Extensions galoisiennes non commutatives : Normalité, Cohomologie non abélienne.

Philippe Nuss

EXTENSIONS GALOISIENNES NON COMMUTATIVES : NORMALITÉ, COHOMOLOGIE NON ABÉLIENNE

PHILIPPE NUSS

Institut de Recherche Mathématique Avancée, Université Louis-Pasteur et CNRS, 7, rue René-Descartes, 67084 Strasbourg Cedex, France. e-mail : nuss@math.u-strasbg.fr

Abstract. We study various types of noncommutative Galois extensions and present some examples. We state a criterion which decides whether a given automorphism of a Galois extension belongs to the corresponding Galois group or not. We then compute Borovoi's nonabelian cohomology sets (in degree 0, 1, 2) of the Galois group with coefficients in a crossed module associated to the Galois extension.

Résumé. Nous étudions divers types d'extensions galoisiennes d'anneaux non commutatifs et considérons quelques exemples. Nous énonçons un critère qui permet de décider si un automorphisme donné d'une extension galoisienne appartient ou non au groupe de Galois. Nous calculons la cohomologie non abélienne de Borovoi en degré 0, 1 et 2 du groupe de Galois à coefficients dans un module croisé associé à l'extension galoisienne.

Mathematics Subject Classifications (1991) : 16W20, 16H05, 16K20, 18G50, 08A35.

Key-words : Galois-extension, non-commutative ring, idempotent, quaternion, crossed-module, non-abelian cohomology.

Mots-clés : Extension galoisienne, anneau non commutatif, idempotent, quaternion, module croisé, cohomologie non abélienne.

SOMMAIRE

Introduction
1.- Définition des extensions galoisiennes et propriétés
2.- Exemples
3.- Critère de normalité d'une extension galoisienne
4.- Coefficients d'entrelacement et descente galoisienne
5.- Cohomologie non abélienne des extensions galoisiennes d'Azumaya - Le cas des quaternions

INTRODUCTION

Cet article s'articule autour de trois thèmes relatifs aux extensions galoisiennes non commutatives : l'étude de différents types de telles extensions, l'examen du problème de la normalité et la présentation de calculs explicites de cohomologie non abélienne dans certains cas particuliers.

La théorie de Galois classique des corps commutatifs a été généralisée, dans un premier temps, aux anneaux commutatifs quelconques par Auslander, Chase, Goldman, Harrison, A. Rosenberg et Sweedler (voir notamment [CS]), puis a été étendue par Kreimer et Takeuchi [KT] qui non seulement se placent dans le cas non commutatif, mais encore remplacent l'action du groupe de Galois par celle d'une algèbre de Hopf quelconque. L'archétype d'extension galoisienne non commutative considéré dans ce travail est dû à Le Bruyn, Van den Bergh et Van Oystaeyen [LVV]. Rappelons dès à présent sa définition. On fixe un groupe fini G d'ordre $|G|$ opérant par automorphismes sur un anneau S non nécessairement commutatif. Soit $R = S^G$ l'anneau des invariants de S sous G. L'extension S/R est dite *G-galoisienne* lorsque les deux conditions suivantes sont remplies : $S \otimes_R S$

est isomorphe par un morphisme canonique de S-modules à gauche Γ (voir § 1) à la somme directe de $|G|$ copies de S et le R-anneau S est fidèlement plat en tant que R-module à gauche. Dans le cas particulier où S est un anneau ou un corps commutatif, on recouvre les notions antérieures d'extensions galoisiennes correspondantes.

Dans le cas non commutatif, la fidèle platitude pose un problème, ce qui n'est guère étonnant vu le caractère géométrique de cette propriété. Ainsi, lorsque S/R est une extension G-galoisienne et H un sous-groupe de G, il n'y a aucune raison *a priori* que l'extension S/S^H reste fidèlement plate. Pour conserver la fidèle platitude, il est nécessaire de rajouter des hypothèses supplémentaires, par exemple de ne considérer que des extensions galoisiennes au-dessus d'un corps (*cf.* le Théorème 3.7 de [Sch]). Dans ce travail, nous introduisons une classe d'extensions, appelées *galoisiennes strictes*, qui possèdent, elles aussi, la propriété de stabilité requise par rapport aux sous-groupes de G. Nous montrons que les extensions galoisiennes strictes sont des cas particuliers d'extensions galoisiennes.

Dans un deuxième temps, nous nous intéressons à la question naturelle suivante : à quelles conditions une extension G-galoisienne S/R est-elle *normale*, c'est-à-dire telle que le groupe des automorphismes $\mathrm{Aut}(S/R)$ coïncide avec le groupe de Galois G ? Pour les anneaux commutatifs, un théorème dû à Chase, Harrison et Rosenberg nous apprend que c'est le cas dès que l'anneau S ne possède pas d'idempotents non triviaux [CHR]. Ce résultat ne s'étend pas aux extensions galoisiennes non commutatives, comme le montre l'exemple des quaternions qui nous sert de *Leitfaden* dans ce travail. Nous énonçons un critère permettant de déterminer dans le cas général si un automorphisme donné $f \in \mathrm{Aut}(S/R)$ appartient ou non à G (théorème 3.2).

Le troisième thème est l'étude de la cohomologie non abélienne de Borovoi $\mathbb{H}^i(G, \mathscr{M}_\psi)$ ($i = -1, 0, 1$) de G à coefficients dans un objet $\mathscr{M}_\psi$ canoniquement attaché à certaines extensions G-galoisiennes ψ. La cohomologie non abélienne, bien connue en degré 0 et 1 [Ser2], a été étendue de manière algébrique au degré 2 par Dedecker, vers 1964, à l'aide de cocycles explicites ([Ded1], [Ded2]). D'autres approches, plus géométriques, ont été proposées ultérieurement par Giraud (à l'aide de gerbes), Duskin (liens d'un bouquet), Breen (bitorseurs) *et al.* (voir notamment [Bre]). Dans la construction de sa théorie, Dedecker reconnut la nécessité de prendre pour systèmes de coefficients un objet familier des topologues, les modules croisés. Dans [Bor], Borovoi propose une théorie d'hypercohomologie non abélienne, fortement inspirée de celle de Dedecker, pour laquelle les systèmes de coefficients retenus sont encore les modules croisés, munis de surcroît d'une action du groupe dont on veut calculer la cohomologie. Ce procédé est particulièrement adapté au cas de certaines extensions galoisiennes, appelées centrales (en particulier les extensions d'Azumaya), pour lesquelles on dispose de manière naturelle d'un tel module croisé. Une extension G-galoisienne $\psi : R \longrightarrow S$ est dite *centrale* (respectivement *d'Azumaya*) si l'anneau R est dans le centre de S (respectivement si R est un corps commutatif et S est une R-algèbre d'Azumaya) ; les extensions quaternioniques fournissent des exemples d'extensions galoisiennes d'Azumaya. Nous attachons à une extension galoisienne centrale ψ un module croisé $\mathscr{M}_\psi$ muni d'une action de G, ce qui permet de donner un sens à $\mathbb{H}^i(G, \mathscr{M}_\psi)$ ($i = -1, 0, 1$). Nous déterminons les $\mathbb{H}^i(G, \mathscr{M}_\psi)$ en termes de cohomologie usuelle de G dans le cas des extensions galoisiennnes d'Azumaya, ce qui rend leur calcul possible dans le cas des extensions quaternioniques.

Détaillons maintenant le contenu de chacune des cinq sections constituant ce travail. Dans la première section, nous distinguons (définitions 1.1) et comparons (proposition 1.3) trois types d'extensions galoisiennes non commutatives : les extensions semi-galoisiennes, galoisiennes et galoisiennes strictes. Nous démontrons que ces dernières possèdent les bonnes propriétés de stabilité par rapport aux sous-groupes du groupe de Galois (théorème 1.9). Nous caractérisons aussi les extensions galoisiennes par l'existence de bases galoisiennes (théorème 1.5). La seconde section est consacrée à la présentation de quelques exemples d'extensions galoisiennes : extensions triviales,

quaternioniques, algèbres des matrices diagonales. Dans la troisième section, nous donnons un analogue du théorème de Chase, Harrison et Rosenberg adapté au cas non commutatif. Il s'agit, pour une extension G-galoisienne S/R, d'un critère qui permet de déterminer si un automorphisme donné f de l'extension appartient ou non à G (théorème 3.2). Ce critère fait intervenir $|G|$ éléments de S (dépendant de f), appelés *coefficients d'entrelacement*, que nous interprétons, dans la quatrième section (proposition 4.2), en termes de descente galoisienne (voir [Nus]). Dans la cinquième section, nous établissons, pour les extensions galoisiennes d'Azumaya $\psi : R \longrightarrow S$, un isomorphisme entre l'hypercohomologie de Borovoi $\mathbb{H}^i(G, \mathscr{M}_\psi)$ et la cohomologie abélienne $\mathrm{H}^{i+1}(G, R^\times)$ $(i = -1, 0, 1)$ (proposition 5.7). En particulier, nous calculons explicitement ces derniers groupes dans le cas des extensions quaternioniques sur le corps des nombres réels, des nombres p-adiques ainsi que sur un corps fini (corollaire 5.8).

1. DÉFINITION DES EXTENSIONS GALOISIENNES ET PROPRIÉTÉS

Fixons un groupe fini G d'ordre $|G| = n$ et d'élément neutre e. Un morphisme d'anneaux $\psi : R \longrightarrow S$ est appelé une *G-extension* si ψ est injectif et si G agit par automorphismes d'anneaux sur S de telle sorte que l'opération est triviale sur l'image de ψ ; on identifie alors R à $\psi(R)$ et on note $g(s)$ l'action d'un élément g de G sur un élément s de S. Ainsi G agit sur S par automorphismes de R-anneaux.

Considérons l'anneau $S(G)$ des applications de G dans S muni de la multiplication point par point et, pour tout $g \in G$, la fonction de Dirac $\delta_g \in S(G)$ en g (nulle partout sauf sur l'élément g où elle prend la valeur 1). Comme S-module à gauche, $S(G)$ est isomorphe au S-module libre de rang n et de base $(\delta_g)_{g\in G}$. Par transfert de structure, ce S-module hérite du produit donné par

$$(s\delta_g)(t\delta_h) = st\boldsymbol{\delta}_{g,h}\delta_g \tag{1}$$

pour $s, t \in S$, $g, h \in G$, avec $\boldsymbol{\delta}_{g,h}$ le symbole de Kronecker de g et de h. L'élément unité pour ce produit est $\sum_{g\in G} \delta_g$. Dans la suite, nous confondrons $S(G)$ et le S-module libre de rang n, de base $(\delta_g)_{g\in G}$ muni du produit (1). Le morphisme de S-modules à gauche ϕ de S vers $S(G)$ défini par

$$\phi(s) = \sum_{g\in G} g(s)\delta_g$$

munit $S(G)$ d'une structure de S-anneau induisant la structure de S-bimodule donnée, pour tout $g \in G$ et $s \in S$, par l'égalité

$$\delta_g s = g(s)\delta_g \tag{2}$$

et étendue à $S(G)$ en entier par S-linéarité à gauche. On introduit un morphisme Γ de S-modules à gauche et un morphisme Γ' de S-modules à droite de $S\otimes_R S$ vers $S(G)$ par les expressions

$$\Gamma(s\otimes t) = \sum_{g\in G} sg(t)\delta_g = \sum_{g\in G} s\delta_g t \quad \text{et} \quad \Gamma'(s\otimes t) = \sum_{g\in G} g(s)\delta_g t$$

pour tout $s, t \in S$. Les morphismes Γ et Γ' diffèrent par un automorphisme involutif de $S(G)$. En effet, l'endomorphisme υ du groupe abélien $S(G)$ défini par

$$\upsilon\left(\sum_{g\in G} s_g\delta_g\right) = \sum_{g\in G} g(s_{g^{-1}})\delta_g$$

vérifie $\upsilon^2 = \mathrm{id}$ et $\Gamma' = \upsilon \circ \Gamma$.

Soit $\mu : S \otimes_R S \longrightarrow S$ la multiplication donnée par $\mu(s \otimes t) = st$ pour $s \otimes t \in S \otimes_R S$. Le morphisme de S-bimodules $\tilde{\mu}$ de $S(G)$ vers S défini par

$$\tilde{\mu}\Big(\sum_{g \in G} s_g \delta_g\Big) = s_e$$

vérifie

$$\tilde{\mu} \circ \Gamma = \tilde{\mu} \circ \Gamma' = \mu. \tag{3}$$

Définitions 1.1. Soit $\psi : R \longrightarrow S$ une G-extension où G est un groupe fini.
• La G-extension ψ est dite *semi-normale* si l'anneau $S^G = \{s \in S \mid g(s) = s, \quad \forall g \in G\}$ des invariants de S sous G est exactement R.
• La G-extension ψ est dite *normale* si elle est semi-normale et si G est isomorphe au groupe $\mathrm{Aut}(S/R)$ des automorphismes de l'anneau S laissant R tout entier invariant point par point.
• La G-extension ψ est dite *G-semi-galoisienne* si elle est semi-normale et si Γ est un isomorphisme d'anneaux.
• La G-extension ψ est dite *G-galoisienne* si ψ est fidèlement plat (*i.e.* si S est un R-module à gauche fidèlement plat) et si Γ est un isomorphisme d'anneaux.
• La G-extension ψ est dite *G-galoisienne stricte* si elle est semi-normale, si $n = |G|$ est inversible dans S et si Γ est un isomorphisme d'anneaux.
• Enfin, un *morphisme de G-extensions de $\psi_1 : R \longrightarrow S_1$ vers $\psi_2 : R \longrightarrow S_2$* est un morphisme ρ de R-anneaux de S_1 vers S_2 qui est G-équivariant, *i.e.* qui vérifie, pour tout $g \in G$ et tout $s \in S_1$,

$$\rho\big(g(s)\big) = g\big(\rho(s)\big).$$

On en déduit la catégorie $\mathfrak{Ext}\,(R, G)$ des G-extensions au-dessus de R, qui contient comme sous-catégories pleines les catégories dont les objets sont les extensions G-galoisiennes, G-semi-galoisiennes et G-galoisiennes strictes. En particulier, nous noterons $\mathfrak{Gal}\,(R, G)$ la catégorie des extensions G-galoisiennes au-dessus de R.

Remarques : 1) Il est immédiat qu'une extension galoisienne stricte est semi-galoisienne. Nous allons montrer ci-dessous (proposition 1.3) qu'une extension galoisienne est également semi-galoisienne et qu'une extension galoisienne stricte est galoisienne.

2) Une extension G-semi-galoisienne $\psi : R \longrightarrow S$ est une extension $\mathcal{H}$-galoisienne au sens de Kreimer et Takeuchi [KT] (voir aussi Ulbrich [Ulb]) pour l'algèbre de Hopf $\mathcal{H} = \mathbf{Z}^G$ des applications sur G à valeurs dans l'anneau des entiers $\mathbf{Z}$. C'est encore un $\mathcal{H}$-torseur sur k au sens de Deligne et Milne [DM] dans le cas où S est une algèbre commutative sur un corps commutatif k.

3) Alors que toute extension G-semi-galoisienne d'anneaux commutatifs est automatiquement galoisienne (Corollaire 1.10 de [KT]), il convient d'opérer une distinction dans le cas non commutatif.

