du chapitre I; A, N $\hat{N}$, G, Q, δ, $(h_o \circ \sigma)$, m sont devenus respectivement X, Y, D, E, Z, γ, ζ et $-\omega$.

Lorsque E est abélien, il s'agit essentiellement de relever la fonction ψ en un élément de $\mathrm{Alt}(E,X)$ (II, proposition 1). Quand X est d'exposant p, on a une condition nécessaire et suffisante:

Proposition 2. *Supposons que* X *soit d'exposant* p *et* E *abélien. Soient* $\xi \in \mathrm{Hom}(Y,\mathcal{F}(Z,X))$, $\zeta \in \mathcal{F}(Z,\mathrm{Hom}(Y,X))$ *liées par*

$$\zeta(s)(y) = \xi(y)(s) \qquad (s \in Z,\ y \in Y).$$

Il existe $\Psi \in \mathrm{Alt}(E,X)$ *tel que*

(a) ψ *soit la restriction de* Ψ *à* Y

et *(b)* $\Psi(\sigma_E(s),i(y)) = \zeta(s)(y) \qquad (s \in Z, y \in Y).$

si et seulement si on a (1), (2) et (3):

(1) $\quad H^2(Z,{}_Y\psi)(\Gamma) = 0$

(2) $\quad d\zeta = {}_Y\psi \circ \gamma$

(3) $\quad H^2(Z,\xi)(\Gamma) = 0$

et Ψ *est définie par* $g = \Psi \circ (\sigma_E \times \sigma_E)$ *antisymétrique telle que*

(5) $\quad d_Z g = -\xi \circ \gamma.$

Démonstration. Soit $\Psi \in \mathrm{Alt}(E,X)$ telle que (a) et (b) soient vraies. Si $e \in E$, ${}_E\Psi(e)$ est un morphisme de E dans X. Par restriction à Y, on obtient un morphisme F de E dans $\mathrm{Hom}(Y,X)$ qui prolonge ${}_Y\psi$ (d'après (a)). Selon le lemme 1 et son corollaire la condition (1) est nécessaire à son existence et $(F \circ \sigma_E)$ - qui doit être égal à ζ selon (b) - vérifie (2). Alors Ψ est caractérisée par $g = \Psi \circ (\sigma_E \times \sigma_E)$. Si E est écrit sur le support $Y \times Z$, à l'aide de γ, on a alors pour s, $t \in Z$ et y, $z \in Y$,

$$\Psi((y,s),(z,t)) = \psi(y,z) + \zeta(s)(z) - \zeta(t)(y) + g(s,t).$$

On voit que Ψ est additive en la première variable si et seulement si

$$g(s_1+s_2,t) = g(s_1,t) + g(s_2,t) + \xi(\gamma(s_1,s_2))(t)$$

soit la relation (5). Cette relation n'admet de solutions en g que si et seulement si (4) est satisfaite.

Considérons donc une solution de (5), soit f, et, pour exprimer l'additivité en la seconde variable, soit la fonction G de Z^3 dans X définie par

$$G(t,s_1,s_2) = - f(t,s_1+s_2) + f(t,s_1) + f(t,s_2) - \zeta(t)(\gamma(s_1,s_2)).$$

Les éléments s_1 et s_2 de Z étant fixés, en dérivant cohomologiquement en t, on a

$$\begin{aligned} &- G(t_1+t_2,s_1,s_2) + G(t_1,s_1,s_2) + G(t_2,s_1,s_2) \\ &= \xi(\gamma(t_1,t_2))(s_1+s_2) - \xi(\gamma(t_1,t_2))(s_1) - \xi(\gamma(t_1,t_2))(s_2) \\ &\quad - \zeta(t_1)(\gamma(s_1,s_2)) - \zeta(t_2)(\gamma(s_1,s_2)) + \zeta(t_1+t_2)(\gamma(s_1,s_2)) \\ &= - \psi(\gamma(s_1,s_2),\gamma(t_1,t_2)) - \psi(\gamma(t_1,t_2),\gamma(s_1,s_2)) \\ &= 0 \end{aligned}$$

(on a utilisé le fait que f satisfait à (5), puis la relation (2), enfin l'hypothèse "ψ alternée")

Donc G est additive en la première variable. En outre l'application $G_{Z \times Z}$ n'est autre, par définition, que $(d\, f_Z - \xi \circ \gamma)$; c'est un 2-cobord de Z dans $\mathcal{F}(Z,X)$ à valeurs dans Hom(Z,X). Mais Hom(Z,X) est facteur direct de $\mathcal{F}(Z,X)$, car X est d'exposant p. Donc $G_{Z \times Z}$ est dérivée d'une application de Z dans Hom(Z,X), et il existe $h: Z \times Z \longrightarrow X$, additive en la première variable, telle que

$$G(t,s_1,s_2) = - h(t,s_1+s_2) + h(t,s_1) + h(t,s_2).$$

Soit $f' = f - h$. On a

$$df'_Z = \xi \circ \gamma \qquad \text{(par définition de G)}$$

et $$d_Z f' = d_Z f - d_Z h = d_Z f = - \xi \circ \gamma.$$

Considérons maintenant l'antisymétrisée g de f'. C'est une solution de (5), car $d_Z g = (d_Z f' - df'_Z)/2 = - \xi \circ \gamma$. Il est clair que Ψ , définie par ψ, ζ et g est antisymétrique et additive en la première variable, donc alternée de Z dans X.

