# Résultats de classification pour les twists gradués d'algèbres de Hopf

Maeva Paradis



UNIVERSITÉ CLERMONT AUVERGNE

ECOLE DOCTORALE DES SCIENCES FONDAMENTALES

UMR 6620 - Laboratoire de Mathématiques Blaise Pascal

Thèse présentée pour obtenir le grade universitaire de Docteur

Discipline : Mathématiques

Spécialité : Algèbre

**Maëva PARADIS**

# Résultats de classification pour les twists gradués d'algèbres de Hopf

Graded twist of Hopf algebras classification results

Sous la direction de Julien BICHON

Soutenance le 23/10/2020 à 14h00 devant le jury composé de :

| | | |
|---|---|---|
| Sonia NATALE | Université de Córdoba | Rapporteur et Examinateur |
| Peter SCHAUENBURG | Université de Bourgogne | Rapporteur et Examinateur |
| Simon RICHE | Université Clermont Auvergne | Examinateur |
| Julien BICHON | Université Clermont Auvergne | Directeur de thèse et Examinateur |

# Remerciements

Mes premiers remerciements vont à mon directeur de thèse Julien, qui a su me faire confiance il y a trois ans en me proposant de travailler sur ce sujet. Vous avez su me guider, m'aider, répondre à mes questions même quand elles étaient naïves. Merci d'avoir été à l'écoute lorsque le moral n'était plus au beau fixe, et d'y avoir encore cru pour nous deux afin de me remettre en selle ! Merci pour cette belle expérience et l'orientation que vous avez su donner à mon avenir avec vos précieux conseils.

Je remercie Sonia Natale, Peter Schauenburg et Simon Riche pour avoir accepté de participer en tant que rapporteurs et membres du jury à l'évaluation de cette thèse.

J'ai également beaucoup de gratitude pour le soutien qu'a pu m'apporter Marusia, "ma marraine de thèse". Tu as su m'épauler, me guider, non pas sur le plan mathématique, mais sur le plan humain lors des moments de flottement, toujours avec bienveillance et sans jugement, merci.

J'en profite aussi pour remercier mes collègues de laboratoire, l'équipe GAAO, et tout ceux qui ont été présent tout au long cette thèse, pour échanger quelques mots dans les couloirs, boire un verre dans un bar... À mes professeurs devenus collègues, aux compagnons de thèse, Rénald, Arnaud, Sophie, Franck, Valentin, Damien... Merci à Valérie Sourlier, amicalement dévouée à trouver des solutions pour résoudre mes problèmes ! Merci à Sylvie Chassagne pour son aide administrative.

C'est ici que je dois remercier Annick Montori qui a toujours su remonter le moral des troupes lors de l'agrégation ! Merci pour ton soutien sans faille, j'espère que la retraite fait ton bonheur !

Un grand merci à mes amis, restés en Auvergne ou partis s'expatrier au grès du travail en région Parisienne... Elodie, Marion, Aurore, Armonie, Bruno, Thyda, Mickaël... Je n'arriverai probablement pas à citer individuellement tous ceux qui ont joué un rôle dans ces trois années de travail, mais je les remercie du fond du coeur. Un merci particulier à Elodie dite "la survoltée", qui m'a permis de me relever dans un moment de doute, et qui a tout fait pour

me changer les idées.

Que serait cette thèse sans Thibault, Professeur Agrégé de Mathématiques, que j'aime fort, et que je remercie pour ces coups de pied au derrière quand c'était nécessaire ! C'est le rôle d'un meilleur ami, et tu le joues à merveille !

Je remercie également ma famille qui loin de comprendre les tenants et aboutissants de cette thèse, ni le travail que cela représente, m'a soutenu depuis le début et a toujours cru en moi. Maman, Papa merci de m'avoir donné l'opportunité de faire des études. Merci à ma mamie, qui a toujours été fière de parler de mon travail ! Merci à Rodolphe qui est fière de sa soeur, même sans lui dire !

Enfin, mes derniers remerciements vont à la personne la plus chère à mon coeur, Jonathan. Voilà deux ans que tu partages ma vie, tu as donc aussi partagé cette thèse avec moi. Tu as cru en moi quand je n'y arrivai plus, toujours avec amour, sans jugement, et tu as été d'un grand soutien pour mes candidatures post-thèse. Je suis chanceuse que tu décide de partir avec moi, construire notre vie à Aurillac ! J'espère que ce poste sera une opportunité d'épanouissement pour nous deux et les perspectives d'un bel avenir commun, je t'aime !

# Résumé

Ce travail de thèse contribue à la classification à isomorphisme près des algèbres de Hopf obtenues comme twists gradués d'algèbres de fonction sur des groupes finis par des actions cocentrales de groupes cycliques.

Plus généralement, nous étudions le problème d'isomorphisme pour les algèbres de Hopf s'insérant dans des extensions cocentrales abéliennes.

Nous appliquons ensuite ces résultats de classification à divers exemples concrets impliquant les groupes spéciaux linéaires sur des corps finis, les groupes symétriques et alternés, et les groupes diédraux.

# Abstract

This thesis work contributes to isomorphism classification for Hopf algebras that are obtained as graded twistings of function algebras on finite groups by cocentral actions of cyclic groups.

More generally, we also consider the isomorphism problem for finite-dimensional Hopf algebras fitting into abelian cocentral extensions.

Finally, we apply our classification results to a number of concrete examples like special linear groups over finite fields, alternating groups and dihedral groups.

# Table des matières

# Chapitre 1

# Introduction

Les algèbres de Hopf sont une généralisation des groupes de grande envergure. Dans le cadre semi-simple (par conséquent de dimension finie), le cadre le plus proche de celui des groupes finis, tous les exemples connus proviennent de groupes à travers diverses constructions sophistiquées. Une question fondamentale est donc de savoir si une algèbre de Hopf semi-simple est constructible à partir d'un groupe en un sens approprié (voir [2, Problème 3.9]).

Une réponse à cette question, positive ou non, laisserait encore beaucoup de travail quant au problème de classification de telles algèbres de Hopf.

À travers cette thèse, nous contribuons à ce problème de classification, en particulier pour les algèbres de Hopf obtenues comme twists gradués d'algèbres de fonctions sur un groupe fini.

La construction du twist gradué d'algèbre de Hopf, qui diffère en général de la construction du twist classique par un 2-cocycle (voir [9]), a été introduite dans [4], et correspond à une formalisation de la construction de [27] qui résout le problème de réalisation des catégories de Kazhdan-Wenzl [19] par des groupes quantiques.

Les données sont celles d'une algèbre de Hopf $A$, graduée et sur laquelle agit un groupe $\Gamma$. L'algèbre de Hopf twistée qui en résulte possède un certain nombre de caractéristiques plaisantes, liées à l'algèbre de départ. Parmi ces caractéristiques, la suivante possède un intérêt particulier : si $A = \mathcal{O}(G)$ est l'algèbre des fonctions d'un groupe algébrique linéaire $G$ et si $\Gamma$ est d'ordre premier, alors tous les quotients non commutatifs de l'algèbre twistée sont encore des twists gradués de $\mathcal{O}(H)$, où $H$ est un sous-groupe fermé de $G$ bien choisi. Ceci s'applique en particulier à $\mathcal{O}_{-1}(\mathrm{SL}_2(\mathbb{C}))$, dont les quotients non commutatifs sont traités et classifiés dans [28, 3].

Les résultats dans [4, 5] laissent cependant ouverte la question de la classification à iso-

morphisme près des algèbres de Hopf obtenues comme twists gradués, et c'est précisément le problème que nous allons traiter dans ce manuscrit.

On démontrera trois résultats d'isomorphisme pour les twists gradués d'algèbres de Hopf des fonctions sur un groupe fini. Ces résultats ont tous en commun des hypothèses cohomologiques fortes sur le groupe sous-jacent, que nous pensons difficiles à éliminer pour obtenir des résultats généraux, mais qui sont pourtant suffisamment larges pour couvrir un certain nombre de cas intéressants.

Nous obtenons des résultats de classification pour les algèbres de Hopf étant des twists gradués de :

1. $\mathcal{O}(\mathrm{SL}_n(\mathbb{F}_q))$ par $\mathbb{Z}_m$, où $q$ est une puissance d'un nombre premier, $m = \mathrm{PGCD}(n, q-1)$ est premier et $(n, q) \notin \{(2, 9), (3, 4)\}$ (voir le théorème 5.1.2) ;
2. $\mathcal{O}(\widetilde{A_n})$ par $\mathbb{Z}_2$, où $\widetilde{A_n}$ est l'unique revêtement de Schur du groupe alterné $A_n$, avec $n \neq 6$ (voir le théorème 5.2.1) ;
3. $\mathcal{O}(\widetilde{S_n})$ par $\mathbb{Z}_2$, où $\widetilde{S_n}$ est l'un des deux revêtements de Schur du groupe symétrique $S_n$, avec $n \neq 6$ (voir le théorème 5.2.2).

Tandis que les deux premiers théorèmes d'isomorphisme (théorème 3.0.1 et théorème 3.0.3) sont obtenus assez directement et au début du manuscrit (dans le chapitre 3), le troisième (théorème 4.4.4) est obtenu en considérant le problème plus général de la classification des algèbres de Hopf s'inscrivant dans une extension cocentrale abélienne.

C'est un sujet classique dans le domaine, qui a été beaucoup étudié et pour lequel plusieurs résultats de classification ont été obtenus [21, 26, 16]. La plupart de notre analyse dans le chapitre 4 est donc bien connue des spécialistes, mais nous pensons que certaines formulations et notre concentration sur les extensions universelles apportent une nouveauté, et nous obtenons de nouveaux résultats dans ce cadre.

En effet, nous obtenons des résultats de classification (c'est-à-dire des paramétrisations par des données théoriques de groupe, concrètes et explicitement connues) pour des algèbres de Hopf non commutatives $A$ s'inscrivant dans une extension abélienne cocentrale $k \to \mathcal{O}(H) \to A \to k\mathbb{Z}_m$ dans les cas suivants :

1. $H = \mathrm{PSL}_2(\mathbb{F}_p)$, avec $p$ premier impair et $m = 2$ ;
2. $H = A_n$, avec $n = 5$ ou $n \geq 8$ et $m = 2$ ;
3. $H = A_5$, pour tout $m \geq 1$ ;
4. $H = S_n$, avec $n \neq 6$ et $m = 2$ ;

5. $H = D_n$, le groupe diédral d'ordre $2n$ avec $n$ impair et $m \geq 1$ ;
6. $H = D_n$ avec $n$ pair, avec l'extension universelle précédente et $m = 2$ ;
7. $H = \mathbb{Z}_p \times \mathbb{Z}_p$ avec $p$ premier impair et $m$ une puissance d'un nombre premier tel que $m|(p-1)$.

Parmi ces exemples, il est intéressant de noter que celui avec $D_n$ et $n$ pair est certainement le plus complexe et ne découle pas d'un résultat général, bien que la structure de ce groupe ne soit certainement pas la plus riche.

La rédaction de ce manuscrit de thèse est basée sur l'article rédigé conjointement avec Julien Bichon "Some isomorphism results for graded twistings of function algebras on finite groups", arXiv : 2003.05172.

Il est organisé de la façon suivante :

Dans le second chapitre, nous donnerons le vocabulaire nécessaire ainsi que les notations associées, et nous présenterons des résultats préliminaires. En troisième partie, nous présenterons nos deux premiers résultats d'isomorphisme dans le cas des twists gradués d'algèbres de fonctions sur un groupe fini. Le quatrième chapitre étudiera le cadre plus général des extensions abéliennes cocentrales, dont les twists gradués font partie. Nous obtiendrons alors notre troisième résultat d'isomorphisme dans ce cadre. Enfin, pour terminer, le dernier chapitre sera un chapitre d'applications de ces résultats sur les exemples mentionnés précédemment.

**Notations et conventions.** Nous travaillerons sur un corps fixé $k$, que l'on suppose algébriquement fermé et de caractéristique zéro.

Nous supposerons le lecteur familier de la théorie des algèbres de Hopf, pour laquelle [25] est une référence classique, et nous adopterons les conventions usuelles : par exemple $\Delta$, $\varepsilon$ et $S$ représentent respectivement la co-multiplication, la co-unité et l'antipode pour une algèbre de Hopf. Nous utiliserons également les notations de Sweedler de manière standard.