Rappelons, traduite dans notre langage, l'importante proposition 1.9 de [KT] traitant de la fidèle platitude et reposant de manière essentielle sur un résultat de Nakayama [Nak] :

Proposition 1.2. *Soit $\psi : R \longrightarrow S$ une extension semi-galoisienne. Les quatre propositions suivantes sont équivalentes :*
1) R est facteur direct du R-module à droite S ; 1') R est facteur direct du R-module à gauche S ;
2) S est un R-module à droite fidèlement plat ; 2') S est un R-module à gauche fidèlement plat.

Nous allons à présent montrer le résultat suivant :

Proposition 1.3. *Soit $\psi : R \longrightarrow S$ une G-extension. On a alors les implications suivantes :*
$$(\psi \text{ est galoisienne stricte}) \Longrightarrow (\psi \text{ est galoisienne}) \Longrightarrow (\psi \text{ est semi-galoisienne})$$
$$\Longrightarrow (\psi \text{ est séparable})$$

Rappelons qu'une extension ψ est dite *séparable* s'il existe un élément E dans $S \otimes_R S$, appelé *élément de séparabilité pour* ψ, tel que $\mu(E) = 1$ et $Es = sE$ pour tout $s \in S$. Il revient au même de demander que la surjection μ soit scindée en tant que morphisme de S-bimodules.

Avant de démontrer la proposition 1.3, introduisons quelques notations. Soit $\psi : R \longrightarrow S$ une extension galoisienne. Notons η_g l'élément $\Gamma^{-1}(\delta_g) \in S \otimes_R S$ qui, d'après (3), vérifie l'égalité $\mu(\eta_g) = \boldsymbol{\delta}_{g,e}$ et, d'après (2), la formule

$$\eta_g s = g(s)\eta_g. \tag{4}$$

Considérons en particulier $\eta_e = \Gamma^{-1}(\delta_e)$ décomposé sous la forme $\eta_e = \sum_{i=1}^{m} x_i \otimes y_i \in S \otimes_R S$. Par définition, $\Gamma(\eta_e) = \delta_e \in S(G)$, ce qui se traduit par l'égalité

$$\sum_{i=1}^{m} x_i g(y_i) = \boldsymbol{\delta}_{g,e}. \tag{5}$$

En remarquant que $\Gamma'(\eta_e) = \delta_e$, on tire de manière symétrique l'égalité :

$$\sum_{i=1}^{m} g(x_i) y_i = \boldsymbol{\delta}_{g,e}. \tag{5'}$$

Soient $\psi : R \longrightarrow S$ une G-extension et n l'ordre de G. Supposons que ψ est semi-normale. Dans ce cas, il existe un morphisme de R-bimodules de S vers R appelé *trace*, noté $\mathrm{tr}_{S/R}$ ou tr, et défini par

$$\mathrm{tr}(s) = \sum_{g \in G} g(s).$$

Il vérifie $\mathrm{tr} \circ \psi = n \cdot \mathrm{id}_R$. Etant donnée une extension semi-galoisienne S/R, il est commode d'introduire le morphisme R-linéaire à droite φ_i de S vers R défini par

$$\varphi_i(s) = \mathrm{tr}(y_i s).$$

Lemme 1.4. *1) Soit $\psi : R \longrightarrow S$ une G-extension semi-galoisienne. Alors S est projectif de type fini comme R-module à droite ou à gauche.*

2) Si ψ est G-galoisienne, le morphisme tr *est surjectif. Si ψ est G-galoisienne stricte,* tr *est un morphisme surjectif scindé et donc R est en facteur direct dans S. Dans tous les cas, S est R-générateur à droite ou à gauche.*

Rappelons qu'un R-module M est *R-générateur à gauche* (respectivement *à droite*) s'il existe des morphismes $f_1, \ldots, f_n$ de R-modules à gauche (respectivement à droite) de M vers R et des éléments $m_1, \ldots, m_n$ tels que $\sum_{i=1}^{n} f_i(m_i) = 1$.

Démonstration du lemme 1.4 : 1) Du calcul

$$\sum_{i=1}^{m} x_i\varphi_i(s) = \sum_{i=1}^{m}\sum_{g\in G} x_i g(y_i s) = \sum_{g\in G}\left(\sum_{i=1}^{m} x_i g(y_i)\right) g(s) = s$$

on déduit, en utilisant (5), l'égalité

$$\sum_{i=1}^{m} x_i\varphi_i(s) = s \tag{6}$$

qui montre que la famille $\{(x_i,\varphi_i)_{i=1,\ldots,m}\}$ forme une base duale du R-module à droite S. D'après [DI, lemme 1.3], S est un R-module à droite projectif de type fini. En considérant le morphisme R-linéaire à gauche φ_i' de S vers R défini par $\varphi_i'(s) = \mathrm{tr}(sx_i)$, on montre, en utilisant (5'), que $\sum_{i=1}^{m} \varphi_i'(s)y_i = s$ et on en déduit que S est un R-module à gauche projectif de type fini. Λ

2) i) Lorsque ψ est une extension G-galoisienne, ψ est fidèlement plat et donc $\mathrm{tr} : S \longrightarrow R$ est surjectif si et seulement si le morphisme $\mathrm{tr}\otimes\mathrm{id}_S : S\otimes_R S \longrightarrow S$ est surjectif. Si l'on écrit ce dernier sous la forme

$$(\mathrm{tr}\otimes\mathrm{id}_S)(s\otimes t) = \sum_{g\in G} g^{-1}(s)t$$

(pour $s,t\in S$) et si l'on considère le morphisme surjectif T de $S(G)$ vers S défini par

$$T(s\delta_g) = g^{-1}(s),$$

on vérifie que $\mathrm{tr}\otimes\mathrm{id}_S = T\circ\Gamma$. Ainsi $\mathrm{tr}\otimes\mathrm{id}_S$ est la composée de morphismes surjectifs, donc est surjectif tout comme tr.

ii) Si l'on suppose que n est inversible dans S, alors le morphisme ψ/n est une section de tr et tr est surjectif et scindé.

iii) La trace $\mathrm{tr}\in \mathrm{Hom}_R(S_R, R)$ (respectivement $\mathrm{tr}\in \mathrm{Hom}_R({}_RS, R)$) étant surjective, il existe un élément $u\in S$ tel que $\mathrm{tr}(u) = 1$. Cela suffit (voir [DI]) à montrer que S est générateur comme R-module à droite (respectivement à gauche). Λ

Démonstration de la proposition 1.3 : Remarquons d'abord qu'une extension galoisienne est semi-galoisienne. En effet, si ψ est fidèlement plat, l'exactitude du complexe d'Amitsur associé à ψ entraîne que les invariants de S sous G sont exactement R (voir [LVV]) ; donc ψ est semi-normale.

Montrons la première implication. Soit ψ une extension G-galoisienne stricte. D'après le lemme 1.4, R est en facteur direct dans S et on conclut à l'aide de la proposition 1.2.

La troisième implication est immédiate lorsqu'on remarque que, d'après les égalités (3) et (4), η_e est un élément de séparabilité. Λ

Donnons à présent une caractérisation des extensions galoisiennes : il s'agit de l'analogue non commutatif du théorème 1.3 de [CHR].

Théorème 1.5. *Soit $\psi : R \longrightarrow S$ une G-extension semi-normale. Les propositions suivantes sont alors équivalentes :*

(1) *$\psi : R \longrightarrow S$ est une extension G-galoisienne.*

(2) *Γ est surjective.*

(3) *Il existe un entier naturel m et $2m$ éléments $x_1,\ldots,x_m$, $y_1,\ldots,y_m$ de S tels que l'équation (5) (ou (5')) est vérifiée.*

(4) *Γ' est bijective.*

Définition 1.6. Si l'extension $\psi : R \longrightarrow S$ est G-galoisienne, le $2m$-uplet $(x_1, \ldots, x_m; y_1, \ldots, y_m)$ apparaissant dans le théorème 1.5 est appelée *base galoisienne de* ψ.

Une base galoisienne de ψ est donc une collection ordonnée $(x_1, \ldots, x_m; y_1, \ldots, y_m)$ d'éléments non nuls de S tels que

$$\Gamma\left(\sum_{i=1}^{m} x_i \otimes y_i\right) = \delta_e \in S(G).$$

Il s'ensuit qu'une base galoisienne vérifie l'équation (5) et donc que

$$\Gamma\left(\sum_{i=1}^{m} x_i \otimes g(y_i)\right) = \delta_{g^{-1}}.$$

Démonstration du théorème 1.5 :
1) $\Longrightarrow$ 2) vient par définition.
2) $\Longrightarrow$ 3) Par surjectivité de Γ, il existe $\eta_e \in S \otimes_R S$ tel que $\Gamma(\eta_e) = \delta_e \in S(G)$. Il existe donc un entier naturel m et $2m$ éléments $x_1, \ldots, x_m$, $y_1, \ldots, y_m$ de S tels que

$$\eta_e = \sum_{i=1}^{m} x_i \otimes y_i.$$

En appliquant Γ aux deux membres on déduit (5).
3) $\Longrightarrow$ 1) Soit $(x_1, \ldots, x_m; y_1, \ldots, y_m)$ une base galoisienne de ψ. Commençons par montrer que Γ est surjective. Pour $g \in G$, prenons $\eta_g = \Gamma^{-1}(\delta_g)$. Vérifions que son expression est donnée par

$$\eta_g = \sum_{i=1}^{m} x_i \otimes g^{-1}(y_i). \tag{7}$$

En effet, on a : $\Gamma\big(\sum_{i=1}^{m} x_i \otimes g^{-1}(y_i)\big) = \sum_{h \in G} \sum_{i=1}^{m} x_i (hg^{-1})(y_i)\delta_h$; or $\sum_{i=1}^{m} x_i (hg^{-1})(y_i)$ n'est non nul que si $h = g$, auquel cas cette expression vaut 1. Ainsi $\Gamma\big(\sum_{i=1}^{m} x_i \otimes g^{-1}(y_i)\big) = \delta_g$, d'où (7). Soit $\sum_{g \in G} s_g \delta_g$ un élément de $S(G)$. En utilisant l'expression (7) et la S-linéarité à gauche de Γ, on voit que $\Gamma\left(\sum_{g \in G} s_g \eta_g\right) = \sum_{g \in G} s_g \delta_g$ et donc que Γ est surjective.

Montrons maintenant que Γ est injective. Soit $\sum_{j=1}^{k} s_j \otimes t_j$ un élément de $S \otimes_R S$ d'image nulle par Γ, autrement dit, pour tout $h \in G$, on a : $\sum_{j=1}^{k} s_j h(t_j) = 0$. En composant par h^{-1}, cette formule implique que, pour tout h dans G, on a : $\sum_{j=1}^{k} h^{-1}(s_j) t_j = 0$. Par conséquent, pour tout g dans G, on a :

$$\sum_{j=1}^{k} g(s_j) t_j = 0.$$

En utilisant à nouveau le morphisme R-linéaire à droite φ_i de S vers R, défini par $\varphi_i(s) = \mathrm{tr}(y_i s)$, ainsi que l'égalité (6), on trouve

$$\sum_{j=1}^{k} s_j \otimes t_j = \sum_{j=1}^{k}\sum_{i=1}^{m} x_i \varphi_i(s_j) \otimes t_j = \sum_{j=1}^{k}\sum_{i=1}^{m} x_i \otimes \varphi_i(s_j) t_j =$$
$$= \sum_{j=1}^{k}\sum_{i=1}^{m} x_i \otimes \sum_{g\in G} g(y_i) g(s_j) t_j = \sum_{i=1}^{m} x_i \otimes \sum_{g\in G} g(y_i) \Big(\sum_{j=1}^{k} g(s_j) t_j\Big) = 0.$$

3) $\Longleftrightarrow$ 4) est triviale puisque $\Gamma' = \upsilon \circ \Gamma$. Λ

Lemme 1.7. *Soit $\psi : R \longrightarrow S$ une extension G-galoisienne. Le module $S \otimes_R S$ est muni d'une structure de S-anneau pour le produit $*$ défini par*

$$(s_1 \otimes t_1) * (s_2 \otimes t_2) = \sum_{g\in G} s_1 g(t_1) s_2 g(t_2) \eta_g. \tag{8}$$

Si R est dans le centre de S, le produit $*$ coïncide avec le produit usuel $\cdot$ sur $S \otimes_R S$ donné par

$$(s_1 \otimes t_1) \cdot (s_2 \otimes t_2) = s_1 s_2 \otimes t_1 t_2.$$

Démonstration : Le produit $*$ est obtenu par transfert de structure via Γ à partir du produit (1) sur $S(G)$. Dans le cas où R est dans le centre de S, on vérifie que Γ est un isomorphisme d'anneaux de $(S \otimes_R S, \cdot)$ vers $S(G)$ muni du produit (1). Par conséquent, les deux produits $*$ et $\cdot$ coïncident. Λ

Dans le cas où la dimension de S sur R a un sens, on peut énoncer le résultat suivant reliant cette dimension à l'ordre du groupe de Galois G :

Lemme 1.8. *Soit $\psi : R \longrightarrow S$ une extension G-galoisienne et n l'ordre du groupe G. Supposons que R est une algèbre à division et que la dimension à gauche $[S : R]_l$ de S sur R coïncide avec la dimension à droite $[S : R]_r$. On a alors :*

$$[S : R]_l = n = [S : R]_r.$$

Démonstration : Soit $d = [S : R]_l = [S : R]_r$. On voit que $S \otimes_R S$ est un R-espace vectoriel de dimension d^2, alors que $S(G)$ est de dimension nd, d'où $n = d$. Λ

Théorème 1.9. *Soit $\psi : R \longrightarrow S$ une extension G-galoisienne stricte.*

1) Si H est un sous-groupe de G, on pose $U = S^H$ et on appelle $\theta : U \longrightarrow S$ et $\theta' : R \longrightarrow U$ les inclusions canoniques. Alors θ est une extension H-galoisienne stricte et θ' est une extension séparable fidèlement plate.

2) Si, de plus, H est un sous-groupe distingué de G, alors θ' est une extension G/H-galoisienne stricte.

Démonstration : 1) D'après le théorème de Lagrange, l'ordre de H divise $n = |G|$, donc est inversible dans l'anneau S. Soit $(x_1, \ldots, x_m;\ y_1, \ldots, y_m)$ une base galoisienne de ψ. L'égalité (5) est vraie pour tout $g \in G$, donc pour tout $g \in H$. On en déduit, d'après le théorème 1.5, que θ est une

extension H-galoisienne stricte. D'après le résultat de [LVV] (Proposition II 5.1.2) traitant de la transitivité de la séparabilité, on conclut que θ' est séparable.

Les extensions ψ et θ étant galoisiennes strictes, elles sont aussi fidèlement plates d'après la proposition 1.3. On conclut que θ' est fidèlement plate à l'aide de la Proposition 7 de [Bou] (Chap. I § 3 n° 4).

2) Supposons maintenant que H est distingué dans G. Le groupe quotient G/H agit sur U par

$$\bar{g}(u) = g(u)$$

pour $u \in U$, $\bar{g} \in G/H$ et g un représentant de $\bar{g}$ dans G. On a aussi : $U^{G/H} = S^G = R$. De plus, l'ordre du quotient divisant l'ordre de G, il est inversible dans S.