Corollaire. *Hypothèses et notations des propositions 1 et 2:* X *d'exposant* p *et* E *abélien. Pour que* μ *soit un cobord, il faut et il suffit que*

(4) $$H^2(Z,\xi)(\Gamma) = 0.$$

Démonstration. Selon la proposition 1, μ est un 3-cobord si et seulement si il existe une extension de E par X qui se restreint en Θ sur Y, l'opération sur D étant définie par ζ. Puisque $\mathrm{Ext}^2(Z,X)$ est nul, la restriction $\mathrm{Ext}^1(E,X) \longrightarrow \mathrm{Ext}^1(Z,X)$ est surjective. Selon la proposition 1 du chapitre II, il suffit donc qu'il existe Ψ satisfaisant aux conditions énoncées dans la proposition 2.

Remarque: Si Z est somme directe de groupes cycliques et si l'un des groupes Z, Y est d'exposant p, Γ est défini par $\lambda \in \mathrm{Hom}(\Omega_1(Z),Y/pY)$ et $\mathcal{H}^2(Z,\xi)(\Gamma)$ défini par $(\xi_p \circ \lambda)$, où $\xi_p \in \mathrm{Hom}(Y/pY,\mathcal{F}(Z,X))$ est induit par ξ. La condition (4) équivaut alors à $\xi_p(\lambda(s))(t) = 0$ si $s \in \Omega_1(Z)$ et $t \in Z$. Supposons pour simplifier X et Y et Z d'exposants p. La condition (1) équivaut à

(1') $\qquad {}_Y\psi \circ \lambda = 0.$

Soit $\bar{Y} = Y/\mathrm{Im}\,\lambda$. Si (1') est vraie, la fonction ψ définit $\bar{\psi} \in \mathrm{Alt}(\bar{Y},X)$ et il existe $\bar{\zeta} : Z \longrightarrow \mathrm{Hom}(\bar{Y},X)$ telle que $d\bar{\zeta} = {}_{\bar{Y}}\bar{\psi} \circ \bar{\gamma}$(notations évidentes). L'application $\bar{\zeta}$ définit ζ telle que (2) et $\zeta(t)$ est nulle sur l'image de λ; la condition (4) est donc satisfaite. L'image de $\mathcal{H}^2(E,X)$ dans $\mathcal{H}^2(Y,X)$ est donc caractérisée par la relation (1').

Proposition 3. *Supposons* X *et* Y *d'exposant* p *et* Z *de type fini. Soient* ζ *telle que* (2) *et* μ *définie par* (3), $\Gamma_o = \lambda \in \mathrm{Hom}(\Omega_1(Z),Y)$, $\Theta_o = \nu$.

(a) Il existe $\zeta_o \in \mathrm{Hom}(Z,\mathrm{Hom}(Y,X))$ *tel que, pour tout* $s \in Z$, $\zeta(s)$ *et* $\zeta_o(s)$ *coïncident sur les images de* ϕ *et de* λ.

(b) Pour que μ *soit un 3-cobord, il est nécessaire que*

(6) $\qquad$ si $(s,t) \in Z^2$, $\zeta(s)(\lambda(t)) = \nu(\phi(s,t))$,

(7) $\qquad$ si $(s,t,u) \in Z^3$, $\zeta(s)(\phi(t,u)) + \zeta(u)(\phi(s,t)) + \zeta(t)(\phi(u,s)) = 0$,

et il suffit que $\mu_o : Z^3 \longrightarrow X$ *défini par*

(8) $\quad \mu_o(s,t,u) = \zeta_o(s)(\gamma_o(t,u)) - \beta_o(\gamma_1(s,t),\gamma_1(s+t,u)) + \beta_o(\gamma_1(t,u),\gamma_1(s,t+u))$

soit un 3-cobord et que la relation (7) *soit vraie*.

Démonstration. Notons $\mu(\beta,\gamma,\zeta)$ le cocycle défini par la relation (3). La relation (1) implique que ${}_Y\psi$ est nulle sur les images de ϕ et de λ. Posons

$$Y_o = \mathrm{Im}\,\lambda + \mathrm{Im}\,\phi .$$

On a donc $\psi(t,s) = \psi(s,t) = 0$ dès que $t \in Y_o$. Selon (2) et ce qui précède, en composant ζ avec la restriction de $\mathrm{Hom}(Y,X)$ dans $\mathrm{Hom}(Y_o,X)$, on obtient un morphisme de Z dans $\mathrm{Hom}(Y_o,X)$, lequel est restriction d'un morphisme ζ_o de Z dans $\mathrm{Hom}(Y,X)$, ce qui démontre (a).