Une convention un peu moins courante est que nous supposerons que les algèbres de Hopf ont un antipode bijective. Nous supposerons également une certaine familiarité du lecteur avec l'algèbre homologique de base, pour laquelle [12, 14] sont des références pratiques, et en particulier nous utiliserons [14] comme référence pour les calculs du multiplicateur de Schur. D'autres notations spécifiques seront introduites dans le texte.

# Chapitre 2

# Préliminaires

Cette partie contient plusieurs rappels sur les morphismes d'algèbres de Hopf, les graduations cocentrales, et la construction du twist gradué. Elle permet également d'introduire quelques résultats préliminaires pour la suite.

## 2.1 Morphismes d'algèbres de Hopf cocentraux, graduations cocentrales

Le concept de morphisme cocentral d'algèbres de Hopf est dual à la notion familière de morphisme central d'algèbres. La définition précise donnée dans [1] est rappelée ci-dessous. Une exposition détaillée de ces notions est donnée dans les références [6, 7].

**Définition 2.1.1.**

1. Un morphisme d'algèbres de Hopf $p : A \to B$ est dit *cocentral* si pour tout $a \in A$, on a $p(a_{(1)}) \otimes a_{(2)} = p(a_{(2)}) \otimes a_{(1)}$.
2. Un morphisme d'algèbres de Hopf $p : A \to B$ est dit *universel* si pour tout morphisme d'algèbres de Hopf cocentral $q : A \to C$, il existe un unique morphisme d'algèbres de Hopf $f : B \to C$ tel que $f \circ p = q$.
3. On dit qu'une algèbre de Hopf possède un *groupe graduateur universel* si il existe un morphisme d'algèbres de Hopf cocentral universel $p : A \to k\Gamma$ pour un certain groupe $\Gamma$. Ce groupe unique $\Gamma$ est appelé le groupe graduateur universel de $A$.

*Remarques* 2.1.2.

1. Si $p : A \to B$ est un morphisme d'algèbres de Hopf cocentral surjectif, alors $B$ est nécessairement cocommutative.
2. Étant donnée une algèbre de Hopf $A$, l'existence d'un morphisme d'algèbres de Hopf cocentral universel $A \to B$ est facilement montré comme suit : soit $X$, le sous-espace vectoriel de $A$ engendré par les éléments

$$\varphi(a_{(1)})a_{(2)} - \varphi(a_{(2)})a_{(1)},\ \varphi \in A^*,\ a \in A.$$

Il est facile de voir que $X$ est un co-idéal de $A$, et alors l'idéal $I$ engendré par $X$ est un idéal de Hopf de $A$. Le morphisme d'algèbres de Hopf quotient $p : A \to A/I$ est alors cocentral universel. L'unicité du morphisme d'algèbres de Hopf cocentral universel est triviale d'après la définition.

3. Si $G$ est un groupe algébrique linéaire, notons $\mathcal{O}(G)$ l'algèbre des fonctions coordonnées sur $G$. Si $H \subset G$ est un sous-groupe fermé, l'application de restriction $\mathcal{O}(G) \to \mathcal{O}(H)$ est cocentrale si et seulement si $H$ est central dans $G : H \subset Z(G)$, et l'application de restriction $\mathcal{O}(G) \to \mathcal{O}(Z(G))$ est cocentrale universelle.

4. Si une algèbre de Hopf $A$ est cosemisimple, il est facile de voir, en utilisant la décomposition de Peter-Weyl de $A$ (décomposition de $A$ en somme directe de sous-cogèbres de matrices), que $A$ possède un groupe graduateur universel.

Le lemme suivant sera utilisé de nombreuses fois dans la suite du texte.

**Lemme 2.1.3.** *Soient $A$, $B$ des algèbres de Hopf ayant le même groupe graduateur universel cyclique $\Gamma_0$ et supposons donnés deux morphismes d'algèbres de Hopf cocentraux et surjectifs $p : A \to k\Gamma$ et $q : B \to k\Gamma$ pour un certain groupe fini cyclique $\Gamma$, et un isomorphisme d'algèbres de Hopf $f : A \to B$. Alors il existe $u \in \mathrm{Aut}(\Gamma)$ tel que $u \circ p = q \circ f$.*

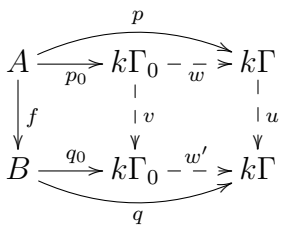
*Démonstration.*

Soient $p_0 : A \to k\Gamma_0$ et $q_0 : B \to k\Gamma_0$ les morphismes cocentraux universels d'algèbres de Hopf correspondants. Le morphisme d'algèbres de Hopf $q_0 \circ f : A \to k\Gamma_0$ est alors cocentral, donc il existe un unique morphisme de groupes $v : \Gamma_0 \to \Gamma_0$ tel que $v \circ p_0 = q_0 \circ f$.

Comme $q_0 \circ f$ est surjectif, le morphisme $v$ l'est aussi, et ainsi, puisque $\Gamma_0$ est fini, $v$ est un automorphisme.

Les morphismes d'algèbres de Hopf $p : A \to k\Gamma$ et $q : B \to k\Gamma$ sont cocentraux et surjectifs. Par universalité de $p_0$ et $q_0$, on obtient l'existence de deux morphismes de groupes surjectifs $w, w' : \Gamma_0 \to \Gamma$ tels que $w \circ p_0 = p$ et $w' \circ q_0 = q$.

Posons $N = \mathrm{Ker}(w)$ et $N' = \mathrm{Ker}(w')$. On a alors $|N| = \frac{|\Gamma_0|}{|\Gamma|} = |N'|$. L'unicité d'un sous-groupe d'ordre donné dans un groupe cyclique nous donne que $N = N' = v(N)$, et il existe ainsi un unique morphisme de groupes $u : \Gamma \to \Gamma$ tel que $u \circ w = w' \circ v$ :



On obtient que $u \circ p = u \circ w \circ p_0 = w' \circ v \circ p_0 = w' \circ q_0 \circ f = q \circ f$, comme souhaité, ce qui conclut la preuve. □

**Définition 2.1.4.** Soit $A$ un algèbre de Hopf et soit $\Gamma$ un groupe. Une *graduation cocentrale* de $A$ par $\Gamma$ est une décomposition en somme directe $A = \oplus_{g\in\Gamma} A_g$ telle que pour tout $g, h \in \Gamma$ on ait :

1. $A_g A_h \subset A_{gh}$ et $1 \in A_e$,
2. $\Delta(A_g) \subset A_g \otimes A_g$ et $S(A_g) \subset A_{g^{-1}}$.

Notons que les conditions $1 \in A_e$ et $S(A_g) \subset A_{g^{-1}}$ résultent des autres. Les graduations cocentrales par $\Gamma$ correspondent aux morphismes d'algèbres de Hopf cocentraux $p : A \to k\Gamma$. En effet, pour un morphisme d'algèbres de Hopf cocentral donné $p : A \to k\Gamma$, la graduation correspondante est définie par :

$$A_g = \{a \in A \mid a_{(1)} \otimes p(a_{(2)}) = a \otimes g = a_{(2)} \otimes p(a_{(1)})\}.$$

Occasionnellement, on notera l'ensemble $A_g$ par $A_{g,p}$ pour indiquer plus explicitement la dépendance sur $p$, dans les cas où il y a risque de confusion.

Inversement, si l'on se donne une graduation cocentrale par $\Gamma$, le morphisme d'algèbres de Hopf cocentral $p : A \to k\Gamma$ correspondant est défini par $p_{|A_g} = \varepsilon(-)g$, et il est surjectif si et seulement si $A_g \neq \{0\}$ pour tout $g \in \Gamma$. Nous passerons librement de la notion de morphisme d'algèbres de Hopf cocentral à celle de graduation cocentrale.

Comme le morphisme d'algèbres de Hopf cocentral correspondant est surjectif, les graduations cocentrales ont la propriété de graduation forte que $A_g A_h = A_{gh}$ pour tout $g, h \in \Gamma$ (voir par exemple la référence [5, proposition 2.2]).

Voici une application utile, utilisée plus tard dans la preuve du lemme 2.2.8.

**Lemme 2.1.5.** *Soit $p : A \to k\Gamma$ un morphisme d'algèbres de Hopf cocentral surjectif. Soient $g \in \Gamma$ et $y, z \in A$ tels que $xy = xz$ pour tout $x \in A_g$. Alors $y = z$.*

*Démonstration.*

Puisque $A_e = A_{g^{-1}} A_g$, il existe $x_1, \ldots, x_m \in A_{g^{-1}}$ et $y_1, \ldots, y_m \in A_g$ tels que $1 = \sum_{i=1}^m x_i y_i$. En utilisant notre hypothèse, on écrit alors :

$$y = 1.y = \sum_{i=1}^m x_i y_i y = \sum_{i=1}^m x_i y_i z = 1.z = z.$$

Cela achève la preuve. □

## 2.2 Actions cocentrales et twist gradué

La notion suivante est introduite dans la référence [4] sous le nom "d'action cocentrale invariante".

Dans ce manuscrit, pour simplifier la terminologie, on parlera simplement "d'action cocentrale".

**Définition 2.2.1.** Une *action cocentrale* d'un groupe $\Gamma$ sur une algèbre de Hopf $A$ est la donnée d'une paire $(p, \alpha)$ où $p : A \to k\Gamma$ est un morphisme d'algèbres de Hopf cocentral surjectif et $\alpha : \Gamma \to \mathrm{Aut}_{\mathrm{Hopf}}(A)$ est un morphisme de groupes, munis tous les deux de la condition de compatibilité $p \circ \alpha_g = p$ pour tout $g \in \Gamma$.

Selon le point de vue équivalent de la graduation, la condition de compatibilité correspond à $\alpha_g(A_h) = A_h$ pour tout $g, h \in \Gamma$.

**Définition 2.2.2.** Étant donnée une action cocentrale $(p, \alpha)$ d'un groupe $\Gamma$ sur une algèbre de Hopf $A$, le *twist gradué* $A^{p,\alpha}$ est l'algèbre de Hopf ayant $A$ comme cogèbre sous-jacente, et dont le produit et l'antipode sont définis par :

$$\forall a \in A_g, b \in A_h,\ a \cdot b = a\alpha_g(b), \qquad S(a) = \alpha_{g^{-1}}(S(a)).$$

La présente définition d'un twist gradué diffère de la définition originale de la référence [4], mais elle lui est équivalente (pour cela, voir [5, remarque 2.4], la structure d'algèbre sous-jacente est celle d'un twist dans le sens de la référence [30]).

**Lemme 2.2.3.** *Soit $q : A \to B$ le morphisme d'algèbres de Hopf cocentral universel et soit $(p, \alpha)$ une action cocentrale d'un groupe $\Gamma$ sur $A$. Alors $q : A^{p,\alpha} \to B$ est encore le morphisme d'algèbres de Hopf cocentral universel.*

*Démonstration.*

Rappelons que d'après la remarque 2.1.2, on peut supposer que $q$ est le morphisme quotient $A \to A/I$ où $I$ est l'idéal de $A$ engendré par $X$, le sous-espace vectoriel de $A$ engendré par les éléments $\varphi(a_{(1)})a_{(2)} - \varphi(a_{(2)})a_{(1)},\ \varphi \in A^*,\ a \in A$. Le sous-espace $X$ est également le sous-espace vectoriel de $A$ engendré par les éléments

$$\varphi(a_{(1)})a_{(2)} - \varphi(a_{(2)})a_{(1)},\ \varphi \in A^*,\ a \in A_g,\ g \in \Gamma.$$

Soit $I'$ l'idéal de $A^{p,\alpha}$ engendré par $X$. Le calcul suivant, pour $a \in A_g, b \in A_h, c \in A_r$,

$$\begin{aligned} a \cdot \Big(\varphi(b_{(1)})b_{(2)} - \varphi(b_{(2)})b_{(1)}\Big) \cdot c &= \varphi(b_{(1)})a\alpha_g(b_{(2)})\alpha_{gh}(c) - \varphi(b_{(2)})a\alpha_g(b_{(1)})\alpha_{gh}(c) \\ &= a\left(\varphi\alpha_{g^{-1}}(\alpha_g(b_{(1)}))\alpha_g(b_{(2)}) - \varphi\alpha_{g^{-1}}(\alpha_g(b_{(2)}))\alpha_g(b_{(1)})\right)\alpha_{gh}(c) \end{aligned}$$

montre que $I' \subset I$. De manière symétrique, puisque $ab = a \cdot \alpha_{g^{-1}}(b)$ pour $a \in A_g$ et $b \in A$, on a $I \subset I'$, et par conséquent $I = I'$.