D'après 1), l'extension θ est H-galoisienne stricte et donc le morphisme $\mathrm{tr}_{S/U}$ est surjectif. Fixons $s_0 \in S$ tel que $\mathrm{tr}_{S/U}(s_0) = 1$. D'autre part, soit $(x_1, \ldots, x_m; y_1, \ldots, y_m)$ une base galoisienne de ψ. Définissons les trois éléments de U

$$x'_i = \mathrm{tr}_{S/U}(s_0 x_i), \quad y'_i = \mathrm{tr}_{S/U}(y_i) \ \text{ et } \ z_g = \sum_{i=1}^{n} x'_i g(y'_i).$$

Un calcul montre que $z_g = 0$ dès que $g \notin H$ et $z_h = 1$ pour $h \in H$. Ainsi

$$\sum_{i=1}^{n} x'_i \bar{g}(y'_i) = \delta_{\bar{g},\bar{e}},$$

ce qui implique que $(x'_1, \ldots, x'_m; y'_1, \ldots, y'_m)$ est une base galoisienne de θ'. D'après le théorème 1.5, θ' est donc une extension G/H-galoisienne. Le fait qu'elle est stricte est clair. Λ

2. EXEMPLES

Pour illustrer les concepts introduits au paragraphe 1, donnons quelques exemples.

2.1. Extensions galoisiennes triviales. Soit R un anneau et G un groupe fini opérant trivialement sur R. Alors G opère sur $R(G)$ par

$$g(r\delta_h) = r\delta_{hg^{-1}}$$

pour $r \in R$ et $g, h \in G$. On vérifie que l'extension $\psi_{R,G} : R \longrightarrow R(G)$ donnée par $\psi_{R,G}(r) = \sum_{g \in G} r\delta_g$ est G-galoisienne. Une extension galoisienne $\psi : R \longrightarrow S$ est appelée *extension galoisienne triviale* si elle est isomorphe dans la catégorie $\mathfrak{Gal}(R, G)$ à l'extension $\psi_{R,G}$.

Théorème 2.1. *Soit $\psi : R \longrightarrow S$ une extension G-galoisienne (respectivement G-galoisienne stricte). Le groupe G agit sur l'anneau $(S \otimes_R S, *)$ par*

$$g(s \otimes t) = s \otimes g(t)$$

et le morphisme ε_1 de S vers $S \otimes_R S$ défini par $\varepsilon_1(s) = s \otimes 1$ est une extension G-galoisienne triviale (respectivement G-galoisienne stricte triviale).

Démonstration : 1) Soit $\psi : R \longrightarrow S$ une extension G-galoisienne. On vérifie, en utilisant la formule (7), que l'action de G sur les éléments η_h est donnée par

$$g(\eta_h) = \eta_{hg^{-1}}$$

pour $g, h \in G$. On en déduit les égalités

$$g\big((s\otimes t) * (u\otimes v)\big) = \sum_{h\in G} sh(t)uh(v)\eta_{hg^{-1}} = \sum_{k\in G} skg(t)ukg(v)\eta_k =$$
$$\big(s\otimes g(t)\big) * \big(u\otimes g(v)\big) = g(s\otimes t) * g(u\otimes v)$$

qui montrent que l'action du groupe G sur $S\otimes_R S$ est compatible au produit $*$ donné par (8). Par fidèle platitude de ψ, l'anneau des invariants de $S\otimes_R S$ sous G est isomorphe à $S\otimes_R(S^G)$, donc à S. Montrons que $\Gamma_{S\otimes_R S/S}$ est un isomorphisme. Pour ce faire, remarquons que la structure de S-bimodule de $S\otimes_R S$ induite par ε_1 est définie par

$$s\cdot(t\otimes u) = st\otimes u \quad \text{et} \quad (t\otimes u)\cdot s = \sum_{g\in G} tg(u)s\eta_g.$$

On en déduit un isomorphisme Υ_1 de $(S\otimes_R S)\otimes_S(S\otimes_R S)$ vers $S\otimes_R S\otimes_R S$ donné par

$$\Upsilon_1\big((s\otimes t)\otimes(u\otimes v)\big) = \sum_{g\in G} sg(t)u\eta_g\otimes v \quad \text{et d'inverse} \quad \Upsilon_1^{-1}(s\otimes t\otimes v) = (s\otimes t)\otimes(1\otimes v),$$

pour $s, t, u, v \in S$. Soit Υ_2 l'isomorphisme canonique de $S\otimes_R\big(S(G)\big)$ vers $(S\otimes_R S)(G)$. On a :

$$\Gamma_{S\otimes_R S/S}\circ\Upsilon_1^{-1} = \Upsilon_2\circ(\mathrm{id}_S\otimes\Gamma_{S/R})$$

puisque les deux termes évalués sur $s\otimes t\otimes v$ valent $\sum_{g\in G} s\otimes tg(v)\delta_g$. Ainsi ε_1 est une extension G-galoisienne.

Pour $g \in G$, notons g à la fois l'automorphisme de $S\otimes_R S$ et l'automorphisme de $S(G)$ donnés respectivement par

$$g(s\otimes t) = s\otimes g(t) \quad \text{et} \quad g\left(\sum_{h\in G} s_h\delta_h\right) = \sum_{h\in G} s_h\delta_{hg^{-1}}.$$

On vérifie la relation

$$g\circ\Gamma = \Gamma\circ g$$

qui montre la trivialité de ε_1.

2) Soit $\psi : R \longrightarrow S$ une extension G-galoisienne stricte. La fidèle platitude de ψ permet d'injecter S dans $S\otimes_R S$ (exactitude du complexe d'Amitsur, voir par exemple [Nus]) et donc $|G|$ est encore inversible dans $S\otimes_R S$. Λ

2.2. L'algèbre des quaternions en caractéristique différente de 2. Soit F un corps commutatif de caractéristique différente de 2 et a, b deux éléments non nuls de F. On note $\mathrm{H}_{a,b}$ *l'algèbre des quaternions* $(\dfrac{a,b}{F})$ sur F, engendrée par les générateurs i et j et les relations $i^2 = a$, $j^2 = b$ et $ij = -ji$. Il est bien connu ([Ros]) que $\mathrm{H}_{a,b}$ est une F-algèbre centrale simple de dimension 4 isomorphe soit à l'algèbre de matrices $M_2(F)$, soit à un corps gauche, suivant que le symbole de Hilbert $(a, b)_F$ vaut 1 ou -1. Le groupe de Klein $V = (\mathbf{Z}/2\mathbf{Z})\times(\mathbf{Z}/2\mathbf{Z})$ engendré par α et β opère sur $\mathrm{H}_{a,b}$ par

$$\begin{aligned} \alpha(i) &= i, \quad & \alpha(j) &= -j, \\ \beta(i) &= -i, \quad & \beta(j) &= j. \end{aligned}$$

Dans [Nus, lemme 4.3.2], nous avons montré que l'extension $F \longrightarrow \mathrm{H}_{a,b}$ est V-galoisienne. La trace $\mathrm{tr} : \mathrm{H}_{a,b} \longrightarrow F$ est donnée par $\mathrm{tr}(a_0 + a_1 i + a_2 j + a_3 k) = 4a_0$, où l'on a posé $k = ij$. On a :

$$\Gamma\big(\frac{1}{4}(1\otimes 1 + \frac{i\otimes i}{a} + \frac{j\otimes j}{b} - \frac{k\otimes k}{ab})\big) = \delta_e.$$

Par conséquent $\mathcal{B}_{a,b} = (1/2, i/2a, j/2, -k/2a; 1/2, i/2, j/2b, k/2b)$ constitue une base galoisienne de $\psi : F \longrightarrow \mathrm{H}$.

A titre d'exemple, explicitons l'action de V sur $\mathrm{H}_{1,1}$. Il est bien connu que $\mathrm{H}_{1,1}$ est isomorphe à $M_2(F)$ par l'isomorphisme de F-algèbres ξ défini par

$$\xi(i) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ et } \xi(j) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

On vérifie aisément que l'action de V sur $\mathrm{H}_{1,1}$ se transporte par ξ en l'action de V sur $M_2(F)$ donnée sur un élément $\begin{pmatrix} x & y \\ z & t \end{pmatrix}$ de $M_2(F)$ par les formules

$$\alpha\begin{pmatrix} x & y \\ z & t \end{pmatrix} = \begin{pmatrix} x & -y \\ -z & t \end{pmatrix} \text{ et } \beta\begin{pmatrix} x & y \\ z & t \end{pmatrix} = \begin{pmatrix} t & z \\ y & x \end{pmatrix}.$$

Supposons que F est le corps des réels $\mathbf{R}$ et que $a = b = -1$, de sorte que $\mathrm{H}_{-1,-1}$ est le corps $\mathbf{H}$ des quaternions de Hamilton. Soit W le sous-groupe de V engendré par α. L'anneau des invariants de $\mathbf{H}$ sous W est le corps des complexes $\mathbf{C}$. On voit donc, d'après le théorème 1.9, que $\mathbf{C} \longrightarrow \mathbf{H}$ est une extension $\mathbf{Z}/2\mathbf{Z}$-galoisienne. La trace $\mathrm{tr} : \mathbf{H} \longrightarrow \mathbf{C}$ est donnée par $\mathrm{tr}(a_0 + a_1 i + a_2 j + a_3 k) = 2(a_0 + a_1 i)$ et l'on vérifie que $(1/\sqrt{2}, -j/\sqrt{2}; 1/\sqrt{2}, j/\sqrt{2})$ est une base galoisienne de $\mathbf{C} \longrightarrow \mathbf{H}$. Par le théorème 1.9 on retrouve le fait que $\mathbf{R} \longrightarrow \mathbf{C}$ est extension $\mathbf{Z}/2\mathbf{Z}$-galoisienne de base galoisienne $(1/\sqrt{2}, -i/\sqrt{2}; 1/\sqrt{2}, i/\sqrt{2})$.

2.3. Un contre-exemple : l'algèbre des quaternions en caractéristique 2. Soit F un corps de caractéristique 2, soient a et b deux éléments de F. Rappelons [Bla] que l'algèbre des quaternions associée à cette situation, notée $H_{a,b} = [\frac{a,b}{F})$, est engendrée par les générateurs e_1 et e_2 et les relations $e_1^2 = e_1 + a$, $e_2^2 = b$ et $e_2 e_1 = e_1 e_2 + e_2$ [Bla]. L'anneau $H_{a,b}$ est un corps si et seulement si le polynôme

$$X_0^2 + X_0 X_1 + a X_1^2 + b(X_2^2 + X_1 X_2 + a X_3^2) \in F[X_0, X_1, X_2, X_3]$$

a pour unique zéro le quadruplet $(0, 0, 0, 0)$. Plaçons-nous dans le cas où $H_{a,b}$ est un corps, avec $b = c^2$ un carré dans F. L'extension $\psi : F \longrightarrow H_{a,b}$ n'est pas galoisienne. En effet, d'après le lemme 1.8, si ψ était G-galoisienne pour un groupe G, nécessairement G serait isomorphe à $\mathbf{Z}/4\mathbf{Z}$ ou au groupe de Klein V.

- Supposons $G = V$. Soit g un élément de V. On a : $g(e_2)^2 = g(e_2^2) = b = c^2$. Donc $g(e_2)$, tout comme e_2, est racine dans $H_{a,b}$ de l'équation $X^2 + c^2 = 0$ qui est équivalente à l'équation $(X + c)^2 = 0$, puisque l'élément c est central dans $H_{a,b}$. Ceci prouve que $g(e_2) = e_2$ pour tout $g \in G$, ce qui est en contradiction avec le fait que $H_{a,b}^V = F$.

- Supposons $G = \mathbf{Z}/4\mathbf{Z}$. Soit u un générateur de G. Comme ci-dessus, on montre que $u(e_2)$, tout comme e_2, est racine dans $H_{a,b}$ de l'équation $X^4 + c^4 = 0$ qui est équivalente à l'équation $(X + c)^4 = 0$, ce qui conduit au même type de contradiction.

2.4. L'algèbre des matrices diagonales. Soit F une algèbre à division et n un entier ≥ 2. Pour $0 \leq i \leq n-1$, notons ε_i l'élément $(0, \cdots, 0, 1, 0, \cdots, 0)$ de F^n avec l'unité de F à la $i+1$-ème place. On munit F^n de la structure d'anneau produit. Le groupe $\mathbf{Z}/n\mathbf{Z}$ opère sur l'anneau F^n par permutation cyclique sur les ε_i. Les invariants sous $\mathbf{Z}/n\mathbf{Z}$ de F^n forment un anneau isomorphe à F. On note $\psi : F \longrightarrow F^n$ le morphisme diagonal, nécessairement fidèlement plat, puisque F est un corps.

Nous affirmons que l'extension ψ est galoisienne. Pour montrer cela, il suffit de prouver que l'application $\Gamma : F^n \otimes_F F^n \longrightarrow F^n(\mathbf{Z}/n\mathbf{Z})$ est surjective, puisque $F^n \otimes_F F^n$ et $F^n(\mathbf{Z}/n\mathbf{Z})$ sont des F-espaces vectoriels de même dimension. Ecrivons $F^n(\mathbf{Z}/n\mathbf{Z}) = S_0 \oplus S_1 \oplus \cdots \oplus S_{n-1}$ avec $S_i = F^n$ et notons $\varepsilon_{(i,j)}$ la base de $F^n(\mathbf{Z}/n\mathbf{Z})$ de telle sorte que $\varepsilon_{(i,0)}, \varepsilon_{(i,1)}, \ldots, \varepsilon_{(i,n-1)}$ soit la base canonique de S_i pour $0 \leq i \leq n-1$. On vérifie alors les formules

$$\Gamma(\varepsilon_i \otimes \varepsilon_{i-j}) = \varepsilon_{(j,i)} \quad \text{pour } 0 \leq j \leq i \quad \text{et} \quad \Gamma(\varepsilon_i \otimes \varepsilon_{i+j}) = \varepsilon_{(n-j,i)} \quad \text{pour } 0 \leq j \leq i-1, \tag{9}$$

desquelles résulte la surjectivité de Γ. On remarquera que l'extension ψ est galoisienne stricte dès que la caractéristique du corps F ne divise pas n. La trace $\mathrm{tr} : F^n \longrightarrow F$ est donnée par $\mathrm{tr}\left(\sum_{i=0}^{n-1} a_i \varepsilon_i\right) = \sum_{i=0}^{n-1} a_i$. Une base galoisienne se déduit des formules (9), en remarquant que $\delta_i = \sum_{j=0}^{n-1} \varepsilon_{(j,i)}$. Plus précisément, si $1 \leq i \leq n-1$, on a :

$$\delta_i = \Gamma(\varepsilon_0 \otimes \varepsilon_{n-i} + \varepsilon_1 \otimes \varepsilon_{n-i+1} + \ldots + \varepsilon_{i-1} \otimes \varepsilon_{n-1} + \varepsilon_i \otimes \varepsilon_0 + \varepsilon_{i+1} \otimes \varepsilon_1 + \ldots + \varepsilon_{n-1} \otimes \varepsilon_{n-1-i}) \quad \text{et}$$
$$\delta_0 = \Gamma(\varepsilon_0 \otimes \varepsilon_0 + \varepsilon_1 \otimes \varepsilon_1 + \ldots + \varepsilon_{n-1} \otimes \varepsilon_{n-1}).$$

Ainsi, $(\varepsilon_0, \varepsilon_1, \ldots \varepsilon_{n-1}; \varepsilon_0, \varepsilon_1, \ldots \varepsilon_{n-1})$ forme une base galoisienne de ψ.