Lemme 2. *Soient* G *un groupe,* x *et* y *des éléments de* G *tels que* $[y,x]$ *et* y *commutent à* $g = [[y,x],y]$. *On a, pour tout entier naturel* k,

$$[x,y^k] = [x,y]^k g^{\binom{k}{2}}.$$

(Démonstration élémentaire par récurrence sur k depuis l'identité

$$[x,yz] = [x,y][x,z][[z,x],y])$$

Corollaire. *Soit* U *un* p-*groupe de classe au plus* 3, *tel que* $[U,[U,U]]$ *soit d'exposant au plus* p. *Si* p *est impair, on a, quels que soient* x, y $\in$ U,

$$[x,y^p] = [x,y]^p.$$

Sous les hypothèses particulières de la proposition 3, dans un groupe extension de Z par D comme la proposition 1 l'envisage, l'identité énoncée dans le corollaire précédent se traduit par (6). De même, dans un tel groupe la formule de Jacobi fournit (7); en effet, si ρ est une section depuis Z, on a

$$[\rho(s),[\rho(t),\rho(u)]] = \zeta(s)(\phi(t,u)).$$

Il résulte de la proposition 1 que si μ est un 3-cobord, un tel groupe existe et les relations (6) et (7) sont vraies.

Posons, ζ_o vérifiant (a),

$$\zeta = \zeta_o + \zeta_1.$$

Quel que soit $s \in Z$, $\zeta(s)$ et $\zeta_o(s)$ coïncident sur Y_o, tandis que $\zeta_1(s)$ est nul sur Y_o. Par conséquent la relation (6) (resp. (7)) est vraie simultanément pour ζ et ζ_o, tandis que $d\zeta_o$ est nul.

D'autre part, la relation (7) est trivialement vraie pour ζ_1 et on a

$$(6)_1 \qquad \zeta_1(s)(\lambda(t)) = 0 \qquad (s,t) \in Z^2,$$

et de (2) on déduit

$$(2)_1 \qquad d\zeta_1 = {}_Y\psi \circ \gamma.$$

Parallèlement, le 2-cocycle β se décompose en $\beta = \beta_o + \beta_1$, où β_o est dans la classe $(\nu,0)$, projection abélienne de $\Theta = (\nu,\psi)$, et $\beta_1 = \psi/2$ est dans la classe $(0,\psi)$ (cf les propositions 1 et 2 du chapitre II). On voit que

$$\mu(\beta,\gamma,\zeta) = (\beta_o,\gamma,\zeta_o) + \mu(\beta_1,\gamma,\zeta_1),$$

les 2 termes de droite étant des 3-cocycles définis par la formule de la proposition 1 (grâce à $(2)_1$). Il résulte de la relation (1) que ${}_Y\psi \circ \phi$ est nul, d'où

$$\mu(\beta_1,\gamma,\zeta_1) = \mu(\beta_1,\gamma_o,\zeta_1)$$

et $${}_Y\psi \circ \gamma = {}_Y\psi \circ \gamma_o .$$

La relation $(6)_1$ garantit que $\mu(\beta_1,\gamma_o,\zeta_1)$ est un cobord (proposition 2 et corollaire)

Le terme restant $\mu(\beta_o,\gamma,\zeta_o)$correspond au cas où D est remplacé par sa projection abélienne D_o, et ζ par ζ_o. Plus précisément la classe de μ est l'image de Γ par le morphisme $\partial^2(Z,\Theta_o) = \partial_{\Theta_o}$, l'énoncé de la proposition 1 se réduisant dans ce cas à l'exactitude de la suite

$$H^2(Z,D_o) \longrightarrow H^2(Z,Y) \xrightarrow{\partial_{\Theta_o}} H^3(Z,X).$$

L'application qui à Γ associe la classe de $\mu(\beta_o,\gamma,0)$ est donc additive en Γ, et si $\partial_{\Theta_o}(\Gamma)$ est nul, (6) et (7) sont vraies.

Selon le corollaire de la proposition 2, $\mu(\beta\ ,\gamma\ ,0)$ est un cobord. Selon la proposition démontrée au chapitre III, l'application qui à (s,t,u) associe $\zeta_o(s)(\gamma_1(t,u))$ est un cobord si et seulement si (7) est vraie. Au total $\partial_{\Theta_o}(\Gamma)$ est nul si et seulement si μ_o est un cobord et (7) vraie.