De plus, le morphisme quotient $q' : A^{p,\alpha} \to A^{p,\alpha}/I'$, qui est cocentral universel, est égal à $q$, et on obtient donc le résultat annoncé. □

Puisque notre but principal est de comparer les différentes algèbres de Hopf obtenues via le twist gradué, une première chose à faire est de comparer les diverses actions cocentrales, et pour cela on introduit naturellement la notion suivante.

**Définition 2.2.4.** Deux actions cocentrales $(p, \alpha)$ et $(q, \beta)$ d'un groupe $\Gamma$ sur une algèbre de Hopf $A$ sont dites *équivalentes* si il existe $u \in \mathrm{Aut}(\Gamma)$ et $f \in \mathrm{Aut}_{\mathrm{Hopf}}(A)$ tels que :

$$u \circ p = q \circ f \text{ et } \forall g \in \Gamma, f \circ \alpha_g \circ f^{-1} = \beta_{u(g)}$$

**Lemme 2.2.5.** *Soient $(p, \alpha)$ et $(q, \beta)$ des actions cocentrales d'un groupe $\Gamma$ sur une algèbre de Hopf $A$. Si $(p, \alpha)$ et $(q, \beta)$ sont équivalentes, alors les algèbres de Hopf $A^{p,\alpha}$ et $A^{q,\beta}$ sont isomorphes.*

*Démonstration.*

Par équivalence de $(p, \alpha)$ et $(q, \beta)$, il existe $u \in \mathrm{Aut}(\Gamma)$ et $f \in \mathrm{Aut}_{\mathrm{Hopf}}(A)$ vérifiant :

$$u \circ p = q \circ f \text{ et } \forall g \in \Gamma, f \circ \alpha_g \circ f^{-1} = \beta_{u(g)}.$$

La condition $u \circ p = q \circ f$ assure que $f(A_g) = A_{u(g)}$ pour tout $g \in \Gamma$.
Ainsi pour $a \in A_g$ et $b \in A$, on a :

$$f(a \cdot b) = f(a\alpha_g(b)) = f(a)f(\alpha_g(b)) = f(a)\beta_{u(g)}(f(b)) = f(a) \cdot f(b).$$

Donc $f$ est un isomorphisme d'algèbres de Hopf de $A^{p,\alpha}$ vers $A^{q,\beta}$, et ainsi $A^{p,\alpha} \simeq A^{q,\beta}$. □

Introduisons également une notion d'équivalence faible pour ces actions cocentrales.

**Définition 2.2.6.** Deux actions cocentrales $(p, \alpha)$ et $(q, \beta)$ d'un groupe $\Gamma$ sur une algèbre de Hopf $A$ sont dites *faiblement équivalentes* si il existe $u \in \mathrm{Aut}(\Gamma)$ et un isomorphisme d'algèbres de Hopf $f : A_{e,p} \to A_{e,q}$ tels que :

$$\forall g \in \Gamma, f \circ (\alpha_g)_{|A_{e,p}} \circ f^{-1} = (\beta_{u(g)})_{|A_{e,q}}.$$

Bien sûr, des actions cocentrales équivalentes sont également faiblement équivalentes.

**Lemme 2.2.7.** *Deux actions cocentrales équivalentes $(p, \alpha)$ et $(q, \beta)$ d'un groupe $\Gamma$ sur une algèbre de Hopf $A$ sont faiblement équivalentes.*

*Démonstration.*

Par équivalence de $(p, \alpha)$ et $(q, \beta)$, il existe $u \in \mathrm{Aut}(\Gamma)$ et $f \in \mathrm{Aut}_{\mathrm{Hopf}}(A)$ vérifiant :

$$u \circ p = q \circ f \text{ et } \forall g \in \Gamma, f \circ \alpha_g \circ f^{-1} = \beta_{u(g)}.$$

Alors par le même raisonnement que précédemment, la condition $u \circ p = q \circ f$ donne $f(A_{g,p}) = A_{u(g),q}$, pour tout $g \in \Gamma$, et ainsi $f(A_{e,p}) = A_{e,q}$. Finalement, le morphisme $f_{|A_{e,p}}$ permet d'obtenir la condition de faible équivalence entre $(p, \alpha)$ et $(q, \beta)$, ce qui conclut la preuve. □

L'existence d'un isomorphisme d'algèbres de Hopf entre $A^{p,\alpha}$ et $A^{q,\beta}$ oblige-t-il les actions cocentrales $(p, \alpha)$ et $(q, \beta)$ a être faiblement équivalentes ? Ce n'est pas clair en général. Cependant, c'est vrai dans le cas particulier suivant.

**Lemme 2.2.8.** *Soit $A$ une algèbre de Hopf commutative, ayant un groupe graduateur universel cyclique fini, et soient $(p, \alpha)$, $(q, \beta)$ des actions cocentrales d'un groupe cyclique $\Gamma$ sur $A$. Si les algèbres de Hopf $A^{p,\alpha}$ et $A^{q,\beta}$ sont isomorphes, alors les actions cocentrales $(p, \alpha)$ et $(q, \beta)$ sont faiblement équivalentes.*

*Démonstration.*

Comme $A^{p,\alpha} \simeq A^{q,\beta}$, il existe $f : A^{p,\alpha} \to A^{q,\beta}$ un isomorphisme d'algèbres de Hopf. D'après le lemme 2.2.3, les conditions sont réunies pour appliquer le lemme 2.1.3. Ainsi, il existe $u \in \mathrm{Aut}(\Gamma)$ tel que $u \circ p = q \circ f$. On a alors $f(A_{g,p}) = A_{u(g),q}$ pour tout $g \in \Gamma$, et en particulier, $f(A_{e,p}) = A_{e,q}$.

Pour $a \in A_g$ et $b \in A_e$, on a :

$$f(a\alpha_g(b)) = f(a \cdot b) = f(a) \cdot f(b) = f(a)\beta_{u(g)}(f(b)).$$

Par commutativité de $A$, on a donc :

$$f(a\alpha_g(b)) = f(\alpha_g(b)a) = f(\alpha_g(b) \cdot a) = f(\alpha_g(b)) \cdot f(a) = f(\alpha_g(b))f(a) = f(a)f(\alpha_g(b)).$$

Ainsi $f(a)\beta_{u(g)}(f(b)) = f(a)f(\alpha_g(b))$ pour tout $a \in A_g$. D'après le lemme 2.1.5, on obtient alors :

$$\beta_{u(g)}(f(b)) = f(\alpha_g(b)), \text{ i.e. } f \circ \alpha_g \circ f^{-1} = \beta_{u(g)} \text{ sur } A_e.$$

Finalement, les actions $(p, \alpha)$ et $(q, \beta)$ sont faiblement équivalentes. □

## 2.3 Twists gradués d'algèbres de fonction

Dans cette partie, nous traduisons en termes de groupes les notions discutées dans la partie précédente. Plaçons nous dans le cas où $A = \mathcal{O}(G)$, l'algèbre des fonctions sur un groupe fini $G$ (ce qui bien sûr fonctionnerait également lorsque $G$ est un groupe algébrique, mais pour simplifier, on se restreindra au cas fini).

Les traductions sont assez évidentes, mais elles sont pratiques et induisent quelques notations supplémentaires. Comme d'habitude, si $\Gamma$ est un groupe, le groupe dual $\mathrm{Hom}(\Gamma, k^\times)$ est noté $\widehat{\Gamma}$.

Si $G$ est un groupe et $T \subset G$ est un sous-groupe, on note $\mathrm{Aut}_T(G)$ le groupe des automorphismes de $G$ qui préservent $T$, et $\mathrm{Aut}_T^\circ(G)$ le sous-groupe des automorphismes qui fixent chaque élément de $T$.

1. Une action cocentrale $(p, \alpha)$ d'un groupe fini $\Gamma$ sur $\mathcal{O}(G)$ correspond à une paire $(i, \alpha)$ où $i : \widehat{\Gamma} \to Z(G)$ est un morphisme de groupes injectif et $\alpha : \Gamma \to \mathrm{Aut}^\circ_{i(\widehat{\Gamma})}(G)$ est un morphisme de groupes. Nous considérerons à présent les actions cocentrales de $\Gamma$ sur $\mathcal{O}(G)$ comme des paires $(i, \alpha)$, appelées simplement actions cocentrales sur $G$, et on notera le twist gradué correspondant $\mathcal{O}(G)^{p,\alpha}$ plus simplement par $\mathcal{O}(G)^{i,\alpha}$.
2. Deux actions cocentrales $(i, \alpha)$ et $(j, \beta)$ sont équivalentes si il existe $u \in \mathrm{Aut}(\Gamma)$ et $f \in \mathrm{Aut}(G)$ tels que :

$$i \circ \widehat{u} = f \circ j \text{ et } \forall g \in \Gamma,\ f^{-1} \circ \alpha_g \circ f = \beta_{u(g)},\ \text{où } \widehat{u} = - \circ u.$$

3. Deux actions cocentrales $(i, \alpha)$ et $(j, \beta)$ sont faiblement équivalentes si il existe $u \in \mathrm{Aut}(\Gamma)$ et un isomorphisme $f : G/j(\widehat{\Gamma}) \to G/i(\widehat{\Gamma})$ tels que pour tout $g \in \Gamma$, $f^{-1} \circ \overline{\alpha}_g \circ f = \overline{\beta_{u(g)}}$, où $\overline{\alpha_g}$ et $\overline{\beta_{u(g)}}$ sont les automorphismes de $G/i(\widehat{\Gamma})$ et $G/j(\widehat{\Gamma})$ induits par $\alpha_g$ et $\beta_{u(g)}$ respectivement.

Supposons que le groupe fini $G$ possède un centre cyclique. Il y a alors une manière pratique de décrire les classes d'équivalence d'actions cocentrales de $\mathbb{Z}_m$ sur $G$ que nous décrivons maintenant.

Pour $m$ un diviseur de $|Z(G)|$, soit $T_m$ l'unique sous-groupe d'ordre $m$ de $Z(G)$, et soit $\mathbb{X}_m(G)$ l'ensemble des éléments $\alpha_0 \in \mathrm{Aut}^\circ_{T_m}(G)$ tels que $\alpha_0^m = \mathrm{id}_G$, modulo la relation d'équivalence :

$$\alpha_0 \sim \beta_0 \iff \exists f \in \mathrm{Aut}_{T_m}(G) \text{ et } l \text{ premier avec } m \text{ tels que } f^{-1} \circ \alpha_0 \circ f = \beta_0^l \text{ et } f_{|T_m} = (-)^l.$$

Pour $\alpha_0 \in \mathrm{Aut}^\circ_{T_m}(G)$, on note $\ddot{\alpha_0}$ sa classe d'équivalence dans $\mathbb{X}_m(G)$. On notera aussi $\mathbb{X}_m^\bullet(G)$ l'ensemble des classes d'équivalence $\ddot{\alpha_0}$ tels que $\alpha_0$ n'induise pas l'identité sur $G/T_m$.

**Lemme 2.3.1.** *Si $G$ est un groupe fini avec un centre cyclique et $m$ est un diviseur de $|Z(G)|$, on a une bijection $\mathbb{X}_m(G) \simeq \{$classes d'équivalence d'actions cocentrales de $\mathbb{Z}_m$ sur $G\}$.*

*Démonstration.*

Fixons un générateur $g$ de $\mathbb{Z}_m$, ainsi qu'un morphisme de groupes injectif $i : \widehat{\mathbb{Z}_m} \to Z(G)$ tel que $T_m = i(\widehat{\mathbb{Z}_m})$. À tout élément $\alpha_0 \in \mathrm{Aut}^\circ_{T_m}(G)$, on associe l'action cocentrale $(i, \alpha)$ de $\mathbb{Z}_m$ sur $G$ telle que $\alpha_g = \alpha_0$.

Définissons $\Psi : \mathbb{X}_m(G) \longrightarrow \{\text{classes d'équivalence d'actions cocentrales de } \mathbb{Z}_m \text{ sur } G\}$ qui envoie $\ddot{\alpha_0}$ sur $\mathrm{cl}((i,\alpha))$, où $i$ et $\alpha$ sont définis au dessus.

Montrons que $\Psi$ réalise la bijection.