2.5. Une extension séparable non galoisienne. Commençons par remarquer que si R est un anneau, si G est un groupe d'ordre n inversible dans R et si $R[G]$ est le R-anneau de groupe de G, alors l'inclusion canonique $\psi : R \longrightarrow R[G]$ est une extension séparable. En effet, $E = \dfrac{1}{n} \displaystyle\sum_{g \in G} g \otimes g^{-1}$ convient comme élément de séparabilité pour ψ.

Soient F un corps commutatif de caractéristique distincte de 2 et de 3, $\mathfrak{S}_3$ le groupe symétrique sur 3 éléments et $\mathfrak{A}_3$ le groupe alterné correspondant. Notons $F[G]$ la F-algèbre de groupe pour $G = \mathfrak{S}_3$ ou $\mathfrak{A}_3$. L'inclusion canonique $F \longrightarrow F[\mathfrak{S}_3]$ est séparable et, d'après la Proposition II 5.1.2 de [LVV], l'extension $\psi : F[\mathfrak{A}_3] \longrightarrow F[\mathfrak{S}_3]$ est également séparable. Montrons que ψ n'est pas galoisienne. Supposons le contraire. Pour des raisons de dimensions, le seul groupe H qui puisse réaliser un isomorphisme entre $F[\mathfrak{S}_3] \otimes_{F[\mathfrak{A}_3]} F[\mathfrak{S}_3]$ et $F[\mathfrak{S}_3](H)$ est d'ordre deux. Notons α le générateur d'ordre 3 et β le générateur d'ordre 2 de $\mathfrak{S}_3$, avec $\alpha\beta = \beta\alpha^2$, de sorte que $\mathfrak{A}_3$ est le groupe cyclique engendré par α. Soit u un automorphisme d'algèbre non trivial de $F[\mathfrak{S}_3]$ laissant $F[\mathfrak{A}_3]$ fixe point par point. Nécessairement $u(\alpha) = \alpha$ et $u(\beta) = \alpha\beta$ ou $\alpha^2\beta$. Il en résulte que u est d'ordre 3, ce qui est en contradiction avec l'ordre de H.

3. CRITÈRE DE NORMALITÉ D'UNE EXTENSION GALOISIENNE

Soit $\psi : R \longrightarrow S$ une extension G-galoisienne, fixée dans le reste du paragraphe. On rappelle que n est l'ordre de G. On note $\mathrm{Aut}(S/R)$ le groupe des automorphismes d'anneau de S laissant R invariant point par point et $\mathrm{Aut}_R(S)$ le groupe des automorphismes de S comme R-module (à droite). On a les inclusions de groupes : $G \subseteq \mathrm{Aut}(S/R) \subseteq \mathrm{Aut}_R(S)$. La question suivante se pose : quand G coïncide-t-il avec $\mathrm{Aut}(S/R)$?

3.1. Le cas général. Soit $\psi : R \longrightarrow S$ une extension G-galoisienne quelconque. Rappelons que $(\delta_g)_{g\in G}$ désigne la base canonique de $S(G)$, le S-module à gauche libre de rang n défini au § 1, et que l'on pose

$$\eta_g = \Gamma^{-1}(\delta_g) = \sum_{i=1}^{m} x_i \otimes g^{-1}(y_i),$$

où $(x_1, \ldots, x_m; y_1, \ldots, y_m)$ est une base galoisienne de ψ (théorème 1.5). Soient $f, f' \in \mathrm{Aut}(S/R)$ deux automorphismes fixés du R-anneau S. On note θ le morphisme S-linéaire à gauche de $S(G)$ dans S égal à

$$\theta^{f,f'} = \mu \circ (f \otimes f') \circ \Gamma^{-1}.$$

Pour tout $g \in G$, on définit, comme Chase, Harrison et Rosenberg dans le cas commutatif, un élément $\sigma_g^{f,f'} \in S$ par

$$\sigma_g^{f,f'} = \theta^{f,f'}(\delta_g) = \sum_{i=1}^{m} f(x_i) f'\big(g^{-1}(y_i)\big). \tag{10}$$

Définition 3.1. On appelle *coefficients d'entrelacement du couple* $(f, f') \in \mathrm{Aut}(S/R)^2$ la collection des n éléments $(\sigma_g^{f,f'})_{g\in G}$ de S définis ci-dessus.

On se convainc immédiatement que les deux égalités suivantes sont vérifiées pour tout $\varphi \in \mathrm{Aut}(S/R)$:

$$\sigma_g^{f,f'} = \sigma_e^{f,f'g^{-1}} \tag{11}$$

et

$$\varphi(\sigma_g^{f,f'}) = \sigma_g^{\varphi\circ f, \varphi\circ f'}. \tag{12}$$

Dans la suite nous nous intéresserons particulièrement à $\sigma_g^{f,h}$ pour $f \in \mathrm{Aut}(S/R)$ et $g, h \in G$. Le but de ce paragraphe est de démontrer le théorème suivant.

Théorème 3.2. *Soit $\psi : R \longrightarrow S$ une extension G-galoisienne et $f \in \mathrm{Aut}(S/R)$. Alors l'automorphisme f appartient à G si et seulement si les n coefficients d'entrelacement $(\sigma_g^{f,e})_{g\in G}$ appartiennent à l'ensemble $\{0, 1\}$.*

De ce résultat il s'ensuit que, pour tester l'appartenance d'un automorphisme f de $\mathrm{Aut}(S/R)$ au groupe de Galois, il n'est pas nécessaire de connaître explicitement tous les éléments de G afin de retrouver f dans la liste. Il suffit de déterminer les valeurs prises par les éléments de G sur la deuxième moitié d'une base galoisienne (*i.e.* les $g(y_i)$), puis de calculer les n coefficients d'entrelacement $(\sigma_g^{f,e})_{g\in G}$. Du théorème 3.2 découle immédiatement le résultat suivant :

Corollaire 3.3. *Soit $\psi : R \longrightarrow S$ une extension G-galoisienne. S'il existe $f \in \mathrm{Aut}(S/R)$ et $g \in G$ tels que $\sigma_g^{f,e} \notin \{0, 1\}$, alors ψ n'est pas normale.*

Exemple 3.4. Prenons l'automorphisme de $\mathbf{R}$-algèbre f de $\mathbf{H}$ donné par $f(1) = 1$, $f(i) = j$, $f(j) = k$ et $f(k) = i$. En calculant $\sigma_\gamma^{f,e}$ à l'aide de la base galoisienne $\mathcal{B}_{-1,-1}$ obtenue dans l'exemple 2.2, on trouve

$$\sigma_\gamma^{f,e} = \frac{1}{4}\big(1 + (-j)\cdot(-i) + (-k)\cdot(-j) + (-i)\cdot k\big) = \frac{1}{4}(1 - i + j - k)$$

qui n'est pas un idempotent. Cela montre que l'extension V-galoisienne quaternionique $\psi : \mathbf{R} \longrightarrow \mathbf{H}$ n'est pas normale (ce fait se déduit par ailleurs du théorème de Skolem-Nœther [FD] qui nous assure que $\mathrm{Aut}(\mathbf{H}/\mathbf{R})$ s'identifie au quotient $\mathbf{H}^\times/\mathbf{R}^\times$).

Avant de démontrer le théorème 3.2, énonçons deux résultats techniques.

Lemme 3.5. *Pour g, h, k trois éléments quelconques de G, on a l'égalité suivante :*

$$\sigma_g^{h,k} = \delta_{g,h^{-1}k}.$$

Démonstration : D'après (12), on a : $\sigma_g^{h,k} = h(\sigma_g^{e,h^{-1}k}) = h\big(\sum_{i=1}^{m} x_i(h^{-1}kg^{-1})(y_i)\big)$. Comme $\Gamma(\eta_g) = \delta_g$, on en conclut que $\sum_{i=1}^{m} x_i(h^{-1}kg^{-1})(y_i) = \delta_{g,h^{-1}k}$. Λ

Proposition 3.6. *Sous les hypothèses précédentes, on a, pour tout $f, f' \in \mathrm{Aut}(S/R)$, $g \in G$ et $s \in S$, les égalités :*

$$\sigma_g^{f,f'} f'(s) = f\big(g(s)\big)\sigma_g^{f,f'} \tag{13.1}$$

$$\sum_{g\in G} \sigma_g^{f,f'} = 1 \tag{13.2}$$

$$f'(s) = \sum_{g\in G} f\big(g(s)\big)\sigma_g^{f,f'}. \tag{13.3}$$

De plus, si $(\tau_g^{f,f'})_{g\in G}$ est une collection d'éléments de S indexés par G vérifiant (13.1), (13.2) *et* (13.3), *alors*

$$\tau_g^{f,f'} = \sigma_g^{f,f'}$$

pour tout $g \in G$.

Démonstration : En appliquant $(f\otimes f')\circ\Gamma$ aux deux membres de l'égalité (2), un calcul utilisant la multiplicativité de f et f' nous donne la relation suivante dans $S\otimes_R S$:

$$\sum_{i=1}^{m} f(x_i)\otimes f'(g^{-1}y_i)f'(s) = \sum_{i=1}^{m} f\big(g(s)\big)f(x_i)\otimes f'(g^{-1}y_i).$$

Il suffit de composer avec la multiplication μ pour obtenir la première relation.

La seconde identité provient de l'égalité

$$\sum_{g\in G} \eta_g = 1\otimes 1$$

obtenue en remarquant que $(\Gamma^{-1}\circ\Gamma)(1\otimes 1) = 1\otimes 1$, et donc que $\Gamma^{-1}\left(\sum_{g\in G}\delta_g\right) = 1\otimes 1$.

La troisième égalité résulte immédiatement des deux précédentes : il suffit de sommer la première formule sur tous les éléments g de G.

Unicité. Soit $(\tau_g^{f,f'})_{g\in G}$ une collection d'éléments de S vérifiant (13.1) et (13.2) (et donc automatiquement (13.3)). On a :

$$\sigma_g^{f,f'} = \sum_{i=1}^{m} f(x_i)f'(g^{-1}y_i) = \sum_{h\in G}\sum_{i=1}^{m} f(x_i)f\big(h(g^{-1}y_i)\big)\tau_h^{f,f'}$$

d'après (13.3) appliqué à $\tau_h^{f,f'}$. Donc

$$\sigma_g^{f,f'} = \sum_{h\in G} f\left(\sum_{i=1}^{m} x_i h(g^{-1}y_i)\right)\tau_h^{f,f'} = \sum_{h\in G} f(\sigma_g^{e,h})\tau_h^{f,f'} = \tau_g^{f,f'},$$

d'après le lemme 3.5. Λ

Démonstration du théorème 3.2 : Fixons $g \in G$. Si $f \in G$, d'après le lemme 3.5, $\sigma_g^{f,e}$ est égal soit à 1, soit à 0, suivant que $f^{-1}g^{-1} = e$ ou non.

Inversement, fixons $f \in \mathrm{Aut}(S/R)$. Si $\sigma_g^{f,e} \in \{0,1\}$ pour tout $g \in G$, alors d'après (12), $\sigma_g^{f,h} \in \{0,1\}$ pour tout $g, h \in G$. D'après (13.2), il existe alors, pour tout $h \in G$, un unique $g_h \in G$ tel que

$$\sigma_g^{f,h} = \delta_{g,g_h}.$$

Par conséquent, la formule (13.3) implique que $h(s) = (fg_h)(s)$, pour tout $s \in S$, et donc $f = hg_h^{-1} \in G$.

Λ

3.2. Le cas commutatif. Chase, Harrison et Rosenberg ont obtenu, pour une extension G-galoisienne d'anneaux commutatifs S/R, une condition suffisante pour avoir l'égalité des groupes G et $\mathrm{Aut}(S/R)$. Pour être complet, rappelons ce résultat et illustrons-le par un exemple. Nous conservons les notations précédentes.

Théorème (Chase - Harrison - Rosenberg). *Soit $\psi : R \longrightarrow S$ une extension G-galoisienne d'anneaux commutatifs. Si S ne possède pas d'autre élément idempotent que 0 et 1, alors $G = \mathrm{Aut}(S/R)$.*

Exemple 3.7. Soit $\psi : F \longrightarrow F^n$ l'extension $\mathbf{Z}/n\mathbf{Z}$-galoisienne des matrices diagonales (exemple 2.4). Soient $f \in \mathrm{Aut}(F^n/F)$ et $f(\varepsilon_i) = \sum_{j=0}^{n-1} a_{ij}\varepsilon_j$. La relation $f(\varepsilon_i)^2 = f(\varepsilon_i)$ implique que les $a_{ij} \in \{0,1\}$. Comme f stabilise F, on a : $f\left(\sum_{i=0}^{n-1}\varepsilon_i\right) = \sum_{i=0}^{n-1}\varepsilon_i$, d'où l'on déduit que, pour tout j, on a : $\sum_{i=0}^{n-1} a_{ij} = 1$. Ainsi (a_{ij}) représente une matrice de permutation. Réciproquement, n'importe quelle matrice de permutation définit un automorphisme de l'extension $\psi : F \longrightarrow F^n$, ce qui prouve que $\mathrm{Aut}(F^n/F)$ est égal au groupe $\mathfrak{S}_n$ des permutations de n éléments.

Si $n \geq 3$, on obtient ainsi un exemple d'extension $\mathbf{Z}/n\mathbf{Z}$-galoisienne $F \longrightarrow F^n$ telle que le groupe $\mathrm{Aut}(F^n/F)$ contient strictement le groupe de Galois. Conformément au théorème de Chase-Harrison-Rosenberg, l'anneau F^n possède des idempotents différents de 0 et de 1 (les ε_i par exemple). On notera en passant que la réciproque de ce théorème est fausse, puisque dans le cas $n = 2$, malgré la présence d'idempotents non triviaux, le groupe $\mathrm{Aut}(F^2/F)$ coïncide avec le groupe de Galois $\mathbf{Z}/2\mathbf{Z}$.

Le théorème de Chase - Harrison - Rosenberg ne s'applique pas en général aux extensions non commutatives, comme le montre l'exemple suivant.

Exemple 3.8. Reprenons le corps $\mathbf{H} = (\frac{-1,-1}{\mathbf{R}})$ des quaternions de Hamilton (qui ne possède pas d'idempotents non triviaux) et l'extension quaternionique $\psi : \mathbf{R} \longrightarrow \mathbf{H}$. D'après le théorème de Skolem-Nœther [FD], le groupe $\mathrm{Aut}(\mathbf{H}/\mathbf{R})$ est composé des automorphismes intérieurs. Soit

$\varrho : \mathbf{H}^\times \longrightarrow \mathrm{Aut}(\mathbf{H}/\mathbf{R})$ l'homomorphisme de groupes qui à $h \in \mathbf{H}$ associe la conjugaison ϱ_h par h. On a la suite exacte :

$$1 \longrightarrow \mathbf{R}^\times \longrightarrow \mathbf{H}^\times \xrightarrow{\varrho} \mathrm{Aut}(\mathbf{H}/\mathbf{R}) \longrightarrow 1$$

qui implique que $\mathrm{Aut}(\mathbf{H}/\mathbf{R})$ contient strictement V. Par exemple, la conjugaison $f \in \mathrm{Aut}(\mathbf{H}/\mathbf{R})$ par l'élément $(1+i+j+k)/4$, est telle que $f(1) = 1$, $f(i) = j$, $f(j) = k$ et $f(k) = i$. Elle n'appartient donc pas à V.