On aurait aimé démontrer que (6) et (7) donnent des conditions suffisantes. C'est le cas si E est abélien (proposition 2). Supposons plus généralement que $(\nu \circ \phi)$ soit nul, et les relations (2), (6) et (7). La proposition 2 s'applique à la projection abélienne E_o de E (alors (4) et (6) coïncident avec $\xi \circ \lambda = 0$), si bien que $\mu(\beta_1,\gamma_o,\zeta)$ et $\mu(\beta_1,\gamma_o,\zeta_1)$ sont des cobords. Leur différence, à savoir $((s,t,u) \longrightarrow \zeta_o(s)(\gamma_o(t,u)))$, est un cobord. Par (7), l'application $((s,t,u) \longrightarrow \zeta_o(s)(\gamma_1(t,u)))$ est aussi un cobord. Donc $\mu(\beta_o,\gamma,\zeta_o)$ est un cobord si et seulement si $\mu(\beta_o,\gamma,0)$ est un cobord. Cette dernière condition équivaut à l'existence d'une extension centrale de Z par D_o dont la restriction à Y réalise Γ, ou encore à l'existence d'une fonction alternée Φ de Z^2 dans D_o, d'image ϕ modulo X. L'égalité $\nu \circ \phi = 0$ exprime que la restriction de Θ_o à l'image de ϕ est nulle, donc Im ϕ se remonte dans $\Omega_1(D_o) = X + \operatorname{Ker} \nu$ et il en résulte que ϕ se factorise effectivement à travers π'_o par une application alternée de Z^2 dans D_o. On a donc la

<u>Proposition</u> 4. <u>*Hypothèses et notations de la proposition*</u> *3.* <u>*Si*</u> $(\nu \circ \phi)$ <u>*est nul,*</u> μ

est un 3-cobord si et seulement si (6) *et* (7) *sont vraies.*

Proposition 5. *Soient* q *une puissance de* p, K *le groupe additif de* $\mathbb{K} = GF(q)$. *Soit* U *un* **p**-*groupe de classe 3 admettant un groupe cyclique d'automorphismes* H *d'ordre* $(q-1)$ *opérant irréductiblement sur chacun des quotients de la suite centrale descendante de* U. *Alors* U.H *est isomorphe à l'un des produits semi-directs* $V[\sigma].K^{\times}$ *où* $\sigma \in \mathfrak{G} = \mathrm{Aut}(\mathbb{K})$ *et* $V[\sigma]$ *est de support* $K_1 \times K_o \times K$ *avec les lois*

$$(x,y,z,)(x',y',z') = (x+x'+\omega(z,z')+\zeta(z,y')\ ,\ y+y'+\gamma(z,z')\ ,\ z+z')$$

$$\lambda(x,y,z)\lambda^{-1} = (\rho(\lambda)x, \lambda^{1+\sigma}y, \lambda z) \qquad (\lambda \in K^{\times}),$$

et soit (i) $K_1 = K_o = K$, $\sigma^2 \neq 1$, $\gamma(s,t) = \gamma_1(s,t) = st^{\sigma} - s^{\sigma}t$, $\zeta(s,t) = st$, $\omega(s,t) = s^2t^{\sigma} + st^{1+\sigma}$ et $\rho(\lambda) = \lambda^{2+\sigma}$.

soit (ii) $K_1 = K_o = K$, $\sigma^2 \neq 1$, $\gamma = \gamma_1$, $\zeta(s,t) = st^{\sigma} - s^{\sigma^2}t$, $\rho(\lambda) = \lambda^{1+\sigma+\sigma^2}$, $\omega(s,t) = \omega_2(s,t) = s^{1+\sigma}t^{\sigma^2} + s^{\sigma+\sigma^2}t + s^{\sigma}t^{1+\sigma^2} - s^{1+\sigma^2}t^{\sigma}$.

soit (iii) $K_o = K$, K_1 est le groupe additif du corps des points fixes de σ, $\gamma = \gamma_1$, $\zeta(s,t) = \mathrm{Tr}_{\mathbb{K}/\mathbb{K}_1}(b(st^{\sigma} - s^{\sigma^2}t))$ où $b \in K^{\times}$, $\rho(\lambda) = \lambda^{1+\sigma+\sigma^2}$, σ est d'ordre 3, $\omega(s,t) = \mathrm{Tr}_{\mathbb{K}/\mathbb{K}_1}(b\omega_2(s,t))$,

soit (iv) $K_1 = K$, K_o est le groupe additif du corps des points fixes de σ, σ est d'ordre 2, $\gamma(s,t) = a_o(st^{\sigma} - s^{\sigma}t)$, où $a_o + a_o^{\sigma} = 0$, $\zeta(s,t) = st$, $\rho(\lambda) = \lambda^{2+\sigma}$, $\omega(s,t) = a_o(s^2t^{\sigma} + st^{1+\sigma})$.

Démonstration. Les facteurs irréductibles sont nécessairement des groupes d'exposant p. On a donc

$$[U,U] = \Xi(U) \quad \text{(groupe de Frattini)}$$

et H opère fidèlement sur l'espace $Z = U/\Xi(U)$, premier facteur de la suite centrale descendante. Soit

$$X = [[U,U],U].$$

Le groupe U/X est de classe 2, donc du type $U(\sigma)$ ou $U_o(\sigma_o)$ (proposition 6 du chapitre II). Puisque U n'est pas de classe 2, le centre et le groupe dérivé de U sont distincts. Comme X est central, H-stable et non trivial, X est le centre de U. Posons

$$Y = [U,U]/X$$

et notons X, Y et Z additivement.