Soient $\ddot{\alpha_0}, \ddot{\beta}_0 \in \mathbb{X}_m(G)$ tels que $\Psi(\ddot{\alpha_0}) = \Psi(\ddot{\beta}_0)$ i.e. $\mathrm{cl}((i,\alpha)) = \mathrm{cl}((i,\beta))$. Ainsi, les actions $(i,\alpha)$ et $(i,\beta)$ sont équivalentes. Donc il existe $u \in \mathrm{Aut}(\mathbb{Z}_m)$ et $f \in \mathrm{Aut}(G)$ tels que :

$$i \circ \widehat{u} = f \circ i \quad \text{et} \quad f^{-1} \circ \alpha_g \circ f = \beta_{u(g)} \quad \text{où} \quad \widehat{u} = - \circ u.$$

Comme $\mathbb{Z}_m$ est cyclique engendré par $g$, il existe $l$ premier avec $m$ tel que $u(h) = h^l$ pour tout $h \in \mathbb{Z}_m$.

Ainsi, $\beta_{u(g)} = \beta_{g^l} = \beta_0^l$ donc $f^{-1} \circ \alpha_0 \circ f = \beta_0^l$.

De plus, pour $\varphi \in \widehat{\mathbb{Z}_m}$ et pour tout $h \in \mathbb{Z}_m$, on a :

$$f \circ i(\varphi(h)) = i \circ \widehat{u}(\varphi(h)) = i \circ \varphi \circ u(h) = i \circ \varphi(h^l) = i(\varphi(h)^l) = i(\varphi(h))^l.$$

Donc $f_{|T_m} = f_{|i(\widehat{\mathbb{Z}_m})} = (-)^l$.

Les conditions sont donc remplies : $\alpha_0 \sim \beta_0$ i.e. $\ddot{\alpha_0} = \ddot{\beta}_0$. D'où l'injectivité de $\Psi$.

Pour la surjectivité : soit $(j,\beta)$ une action cocentrale de $\mathbb{Z}_m$ sur $G$. On voit facilement que les actions $(j,\beta)$ et $(i,\beta^{l'})$ avec $l$ premier avec $m$ et $ll' \equiv 1[m]$, sont équivalentes.

Il suffit de poser $\widehat{u} := i^{-1} \circ j$ et $u = (-)^l$ où $l$ est premier à $m$. Ainsi en prenant $f = \mathrm{id}$, on a $\beta^{l'}_{u(g)} = \beta^{l'}_{g^l} = \beta_{g^{ll'}} = \beta_g$ donc l'équivalence est réalisée.

Donc $\mathrm{cl}((j,\beta)) = \mathrm{cl}((i,\beta^{l'})) = \Psi(\ddot{\beta}_0)$, où $\beta_0$ est défini par $\beta_g^{l'} = \beta_0$. Donc $\mathrm{cl}((j,\beta))$ possède bien un antécédent par $\Psi$. D'où la surjectivité.

Finalement $\Psi$ est bijective donc :

$$\mathbb{X}_m(G) \simeq \{\text{classes d'équivalence d'actions cocentrales de } \mathbb{Z}_m \text{ sur } G\}.$$

□

## 2.4 Notions requises de théorie de groupes

Cette dernière partie introduit quelques préliminaires de théorie des groupes. Comme à l'habitude, si $G$ est un groupe et $M$ est un $G$-comodule, le second groupe de cohomologie de $G$ à coefficients dans $M$ est noté $H^2(G, M)$. Nous considérerons principalement des $G$-modules triviaux (la seule exception sera dans la preuve du lemme 4.1.3). Si $\tau \in Z^2(G, M)$ est un 2-cocycle (normalisé), sa classe de cohomologie dans $H^2(G, M)$ est notée $[\tau]$, et si $\mu : G \to M$ est une application telle que $\mu(1) = 1$, alors le 2-cobord associé est noté $\partial(\mu)$.

Le premier lemme est probablement bien connu. Nous fournirons néanmoins les détails de la preuve pour une utilisation future.

**Lemme 2.4.1.** *Soit $T$ un sous-groupe central d'un groupe $G$. La suite de groupes suivante est exacte :*

$$1 \to \mathrm{Hom}(G/T, T) \to \mathrm{Aut}_T(G) \to \mathrm{Aut}(G/T) \times \mathrm{Aut}(T)$$

*et l'application de droite est surjective lorsque $|H^2(G/T, T)| \leq 2$ (ou plus généralement lorsque les actions naturelles de $\mathrm{Aut}(G/T)$ et $\mathrm{Aut}(T)$ sur $H^2(G/T, T)$ sont triviales).*

*Démonstration.*

Tout élément de $\mathrm{Aut}_T(G)$ se restreint en un automorphisme de $T$ et induit un automorphisme de $G/T$, ainsi on obtient naturellement le morphisme de groupes de droite.

Soit $\chi \in \mathrm{Hom}(G/T, T)$, on définit l'automorphisme $\tilde{\chi}$ de $G$ par $\tilde{\chi}(x) = x\chi(\pi(x))$, où $\pi : G \to G/T$ est la surjection canonique. L'automorphisme $\tilde{\chi}$ préserve bien $T$ par construction. Ceci définit donc un morphisme de groupes de $\mathrm{Hom}(G/T, T)$ vers $\mathrm{Aut}_T(G)$ (morphisme de gauche), et le morphisme $\chi \longmapsto \tilde{\chi}$ est clairement injectif. Par ailleurs, on voit facilement que son image coïncide avec le noyau de l'application de droite. On obtient donc une suite exacte de morphismes de groupes.

A présent, posons $H = G/T$. D'après la description standard des extensions centrales de groupes, on peut librement supposer que $G = H \times_\tau T$ où $\tau \in Z^2(H, T)$, et le produit de $G$ est défini par :

$$\forall x, y \in H,\ \forall r, s \in T,\ (x, r) \cdot (y, s) = (xy, \tau(x, y)rs).$$

Il est facile de vérifier qu'un élément $\alpha \in \mathrm{Aut}_T(G)$ est défini par $\alpha(x, t) = (\theta(x), \mu(x)u(t))$, où $(\theta, \mu, u)$ est un triplet avec $\theta \in \mathrm{Aut}(H)$, $u \in \mathrm{Aut}(T)$, et $\mu : H \to T$ satisfaisant :

$$\forall x, y \in H,\ u(\tau(x, y))\mu(xy) = \mu(x)\mu(y)\tau(\theta(x), \theta(y)). \quad (\star)$$

Avec cette identification de $G$, la loi de composition de $\mathrm{Aut}_T(G)$ est donnée par :

$$(\theta, \mu, u)(\theta', \mu', u') = (\theta \circ \theta', \mu \circ \theta' \cdot u \circ \mu', u \circ u').$$

L'application $\mathrm{Aut}_T(G) \to \mathrm{Aut}(H) \times \mathrm{Aut}(T)$ provenant de la suite exacte du lemme, correspond alors à la projection sur la première et la troisième composante, et les éléments du noyaux sont exactement ceux de la forme $(\mathrm{id}_H, \mu, \mathrm{id}_T)$ où $\mu : H \to T$ est un morphisme de groupes.

Supposons maintenant que les actions naturelles de $\mathrm{Aut}(H)$ et $\mathrm{Aut}(T)$ sur $H^2(H,T)$ par automorphisme de groupes soient triviales, c'est-à-dire qu'elles laissent stables tous les éléments (c'est évidemment le cas lorsque $|H^2(H,T)| \leq 2$).

Soit $(\theta, u) \in \mathrm{Aut}(H) \times \mathrm{Aut}(T)$. L'action de $\mathrm{Aut}(T)$ sur $H^2(H,T)$ étant triviale, on a $[u \circ \tau] = [\tau]$. De même, l'action de $\mathrm{Aut}(H)$ sur $H^2(H,T)$ étant triviale, on a $[\tau \circ (\theta \times \theta)] = [\tau]$. Donc les cocycles $u \circ \tau$ et $\tau \circ (\theta \times \theta)$ sont cohomologues, et donc il existe $\mu : H \to T$ tel que $u \circ \tau = \partial(\mu)\tau \circ (\theta \times \theta)$, ce qui est exactement la condition $(\star)$ qui permet à $(\theta, \mu, u)$ de définir un élément de $\mathrm{Aut}_T(G)$, et ainsi l'application à droite de la suite exacte est surjective. □

Notre second lemme sera utilisé à la fin du chapitre 4.

**Lemme 2.4.2.** *Soient $H$ un groupe fini, $T$ un groupe cyclique d'ordre $m$, et $\tau \in Z^2(H,T)$. Considérons le groupe $G = H \times_\tau T$. Soient $\alpha, \beta \in \mathrm{Aut}_T^\circ(G)$ (i.e. $\alpha_{|T} = \mathrm{id}_T = \beta_{|T}$), et soient $\overline{\alpha}$, $\overline{\beta}$ les automorphismes induits sur $H$. Supposons que $\mathrm{Hom}(H,T) = \{1\}$ et qu'il existe $\theta \in \mathrm{Aut}(H)$ et $l$ premier avec $m$ tels que :*

$$\theta \circ \overline{\alpha} \circ \theta^{-1} = \overline{\beta}^l \text{ et } [\tau]^l = [\tau \circ (\theta \times \theta)] \in H^2(H,T).$$

*Alors il existe $f \in \mathrm{Aut}_T(G)$ tel que :*

$$f \circ \alpha \circ f^{-1} = \beta^l \text{ et } f_{|T} = (-)^l.$$

*Démonstration.*

Comme énoncé dans la preuve du lemme précédent, rappelons que les éléments de $\mathrm{Aut}_T(G)$ sont représentés par des triplets $(\theta, \mu, u)$ avec $\theta \in \mathrm{Aut}(H)$, $u \in \mathrm{Aut}(T)$ et $\mu : H \to T$ tels que $u \circ \tau = \partial(\mu)\tau \circ (\theta \times \theta)$, avec $(\theta, \mu, u)(x,t) = (\theta(x), \mu(x)u(t))$, pour $(x,t) \in H \times T$.

Par hypothèse, avec les notations que l'on vient de rappeler, on peut écrire $\alpha = (\overline{\alpha}, \phi, \mathrm{id}_T)$ et $\beta = (\overline{\beta}, \gamma, \mathrm{id}_T)$.

Soit $u$ l'automorphisme de $T$ défini par $u = (-)^l$. L'hypothèse $[\tau]^l = [\tau \circ (\theta \times \theta)]$ revient donc à $[u \circ \tau] = [\tau \circ (\theta \times \theta)]$. Par conséquent, il existe $\mu : H \to T$ tel que $u \circ \tau = \partial(\mu)\tau \circ (\theta \times \theta)$ et donc l'existence de ce $\mu$ permet à $\theta$ de s'étendre à un automorphisme $f = (\theta, \mu, u)$ de $\mathrm{Aut}_T(G)$.

On a :

$$\begin{aligned} f \circ \alpha \circ f^{-1} &= (\theta, \mu, u)(\overline{\alpha}, \phi, \mathrm{id}_T)(\theta, \mu, u)^{-1} \\ &= (\theta \circ \overline{\alpha}, \mu \circ \overline{\alpha} \cdot u \circ \phi, u)(\theta^{-1}, u^{-1} \circ ((\mu \circ \theta^{-1})^{-1}), u^{-1}) \\ &= (\theta \circ \overline{\alpha} \circ \theta^{-1}, \chi, \mathrm{id}_T) \\ &= (\overline{\beta}^l, \chi, \mathrm{id}_T) \end{aligned}$$

pour une application $\chi : H \to T$.

Ainsi, $f \circ \alpha \circ f^{-1}$ et $\beta^l$ possèdent la même image par le morphisme de groupes à droite de la suite exacte du lemme précédent, et l'hypothèse $\mathrm{Hom}(H, T) = \{1\}$ implique alors par injectivité que $f \circ \alpha \circ f^{-1} = \beta^l$ dans $\mathrm{Aut}_T(G)$. On a de plus $f_{|T} = u = (-)^l$, ce qui achève la preuve. □

Pour terminer cette partie, on rappelle un dernier lemme, qui sera lui aussi utile à la fin du chapitre 4. Il est bien connu que les automorphismes intérieurs agissent trivialement sur le second groupe de cohomologie d'un groupe. Le lemme suivant écrit ce fait précisément. La démonstration est une vérification simple, mais elle peut aussi s'obtenir facilement à partir des considérations du lemme 2.4.1.