Remarquons aussi que V n'est pas distingué dans $\mathrm{Aut}(\mathbf{H}/\mathbf{R}) = \mathbf{H}^\times/\mathbf{R}^\times$. En effet, si l'on désigne par ϱ_u la conjugaison par l'élément $u \in \mathbf{H}^\times$, on constate que α, β et $\gamma \in V$ correspondent respectivement à ϱ_i, ϱ_j et ϱ_k vus dans $\mathrm{Aut}(\mathbf{H}/\mathbf{R})$. Prenons $u = i+2j$. On vérifie que $\varrho_u \circ \varrho_i \circ \varrho_u = \varrho_v$, où $v = \frac{1}{5}(-3i+4j)$.

Exemple 3.9. Revenons à l'exemple 2.4 avec $n = 3$. Le sextuplet $(\varepsilon_0, \varepsilon_1, \varepsilon_2; \varepsilon_0, \varepsilon_1, \varepsilon_2)$ forme une base galoisienne de ψ. Prenons $f \in \mathrm{Aut}(F^3/F)$ et $g \in \mathbf{Z}/3\mathbf{Z}$ de la manière suivante :

$$f = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad g = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{et} \quad g^{-1} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Alors (10) et un calcul matriciel aisé montrent que

$$\sigma_g^{f,e} = \sum_{i=0}^{2} f(\varepsilon_i) g^{-1}(\varepsilon_i) = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \varepsilon_1 \notin \{0, 1\},$$

et donc $f \notin \mathbf{Z}/3\mathbf{Z}$ et $\mathrm{Aut}(F^3/F)$ contient strictement $\mathbf{Z}/3\mathbf{Z}$, ce que nous savions déjà par ailleurs.

Remarque 3.10 : Dans le cas commutatif, Chase, Harrison et Rosenberg [CHR] montrent que, pour $f, f' \in \mathrm{Aut}(S/R)$ fixés, les $\sigma_g^{f,f'}$ sont nécessairement des idempotents orthogonaux, *i.e.*

$$\sigma_g^{f,f'} \sigma_h^{f,f'} = \delta_{g,h}.$$

Pour les extensions non commutatives, ce fait cesse d'être vrai. La raison en est que l'application $f \otimes f' : (S \otimes_R S, *) \longrightarrow S$ n'est pas nécessairement un morphisme d'anneaux. Prenons par exemple le corps $\mathbf{H}$ des quaternions de Hamilton, $f \in \mathrm{Aut}(\mathbf{H}/\mathbf{R})$ comme dans les exemples 3.4 et 3.8, et enfin γ l'automorphisme de l'exemple 2.2. Nous avons vu (exemple 3.4) que

$$\sigma_\gamma^{f,e} = \frac{1}{4}(1 - i + j - k)$$

qui n'est pas un idempotent.

4. COEFFICIENTS D'ENTRELACEMENT ET DESCENTE GALOISIENNE

Rappelons [Nus] que si $\psi : R \longrightarrow S$ est une extension G-galoisienne et M un S-module à droite, on appelle *donnée de descente galoisienne sur M* une opération du groupe G sur le groupe abélien sous-jacent à M vérifiant, pour tout $g \in G$, $m \in M$ et $s \in S$, l'égalité

$$g(ms) = g(m)g(s).$$

Le module M est alors appelé *galoisien*. D'après le théorème principal de la descente galoisienne [Nus, Th. 4.9], se donner un S-module galoisien M revient à se donner une R-module N et ces

deux modules se déduisent l'un de l'autre par les relations $M \cong N \otimes_R S$ et $N \cong M^G$. Dans ce paragraphe nous considérons le S-module $S(G)$ qui, étant isomorphe à $S \otimes_R S$, est muni d'une structure canonique de module galoisien. Nous rattachons les coefficients d'entrelacement du paragraphe 3 aux données de descente galoisienne canoniques sur $S(G)$.

Conservons les notations du paragraphe 3. Un automorphisme $F \in \mathrm{Aut}_S\big(S(G)\big)$ détermine n^2 éléments $([F]_h^{(g)})_{(g,h)\in G^2}$ de S définis par

$$F(\delta_g) = \sum_{h\in G} [F]_h^{(g)} \delta_h.$$

Définition 4.1. On appelle *système de coefficients attaché à l'automorphisme* F la collection des n^2 éléments $([F]_h^{(g)})_{(g,h)\in G^2}$.

Un ensemble de n^2 éléments $(s_h^{(g)})_{(g,h)\in G^2}$ de S suffit à déterminer entièrement un endomorphisme S-linéaire (à droite) F de $S(G)$ tel que $F(\delta_g) = \sum_{h\in G} s_h^{(g)} \delta_h$. En effet, en utilisant la structure de S-bimodule de $S(G)$, on voit que nécessairement F s'étend à $S(G)$ tout entier par la formule :

$$F(s\delta_g) = F\big(\delta_g g^{-1}(s)\big) = F(\delta_g) g^{-1}(s) = \sum_{h\in G} s_h^{(g)} \delta_h g^{-1}(s) = \sum_{h\in G} s_h^{(g)} \big(hg^{-1}(s)\big)\delta_h.$$

Fixons maintenant $f \in \mathrm{Aut}(S/R)$. En particulier f appartient à $\mathrm{Aut}_R(S)$ qui s'étend à un automorphisme S-linéaire $\tilde{f}$ de $S \otimes_R S$ donné par

$$\tilde{f}(s \otimes t) = f(s) \otimes t.$$

On en déduit un automorphisme S-linéaire $\bar{f}$ de $S(G)$ vérifiant

$$\bar{f} \circ \Gamma = \Gamma \circ \tilde{f}.$$

Proposition 4.2. *Soit $\psi : R \longrightarrow S$ une extension G-galoisiennne et $f \in \mathrm{Aut}(S/R)$. Pour tout $g, h \in G^2$, on a la relation :*

$$\sigma_g^{f,h} = [\bar{f}]_h^{(g)}. \tag{14}$$

Démonstration : Comme $\bar{f} = \Gamma \circ \tilde{f} \circ \Gamma^{-1}$, il vient

$$\bar{f}(\delta_g) = (\Gamma \circ \tilde{f})(\eta_g) = (\Gamma \circ \tilde{f})\big(\sum_{i=1}^m x_i \otimes g^{-1}(y_i)\big) = \Gamma\big(\sum_{i=1}^m f(x_i) \otimes g^{-1}(y_i)\big) = \sum_h \sum_{i=1}^m f(x_i) h\big(g^{-1}(y_i)\big)\delta_h.$$

Le système de coefficients attaché à $\bar{f}$ est donc donné par l'expression :

$$[\bar{f}]_h^{(g)} = \sum_{i=1}^m f(x_i) h\big(g^{-1}(y_i)\big),$$

qui est, d'après (10), la définition de $\sigma_g^{f,h}$. Λ

Le même calcul que ci-dessus montre, en utilisant la linéarité à gauche de Γ, que

$$\bar{f}(s\delta_g) = \sum_{h\in G} \sum_{i=1}^m f(s) f(x_i) h(g^{-1} y_i) \delta_h.$$

Par conséquent, $\bar{f}$ vérifie

$$\bar{f}(s\delta_g) = f(s)\bar{f}(\delta_g).$$

Corollaire 4.3. *Soit $f \in \mathrm{Aut}(S/R)$. Pour tout $g, h \in G$ et tout $s \in S$ on a :*

$$[\bar{f}]_h^{(g)} = [\bar{f}]_e^{(gh^{-1})} = [\bar{f}]_{hg^{-1}}^{(e)}. \tag{15}$$

et

$$[\bar{f}]_h^{(g)} h(s) = (f \circ g)(s)[\bar{f}]_h^{(g)}.$$

Démonstration : La relation (15) se déduit de (14) et de (11), alors que la deuxième égalité est la relation (13.1) en termes de système de coefficients. Λ

Proposition 4.4. *L'équation (15) caractérise les endomorphismes (respectivement les automorphismes) du S-module $S(G)$ qui proviennent d'endomorphismes (respectivement d'automorphismes) du R-module S par extension des scalaires à S.*

Démonstration : Par descente galoisienne sur les morphismes, les endomorphismes du R-module S sont en bijection avec les endomorphismes du S-module $S \otimes_R S$ qui commutent aux données de descente canoniques Φ_h définies par

$$\Phi_h(s \otimes t) = s \otimes h(t) \quad (h \in G,\ s, t \in S)$$

(voir [Nus, corollaire 4.15]). Il est facile de voir que l'action Φ' de G sur le groupe sous-jacent à $S(G)$ définie par

$$\Phi'_h\left(\sum_{g \in G} s_g \delta_g\right) = \sum_{g \in G} s_{gh}\delta_g$$

fait de $S(G)$ un S-module galoisien isomorphe par Γ à $S \otimes_R S$ (il suffit de prouver que $\Phi'_h \circ \Gamma = \Gamma \circ \Phi_h$). Ainsi un élément $F \in \mathrm{Aut}_S\big(S(G)\big)$ commute à tous les Φ'_h $(h \in G)$ si et seulement si il commute à Φ'_h. On vérifie alors aisément que F commute à tous les Φ'_h si et seulement si son système de coefficients satisfait

$$[F]_k^{(gh^{-1})} = [F]_{kh}^{(g)}$$

pour tout $k, h, g \in G$ ou, ce qui revient au même, l'une des deux égalités

$$[F]_h^{(g)} = [F]_e^{(gh^{-1})} = [F]_{hg^{-1}}^{(e)}.$$

Λ

Le lien ainsi établi avec la descente permet de produire des relations sur les coefficients d'entrelacement. Nous donnons ci-dessous un exemple de telles égalités.

Proposition 4.5. *Soient f et $f' \in \mathrm{Aut}(S/R)$. On a l'égalité :*

$$\sigma_e^{f \circ f', h} = \sum_{g \in G} f(\sigma_e^{f', g^{-1}})\sigma_e^{f, hg}.$$

En particulier,

$$\sum_{g \in G} f(\sigma_e^{f^{-1}, g^{-1}})\sigma_e^{f, hg} = \boldsymbol{\delta}_{e,h}.$$

Démonstration : Remarquons que $\widetilde{f \circ f'} = \tilde{f} \circ \tilde{f}'$ et donc que $\overline{f \circ f'} = \bar{f} \circ \bar{f}'$. On a :

$$(\overline{f \circ f'})(\delta_e) = \bar{f}\left(\sum_{g \in G} [\bar{f}']_g^{(e)} \delta_g\right) = \sum_{g \in G} f([\bar{f}']_g^{(e)}) \bar{f}(\delta_g)$$
$$= \sum_{g,h \in G} f([\bar{f}']_g^{(e)})[\bar{f}]_h^{(g)} \delta_h = \sum_{g,h \in G} f([\bar{f}']_g^{(e)})[\bar{f}]_{hg^{-1}}^{(e)} \delta_h.$$

Pour obtenir la première égalité, on remplace les systèmes de coefficients par les coefficients d'entrelacement en utilisant (14). La seconde formule se déduit de la première en prenant $f' = f^{-1}$. Λ

5. COHOMOLOGIE NON ABÉLIENNE DES EXTENSIONS GALOISIENNES D'AZUMAYA - LE CAS DES QUATERNIONS

Dans ce paragraphe, nous introduisons un module croisé $\mathscr{M}_\psi$ naturellement attaché à une extension G-galoisienne $\psi : R \longrightarrow S$ pour laquelle l'anneau R est contenu dans le centre de S. Nous appliquons alors le formalisme de l'hypercohomologie non abélienne $\mathbb{H}^i(G, \mathscr{M}_\psi)$ $(i = -1, 0, 1)$ introduit par Borovoi. Cette théorie se présente comme un avatar de la cohomologie non abélienne de Dedecker (voir [Ded1], [Ded2]). Dans le cas des extensions quaternioniques réelle, p-adique et sur un corps fini $\mathbf{F}_q$, nous calculons explicitement les ensembles d'hypercohomologie non abélienne $\mathbb{H}^i(V, \mathscr{M}_\psi)$ $(i = -1, 0, 1)$.

5.1. Modules croisés. Avant d'aborder la définition des modules croisés, rappelons que si U est un groupe quelconque, un *U-groupe (à gauche)* est un groupe A muni d'une action à gauche de U. Cela signifie que A est un U-ensemble muni d'une structure de groupe invariante par U, *i.e.*, pour tout $u \in U$ et tout $a, b \in A$, on a :

$$^u(ab) = {}^u a\, {}^u b \quad \text{et} \quad {}^u 1 = 1.$$

Définitions 5.1 (voir [Bor] par exemple). Un *module croisé (de groupes)* $\mathscr{M} = (\varrho : H \longrightarrow \Pi)$ est la donnée d'un morphisme de groupes $\varrho : H \longrightarrow \Pi$ et d'une action de Π sur H notée ${}^\pi h$ (avec $h \in H$ et $\pi \in \Pi$) vérifiant les compatibilités suivantes :

$$^{\varrho(h)}(h') = hh'h^{-1} \tag{16}$$
$$\varrho({}^\pi h) = \pi \varrho(h) \pi^{-1} \tag{17}$$

pour tout $h, h' \in H$ et $\pi \in \Pi$ (classiquement, l'égalité (16) est appelée *identité de Peiffer*).

Un *module croisé de U-groupes (à gauche)* $\mathscr{M} = (\varrho : H \longrightarrow \Pi)$ est la donnée d'un module croisé où H et Π sont des U-groupes (à gauche), d'un morphisme équivariant de U-groupes ϱ et de la compatibilité suivante :

$$^u({}^\pi h) = {}^{^u\pi}({}^u h) \tag{18}$$

pour tout $u \in U$, $h \in H$ et $\pi \in \Pi$.

Soient $\mathscr{M}_i = (\varrho_i : H_i \longrightarrow \Pi_i)$ $(i = 1, 2)$ deux modules croisés de U-groupes. Un *morphisme (ξ, ζ) de $\mathscr{M}_1$ dans $\mathscr{M}_2$* est la donnée deux morphismes de U-groupes $\xi : H_1 \longrightarrow H_2$ et $\zeta : \Pi_1 \longrightarrow \Pi_2$ rendant le diagramme

$$\begin{array}{ccc} H_1 & \xrightarrow{\xi} & H_2 \\ {\scriptstyle \varrho_1}\downarrow & & \downarrow{\scriptstyle \varrho_2} \\ \Pi_1 & \xrightarrow{\zeta} & \Pi_2 \end{array}$$

commutatif et vérifiant, pour tout $h \in H_1$ et $\pi \in \Pi_1$, l'égalité

$$\xi({}^{\pi}h) = {}^{\zeta(\pi)}\xi(h).$$

Soient $\mathscr{M}_i = (\varrho_i : H_i \longrightarrow \Pi_i)$ $(i = 1, 2, 3)$ trois modules croisés de U-groupes. La suite

$$1 \longrightarrow \mathscr{M}_1 \xrightarrow{(\xi_1,\zeta_1)} \mathscr{M}_2 \xrightarrow{(\xi_2,\zeta_2)} \mathscr{M}_3 \longrightarrow 1$$

de morphismes de modules croisés de U-groupes est dite *exacte* si le diagramme

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H_1 & \xrightarrow{\xi_1} & H_2 & \xrightarrow{\xi_2} & H_3 & \longrightarrow & 1 \\ & & \varrho_1\downarrow & & \varrho_2\downarrow & & \varrho_3\downarrow & & \\ 1 & \longrightarrow & \Pi_1 & \xrightarrow{\zeta_1} & \Pi_2 & \xrightarrow{\zeta_2} & \Pi_3 & \longrightarrow & 1 \end{array}$$

est commutatif à lignes exactes.