L'extension

$$0 \to Y \to U/X \to Z \to 0$$

est définie par un couple $(\lambda,\phi) \in \mathrm{Hom}(Z,Y) \times \mathrm{Alt}(Z,Y)$. Par hypothèse ϕ n'est pas nulle. Si λ est non nul, λ est un isomorphisme de H-modules. Or l'involution de H opère trivialement sur Y car

$$\text{si } s,\ t \in Z,\ \phi(-t,-s) = \phi(t,s).$$

Donc λ est nul.

L'extension

$$0 \to X \to [U,U] \to Y \to 0$$

est définie par un couple $(\nu,\psi) \in \mathrm{Hom}(Y,X) \times \mathrm{Alt}(Y,X)$. On a nécessairement

$$_Y\psi \circ \phi = 0$$

(corollaire du lemme 1). Mais puisque Y est H-irréductible et $\phi \neq 0$, $_Y\psi = 0$, donc $\psi = 0$ et $[U,U]$ est abélien. Comte-tenu de ce qui précède, la condition (6) de la proposition 3 devient

$$\nu \circ \phi = 0.$$

Puisque Y est H-irréductible, ν est nul, et finalement $[U,U]$ est d'exposant p.

A) <u>Si</u> U/X <u>est</u> <u>isomorphe</u> <u>à</u> $U(\sigma)$ $(\sigma \in \mathfrak{G})$ $(\sigma \neq \sigma_0)$.

Reprenons les notations du chapitre II, où $\mathbb{K} = GF(q)$, avec $\gamma = 1*\sigma$, et identifions Y et Z au groupe additif K de $\mathbb{K}$, H au groupe multiplicatif $K^\times$ de $\mathbb{K}$, opérant naturellement sur Z. Si $\lambda \in K^\times$, λ opère sur Z par $(s \to \lambda s)$ et sur Y par $(s \to \lambda^{1+\sigma}y)$. Selon la proposition 4 du chapitre II, X est isomorphe au groupe additif d'un corps de cardinal $q_1 = p^a$ et, si m est l'ordre du groupe d'automorphismes de X induit par H, a est l'ordre de p dans le groupe multiplicatif des unités de $\mathbb{Z}/m\mathbb{Z}$. Puisque m divise $(q-1)$, q_1 divise q et on peut considérer $GF(q_1)$ (noté $\mathbb{K}_1$) comme un sous-corps de $\mathbb{K}$. L'action de H sur X est définie par une fonction multiplicative ρ de $K^\times$ dans $K_1^\times$, $\lambda \in K^\times$ opérant par $(x \to \rho(\lambda)x)$. Selon le corollaire du lemme 1, l'action de Z sur $[U,U]$ est définie par une application biadditive $\tilde{\zeta}$ de $Z \times Y$ dans X (ζ étant définie comme dans la proposition 2, on pose $\tilde{\zeta}(s,t) = \zeta(s)(t)$). Pour définir $\tilde{\zeta}$, utilisons l'assertion (b) de la proposition 5 du chapitre II. Soit donc $\mathfrak{G}$ le groupe des automorphismes de $\mathbb{K}$, et, pour $(\tau,\pi) \in \mathfrak{G}^2$

soit $a_{\tau,\pi}$ la composante de $\tilde{\zeta}$ sur $(\tau.\pi)$. Sous l'action de H, on a

$$\tilde{\zeta}(\lambda s,\lambda^{1+\sigma}y) = \rho(\lambda)\tilde{\zeta}(s,y) \quad \text{quels que soient } \lambda \in K^{\times},\ s,\ y \in K.$$

Il en résulte que

$$\text{si } a_{\tau,\pi} \neq 0,\ \rho(\lambda) = \lambda^{\tau}\lambda^{(1+\sigma)\pi}.$$

Or la fonction ρ détermine l'ensemble $\{\tau,\pi,\sigma\pi\}$ (assertion (e) de la proposition 5, chapitre II). On en déduit, compte-tenu de $\sigma^2 \neq 1$, que $\tilde{\zeta}$ peut s'écrire

soit (i) $\tilde{\zeta} = a(\tau.\pi) \quad (a \neq 0)$

soit (ii) $\tilde{\zeta} = a(\tau.\tau\sigma) + b(\tau\sigma^2.\tau) \quad (ab \neq 0)$

soit (iii) $\tilde{\zeta} = a(\tau.\tau\sigma) + b(\tau\sigma^2.\tau) + c(\tau\sigma.\tau\sigma^2) \quad (abc \neq 0)$

et la troisième possibilité n'intervient que si σ est d'ordre 3.