**Lemme 2.4.3.** *Soient $H$ un groupe, $x \in H$, et $\tau \in Z^2(H, k^\times)$. Alors on a :*

$$\tau = \partial(\mu_x) \cdot \tau \circ (\mathrm{ad}(x) \times \mathrm{ad}(x)),$$

*où $\mu_x$ est définie par $\mu_x(y) = \tau(xy, x^{-1})\tau(x, y)\tau(x, x^{-1})^{-1}$ pour tout $y \in H$.*

*Démonstration.*

On rappelle la propriété vérifiée par $\tau$, qui sera utilisée à plusieurs reprises dans la démonstration : $\tau(a, bc)\tau(b, c) = \tau(a, b)\tau(ab, c)$ pour tout $a, b, c \in H$.

Soient $y, z \in H$. On a :

$$\begin{aligned}
\partial(\mu_x) \cdot \tau \circ (\mathrm{ad}(x) \times \mathrm{ad}(x))(y,z) &= \mu_x(y)\mu_x(z)\mu_x(yz)^{-1}\tau(xyx^{-1}, xzx^{-1}) \\
&= \tau(xy, x^{-1})\tau(x,y)\tau(x,x^{-1})^{-1}\tau(xz,x^{-1})\tau(x,z) \\
&\quad \tau(x,x^{-1})^{-1}\tau(xyz,x^{-1})^{-1}\tau(x,yz)^{-1}\tau(x,x^{-1})\tau(xyx^{-1},xzx^{-1}) \\
&= \tau(xy,x^{-1})\tau(x,y)\tau(x,x^{-1})^{-1}\tau(x,z) \\
&\quad \tau(xyz,x^{-1})^{-1}\tau(x,yz)^{-1}\tau(xyx^{-1},xz)\tau(xyx^{-1}xz,x^{-1}) \\
&= \tau(xy,x^{-1})\tau(x,y)\tau(x,x^{-1})^{-1}\tau(x,yz)^{-1}\tau(xyx^{-1},x)\tau(xy,z) \\
&= \tau(xy,x^{-1})\tau(x,y)\tau(x,x^{-1})^{-1}\tau(x,yz)^{-1}\tau(xy,1)\tau(x^{-1},x)\tau(xy,x^{-1})^{-1} \\
&= \tau(x,y)\tau(x,x^{-1})^{-1}\tau(x,yz)^{-1}\tau(xy,z)\tau(x^{-1},x) \\
&= \tau(x,y)\tau(x,x^{-1})^{-1}\tau(x,yz)^{-1}\tau(x^{-1},x)\tau(x,yz)\tau(y,z)\tau(x,y)^{-1} \\
&= \tau(x,x^{-1})^{-1}\tau(x^{-1},x)\tau(y,z).
\end{aligned}$$

Or en appliquant la propriété de $\tau$ pour $a = x, b = x$ et $c = x^{-1}$ on obtient :

$$\tau(x,x^{-1}) = \tau(x^{-1},x).$$

Donc $\partial(\mu_x) \cdot \tau \circ (\mathrm{ad}(x) \times \mathrm{ad}(x)) = \tau$, ce qui conclut la preuve. □

# Chapitre 3

# Premiers résultats

Nous sommes à présent prêts à énoncer et démontrer notre premier résultat d'isomorphisme pour les twists gradués d'algèbres de fonctions sur un groupe fini.

**Théorème 3.0.1.** *Soient $G$ un groupe fini ayant un centre cyclique, et $(i,\alpha)$ et $(j,\beta)$ des actions cocentrales d'un groupe cyclique $\Gamma$ sur $G$. Posons $H = G/i(\widehat{\Gamma}) = G/j(\widehat{\Gamma})$. Supposons que $|H^2(H,\widehat{\Gamma})| \leq 2$ (ou plus généralement que les actions naturelles de $\mathrm{Aut}(H)$ et $\mathrm{Aut}(\widehat{\Gamma})$ sur $H^2(H,\widehat{\Gamma})$ sont triviales) et que $\mathrm{Hom}(H,\widehat{\Gamma}) = \{1\}$. Alors les assertions suivantes sont équivalentes :*

1. *les algèbres de Hopf $\mathcal{O}(G)^{i,\alpha}$ et $\mathcal{O}(G)^{j,\beta}$ sont isomorphes ;*
2. *les actions cocentrales $(i,\alpha)$ et $(j,\beta)$ sont équivalentes ;*
3. *les actions cocentrales $(i,\alpha)$ et $(j,\beta)$ sont faiblement équivalentes.*

*Démonstration.*

Notons tout d'abord que comme $Z(G)$ est cyclique, il possède un unique sous-groupe d'ordre fixé. Ainsi, $i(\widehat{\Gamma})$ et $j(\widehat{\Gamma})$ étant deux sous-groupes de $Z(G)$ de même ordre, ils sont égaux : $i(\widehat{\Gamma}) = j(\widehat{\Gamma})$.

L'implication (1) $\Rightarrow$ (3) est donnée par le lemme 2.2.8. De même, l'implication (2) $\Rightarrow$ (1) découle du lemme 2.2.5.

Ainsi, il reste à prouver l'implication (3) $\Rightarrow$ (2) pour conclure la preuve.

Fixons un générateur $g \in \Gamma$. D'après les notations du paragraphe 2.3, comme les actions cocentrales $(i,\alpha)$ et $(j,\beta)$ sont supposées faiblement équivalentes, il existe $u \in \mathrm{Aut}(\Gamma)$ et $f \in \mathrm{Aut}(H)$ tels que $f^{-1} \circ \overline{\alpha_g} \circ f = \overline{\beta_{u(g)}}$.

L'hypothèse faite sur $H^2(H,\widehat{\Gamma})$ permet, grâce au lemme 2.4.1, d'avoir l'existence par surjectivité de $f_0 \in \mathrm{Aut}_{i(\widehat{\Gamma})}(G)$ tel que :

$$\overline{f_0} = f \text{ et } f_{0|i(\widehat{\Gamma})} = i \circ \widehat{u} \circ j^{-1}, \text{ } i.e. \text{ } f_0 \circ j = i \circ \widehat{u}.$$

On rappelle que l'application $f \mapsto \overline{f}$ est le morphisme de groupes $\mathrm{Aut}_{i(\widehat{\Gamma})}(G) \to \mathrm{Aut}(H)$ issu du lemme 2.4.1.

Ainsi on a $\overline{f_0^{-1} \circ \alpha_g \circ f_0} = \overline{\beta_{u(g)}}$ et $(f_0^{-1} \circ \alpha_g \circ f_0)_{|i(\widehat{\Gamma})} = \mathrm{id} = (\beta_{u(g)})_{|i(\widehat{\Gamma})}$ (car rappelons que $\alpha_g$ et $\beta_{u(g)}$ sont dans $\mathrm{Aut}^{\circ}_{i(\widehat{\Gamma})}(G)$ et donc fixent les éléments de $i(\widehat{\Gamma})$).

La condition $\mathrm{Hom}(H, \widehat{\Gamma}) = \{1\}$ et le lemme 2.4.1 assurent enfin par injectivité que $f_0^{-1} \circ \alpha_g \circ f_0 = \beta_{u(g)}$, et on peut conclure que les actions cocentrales $(i, \alpha)$ et $(j, \beta)$ sont équivalentes. □

*Exemple* 3.0.2. Soit $p \geq 3$ un nombre premier. Il y a exactement deux twists gradués non triviaux non isomorphes de $\mathcal{O}(\mathrm{SL}_2(\mathbb{F}_p))$. Les détails seront donnés dans le chapitre 5.

Le théorème précédent a des conséquences intéressantes lorsque $\Gamma = \mathbb{Z}_2$.

**Théorème 3.0.3.** *Soient $G$ un groupe fini ayant un centre cyclique, et $(i, \alpha)$ et $(j, \beta)$ des actions cocentrales de $\mathbb{Z}_2$ sur $G$. Posons $H = G/i(\widehat{\mathbb{Z}_2}) = G/j(\widehat{\mathbb{Z}_2})$. Supposons que $H^2(H, k^\times)$ est cyclique et que $\mathrm{Hom}(H, \mathbb{Z}_2) = \{1\}$. Alors les assertions suivantes sont équivalentes :*

1. *les algèbres de Hopf $\mathcal{O}(G)^{i,\alpha}$ et $\mathcal{O}(G)^{j,\beta}$ sont isomorphes ;*
2. *les actions cocentrales $(i, \alpha)$ et $(j, \beta)$ sont équivalentes ;*
3. *les actions cocentrales $(i, \alpha)$ et $(j, \beta)$ sont faiblement équivalentes.*

*Démonstration.*

Le théorème des coefficients universels nous donne la suite exacte suivante :

$$0 \to \mathrm{Ext}^1(H_1(H, \mathbb{Z}), \mathbb{Z}_2) \to H^2(H, \mathbb{Z}_2) \to \mathrm{Hom}(H_2(H, \mathbb{Z}), \mathbb{Z}_2) \to 0$$

L'hypothèse $\mathrm{Hom}(H, \mathbb{Z}_2) = \{1\}$ implique que $\widehat{H} \simeq H_1(H, \mathbb{Z})$ est d'ordre impair donc le groupe de gauche est trivial. Ainsi, $H^2(H, \mathbb{Z}_2) \simeq \mathrm{Hom}(H_2(H, \mathbb{Z}), \mathbb{Z}_2)$.

De plus, $H_2(H, \mathbb{Z}) \simeq H^2(H, k^\times)$ (toujours d'après le théorème des coefficients universels), comme $H^2(H, k^\times)$ est cyclique, on a alors $|\mathrm{Hom}(H_2(H, \mathbb{Z}), \mathbb{Z}_2)| \leq 2$ et donc $|H^2(H, \mathbb{Z}_2)| \leq 2$.

A présent, on peut appliquer le théorème 3.0.1 et le résultat suit. □

*Remarque* 3.0.4. Il est naturel de se demander si le théorème 3.0.1 s'applique de manière pertinente en dehors du cas $m = 2$.

Il s'applique au moins à l'exemple $G = H \times \mathbb{Z}_m$ où $H$ est un groupe avec $\widehat{H} = \{1\}$ et $|H^2(H, \mathbb{Z}_m)| \leq 2$, et si $H^2(H, \mathbb{Z}_m) \simeq \mathbb{Z}_2$ (ce qui, par le théorème des coefficients universels, arrive si $H^2(H, k^\times) \simeq \mathbb{Z}_2$ et $m$ est pair) au groupe $G$ obtenu à partir de l'extension centrale non scindée $1 \to \mathbb{Z}_m \to G \to H \to 1$ correspondant à la classe de cohomologie non triviale.

# Chapitre 4

# Extensions abéliennes cocentrales d'algèbres de Hopf

Pour approfondir le théorème 3.0.1, il sera pratique de travailler dans le cadre plus général des extensions abéliennes cocentrales. Comme déjà mentionné dans l'introduction, c'est un cadre fréquemment étudié, et bien compris, comme le montrent les références [1, 23, 21, 26, 16, 20] (même dans des situations plus générales, abandonnant l'hypothèse de cocentralité). Nous proposons de détailler la structure des algèbres de Hopf s'insérant dans des extensions cocentrales abéliennes pour deux raisons : à la fois par soucis d'exhaustivité et d'introduction des notations appropriées, et aussi parce que nous pensons que certaines de nos formulations présentent un certain intérêt.

## 4.1 Généralités

Rappelons d'abord le concept et la structure des algèbres de Hopf s'insérant dans une extension cocentrale abélienne.

La référence [1] propose une notion générale de suite exacte d'algèbres de Hopf, mais ici, nous n'auront besoin que de celles qui sont cocentrales.

**Définition 4.1.1.** Une suite de morphismes d'algèbres de Hopf

$$k \to B \xrightarrow{i} A \xrightarrow{p} L \to k$$

est dite exacte et cocentrale si $i$ est injectif, $p$ est surjectif et cocentral, $p \circ i = \varepsilon(-)1$ et $i(B) = A^{\mathrm{cop}} = \{a \in A : (\mathrm{id} \otimes p) \circ \Delta(a) = a \otimes 1.\}$. Lorsque $B$ est commutative, une suite exacte cocentrale comme ci-dessus est appelée *extension abélienne cocentrale*.

*Exemple* 4.1.2. Soit $(i, \alpha)$ une action cocentrale d'un groupe $\Gamma$ sur un groupe algébrique linéaire $G$. Alors

$$k \to \mathcal{O}(G/i(\widehat{\Gamma})) \to \mathcal{O}(G) \to k\Gamma \to k$$

est une extension abélienne cocentrale, ainsi que

$$k \to \mathcal{O}(G/i(\widehat{\Gamma})) \to \mathcal{O}(G)^{i,\alpha} \to k\Gamma \to k.$$

Par conséquent, les twists gradués d'algèbres de fonctions s'insèrent dans des extensions abéliennes cocentrales appropriées.