5.2. Module croisé attaché à une extension galoisienne centrale. Soit $\psi : R \longrightarrow S$ une extension G-galoisienne, $A = \mathrm{Aut}(S/R)$ le groupe des automorphismes d'anneau de S laissant R invariant point par point. On suppose que R est *central* dans S (nous appellerons une telle extension galoisienne *centrale*). On note $S^{\times}$ le groupe des éléments inversibles de S.

Les groupes A et $S^{\times}$ sont des G-groupes à gauche pour les opérations suivantes : le groupe G opère sur A par conjugaison : ${}^{g}f = g \circ f \circ g^{-1}$ (pour $g \in G$ et $f \in A$) et sur $S^{\times}$ par l'action déduite de l'action de G sur l'anneau S. De plus, le groupe A opère à gauche sur $S^{\times}$ par l'action déduite de l'action de A sur l'anneau S, induisant ainsi une action du G-groupe A sur $S^{\times}$. Cela signifie que toutes les opérations précédentes sont compatibles au sens suivant :

$${}^{g}\big(f(s)\big) = {}^{g}f\big(g(s)\big)$$

(pour tout $g \in G$, $f \in A$ et $s \in S^{\times}$). Introduisons maintenant un module croisé canoniquement attaché à une extension galoisienne centrale.

Lemme 5.2. *Soit ϱ le morphisme de groupes de $S^{\times}$ dans A qui associe à l'élément $s \in S^{\times}$ la conjugaison ϱ_s par s :*

$$\varrho_s(t) = sts^{-1} \quad (\text{pour} \quad t \in S).$$

Alors $\mathscr{M}_{\psi} = (\varrho : S^{\times} \longrightarrow A)$ est un module croisé de G-groupes.

Démonstration : L'application ϱ_s est clairement un morphisme d'anneaux inversible d'inverse $\varrho_{s^{-1}}$. La R-linéarité de ϱ et la propriété de stabilisation de R point par point découlent du fait que R est central dans S. Il est évident que ϱ est un morphisme de groupes et qu'il vérifie (17). Montrons que ϱ satisfait l'identité de Peiffer. Pour $f \in A$ et $s, t \in S$ on a :

$$(f\varrho_s f^{-1})(t) = f\varrho_s\big(f^{-1}(t)\big) = f(sf^{-1}(t)s^{-1}) = f(s)tf(s^{-1}) = f(s)tf(s)^{-1} = \varrho_{f(s)}(t).$$

La G-compatibilité se déduit du calcul suivant : pour tout $g \in G$, $f \in A$ et $s, t \in S^{\times}$, on a :

$$\big(\varrho({}^{g}s)\big)(t) = g(s)tg(s)^{-1} = g(sg^{-1}(t)s^{-1}) = g \circ \varrho(s) \circ g^{-1}(t) = \big({}^{g}\varrho(s)\big)(t) \quad \text{et}$$
$${}^{g}({}^{f}s) = g\big(f(s)\big) = (g \circ f \circ g^{-1})\big(g(s)\big) = {}^{g}f\big(g(s)\big) = {}^{{}^{g}f}({}^{g}s).$$

Λ

Exemple 5.3. Soit F un corps commutatif de caractéristique différente de 2, soient a et b deux éléments non nuls de F et $\mathrm{H}_{a,b}$ l'algèbre des quaternions $(\frac{a,b}{F})$ sur F. L'extension $\psi : F \longrightarrow \mathrm{H}_{a,b}$ étant V-galoisienne centrale (voir 2.2), $\mathscr{M}_\psi = \big(\varrho : \mathrm{H}_{a,b}^\times \longrightarrow \mathrm{Aut}(\mathrm{H}_{a,b}/F)\big)$ est un module croisé de V-groupes.

5.3. Hypercohomologie non abélienne. Soit U un groupe et $\mathscr{M}$ un module croisé de U-groupes. Borovoi, s'inspirant des travaux de Dedecker ([Ded1], [Ded2]), construit trois ensembles de cohomologie non abélienne $\mathbb{H}^i(U,\mathscr{M})$ $(i=-1,0,1)$, l'*hypercohomologie de U à coefficients dans $\mathscr{M}$*. Rappelons leur définition (voir [Bor]).

Définitions 5.4. Soit U un groupe et $\mathscr{M} = (\varrho : H \longrightarrow \Pi)$ un module croisé de U-groupes. On définit le *groupe de -1-hypercohomologie de U à valeurs dans $\mathscr{M}$* comme étant le groupe des invariants sous G du noyau de ϱ :

$$\mathbb{H}^{-1}(U,\mathscr{M}) = (\mathrm{Ker}\varrho)^G.$$

On considère les deux ensembles

$$\begin{aligned} C^0 &= \mathrm{App}(G,H)\times\Pi \quad \text{et} \\ Z^0 &= \{(\varphi,\pi)\in C^0 \mid \varphi(g_1g_2) = \varphi(g_1)^{g_1}\big(\varphi(g_2)\big) \ \text{ et } \ {}^g\pi = \varrho\big(\varphi(g)\big)\pi \ \ \forall\, g_1,g_2,g\in G\}, \end{aligned}$$

où $\mathrm{App}(G,H)$ désigne l'ensemble des applications de G dans H. Les éléments de C^0 et Z^0 sont appelés respectivement les 0-*cochaînes* et les 0-*cocycles*. Le groupe H agit à droite sur l'ensemble des 0-cocycles par l'action $*$ définie comme suit :

$$(\varphi,\pi) * h = (\varphi',\pi')$$

où $\varphi'(g)$ et π' sont donnés par les formules :

$$\varphi'(g) = h^{-1}\varphi(g)g(h) \quad \text{et} \quad \pi' = \varrho(h)^{-1}\pi,$$

pour $(\varphi,\pi)\in Z^0$, $h\in H$ et $g\in G$. L'ensemble Z^0/H des orbites pour cette action est noté $\mathbb{H}^0(U,\mathscr{M})$ et est appelé *0-hypercohomologie non-abélienne de U à valeurs dans $\mathscr{M}$*. C'est non seulement un ensemble pointé d'élément distingué la classe du cocycle $(1,1)$, mais encore un groupe, la loi étant induite par la loi de groupe sur C^0 donnée par

$$(\varphi_1,\pi_1)\cdot(\varphi_2,\pi_2) = (\varphi',\pi_1\pi_2) \quad \text{où} \quad \varphi'(g) = {}^{\pi_1}\varphi_2(g)\cdot\varphi_1(g) \ \ (\forall g\in G).$$

On considère les deux ensembles

$$\begin{aligned} C^1 &= \mathrm{App}(G{\times}G,H){\times}\mathrm{App}(G,\Pi) \quad \text{et} \\ Z^1 &= \{(u,\vartheta)\in C^1 \mid u(g,g_1g_2)\cdot{}^{\vartheta(g)g}u(g_1,g_2) = u(gg_1,g_2)\cdot u(g,g_1) \ \text{ et} \\ &\qquad \vartheta(g_1g_2) = \varrho\big(u(g_1,g_2)\big)\cdot\vartheta(g_1)\cdot{}^{g_1}\vartheta(g_2) \ \ \forall g_1,g_2,g\in G\}. \end{aligned}$$

Les éléments de C^1 et Z^1 sont appelés respectivement les 1-*cochaînes* et les 1-*cocycles*. Le groupe C^0 agit à droite sur l'ensemble des 1-cocycles par l'action $*$ définie comme suit

$$(u,\vartheta) * (\varphi,\pi) = (u',\vartheta')$$

où u' et ϑ' sont donnés par les formules :

$$u'(g_1,g_2) = {}^{\pi^{-1}}[\varphi(g_1g_2)\cdot u(g_1,g_2)\cdot {}^{\vartheta(g_1)g_1}\varphi(g_2)^{-1}\cdot\varphi(g_1)^{-1}] \quad \text{et} \quad \vartheta'(g) = \pi^{-1}\cdot\varrho\big(\varphi(g)\big)\cdot\vartheta(g)\cdot {}^{g}\pi,$$

pour $(u,\vartheta)\in Z^1, (\varphi,\pi)\in C^0$ et $g,g_1,g_2\in G$. L'ensemble Z^1/C^0 des orbites pour cette action est noté $\mathbb{H}^1(U,\mathscr{M})$ et est appelé *1-hypercohomologie non-abélienne de U à valeurs dans $\mathscr{M}$.* L'ensemble $\mathbb{H}^1(U,\mathscr{M})$ n'est, en général, pas un groupe, mais un ensemble pointé d'élément distingué la classe du 1-cocycle $(1,1)$.

La suite de cette section présente des résultats qui reposent essentiellement sur le lemme suivant démontré par Borovoi ([Bor, 3.1.2, 3.3.4 et lemme 3.2.3]) :

Lemme 5.5. *Soit U un groupe et $\mathscr{M} = (\varrho : H \longrightarrow \Pi)$ un module croisé de U-groupes tel que ϱ soit injective. Alors le noyau* $\mathrm{Ker}\varrho$ *est central dans H, donc abélien, et on a les isomorphismes de groupes, pour $i=-1$ ou 0 et d'ensembles pointés pour $i=1$:*

$$\mathbb{H}^i(U,\mathscr{M}) \cong \mathrm{H}^{i+1}(U,\mathrm{Ker}\varrho).$$

Ici $\mathrm{H}^i(U,\mathrm{Ker}\varrho)$ désigne le $i^{\text{ème}}$ groupe de cohomologie (abélienne) de U à coefficients dans $\mathrm{Ker}\varrho$.

5.4. Hypercohomologie non abélienne des extensions galoisiennes d'Azumaya. Appliquons le lemme 5.5 au calcul de l'hypercohomologie non abélienne des extensions galoisiennes d'Azumaya, dont les extensions quaternioniques (voir 2.2) constituent des parangons.

Définitions 5.6. Un morphisme d'anneau $\psi : R \longrightarrow S$ est appelé *extension G-galoisienne d'Azumaya* si ψ est une extension G-galoisienne, R un corps commutatif et S une R-algèbre d'Azumaya, *i.e.* une R-algèbre centrale simple.

L'intérêt d'introduire des algèbres d'Azumaya réside dans le fait que leurs groupes d'automorphismes sont bien connus. En effet, si S est une R-algèbre d'Azumaya, le théorème de Skolem-Nœther [FD] montre que la suite

$$1 \longrightarrow R^\times \longrightarrow S^\times \xrightarrow{\varrho} \mathrm{Aut}(S/R) \longrightarrow 1$$

est exacte. Dans le cas particulier où $\psi : R \longrightarrow S$ est une extension G-galoisienne d'Azumaya telle que l'indice de $R^\times$ dans $S^\times$ est infini, la suite exacte précédente prouve que ψ n'est en aucun cas normale.

Proposition 5.7. *Soit $\psi : R \longrightarrow S$ une extension G-galoisienne d'Azumaya. Soit $\mathscr{M}_\psi = \big(\varrho : S^\times \longrightarrow \mathrm{Aut}(S/R)\big)$ le module croisé de G-groupes associé. On a alors les isomorphismes de groupes :*

$$\mathbb{H}^{-1}(G,\mathscr{M}_\psi) \cong R^\times, \quad \mathbb{H}^0(G,\mathscr{M}_\psi) \cong \mathrm{Hom}(G,R^\times) \quad et \quad \mathbb{H}^1(G,\mathscr{M}_\psi) \cong \mathrm{H}^2(G,R^\times).$$

Démonstration : La démonstration repose sur le lemme 5.5 qui, dans le cas des extensions G-galoisiennes d'Azumaya, fournit, pour $i=-1,0,1$, les isomorphismes

$$\mathbb{H}^i(G,\mathscr{M}_\psi) \cong \mathrm{H}^{i+1}(G,R^\times).$$

Etant donné que l'action de G est triviale sur le groupe $R^\times$, il vient que $\mathbb{H}^{-1}(G, \mathscr{M}_\psi)$ est isomorphe à $R^\times$. Il en découle aussi que l'ensemble $Z^1(G, R^\times)$ des 1-cocycles abéliens est constitué des morphismes de groupes de G dans $R^\times$ et que $\mathrm{H}^1(G, R^\times)$ est isomorphe à $Z^1(G, R^\times)$. Λ

Remarquons au passage que l'action de G sur $R^\times$ étant triviale, le groupe $\mathbb{H}^1(G, \mathscr{M}_\psi) \cong \mathrm{H}^2(G, R^\times)$ classifie les extensions centrales de G par $R^\times$.

5.5. Hypercohomologie non abélienne des extensions quaternioniques. Nous appliquons maintenant ce qui précède à un exemple d'extensions galoisiennes d'Azumaya, les extensions quaternioniques.

Corollaire 5.8. *Soit F un corps commutatif de caractéristique différente de 2, soient a et b deux éléments non nuls de F, soit $\mathrm{H}_{a,b}$ l'algèbre des quaternions $(\frac{a,b}{F})$ sur F, soient $\psi : F \longrightarrow \mathrm{H}_{a,b}$ l'extension V-galoisienne quaternionique et $\mathscr{M}_\psi = \big(\varrho : \mathrm{H}_{a,b}^\times \longrightarrow \mathrm{Aut}(\mathrm{H}_{a,b}/F)\big)$ le module croisé de V-groupes associé. Il existe des isomorphismes de groupes :*

$$\mathbb{H}^{-1}(V, \mathscr{M}_\psi) \cong F^\times, \quad \mathbb{H}^0(V, \mathscr{M}_\psi) \cong V \quad \textit{et} \quad \mathbb{H}^1(V, \mathscr{M}_\psi) \cong \mathrm{H}^2(V, F^\times).$$

Si, de plus, $a = b = -1$, on a les isomorphismes de groupes suivants :

$$\mathbb{H}^1(V, \mathscr{M}_\psi) \cong \begin{cases} (\mathbf{Z}/2\mathbf{Z})^3 \textit{ si } F = \mathbf{R} \\ (\mathbf{Z}/2\mathbf{Z})^5 \textit{ si } F \textit{ est le corps } \mathbf{Q}_p \textit{ des nombres } p\textit{-adiques, avec } p \textit{ premier} \neq 2 \\ (\mathbf{Z}/2\mathbf{Z})^7 \textit{ si } F \textit{ est le corps } \mathbf{Q}_2 \textit{ des nombres 2-adiques} \\ (\mathbf{Z}/2\mathbf{Z})^3 \textit{ si } F \textit{ est le corps fini } \mathbf{F}_q \textit{ avec } q = p^n \textit{ et } p \textit{ premier} \neq 2 \end{cases}$$

Démonstration : D'après la proposition 5.7, il nous faut calculer $\mathrm{H}^1(V, F^\times)$ et $\mathrm{H}^2(V, F^\times)$. Le premier de ces groupes est isomorphe à $\mathrm{Hom}(V, F^\times)$, donc à V, puisque l'image d'un générateur de V par un morphisme de groupes de V dans $F^\times$ est nécessairement 1 ou -1, les uniques racines du polynôme $X^2 - 1 \in F[X]$. Abordons le calcul de $\mathrm{H}^2(V, F^\times)$.