La condition de Jacobi apporte les restrictions suivantes (sachant que les applications de la forme $((s,t,u) \longrightarrow \tau(s)\pi(t)\kappa(u))$, où $(\tau,\pi,\kappa) \in \mathfrak{G}^3$, forment une base sur $\mathbb{K}$ de l'espace des applications triadditives de K^3 dans K)

soit (i) $\tilde{\zeta} = a(\pi.\pi)$ ou $\tilde{\zeta} = a(\pi\sigma.\pi)$

soit (ii) $a + b = 0$

soit (iii) $a + b + c = 0$

Le groupe additif engendré par $\rho(K^{\times})$ est sous-jacent au sous-corps de $\mathbb{K}$ engendré par $\rho(K^{\times})$. Puisque X est supposé H-irréductible, ce sous-corps est $\mathbb{K}_1$. Selon les cas on a

(i) $\rho(\lambda) = \lambda^{(2+\sigma)\pi}$ ou $\rho(\lambda) = \lambda^{(1+2\sigma)\pi}$

(ii) $\rho(\lambda) = \lambda^{(1+\sigma+\sigma^2)\tau}$ et $\sigma^3 \neq 1 \qquad (\lambda \in K^{\times})$

(iii) $\rho(\lambda) = \lambda^{(1+\sigma+\sigma^2)\tau}$, $\sigma^3 = 1$.

On en déduit que $\mathbb{K} = \mathbb{K}_1$ dans les cas (i) et (ii), tandis que $\mathbb{K}_1$ est le corps des points fixes de σ dans le cas (iii). En effet, si $\sigma' \in \mathfrak{G}$ fixe point par point $\rho(K^{\times})$, les applications cubiques définies par

(i) $\{1,1,\sigma\}$ et $\{\sigma',\sigma',\sigma\sigma'\}$

ou (ii) $\{1,\sigma,\sigma^2\}$ et $\{\sigma',\sigma\sigma',\sigma^2\sigma'\}$

coïncident, et l'assertion (e) déjà citée implique que $\sigma' = 1$.

Dans le cas (iii), toute image selon $\tilde{\zeta}$ est fixe par σ et on a donc $b = a^{\sigma}$ et $c = a^{\sigma^2}$, d'où $a + a^{\sigma} + a^{\sigma^2} = 0$.

Selon la proposition 1 et la proposition 6 du chapitre II, U peut être représenté sur $K_1 \times K \times K$ à l'aide de la fonction $\tilde{\zeta}$, et d'un système de facteurs de K dans $K_1 \times K$, partiellement défini par le 2-cocycle utilisé pour définir $U(\sigma)$. Pour simplifier la présentation de U, on peut modifier les isomorphismes entre Z, Y, X et K par des isomorphismes préalables de K, de la forme

$s \longrightarrow a_T s^{\sigma_T}$ (T = X, Y, Z) avec $a_X \in K_1$, a_Z, $a_Y \in K$ et $\sigma_T \in \mathfrak{G}$.

On obtient une nouvelle présentation de U avec comme nouvelles fonctions $\tilde{\zeta}'$ et ϕ'

$$a_Y \phi'(s,t)^{\sigma_Y} = a_Z^{1+\sigma}(st^{\sigma} - s^{\sigma}t)^{\sigma_Z}$$

et
$$a_X \tilde{\zeta}'(s,t)^{\sigma_X} = \tilde{\zeta}(a_Z s^{\sigma_Z}, a_Y t^{\sigma_Y}).$$

Si (i) a) $\tilde{\zeta} = a(\pi.\pi)$, il suffit de modifier la présentation de X par $a_X = a^{-1}$ et $\sigma_X = \pi^{-1}$ pour obtenir (i) $\tilde{\zeta}' = (1.1)$ sans changer ϕ.

Si (i) b) $\tilde{\zeta} = a(\pi\sigma.\pi)$, en posant $\sigma_Z = \sigma^{-1}$, $\sigma_Y = 1$, $\sigma_X = \pi$, $a_Z = 1$, $a_Y = -1$ et $a_X = -a$, on obtient (i) $\tilde{\zeta}' = (1.1)$ et $\phi' = (1.\sigma^{-1}) - (\sigma^{-1}.1)$ (on a vu que $U(\sigma)$ et $U(\sigma^{-1})$ sont isomorphes).

Si (ii) $\tilde{\zeta} = a((\tau.\tau\sigma) - (\tau\sigma^2.\tau))$, on se ramène, en modifiant uniquement la présentation de X, à (ii) $\tilde{\zeta}' = (1.\sigma) - (\sigma^2.1)$.

Si (iii), on peut supposer $\tau = 1$ en modifiant X, et choisir a et b tels que $a = b - b^{\sigma}$, de telle sorte que $\tilde{\zeta} = Tr_{\mathbb{K}/\mathbb{K}_1}(b((1.\sigma) - (\sigma^2.1)))$.