À présent, on se restreint aux algèbres de Hopf de dimension finie. Dans ce cas, les extensions abéliennes cocentrales sont de la forme

$$k \to \mathcal{O}(H) \to A \to k\Gamma \to k$$

avec $H, \Gamma$ des groupes finis. Il y a un moyen général de décrire les algèbres de Hopf $A$ s'insérant dans une telle extension abélienne cocentrale utilisant diverses actions et cocycles (voir les références [1, 23]). Puisque nous considérons uniquement le cas où $\Gamma$ est cyclique, il y a une description simple, inspirée de la référence [21], que nous allons donner maintenant. Commençons par un lemme.

**Lemme 4.1.3.** *Soient $H$ un groupe fini, $\theta \in \mathrm{Aut}(H)$ avec $\theta^m = \mathrm{id}_H$ pour un certain $m \geq 1$, et $a : H \to k^\times$. Considérons l'algèbre $A_m(H, \theta, a)$ définie par le quotient du produit libre d'algèbres $\mathcal{O}(H) * k[g]$ munie des relations :*

$$g^m = a, \qquad ge_x = e_{\theta(x)}g, \forall x \in H.$$

*Alors l'ensemble $\{e_x g^i,\ x \in H,\ 0 \leq i \leq m-1\}$ engendre linéairement $A_m(H, \theta, a)$, et est une base si et seulement si $a \circ \theta = a$.*

*Démonstration.*

On voit facilement que l'ensemble $\{e_x g^i,\ x \in H,\ 0 \leq i \leq m-1\}$ engendre linéairement $A_m(H, \theta, a)$ grâce aux relations définies ci-dessus.

Par ailleurs, si $\phi \in \mathcal{O}(H)$, les relations donnent :

$$g\phi = g \sum_{x \in H} \phi(x)e_x = \sum_{x \in H} \phi(x)ge_x = \sum_{x \in H} \phi(x)e_{\theta(x)}g = \sum_{y \in H} \phi(\theta^{-1}(y))e_y g = (\phi \circ \theta^{-1})g.$$

Puisque $a = g^m$, $a$ commute avec $g$. Ainsi, $ag = ga = (a \circ \theta^{-1})g$ c'est-à-dire :

$$\sum_{x \in H} a(x)e_x g = \sum_{x \in H} a(\theta^{-1}(x))e_x g.$$

Donc par linéaire indépendance, $\forall x \in H$, $a(x) = a \circ \theta^{-1}(x)$, i.e. $a \circ \theta = a$.

Pour montrer l'implication réciproque, rappelons une construction générale. Soit $R$ une algèbre commutative, munie d'une action d'un groupe $\Gamma$, $\alpha : \Gamma \to \mathrm{Aut}(R)$, et soit un 2-cocycle $\sigma : \Gamma \times \Gamma \to R^\times$ défini à partir de cette action :

$$\alpha_r(\sigma(s,t))\sigma(r,st) = \sigma(rs,t)\sigma(s,t),\ \forall r,s,t \in \Gamma.$$

Le produit croisé d'algèbres $R\#_\sigma k\Gamma$ est défini comme étant l'algèbre ayant $R \otimes k\Gamma$ comme espace vectoriel sous-jacent, dont le produit est donné par :

$$x\#r \cdot y\#s = x\alpha_r(y)\sigma(r,s)\#rs.$$

Supposons de plus que $\Gamma = \mathbb{Z}_m = \langle g \rangle$ est cyclique. Considérons un élément $a \in R^\times$ étant $\mathbb{Z}_m$-invariant, et définissons l'algèbre $A$ comme le quotient du produit libre $R * k[X]$ par les relations $Xb = \alpha_g(b)X$ et $X^m = a$. Comme $a$ est invariant sous l'action de $\mathbb{Z}_m$, la description classique du second groupe de cohomologie d'un groupe cyclique montre qu'il existe un 2-cocycle $\sigma : \mathbb{Z}_m \times \mathbb{Z}_m \to R^\times$ tel que $\sigma(g,g)\cdots\sigma(g,g^{m-1}) = a$. Ceci provient de la surjectivité du morphisme :

$$\begin{aligned} Z^2(\mathbb{Z}_m, R^\times) &\longrightarrow (R^\times)^{\mathbb{Z}_m} \\ \sigma &\longmapsto \sigma(g,g)\sigma(g,g^2)...\sigma(g,g^{m-1}), \end{aligned}$$

où $(R^\times)^{\mathbb{Z}_m}$ désigne les invariants de $R^\times$ sous l'action de $\mathbb{Z}_m$.

On obtient alors un morphisme d'algèbres

$$\begin{aligned} A &\longrightarrow R\#_\sigma k\mathbb{Z}_m \\ b \in R,\ X &\longmapsto b\#1,\ 1\#g. \end{aligned}$$

En appliquant cela à $R = \mathcal{O}(H)$, l'action de $\mathbb{Z}_m$ sur $R$ induit par $\theta$ et l'hypothèse que $a$ est invariant ($a \circ \theta = a$), nous donnent que l'ensemble $\{e_x g^i,\ x \in H,\ 0 \leq i \leq m-1\}$ est linéairement indépendant, puisque son image $\{1\#g,\ e_x\#1,\ g \in \Gamma,\ x \in H\}$ est libre dans le produit croisé d'algèbres $\mathcal{O}(H)\#_\sigma k\mathbb{Z}_m$. □

**Définition 4.1.4.** Soit $m \geq 1$. Un *m-datum* est un quadruplet $(H, \theta, a, \tau)$ tel que $H$ est un groupe fini, $\theta \in \mathrm{Aut}(H)$ est un automorphisme tel que $\theta^m = \mathrm{id}_H$, $a : H \to k^\times$ est une application telle que $a \circ \theta = a$ et $a(1) = 1$, et $\tau : H \times H \to k^\times$ est un 2-cocycle tel que pour tout $x, y \in H$

$$\left(\prod_{i=0}^{m-1} \tau(\theta^i(x), \theta^i(y))\right) a(x)a(y) = a(xy).$$

À présent, montrons que les $m$-data définis ci-dessus, produisent des algèbres de Hopf s'insérant dans des extensions abéliennes cocentrales, et que de telles algèbres ne se rencontrent que dans ce cas de figure.

**Proposition 4.1.5.** *Soit $(H, \theta, a, \tau)$ un m-datum, et considérons l'algèbre $A_m(H, \theta, a)$ définie par le quotient du produit libre d'algèbres $\mathcal{O}(H) * k[g]$ avec les relations :*

$$g^m = a, \qquad ge_x = e_{\theta(x)}g, \forall x \in H.$$

1. *Il existe une unique structure d'algèbre de Hopf sur $A_m(H, \theta, a)$ prolongeant celle de $\mathcal{O}(H)$ et telle que :*

$$\Delta(g) = \sum_{y,z \in H} \tau(y, z)e_y g \otimes e_z g, \qquad \varepsilon(g) = 1.$$

   *Notons $A_m(H, \theta, a, \tau)$ l'algèbre de Hopf ainsi obtenue.*

2. *L'algèbre de Hopf $A_m(H, \theta, a, \tau)$ est de dimension $m|H|$ et s'insère dans une extension abélienne cocentrale*

$$k \to \mathcal{O}(H) \to A_m(H, \theta, a, \tau) \xrightarrow{p} k\mathbb{Z}_m \to k$$

   *où $p$ est le morphisme d'algèbres de Hopf défini par $p_{|\mathcal{O}(H)} = \varepsilon$ et $p(g) = g$ (ici $g$ représente un générateur fixé de $\mathbb{Z}_m$).*

*Démonstration.*

Soit $\Delta_0 : \mathcal{O}(H) * k[g] \longrightarrow A_m(H, \theta, a, \tau) \otimes A_m(H, \theta, a, \tau)$ le morphisme d'algèbres défini comme dans l'énoncé de la proposition. On vérifie que $\Delta_0$ est compatible avec les relations de $A_m(H, \theta, a, \tau)$. Soit $x \in H$, on a alors :

$$\begin{aligned}
\Delta_0(ge_x) &= \Big(\sum_{y,z \in H} \tau(y, z)e_y g \otimes e_z g\Big)\Big(\sum_{rs=x} e_r \otimes e_s\Big) \\
&= \sum_{y,z,rs=x} \tau(y, z)e_y g e_r \otimes e_z g e_s \\
&= \sum_{y,z,rs=x} \tau(y, z)e_y e_{\theta(r)} g \otimes e_z e_{\theta(s)} g \\
&= \sum_{rs=x} \tau(\theta(r), \theta(s))e_{\theta(r)} g \otimes e_{\theta(s)} g.
\end{aligned}$$

$$\begin{aligned}\Delta_0(e_{\theta(x)}g) &= (\sum_{rs=\theta(x)} e_r \otimes e_s)(\sum_{y,z\in H} \tau(y,z)e_y g \otimes e_z g)\\ &= \sum_{y,z,rs=\theta(x)} \tau(y,z)e_r e_y g \otimes e_s e_z g\\ &= \sum_{rs=\theta(x)} \tau(r,s)e_r g \otimes e_s g\\ &= \sum_{ty=x} \tau(\theta(y),\theta(t))e_{\theta(y)}g \otimes e_{\theta(t)}g.\end{aligned}$$

Donc $\Delta_0(ge_x) = \Delta_0(e_{\theta(x)}g)$ pour $x \in H$. De plus :

$$\Delta_0(a) = \Delta_0(\sum_{x\in H} a(x)e_x) = \sum_{x\in H} a(x) \sum_{yz=x} e_y \otimes e_z = \sum_{y,z\in H} a(yz)e_y \otimes e_z.$$

Par ailleurs, on a :

$$\begin{aligned}\Delta_0(g^m) = \Delta_0(g)^m &= \sum_{r,s} \sum_{i=0,\dots,m-1} \tau(\theta^i(r),\theta^i(s))e_{\theta^{m-1}(r)}g^m \otimes e_{\theta^{m-1}(s)}g^m\\ &= \sum_{y,z} \sum_{i=1,\dots,m} \tau(\theta^i(y),\theta^i(z))e_{\theta^m(y)}a \otimes e_{\theta^m(z)}a\\ &= \sum_{y,z,x,x'} \sum_{i=1,\dots,m} \tau(\theta^i(y),\theta^i(z))e_y a(x)e_x \otimes e_z a(x')e_{x'}\\ &= \sum_{y,z} \sum_{i=0,\dots,m-1} \tau(\theta^i(y),\theta^i(z))a(y)a(z)e_y \otimes e_z.\end{aligned}$$

Or par hypothèse, $(H,\theta,a,\tau)$ est un $m$-datum donc pour tout $y,z \in H$, on a $\sum_{i=0,\dots,m-1} \tau(\theta^i(y),\theta^i(z))a(y)a(z) = a(yz)$ donc $\Delta_0(a) = \Delta_0(g^m)$, et finalement, $\Delta_0$ préserve les relations de $A_m(H,\theta,a)$. Par conséquent, $\Delta_0$ induit par passage au quotient $\Delta$.

En résumé, la structure d'algèbre de Hopf est bien définie sur $A_m(H,\theta,a)$. Par ailleurs, comme la base $\{e_x g^i,\ x \in H,\ 0 \le i \le m-1\}$ contient $m|H|$ éléments, l'algèbre $A_m(H,\theta,a)$ est bien de dimension $m|H|$.

Pour terminer, l'algèbre $A_m(H,\theta,a,\tau)$ possède une graduation cocentrale $A_m(H,\theta,a,\tau) = \oplus_{k=0}^{m-1}\mathcal{O}(H)g^k$ dont le morphisme $p$ est issu (voir la suite de la définition 2.1.4) et ainsi on peut construire l'extension abélienne cocentrale de l'énoncé, ce qui conclut la démonstration. □

**Proposition 4.1.6.** *Soit $A$ une algèbre de Hopf de dimension finie, s'insérant dans une extension abélienne cocentrale*

$$k \to \mathcal{O}(H) \to A \to k\mathbb{Z}_m \to k$$

*Alors il existe un $m$-datum $(H,\theta,a,\tau)$ tel que $A \simeq A_m(H,\theta,a,\tau)$ comme algèbres de Hopf.*

*Démonstration.*

Pour simplifier les notations, on identifiera $\mathcal{O}(H)$ avec son image dans $A$, c'est-à-dire $A_e = \mathcal{O}(H)$. L'hypothèse de dimension finie assure que l'extension est clivée (voir par exemple les références [24, théorème 3.5] ou [29, théorème 2.4]).