5.5.1. Le cas réel. On suppose que F est le corps des réels $\mathbf{R}$ et que $a = b = -1$, de sorte que $\mathrm{H}_{-1,-1}$ est le corps $\mathbf{H}$ des quaternions de Hamilton.

Remarquons que le groupe multiplicatif $\mathbf{R}^\times$ est isomorphe au groupe $\mathbf{Z}/2\mathbf{Z}\times\mathbf{R}$. De la suite exacte

$$\mathrm{H}^2(V, \mathbf{R}) \longrightarrow \mathrm{H}^2(V, \mathbf{R}^\times) \longrightarrow \mathrm{H}^2(V, \mathbf{Z}/2\mathbf{Z}) \longrightarrow \mathrm{H}^3(V, \mathbf{R})$$

extraite de la longue suite exacte associée à la suite exacte courte $0 \longrightarrow \mathbf{R} \longrightarrow \mathbf{R}^\times \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow 0$, on déduit l'isomorphisme

$$\mathrm{H}^2(V, \mathbf{R}^\times) \cong \mathrm{H}^2(V, \mathbf{Z}/2\mathbf{Z}),$$

étant donné que $\mathrm{H}^*(V, \mathbf{R})$ est nul pour $* \geq 1$ puisque $|V| = 4$ est inversible dans $\mathbf{R}$. Par la formule de Künneth, $\mathrm{H}^2(V, \mathbf{Z}/2\mathbf{Z}) = \mathrm{H}^2(V, \mathbf{F}_2)$ est isomorphe à

$$\begin{aligned} \big(\mathrm{H}^0(\mathbf{Z}/2\mathbf{Z}, \mathbf{F}_2) \otimes_{\mathbf{F}_2} \mathrm{H}^2(\mathbf{Z}/2\mathbf{Z}, \mathbf{F}_2)\big) \oplus \big(\mathrm{H}^1(\mathbf{Z}/2\mathbf{Z}, \mathbf{F}_2) \otimes_{\mathbf{F}_2} \mathrm{H}^1(\mathbf{Z}/2\mathbf{Z}, \mathbf{F}_2)\big) \\ \oplus \big(\mathrm{H}^2(\mathbf{Z}/2\mathbf{Z}, \mathbf{F}_2) \otimes_{\mathbf{F}_2} \mathrm{H}^0(\mathbf{Z}/2\mathbf{Z}, \mathbf{F}_2)\big). \end{aligned}$$

Les isomorphismes $\mathrm{H}^0(\mathbf{Z}/2\mathbf{Z}, \mathbf{F}_2) \cong \mathbf{Z}/2\mathbf{Z}$, $\mathrm{H}^1(\mathbf{Z}/2\mathbf{Z}, \mathbf{F}_2) \cong \mathbf{Z}/2\mathbf{Z}$ et $\mathrm{H}^2(\mathbf{Z}/2\mathbf{Z}, \mathbf{F}_2) \cong \mathbf{Z}/2\mathbf{Z}$ [Wei, théorème 6.2.2] établissent alors le résultat annoncé.

5.5.2. Le cas p-adique ($p \neq 2$). Soit p un nombre premier impair, $\mathbf{Q}_p$ le corps des nombres p-adiques et $\mathbf{Z}_p$ son anneau des entiers. Désignons par $\mathbf{H}_p$ l'algèbre des quaternions $(\frac{-1,-1}{\mathbf{Q}_p})$.

Calculons $\mathrm{H}^2(V, \mathbf{Q}_p^\times)$. Il est bien connu [Ser1] que, si $p \neq 2$, le groupe multiplicatif $\mathbf{Q}_p^\times$ est isomorphe au groupe

$$\mathbf{Z}_p \times \mathbf{Z} \times \mathbf{Z}/(p-1)\mathbf{Z}.$$

La suite exacte courte $0 \longrightarrow \mathbf{Z}_p \longrightarrow \mathbf{Q}_p^\times \longrightarrow \mathbf{Z}\times\mathbf{Z}/(p-1)\mathbf{Z} \longrightarrow 0$ induit la suite exacte

$$\mathrm{H}^2(V, \mathbf{Z}_p) \longrightarrow \mathrm{H}^2(V, \mathbf{Q}_p^\times) \longrightarrow \mathrm{H}^2\big(V, \mathbf{Z}\times\mathbf{Z}/(p-1)\mathbf{Z}\big) \longrightarrow \mathrm{H}^3(V, \mathbf{Z}_p)$$

extraite de la longue suite exacte de cohomologie. Comme $|V| = 4$ est inversible dans $\mathbf{Z}_p$ pour p impair, on déduit l'isomorphisme

$$\mathrm{H}^2(V, \mathbf{Q}_p^\times) \cong \mathrm{H}^2\big(V, \mathbf{Z}\times\mathbf{Z}/(p-1)\mathbf{Z}\big).$$

Soit M le groupe additif $\mathbf{Z}\times\mathbf{Z}/(p-1)\mathbf{Z}$, vu comme V-module trivial. Calculons $\mathrm{H}^2(V, M)$ à l'aide du Théorème des coefficients universels [CE] qui nous assure que ce groupe s'inscrit dans la suite exacte courte scindée

$$0 \longrightarrow \mathrm{Ext}^1_{\mathbf{Z}}\big(\mathrm{H}_1(V, \mathbf{Z}), M\big) \longrightarrow \mathrm{H}^2(V, M) \longrightarrow \mathrm{Hom}_{\mathbf{Z}}\big(\mathrm{H}_2(V, \mathbf{Z}), M\big) \longrightarrow 0. \tag{19}$$

Lemme 5.9. *Soit V le groupe de Klein. On a les isomorphismes :*

$$\mathrm{H}_1(V, \mathbf{Z}) \cong V \quad \textit{et} \quad \mathrm{H}_2(V, \mathbf{Z}) \cong \mathbf{Z}/2\mathbf{Z}.$$

Démonstration : Comme V est un $\mathbf{Z}$-module trivial, le module $\mathrm{H}_1(V, \mathbf{Z})$ de 1-homologie de V à coefficients dans $\mathbf{Z}$ est l'abélianisé $V/[V, V]$ de V, donc V.

Pour calculer $\mathrm{H}_2(V, \mathbf{Z}) = \mathrm{H}_2\big((\mathbf{Z}/2\mathbf{Z})^2, \mathbf{Z}\big)$, appliquons la formule de Künneth [Wei, proposition 6.1.13] qui fournit une suite exacte courte scindée

$$0 \longrightarrow (\mathrm{H}_0 \otimes \mathrm{H}_2)^2 \oplus (\mathrm{H}_1 \otimes \mathrm{H}_1) \longrightarrow \mathrm{H}_2(V, \mathbf{Z}) \longrightarrow \mathrm{Tor}_1^{\mathbf{Z}}(\mathrm{H}_0, \mathrm{H}_0) \longrightarrow 0,$$

où l'on a posé $\mathrm{H}_i = \mathrm{H}_i(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z})$ pour $i = 0, 1, 2$. Les isomorphismes $\mathrm{H}_0 \cong \mathbf{Z}$ (qui nous assure, en particulier, la nullité de $\mathrm{Tor}_1^{\mathbf{Z}}(\mathrm{H}_0, \mathrm{H}_0)$), $\mathrm{H}_1 \cong \mathbf{Z}$ et $\mathrm{H}_2 = 0$ [Wei, exemple 6.2.3] permettent de conclure que $\mathrm{H}^2(V, \mathbf{Z})$ est isomorphe à $\mathbf{Z}/2\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}/2\mathbf{Z}$, donc à $\mathbf{Z}/2\mathbf{Z}$. Λ

Suite de la démonstration du corollaire 5.8 : La suite exacte (19) s'écrit donc

$$0 \longrightarrow \mathrm{Ext}^1_{\mathbf{Z}}\big((\mathbf{Z}/2\mathbf{Z})^2, M\big) \longrightarrow \mathrm{H}^2(V, M) \longrightarrow \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}/2\mathbf{Z}, M) \longrightarrow 0. \tag{20}$$

Or, nous avons les isomorphismes

$$\begin{aligned} \mathrm{Ext}^1_{\mathbf{Z}}\big((\mathbf{Z}/2\mathbf{Z})^2, M\big) &\cong \mathrm{Ext}^1_{\mathbf{Z}}(\mathbf{Z}/2\mathbf{Z}, M)^2 \quad \text{[Wei, proposition 3.3.4]} \\ &\cong (M/2M)^2 \quad \text{[Wei, calcul 3.3.2]} \\ &\cong (\mathbf{Z}/2\mathbf{Z})^4. \end{aligned}$$

Pour terminer, remarquons que $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}/2\mathbf{Z}, M)$ est isomorphe à $\mathbf{Z}/2\mathbf{Z}$. En effet l'image $(x, y) \in M = \mathbf{Z}\times\mathbf{Z}/(p-1)\mathbf{Z}$ du générateur de $\mathbf{Z}/2\mathbf{Z}$ est d'ordre 2 dans M et donc vérifie : $x = 0$ et

$y \in {}_2(\mathbf{Z}/2m\mathbf{Z})$, donc $y = 0$ ou $y = m$ (où l'on a posé $p-1 = 2m$). Ainsi $\mathrm{H}^2(V, \mathbf{Q}_p^\times) = V \times (\mathbf{Z}/2\mathbf{Z}) \cong (\mathbf{Z}/2\mathbf{Z})^5$.

5.5.3. Le cas 2-adique. Soit $\mathbf{Q}_2$ le corps des nombres 2-adiques, $\mathbf{Z}_2$ son anneau des entiers et $\mathbf{H}_2$ l'algèbre des quaternions $(\frac{-1,-1}{\mathbf{Q}_2})$. On calcule $\mathrm{H}^2(V, \mathbf{Q}_2^\times)$ à l'aide de la suite exacte (20) dans laquelle on a remplacé cette fois-ci M par le V-module trivial $\mathbf{Q}_2^\times$, isomorphe [Ser1] au groupe additif

$$\mathbf{Z}_2 \times \mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}.$$

Le groupe $\mathrm{Ext}^1_{\mathbf{Z}}\big((\mathbf{Z}/2\mathbf{Z})^2, M\big)$ est isomorphe à $(M/2M)^2$, donc à $\big((\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}_2/2\mathbf{Z}_2) \times (\mathbf{Z}/2\mathbf{Z})\big)^2$, ce qui implique que $\mathrm{Ext}^1_{\mathbf{Z}}\big((\mathbf{Z}/2\mathbf{Z})^2, M\big)$ est isomorphe à $(\mathbf{Z}/2\mathbf{Z})^6$ en utilisant l'identification $\mathbf{Z}_2/2\mathbf{Z}_2 \cong \mathbf{Z}/2\mathbf{Z}$.

Pour terminer, on remarque que $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z})$ et $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}_2)$ sont des groupes triviaux, puisque la multiplication par 2 est injective dans $\mathbf{Z}$ et dans $\mathbf{Z}_2$, et donc $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}/2\mathbf{Z}, M)$ est isomorphe à $\mathbf{Z}/2\mathbf{Z}$. Ainsi $\mathrm{H}^2(V, \mathbf{Q}_2^\times) = (\mathbf{Z}/2\mathbf{Z})^6 \times (\mathbf{Z}/2\mathbf{Z}) \cong (\mathbf{Z}/2\mathbf{Z})^7$.

5.5.4. Le cas des corps finis. Soit $\mathbf{F}_q$ le corps fini à $q = p^n$ éléments, avec p premier $\neq 2$ et $\mathbf{H}'_q$ l'algèbre des quaternions $(\frac{-1,-1}{\mathbf{F}_q})$. Rappelons que $\mathbf{H}'_q$ est nécessairement une algèbre de matrices, en vertu du théorème de Wedderburn qui affirme qu'il n'existe pas de corps non commutatif fini. On calcule à nouveau $\mathrm{H}^2(V, \mathbf{F}_q^\times)$ à l'aide du théorème des coefficients universels (20) sachant que le groupe multiplicatif $\mathbf{F}_q^\times$ est isomorphe au groupe cyclique $M = \mathbf{Z}/(q-1)\mathbf{Z}$. Il faut donc, comme dans le cas p-adique, déterminer $\mathrm{Ext}^1_{\mathbf{Z}}\big((\mathbf{Z}/2\mathbf{Z})^2, M\big) = (M/2M)^2$ et $\mathrm{Hom}_{\mathbf{Z}}\big(\mathbf{Z}/2\mathbf{Z}, M\big)$. Etant donné que $p \neq 2$, le nombre $q-1$ est pair, donc $(M/2M)^2$ est isomorphe à $(\mathbf{Z}/2\mathbf{Z})^2$ et $\mathrm{Hom}_{\mathbf{Z}}\big(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/(q-1)\mathbf{Z}\big)$ à $\mathbf{Z}/2\mathbf{Z}$. Λ

Corollaire 5.10. *Soit F un corps commutatif de caractéristique différente de 2, soient a et b deux éléments non nuls de F, tels que $H_{a,b}$ est un corps. Le groupe A^V des invariants sous V de $A = \mathrm{Aut}(H_{a,b}/F)$ est isomorphe à V.*

Démonstration : On applique dans le cas des quaternions la portion

$$1 \longrightarrow \mathbb{H}^{-1}(U, \mathscr{M}) \longrightarrow \mathrm{H}^0(U, H) \longrightarrow \mathrm{H}^0(U, \Pi) \longrightarrow \mathbb{H}^0(U, \mathscr{M}) \longrightarrow \mathrm{H}^1(U, H)$$

de la suite exacte longue associée à un module croisé $\mathscr{M} = (\varrho : H \longrightarrow \Pi)$ de U-groupes [Bor, corollaire 3.4.3]. Elle s'écrit

$$1 \longrightarrow F^\times \longrightarrow F^\times \longrightarrow A^V \longrightarrow V \longrightarrow \mathrm{H}^1(V, H_{a,b}^\times).$$

On conclut en remarquant que $\mathrm{H}^1(V, H_{a,b}^\times)$ est trivial, d'après l'analogue non commutatif du théorème 90 de Hilbert (voir [Nus, corollaire 6.21]). Λ

Dans le cas des quaternions de Hamilton, explicitons l'isomorphisme de A^V avec V en retrouvant "à la main" les invariants de A sous V. Pour $[h]$, la classe dans $\mathbf{H}^\times/\mathbf{R}^\times$ d'un élément h de $\mathbf{H}^\times$, notons $\varrho_{[h]}$ l'automorphisme intérieur de $\mathbf{H}$ défini par

$$\varrho_{[h]}(q) = hqh^{-1}$$

pour tout $q \in \mathbf{H}$. D'après le théorème de Skolem-Nœther, tout automorphisme $f \in A$ est de la forme $\varrho_{[h]}$ pour un certain $h \in \mathbf{H}^\times$ (rappelons que $\alpha = \varrho_{[i]}, \beta = \varrho_{[j]}$ et $\gamma = \varrho_{[k]}$). L'automorphisme

$f = \varrho_{[h]}$ est invariant par tout élément $v = \varrho_{[u]} \in V$ si et seulement si $v \circ f \circ v^{-1}(h') = f(h')$, pour tout $h' \in \mathbf{H}$. Donc

$$v(h)h'v(h^{-1}) = hh'h^{-1} \tag{21}$$

pour tout $v \in V$ et tout $h' \in \mathbf{H}$. En particulier pour $h' = v(h)$, on a $v(h)h = hv(h)$, pour tout $V \in V$, ou encore $uhu^{-1}h = huhu^{-1}$, c'est-à-dire

$$[h^{-1}, u] = [u, h],$$

pour tout $u \in \{i, j, k\}$ (où $[-,-]$ désigne le commutateur dans $\mathbf{H}^\times$). Un calcul aisé montre que si $h = x + yi + zj + tk \in \mathbf{H}^\times$, alors $[h^{-1}, i] = [i, h]$ (respectivement $[h^{-1}, j] = [j, h]$, respectivement $[h^{-1}, k] = [k, h]$) si et seulement si $yz = yt = 0$ (respectivement $zt = zy = 0$, respectivement $ty = tz = 0$). Donc h est nécessairement de la forme $x + yi$, $x + zj$ ou $x + tk$. Si l'on suppose $h = x + yi$, il suffit de prendre $h' = j + k$ dans (21) pour se convaincre que le produit xy est nul. Donc $[h] = [1]$ ou $[h] = [i]$ dans $\mathbf{H}^\times/\mathbf{R}^\times$. Les cas $h = x + zj$ ou $x + tk$ se traitent de manière identique. Ainsi $[h] = [1], [i], [j]$ ou $[k]$ et donc $f = \alpha, \beta$ ou γ. Ces conditions sont suffisantes pour que f appartienne au groupe A^V.