Selon les propositions 3 et 4, il existe une fonction ω de $K \times K$ dans K_1 telle que

$$(d^2\omega)(s,t,u) + \tilde{\zeta}(s,tu^{\sigma} - t^{\sigma}u) = 0 \quad (s,t,u) \in K^3,$$

chaque solution en ω définissant un groupe U satisfaisant aux conditions de l'énoncé La section notée σ tout au long du chapitre I étant stable par H, on doit avoir

$$\text{si } \lambda \in K^{\times},\ \omega(\lambda s, \lambda t) = \rho(\lambda)\omega(s,t).$$

Deux solutions en ω diffèrent donc d'un 2-cocycle H-stable c de Z dans X. Ce 2-cocycle définit une extension de Z par X admettant H comme groupe d'automorphismes. Si l'extension n'est pas abélienne, c'est l'un des groupes classifiés au chapitre II, proposition 5. Mais dans ces groupes de classe 2, l'involution de H opère trivialement sur le groupe dérivé alors que $\rho(-1) = -1$. Donc c est un 2-cocycle abélien et H-stable, dont la classe de cohomologie est déterminée par $f \in Hom(Z,X)$ (chap. II, proposition 2). Si f n'est pas nul, f est un isomorphisme de H-modules; or X et Z ne sont pas H-isomorphes, car $\rho \notin \mathfrak{G}$(cf la proposition 4 du chapitre II). Donc f est nul et c est un cobord de $K \times K$ dans K_1, et $(\omega + c)$ conduit à un groupe isomorphe. A isomorphisme près, il y a donc un seul groupe dans chacun des cas (i), (ii) et (iii)

On obtient ω sans difficulté grâce aux remarques faites à la fin du chapitre précédent. Il existe toujours F triadditive de K^3 dans K_1 telle que

$$\mu(s,t,u) = \tilde{\zeta}(s,\gamma(t,u))$$
$$= F(s,t,u) - F(t,u,s) - F(s,u,t) + F(u,t,s)$$

et
$$\omega(s,t) = F(s,s,t) - F(s,t,s) + F(t,s,t) + F(t,s,s)$$

convient; selon les cas

(i) $F(s,t,u) = stu^{\sigma}$ et $\omega_1(s,t) = s^2t^{\sigma} + st^{1+\sigma}$;

(ii) $F(s,t,u) = st^{\sigma}u^{\sigma^2}$ et

$$\omega_2(s,t) = s^{1+\sigma}t^{\sigma^2} + s^{\sigma+\sigma^2}t + s^{\sigma}t^{1+\sigma^2} - s^{1+\sigma^2}t^{\sigma} ;$$

(iii) $F(s,t,u) = Tr_{\mathbb{K}/\mathbb{K}_1}(bst^{\sigma}u^{\sigma^2})$ et $\omega_3(s,t) = Tr_{\mathbb{K}/\mathbb{K}_1}(b\omega_2(s,t))$

B) <u>Si</u> U/Z(U) <u>est isomorphe à</u> $U_o(\sigma_o)$. (notations du chapitre II)

Pour simplifier l'écriture, posons $q = r^2$.

Identifions encore Z au groupe additif K de $\mathbb{K}$, sur lequel opère naturellement $K^{\times}$, Y au groupe additif K_o de $\mathbb{K}_o = GF(r)$, X au groupe additif K_1 d'un corps fini $\mathbb{K}_1$. On voit comme en A) que $\mathbb{K}_1$ peut être supposé sous-corps de $\mathbb{K}$. L'opération de Z sur le dérivé [U,U] est définie par une application biadditive $\tilde{\zeta}$ de $K \times K_o$ dans K, à valeurs dans K_1. L'action de H sur X suppose l'existence d'une application multiplicative ρ de $K^{\times}$ dans K_1 telle que

$$\tilde{\zeta}(\lambda s,\lambda^{1+r}t) = \rho(\lambda)\tilde{\zeta}(s,t) \qquad (s \in K,\ t \in K_o,\ \lambda \in K^{\times}).$$

Tout élément de K_o est trace d'un élément de $\mathbb{K}$, il existe donc ν biadditive de K^2 dans K et qui factorise en $\tilde{\zeta}$ à travers $(1 \times Tr_{\mathbb{K}/\mathbb{K}_o})$. Selon la proposition 4 du chapitre II, ν s'écrit

$$\nu = \sum a(\tau,\pi)((\tau.\pi) + (\tau.\pi\sigma_o)) ,$$

où (τ,π) parcourt $\mathfrak{G} \times (\mathfrak{G}/\langle\sigma_o\rangle)$ et $a(\tau.\pi) \in K$.

Si $t \in K_o$, soit $s' \in K$ tel que $t = s' + s'^r$; on a alors, pour $\lambda \in K^{\times}$,

$$\lambda^{1+r}s' + (\lambda^{1+r}s')^r = \lambda^{1+r}t,$$

d'où $$\nu(\lambda s,\lambda^{1+r}s') = \tilde{\zeta}(\lambda s,\lambda^{1+r}t) = \rho(\lambda)\tilde{\zeta}(s,t) = \rho(\lambda)\nu(s,s').$$

Il en résulte que si $a(\tau,\pi) \neq 0$, $\rho(\lambda) = \lambda^{\tau}\lambda^{\pi(1+r)}$.