Dans notre cas, cela signifie que pour tout $h \in \mathbb{Z}_m$, il existe un élément inversible $u_h$ dans $A_h$, que nous normalisons pour que $\varepsilon(u_h) = 1$, et par conséquent $p(u_h) = h$, où $p : A \to k\mathbb{Z}_m$ est le morphisme d'algèbres de Hopf cocentral surjectif fourni par l'extension.

On a $A_e u_h \subset A_h$ et pour tout $b \in A_h$, on peut écrire $b = bu_h^{-1}u_h \in A_e u_h$, donc $A_h \subset A_e u_h$ et finalement $A_h = A_e u_h$.

Fixons à présent un générateur $g$ de $\mathbb{Z}_m$ et $u_g$ comme ci-dessus. On a alors $u_g^m \in A_{g^m} = A_e$, et on pose $a = u_g^m$. Puisque $\Delta(A_g) \subset A_g \otimes A_g$, on a $\Delta(u_g) = \sum_{x,y \in H} \tau(x,y) e_x u_g \otimes e_y u_g$ pour des scalaires $\tau(x,y) \in k$. Ces scalaires sont tous non nuls car $\Delta(u_g)$ est inversible.

Les conditions de co-associativité et de co-unité permettent de voir que l'application $\tau : H \times H \to k^\times$ définie à partir des scalaires est ainsi un 2-cocycle.

Par ailleurs, on a $u_g A_e u_g^{-1} \subset A_e$ et on obtient ainsi un automorphisme $\alpha := \mathrm{ad}(u_g)$ de l'algèbre $A_e$, vérifiant $\alpha^m = \mathrm{id}$ puisque $u_g^m \in A_e$ et $A_e$ est commutative.

Par une vérification directe, on obtient que $\alpha$ est bien un automorphisme de cogèbres et ainsi un automorphisme d'algèbres de Hopf sur $A_e = \mathcal{O}(H)$, provenant naturellement d'un automorphisme $\theta$ de $H$, tel que $\alpha(\phi) = \phi \circ \theta^{-1}$ pour $\phi \in \mathcal{O}(H)$.

Il est clair que l'on a $\alpha(a) = a$ car $a \circ \theta = a$, et $\varepsilon(a) = 1$, et on vérifie que la dernière condition définissant un $m$-datum est remplie en comparant $\Delta(u_g)^m$ et $\Delta(a)$.

On obtient ainsi un $m$-datum $(H, \theta, a, \tau)$ et il est facile de voir qu'il existe un morphisme d'algèbres de Hopf $A_m(H, \theta, a, \tau) \to A$, $\phi \in \mathcal{O}(H) \mapsto \phi$, $g \mapsto u_g$.

En combinant le lemme 4.1.3 qui nous fournit une base de $A_m(H, \theta, a, \tau)$ et le premier paragraphe de cette preuve, on conclut finalement que c'est un isomorphisme, ce qui achève la démonstration. □

## 4.2 Équivalence de $m$-data et problèmes d'isomorphisme

La question principale est maintenant de classifier les algèbres de Hopf $A_m(H, \theta, a, \tau)$ à isomorphisme près. Pour cela, la relation d'équivalence suivante sur les $m$-data est naturelle.

**Définition 4.2.1.** Deux $m$-data $(H, \theta, a, \tau)$ et $(H', \theta', a', \tau')$ sont dits équivalents si il existe un isomorphisme de groupes $f : H \to H'$, une application $\varphi : H' \to k^\times$ avec $\varphi(1) = 1$ et $l \in \{1, \dots, m-1\}$ premier avec $m$ tels que les conditions suivantes soient vérifiées, pour tout $x, y \in H'$ :

1. $\theta'^l = f \circ \theta \circ f^{-1}$ ;
2. $\left(\prod_{k=0}^{m-1} \varphi(\theta'^k(y))\right) a'(y)^l = a(f^{-1}(y))$ ;
3. $\left(\prod_{k=0}^{l-1} \tau'(\theta'^{-k}(x), \theta'^{-k}(y))\right) \varphi(xy) = \tau(f^{-1}(x), f^{-1}(y))\varphi(x)\varphi(y)$.

Il n'est pas complètement évident que les relations ci-dessus fournissent une relation d'équivalence, mais cela découle du résultat de base suivant, qui est une réponse partielle au problème de classification des algèbres de Hopf $A_m(H, \theta, a, \tau)$.

**Proposition 4.2.2.** *Soient $(H, \theta, a, \tau)$ et $(H', \theta', a', \tau')$ des $m$-data. Les assertions suivantes sont équivalentes :*

1. *il existe un isomorphisme d'algèbres de Hopf $F : A_m(H, \theta, a, \tau) \to A_m(H', \theta', a', \tau')$ et un automorphisme de groupes $u \in \mathrm{Aut}(\mathbb{Z}_m)$ rendant le diagramme suivant commutatif :*

$$\begin{array}{ccc} A_m(H, \theta, a, \tau) & \xrightarrow{p} & k\mathbb{Z}_m \\ \downarrow{\scriptstyle F} & & \downarrow{\scriptstyle u} \\ A_m(H', \theta', a', \tau') & \xrightarrow{p'} & k\mathbb{Z}_m \end{array}$$

2. *les $m$-data $(H, \theta, a, \tau)$ et $(H', \theta', a', \tau')$ sont équivalents.*

*Démonstration.*

Supposons que $F$ et $u$ soient donnés comme dans l'assertion 1, et posons pour plus de facilité $A = A_m(H, \theta, a, \tau)$ et $B = A_m(H', \theta', a', \tau')$. La commutativité du diagramme permet d'avoir, pour $a \in A_h, h \in \mathbb{Z}_m$ :

$$\begin{aligned} p'(F(a)_{(1)}) \otimes F(a)_{(2)} &= p' \circ F(a_{(1)}) \otimes F(a_{(2)}) \\ &= u \circ p(F(a_{(1)})) \otimes F(a_{(2)}) \\ &= (u \otimes F)(p(a_{(1)}) \otimes a_{(2)}) \\ &= (u \otimes F)(h \otimes a) \\ &= u(h) \otimes F(a). \end{aligned}$$

Ainsi, pour tout $a \in A_h$, $F(a) \in B_{u(h)}$ donc $F(A_h) \subset B_{u(h)}$ et enfin pour tout $h \in \mathbb{Z}_m$, on a $F(A_h) = B_{u(h)}$.

Par conséquent, $F$ induit un isomorphisme de $A_e = \mathcal{O}(H)$ vers $\mathcal{O}(H')$, provenant d'un isomorphisme de groupes $f : H \to H'$ tel que $F(\phi) = \phi \circ f^{-1}$ pour tout $\phi \in \mathcal{O}(H)$.

Considérons un générateur $g$ de $\mathbb{Z}_m$. L'automorphisme $u$ est alors de la forme $u(g) = g^l$ avec $l \in \{1, ..., m-1\}$ premier avec $m$. On a alors $F(A_g) = B_{u(g)} = B_{g^l}$. Puisque $B_{g^l} = B_e g^l$, il existe $\varphi \in \mathcal{O}(H)^\times$ tel que $F(g) = \varphi g^l$. Le fait que $F$ soit un morphisme de cogèbres permet d'obtenir que $\varphi(1) = 1$ et la relation (3) de la définition 4.2.1. En effet, on a :

$$\varepsilon \circ F(g) = \varepsilon(g) \Leftrightarrow \varepsilon(\varphi g^l) = \varepsilon(g) \Leftrightarrow \varepsilon(\varphi)\varepsilon(g^l) = 1 \Leftrightarrow \varphi(1).1^l = 1 \Leftrightarrow \varphi(1) = 1.$$

Et de plus, on utilise le fait que $\Delta \circ F(g) = (F \otimes F) \circ \Delta(g)$. D'une part :

$$\begin{aligned}
\Delta \circ F(g) &= \Delta(\varphi g^l) = \Delta(\varphi)\Delta(g^l) \\
&= \Delta(\sum_{x \in H} \varphi(x) e_x). \sum_{r,s \in H} \prod_{k=0}^{l-1} \tau'(\theta'^k(r), \theta'^k(s)) e_{\theta'^{l-1}(r)} g^l \otimes e_{\theta'^{l-1}(s)} g^l \\
&= \sum_{x,r,s \in H} \varphi(x)(\sum_{yz=x} e_y \otimes e_z). \prod_{k=0}^{l-1} \tau'(\theta'^k(r), \theta'^k(s)) e_{\theta'^{l-1}(r)} g^l \otimes e_{\theta'^{l-1}(s)} g^l \\
&= \sum_{y,z,r,s \in H} \varphi(yz) \prod_{k=0}^{l-1} \tau'(\theta'^k(r), \theta'^k(s)) e_y e_{\theta'^{l-1}(r)} g^l \otimes e_z e_{\theta'^{l-1}(s)} g^l \\
&= \sum_{y,z,r,s \in H} \varphi(yz) \prod_{k=0}^{l-1} \tau'(\theta'^k(r), \theta'^k(s)) \delta_{y,\theta'^{l-1}(r)} e_y g^l \otimes \delta_{z,\theta'^{l-1}(s)} e_z g^l \\
&= \sum_{y,z \in H} \varphi(yz) \prod_{k=0}^{l-1} \tau'(\theta'^{k-l+1}(y), \theta'^{k-l+1}(z)) e_y g^l \otimes e_z g^l \\
&= \sum_{y,z \in H} \varphi(yz) \prod_{j=0}^{l-1} \tau'(\theta'^{-j}(y), \theta'^{-j}(z)) e_y g^l \otimes e_z g^l.
\end{aligned}$$

D'autre part,

$$\begin{aligned}
(F \otimes F) \circ \Delta(g) &= (F \otimes F)(\sum_{y,z \in H} \tau(y,z) e_y g \otimes e_z g) \\
&= \sum_{y,z \in H} \tau(y,z) F(e_y) F(g) \otimes F(e_z) F(g) \\
&= \sum_{y,z \in H} \tau(y,z) e_{f(y)} \varphi g^l \otimes e_{f(z)} \varphi g^l \\
&= \sum_{y,z,r,s \in H} \tau(y,z) \varphi(r) \varphi(s) e_{f(y)} e_r g^l \otimes e_{f(z)} e_s g^l \\
&= \sum_{r,s \in H} \tau(f^{-1}(r), f^{-1}(s)) \varphi(r) \varphi(s) e_r g^l \otimes e_s g^l.
\end{aligned}$$

Finalement on obtient la relation (3) :

$$\varphi(yz)\prod_{j=0}^{l-1}\tau'(\theta'^{-j}(y),\theta'^{-j}(z))=\tau(f^{-1}(y),f^{-1}(z))\varphi(y)\varphi(z).$$

La compatibilité du morphisme d'algèbres $F$ avec la relation $ge_x = e_{\theta(x)}g$ nous permet d'obtenir la relation (1) :

$$\begin{aligned}
F(ge_x)=F(e_{\theta(x)}g) &\Leftrightarrow \varphi g^l e_{f(x)}=e_{f\circ\theta(x)}\varphi g^l\\
&\Leftrightarrow \sum_{y\in H}\varphi(y)e_y g^l e_{f(x)}=\sum_{y\in H}\varphi(y)e_{f\circ\theta(x)}e_y g^l\\
&\Leftrightarrow \sum_{y\in H}\varphi(y)e_y e_{\theta'^l(f(x))}g^l=\sum_{y\in H}\varphi(y)e_{f\circ\theta(x)}e_y g^l\\
&\Leftrightarrow \varphi(\theta'^l(f(x)))e_{\theta'^l(f(x))}g^l=\varphi(f\circ\theta(x))e_{f\circ\theta(x)}g^l\\
&\Leftrightarrow \varphi(\theta'^l(z))e_{\theta'^l(z)}=\varphi(f\circ\theta\circ f^{-1}(z))e_{f\circ\theta\circ f^{-1}(z)}\\
&\Leftrightarrow \theta'^l=f\circ\theta\circ f^{-1}.
\end{aligned}$$

Par ailleurs, par itérations on obtient que :

$$F(g)^m=\sum_{y\in H}\prod_{k=0}^{m-1}\varphi(\theta'^{(k+1)l}(y))a'(y)^l e_y.$$