Montrons, toujours dans le cas des quaternions de Hamilton, que la cohomologie de Borovoi en degré 0 et 1 est, en un sens que nous allons préciser, indépendante de la norme quaternionique. Soit N la norme quaternionique sur $\mathbf{H}$ définie sur un élément $x \in \mathbf{H}$ par $N(x) = x\bar{x}$ et $\mathbf{U} = \mathrm{Ker}(N : \mathbf{H}^\times \longrightarrow \mathbf{R}_{>0})$ le groupe des quaternions de norme 1. On vérifie que l'inclusion de $\mathbf{U}$ dans $\mathbf{H}^\times$ permet de définir un module croisé de V-groupes $\mathscr{U}_\psi : (\varrho_{|\mathbf{U}} : \mathbf{U} \longrightarrow A)$. Le morphisme $\varrho_{|\mathbf{U}}$ reste surjectif. En effet, si $f \in A$, il existe $h \in \mathbf{H}^\times$ avec $\varrho(h) = f$. Mais $\varrho(h)$ étant la conjugaison par h, on a : $\varrho(h) = \varrho_{|\mathbf{U}}\big(h/N(h)\big)$. Notons $\boldsymbol{\mu}_2 = \{1, -1\} = \mathbf{R}^\times \cap \mathbf{U}$ le groupe des racines carrées de l'unité de $\mathbf{R}$.

Proposition 5.11. *Avec les notations précédentes, on a les isomorphismes de groupes suivants :*

$$\mathbb{H}^{-1}(V, \mathscr{U}_\psi) \cong \boldsymbol{\mu}_2, \quad \mathbb{H}^0(V, \mathscr{U}_\psi) \cong \mathbb{H}^0(V, \mathscr{M}_\psi) \quad \textit{et} \quad \mathbb{H}^1(V, \mathscr{U}_\psi) \cong \mathbb{H}^0(V, \mathscr{M}_\psi).$$

Démonstration : Il est facile de vérifier que le diagramme

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathbf{U} & \longrightarrow & \mathbf{H}^\times & \xrightarrow{N} & \mathbf{R}_{>0} & \longrightarrow & 1 \\
 & & {\scriptstyle \varrho_{|\mathbf{U}}}\downarrow & & {\scriptstyle \varrho}\downarrow & & \downarrow & & \\
1 & \longrightarrow & A & \xrightarrow{\mathrm{id}} & A & \longrightarrow & 1 & \longrightarrow & 1
\end{array}$$

(où toutes les flèches non étiquetées sont canoniques) est commutatif à lignes exactes et que toutes les compatibilités sont vérifiées de sorte que la suite de V-modules croisés

$$1 \longrightarrow \mathscr{U}_\psi \longrightarrow \mathscr{M}_\psi \longrightarrow \mathscr{R}_\psi \longrightarrow 1,$$

est exacte (on désigne par $\mathscr{R}_\psi$ le module croisé de groupes $(\mathbf{R}_{>0} \longrightarrow 1)$, le groupe V agissant trivialement). D'après la proposition 3.4.2 de [Bor], on déduit une suite exacte d'hypercohomologie

$$\begin{aligned}
1 \longrightarrow \mathbb{H}^{-1}(V, \mathscr{U}_\psi) \longrightarrow \mathbb{H}^{-1}(V, \mathscr{M}_\psi) \longrightarrow \mathbb{H}^{-1}(V, \mathscr{R}_\psi) \longrightarrow \mathbb{H}^0(V, \mathscr{U}_\psi) \longrightarrow \mathbb{H}^0(V, \mathscr{M}_\psi) \\
\longrightarrow \mathbb{H}^0(V, \mathscr{R}_\psi) \longrightarrow \mathbb{H}^1(V, \mathscr{U}_\psi) \longrightarrow \mathbb{H}^1(V, \mathscr{M}_\psi) \longrightarrow \mathbb{H}^1(V, \mathscr{R}_\psi)
\end{aligned}$$

qui se décompose, dans notre cas, en deux suites exactes

$$1 \longrightarrow \boldsymbol{\mu}_2 \longrightarrow \mathbf{R}^\times \xrightarrow{(\ )^2} \mathbf{R}_{>0} \longrightarrow 1 \quad \text{et}$$

$$\begin{aligned} 1 \longrightarrow \mathbb{H}^0(V, \mathscr{U}_\psi) \longrightarrow \mathbb{H}^0(V, \mathscr{M}_\psi) \longrightarrow \mathrm{H}^1(V, \mathbf{R}_{>0}) \longrightarrow \mathbb{H}^1(V, \mathscr{U}_\psi) \\ \longrightarrow \mathbb{H}^1(V, \mathscr{M}_\psi) \longrightarrow \mathrm{H}^2(V, \mathbf{R}_{>0}), \end{aligned}$$

étant donné que le groupe $\mathbb{H}^i(V, X \longrightarrow 1)$ est, pour $i = -1, 0, 1$, isomorphe au groupe $\mathrm{H}^{i+1}(V, X)$ pour tout groupe abélien X [Bor]. Comme l'ordre de V est inversible dans $\mathbf{R}_{>0}$, les groupes $\mathrm{H}^1(V, \mathbf{R}_{>0})$ et $\mathrm{H}^2(V, \mathbf{R}_{>0})$ sont triviaux, d'où l'assertion. Λ

5.6. Note sur la 0- et la 1-cohomologie de Dedecker. On se donne un module croisé $\mathscr{M} = (\varrho : H \longrightarrow \Pi)$, un groupe U et un morphisme κ de U dans Π. Dedecker associe des ensembles de cohomologie $\mathrm{H}^i_\kappa(U, \mathscr{M})$ pour $i = 0, 1, 2$ de la manière suivante [Ded2]. L'ensemble $\mathrm{H}^0_\kappa(U, \mathscr{M})$ est le groupe défini par

$$\mathrm{H}^0_\kappa(U, \mathscr{M}) = \{h \in H \mid \ {}^{\kappa(u)}h = h \ \ \forall u \in U\},$$

i.e. c'est le sous-groupe de H des éléments κ-invariants. Soit

$$Z^1_\kappa(U, \mathscr{M}) = \{\alpha : U \longrightarrow H \mid \ \alpha(uu') = \alpha(u) \cdot {}^{\kappa(u)}\alpha(u')\},$$

l'ensemble des 1-*cocycles*. Un élément de $Z^1_\kappa(U, \mathscr{M})$ est un κ-homomorphisme croisé. On a une action à gauche $*$ de H sur $Z^1_\kappa(U, \mathscr{M})$ donnée par :

$$h * \alpha = \alpha', \qquad \alpha'(u) = h.\alpha(u) \cdot {}^{\kappa(u)}(h^{-1})$$

pour $\alpha \in Z^1_\kappa(U, \mathscr{M}), h \in H$ et $u \in U$. L'ensemble des orbites pour cette action est notée $\mathrm{H}^1_\kappa(U, \mathscr{M})$ et est appelée *1-cohomologie non-abélienne de U à valeurs dans $\mathscr{M}$ suivant κ.* Ce n'est, en général, qu'un ensemble pointé. L'ensemble $\mathrm{H}^2_\kappa(U, \mathscr{M})$ (appelé 2-*cohomologie épaisse* dans [Ded2]) est défini de manière semblable à la 1-hypercohomologie dans laquelle on aurait remplacé l'action de U par l'action triviale. Le morphisme κ sert uniquement à fixer un élément distingué, la classe de $(\kappa, 1)$ dans le "nuage" d'éléments neutres que possède l'ensemble $\mathrm{H}^2_\kappa(U, \mathscr{M})$.

Proposition 5.12. *Soit $\psi : R \longrightarrow S$ une extension G-galoisienne centrale. Soit $\mathscr{M}_\psi = (\varrho : S^\times \longrightarrow A)$ le module croisé associé et κ l'inclusion canonique de G dans A. Alors les ensembles de cohomologie de Dedecker $\mathrm{H}^0_\kappa(G, \mathscr{M}_\psi)$ et $\mathrm{H}^1_\kappa(G, \mathscr{M}_\psi)$ coïncident avec les ensembles de cohomologie galoisienne non abélienne $H^0(G, S^\times)$ et $H^1(G, S^\times)$ respectivement.*

Pour la cohomologie non abélienne de degré 0 et 1, nous renvoyons à [Ser2]. Les ensembles de cohomologie galoisienne non abélienne $H^0(G, S^\times)$ et $H^1(G, S^\times)$ ont été étudiés dans [Nus, § 6.4]. La proposition 5.12 implique en particulier que

$$\mathrm{H}^0_\kappa(G, \mathscr{M}_\psi) = R^\times$$

et que, si R et S sont des algèbres à division,

$$\mathrm{H}^1_\kappa(G, \mathscr{M}_\psi) = \{1\}$$

d'après le Théorème 90 de Hilbert (voir [Nus, corollaire 6.21]).

Démonstration de la proposition 5.12 : Le point essentiel est de remarquer que, comme κ est injective, le groupe A n'apporte aucune information supplémentaire à la contribution de G. On a par exemple :

$$\mathrm{H}^0_\kappa(G, \mathscr{M}_\psi) = (S^\times)^G = S^\times \cap S^G = R^\times.$$

De même, si on écrit les définitions de $Z^1_\kappa(G, \mathscr{M}_\psi)$ et de $\mathrm{H}^1_\kappa(G, \mathscr{M}_\psi)$, on retombe sur celles de $Z^1(G, S^\times)$ et $H^1(G, S^\times)$ respectivement. Λ

BIBLIOGRAPHIE

[Bla] Blanchard, André. : *Les corps non commutatifs*, Presses Universitaires de France, Paris (1972).

[Bor] Borovoi, M. : Abelian Galois cohomology of reductive groups, *Memoirs of the A.M.S.*, Vol. **132**, Number 626 (1998).

[Bou] Bourbaki, N. : *Éléments de Mathématique, Algèbre commutative*, Chap. 1 et 2, Hermann, Paris (1961).

[Bre] Breen, L. : Bitorseurs et cohomologie non abélienne, in *The Grothendieck Festschrift*, Volume I, Progr. Math. 86, Birkhäuser, Boston - Basel - Berlin (1990).

[CE] Cartan, H., Eilenberg S. : *Homological algebra*, Princeton University Press, Princeton, New Jersey (1956).

[CHR] Chase, S.U., Harrison, D.K., Rosenberg, A. : Galois theory and cohomology of commutative rings, *Memoirs of the A.M.S.*, Number 52 (1965).

[CS] Chase, S.U., Sweedler, M.E. : *Hopf algebras and Galois theory*, Lecture Notes in Math. 97 Springer-Verlag, Berlin - Heidelberg - New York (1969).

[Ded1] Dedecker, P. : Les foncteurs $\mathcal{E}\mathrm{xt}_\Pi$, $\mathbf{H}^2_\Pi$ et H^2_Π non abéliens, *C. R. Acad. Sc. Paris*, t. **258** (1964), 4891 - 4894.

[Ded2] Dedecker, P. : Three dimensional non-abelian cohomology for groups, in *Category Theory, Homology Theory and their Applications II*, Lecture Notes in Math. 92, Springer-Verlag, Berlin - Heidelberg - New York (1969).

[DI] De Meyer, F., Ingraham E. : *Separable algebras over commutative rings*, Lecture Notes in Math. 181, Springer-Verlag, Berlin - Heidelberg - New York (1971).

[DM] Deligne, P., Milne, J. : Tannakian categories, in *Hodge Cycles, Motives, and Shimura Varieties*, Lecture Notes in Math. 900, Springer-Verlag, Berlin - Heidelberg - New York (1982).

[FD] Farb, B., Dennis R.K. : *Noncommutative algebra*, Graduate Texts in Mathematics, Vol. 144, Springer-Verlag, Berlin - Heidelberg - New York (1993).

[Gre] Greither, C. : *Cyclic Galois extensions of commutative rings*, Lecture Notes in Math. 1534, Springer-Verlag, Berlin - Heidelberg (1992).

[Kre] Kreimer, H.F. : A note on the outer Galois theory of rings, *Pacific Journal of Mathematics*, Vol. **31**, No. 2, (1969), 417 - 432.

[KT] Kreimer, H.F., Takeuchi, M. : Hopf algebras and Galois extensions of an algebra, *Indiana Univ. Math. J.*, Vol. **30** (1981), 675 - 692.

[LVV] le Bruyn L., van den Bergh, M., van Oystaeyen, F. : *Graded orders*, Birkhäuser, Boston - Basel (1988).

[Nak] Nakayama, T. : On a generalized notion of Galois extensions of a ring, *Osaka J. Math.*, Vol. **15** (1963), 11 - 23.

[Nus] Nuss, P. : Noncommutative descent and nonabelian cohomology, *K-Theory* **12** (1997) 23 - 74.

[Ros] Rosenberg, J. : *Algebraic K-theory and its applications*, Graduate Texts in Mathematics, Vol. 147, Springer-Verlag, Berlin - Heidelberg - New York (1994).

[Sch] Schneider, H.-J. : Principal homogeneous spaces for arbitrary Hopf algebras, *Israel J. Math.*, Vol. **72**, Nos 1-2 (1990), 167 - 195.

[Ser1] Serre, J.P. : *Cours d'arithmétique*, Presses Universitaires de France, Paris (1970).

[Ser2] Serre, J.P. : *Cohomologie galoisienne*, Lecture Notes in Math. 5, Springer-Verlag, Berlin - Heidelberg - New York (1973).

[Ulb] Ulbrich, K.-H. : Galoiserweiterungen von nicht-kommutativen Ringen, *Communications in Algebra*, Vol. **10** (6) (1982), 655 - 672.

[Wei] Weibel, C.A. : *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics 38, Cambridge University Press, Cambridge (1994).