Selon l'assertion (e) de la proposition 5 du chapitre II, ρ détermine $\{\tau,\pi,\pi\tau\}$ et on en déduit que ν est de la forme

$$\nu = a((\tau.\pi) + (\tau.\pi\sigma_o)) \qquad (a \in K,\ a \neq 0 \text{ et } (\tau,\pi) \in \mathfrak{G}^2).$$

Comme $\rho(K^x)$ engendre $\mathbb{K}$, K_1 est égal à K.

L'existence de l'extension est fonction de la condition (7). On a

$$\tilde{\zeta}(s,\gamma(t,u)) = aa_o^{\pi}s^{\tau}(tu^r - ut^r)^{\pi}$$

et il en résulte - comme en A) - que (7) est vraie si et seulement si $\tau \in \{\pi,\pi\sigma_o\}$.

En transformant la présentation de X, on peut supposer $a = 1$ et $\tau = \pi = 1$. On obtient alors

$$\rho(\lambda) = \lambda^{2+r} \quad \text{et} \quad \tilde{\zeta}(s,t) = st \qquad (\lambda \in K^x,\ s \in K \text{ et } t \in K_o).$$

L'unicité de U à isomorphisme près se démontre exactement comme en A). Un système de facteurs convenable (γ,ω) se calcule de même avec

$$\mu(s,t,u) = a_o s(tu^r - ut^r),\ F(s,t,u) = a_o stu^r,\ \omega(s,t) = a_o(s^2t^r + st^{1+r})$$

La proposition 5 est ainsi démontrée.

Les p-groupes de type (i) se rencontrent comme 3-groupes de Sylow des groupes de Ree ${}^2G_2(q)$ ($p = 3$ et $\sigma^2 = 3$). Dans "caractérisation des groupes de Ree" (même volume) nous utilisons une autre présentation de ces groupes, avec

$$\gamma = -(1{*}\sigma) \text{ et } \omega(s,t) = s^2t^{\sigma} + s^{1+\sigma}t - s^{\sigma}t^2,$$

soit la loi de produit

$$(x,y,z)_M(x',y',z')_M = (x+x'+z^2z'^{\sigma}+z^{1+\sigma}z'-z^{\sigma}z'^2+zy'\ ,\ y+y'+z^{\sigma}z'-zz'^{\sigma}\ ,\ z+z')_M.$$

On obtient un isomorphisme depuis le groupe décrit en (i) par

$$(x,y,z) \longrightarrow (-x-z^{2+\sigma}\ ,\ -y\ ,\ z)_M.$$

Dans [6], J.G.Thompson définit ainsi le produit sur K^3

$$(x,y,z)_T(x',y',z')_T = (x+x'\ ,\ y+y'+xx'^{\sigma}-x^{\sigma}x'\ ,\ z+z'+yx'+x^{\sigma}x'^2+xx'^{1+\sigma}-x^2x'^{\sigma})_T$$

Les applications

$$(x,y,z)_M \longrightarrow (-z,-y,-x+yz)_T \quad \text{et} \quad (x,y,z)_T \longrightarrow (-z+xy,-y,-x)_M$$

sont des isomorphismes réciproques.

Dans [7], J. Tits définit ainsi le produit sur K^3

$$(x,y,z)_J(x',y',z')_J = (x+x' \;,\; y+y'+x^{\sigma}x' \;,\; z+z'-xy'+yx'-x^{1+\sigma}x')_J$$

Les applications

$$(x,y,z)_J \longrightarrow (z-xy-x^{2+\sigma},-y-x^{1+\sigma},-x)_M$$

$$(x,y,z)_M \longrightarrow (-z,-y-z^{1+\sigma},x+yz)_J$$

sont des isomorphismes réciproques.

BIBLIOGRAPHIE

[1] Broué, M. et Enguehard M. Cours de 3ème cycle : caractérisation des groupes de Zassenhaus, Paris, 1980.

[2] Eilenberg, S. et Mac Lane S. Cohomology Theory in Abstract Groups. II. Groups extensions with an abelian kernel. Ann. of Math. 48, p.326-341 (1947).

[3] Higman, G. Suzuki 2-groups.Ill. Jl of Math. 7, p.79-96 (1963).

[4] Huppert, B. Endliche Gruppen I. Springer Verlag. Berlin, 1967.

[5] Mac Lane, S. Homology. Springer Verlag. Berlin, 1967.

[6] Thompson, J.-G. Towards a characterization of $E_2^*(q)$, I. Jl of Algebra 7, p.406-414 (1967).

[7] Tits, J. Les groupes simples de Suzuki et de Ree, Séminaire Bourbaki, 13ème année, 1960/61, n°210.

Michel Enguehard
54, rue de Montdauphin
77240, Cesson
France.