La compatibilité de $F$ avec la relation $g^m = a$ donne la relation (2) :

$$\begin{aligned}
F(g^m)=F(a) &\Leftrightarrow F(g)^m=a\circ f^{-1}\\
&\Leftrightarrow \sum_{y\in H}\prod_{k=0}^{m-1}\varphi(\theta'^{(k+1)l}(y))a'(y)^l e_y=\sum_{x\in H}a(x)e_x\circ f^{-1}\\
&\Leftrightarrow \sum_{y\in H}\prod_{k=0}^{m-1}\varphi(\theta'^{(k+1)l}(y))a'(y)^l e_y=\sum_{x\in H}a(x)e_{f(x)}\\
&\Leftrightarrow \sum_{y\in H}\prod_{k=0}^{m-1}\varphi(\theta'^{(k+1)l}(y))a'(y)^l e_y=\sum_{y\in H}a(f^{-1}(y))e_y\\
&\Leftrightarrow \prod_{k=0}^{m-1}\varphi(\theta'^{(k+1)l}(y))a'(y)^l=a(f^{-1}(y))\\
&\Leftrightarrow \prod_{j=0}^{m-1}\varphi(\theta'^{j}(y))a'(y)^l=a(f^{-1}(y)).
\end{aligned}$$

Réciproquement, si on suppose que les $m$-data $(H,\theta,a,\tau)$ et $(H',\theta',a',\tau')$ sont équivalents, alors on a l'existence de $f$, $l$ et $\varphi$ vérifiant les assertions de la définition 4.2.1. On définit

alors un morphisme d'algèbres $F : A_m(H,\theta,a,\tau) \to A_m(H',\theta',a',\tau')$ par $F(e_x) = e_{f(x)}$ et $F(g) = \varphi g^l$. On vérifie directement que $F$ est un isomorphisme d'algèbres de Hopf, vérifiant $u \circ p = p' \circ F$ où $u$ est donné par $u(g) = g^l$. □

Le résultat que nous venons de démontrer donne la conséquence pratique suivante.

**Corollaire 4.2.3.** *Soit $(H,\theta,a,\tau)$ un $m$-datum.*

1. *Soient $f \in \mathrm{Aut}(H)$ et $l \geq 1$ premier avec $m$. Alors $(H, f\circ\theta^l\circ f^{-1}, a\circ f^{-1}, \tau')$, avec $\tau' = \prod_{k=0}^{l-1} \tau\circ(\theta^k\times\theta^k)\circ(f^{-1}\times f^{-1})$, est un $m$-datum et*

$$A_m(H,\theta,a,\tau) \simeq A_m\left(H, f\circ\theta^l\circ f^{-1}, (a\circ f^{-1})^l, \prod_{k=0}^{l-1}\tau\circ(\theta^k\times\theta^k)\circ(f^{-1}\times f^{-1})\right)$$

   *comme algèbres de Hopf.*

2. *Soit $\tau' \in Z^2(H,k^\times)$ cohomologue à $\tau$. Il existe $a' : H \to k^\times$ tel que $(H,\theta,a',\tau')$ est un $m$-datum et*

$$A_m(H,\theta,a,\tau) \simeq A_m(H,\theta,a',\tau')$$

   *comme algèbres de Hopf.*

*En particulier, si $\theta_1,\dots,\theta_r$ est un ensemble de représentants des classes de conjugaison des éléments dont l'ordre divise $m$ dans $\mathrm{Aut}(H)$, et si $\tau_1,\dots,\tau_s$ est un ensemble de représentants des 2-cocycles dans $H^2(H,k^\times)$, alors il existe $i \in \{1,\dots,r\}$, $j \in \{1,\dots,s\}$ et $a' : H \to k^\times$ tels que $(H,\theta_i,a',\tau_j)$ est un $m$-datum et $A_m(H,\theta,a,\tau) \simeq A_m(H,\theta_i,a',\tau_j)$.*

*Démonstration.*

La première assertion est obtenue facilement via la proposition 4.2.2 précédente. En effet, par construction, il est clair que $(H, f\circ\theta^l\circ f^{-1}, a\circ f^{-1}, \tau')$ est un $m$-datum. Par ailleurs, l'équivalence des algèbres de Hopf est obtenue par équivalence des $m$-data $(H,\theta,a,\tau)$ et $(H, f\circ\theta^l\circ f^{-1}, a\circ f^{-1}, \tau')$ en prenant $f = \mathrm{id}_H$, $l$ comme donné dans l'assertion (1), et $\varphi = \mathbb{1}$.

Pour la seconde assertion, soit $\mu : H \to k^\times$ tel que $\tau' = \tau\partial(\mu)$. Le résultat d'équivalence est là encore une conséquence directe de la proposition précédente en prenant $a' = a\left(\prod_{i=0}^{m-1}\mu\circ\theta^i\right)^{-1}$. Dans ce cas, $f = \mathrm{id}_H$, $l = 1$, et $\varphi = \mu$ réalisent l'équivalence des $m$-data.

La dernière assertion est finalement obtenue en combinant les assertions (1) et (2). □

*Remarque* 4.2.4. Soit $(H,\theta,a,\tau)$ un $m$-datum. Puisque $a\circ\theta = a$, il existe une application $\mu : H \to k^\times$ telle que $\mu\circ\theta = \mu$ et $\mu^m = a$. Le cocycle $\tau' = \tau\partial(\mu)$ satisfait alors

$$\prod_{k=0}^{m-1}\tau'\circ(\theta^k\times\theta^k) = 1.$$

De plus, d'après le corollaire 4.2.3, le $m$-datum $(H, \theta, a, \tau)$ est équivalent à un $m$-datum $(H, \theta, a', \tau')$ avec $a' \in \widehat{H}$. Un tel datum avec $a' \in \widehat{H}$ sera dit *normalisé*. Il est donc tentant de ne travailler qu'avec des data normalisés, mais cela oblige de changer de cocycle pour chaque choix d'automorphisme $\theta$, ce qui peut-être gênant dans la pratique lorsque l'on a de "bons" représentants des cocycles de $H$. Nous travaillerons donc avec la notion générale de $m$-datum, comme fournie dans la définition 4.1.4.

*Remarque* 4.2.5. Fixons $\theta \in \mathrm{Aut}(H)$ avec $\theta^m = \mathrm{id}$. Le groupe de Kac $\mathrm{Opext}_\theta(k\mathbb{Z}_m, \mathcal{O}(H))$ [13] peut être décrit comme l'ensemble des paires $(a, \tau) \in \widehat{H} \times Z^2(H, k^\times)$ telles que $(H, \theta, a, \tau)$ est un $m$-datum normalisé modulo la relation d'équivalence définie par $(a, \tau) \sim (a', \tau') \iff \exists\, \varphi : H \to k^\times$ avec $\varphi \cdot \varphi \circ \theta \in \widehat{H}$, $\left(\prod_{k=0}^{m-1} \varphi \circ \theta^k\right) a' = a$ et $\tau' = \tau \partial(\varphi)$. La loi de groupe est la multiplication classique sur les composantes. Le groupe $\mathrm{Opext}_\theta(k\mathbb{Z}_m, \mathcal{O}(H))$ est connu pour être potentiellement difficilement calculable (voir la référence [22], et la référence [11] pour une contribution récente). Ainsi, le problème de la description des $m$-data à équivalence près, est lui aussi un travail non évident à réaliser.

La proposition 4.2.2 est en général insuffisante pour classifier à isomorphisme près, les algèbres de Hopf $A_m(H, \theta, a, \tau)$. Cependant, dans le cadre du lemme 2.1.3, elle peut être suffisante. Ainsi, nous devons pousser l'analyse des algèbres de Hopf $A_m(H, \theta, a, \tau)$ pour déterminer les conditions d'application du lemme 2.1.3. Pour cela, introduisons un certain nombre de groupes associés à un $m$-datum.

**Définition 4.2.6.** Soit $(H, \theta, a, \tau)$ un $m$-datum.

1. Posons $Z_{\tau,\theta}(H) = \{x \in Z(H) \mid \tau(\theta^i(x), y) = \tau(y, \theta^i(x)),\ \forall y \in H,\ \forall i,\ 0 \leq i \leq m-1\}$. C'est un sous-groupe central de $H$, et on obtient, par restriction, un nouveau $m$-datum $(Z_{\tau,\theta}(H), \theta, a, \tau)$.
2. Soit $H^\theta$ le sous-groupe de $H$ formé des éléments invariants par $\theta$. Le groupe $G(H, \theta, a, \tau)$ est le groupe dont les éléments sont des paires $(x, \lambda) \in H^\theta \times k^\times$ vérifiant $\lambda^m = a(x)$, et dont la loi de groupe est définie par $(x, \lambda) \cdot (y, \mu) = (xy, \tau(x, y)\lambda\mu)$.
3. Notons $G_0(H, \theta, a, \tau)$ le groupe $G(Z_{\tau,\theta}(H), \theta, a, \tau)$, composé ainsi des paires $(x, \lambda) \in Z(H)^\theta \times k^\times$ vérifiant $\lambda^m = a(x)$ et $\tau(x, y) = \tau(y, x)$, $\forall y \in H$.

Il est facile de vérifier que $G(H, \theta, a, \tau)$ est en effet un groupe, s'insérant dans une suite exacte centrale

$$1 \to \mu_m \to G(H, \theta, a, \tau) \to H^\theta \to 1.$$

**Proposition 4.2.7.** *Soit $(H, \theta, a, \tau)$ un $m$-datum. On a l'extension cocentrale universelle suivante :*

$$k \to \mathcal{O}(H/Z_{\tau,\theta}(H)) \to A_m(H, \theta, a, \tau) \to A_m(Z_{\tau,\theta}(H), \theta, a, \tau) \to k.$$

*Démonstration.*

Il est facile de voir qu'il existe un morphisme d'algèbres de Hopf surjectif

$$p : A(H, \theta, a, \tau) \to A(Z_{\tau,\theta}(H), \theta, a, \tau)$$

avec $p(g) = g$ pour $g$ un générateur de $\mathbb{Z}_m$ et tel que pour $\phi \in \mathcal{O}(H)$, $p(\phi)$ est la restriction de $\phi$ à $Z_{\tau,\theta}(H)$.

La propriété de cocentralité de $p$ découle du fait que le groupe $Z_{\tau,\theta}(H)$ est central dans $H$. Il est simple de voir que $p$ induit la suite exacte cocentrale annoncée.

Il faut par ailleurs démontrer l'universalité de $p$. Pour cela, considérons un morphisme d'algèbres de Hopf cocentral $q : A(H, \theta, a, \tau) \to B$. Le caractère cocentral de $q$ amène que $q(e_x) = 0$ si $x \notin Z(H)$, et que pour tout $x \in Z(H)$ et $y \in H$, $\tau(x, y)q(e_x)q(g) = \tau(y, x)q(e_x)q(g)$.

Ainsi, $\tau(x, y)q(e_x) = \tau(y, x)q(e_x)$ et $\tau(x, y) = \tau(y, x)$ si $q(e_x) \neq 0$.

Posons $T := \{x \in H \mid q(e_x) \neq 0\}$. Puisque $q(g)q(e_x)q(g)^{-1} = q(ge_xg^{-1}) = q(e_{\theta(x)})$, on voit alors que si $x \in T$ alors $\theta(x) \in T$ et par itérations $\theta^i(x) \in T$ pour tout $i = 0, ..., m-1$. Ainsi on obtient que $T \subset Z_{\tau,\theta}(H)$. On vérifie facilement ensuite qu'il existe un morphisme d'algèbres de Hopf $f : A(Z_{\tau,\theta}(H), \theta, a, \tau) \to B$ avec $f(e_x) = q(e_x)$ et $f(g) = q(g)$, comme demandé. □

Procédons à présent à l'analyse de la structure de l'algèbre de Hopf $A_m(H, \theta, a, \tau)$, avec pour commencer un résultat basique.

**Proposition 4.2.8.** *Soit $(H, \theta, a, \tau)$ un $m$-datum.*

1. *L'algèbre de Hopf $A_m(H, \theta, a, \tau)$ est commutative si et seulement si $\theta = \mathrm{id}_H$. Plus généralement, l'abélianisé de $A_m(H, \theta, a, \tau)$ est l'algèbre de Hopf $\mathcal{O}(G(H, \theta, a, \tau))$.*
2. *L'algèbre de Hopf $A_m(H, \theta, a, \tau)$ est cocommutative si et seulement si $H$ est abélien et $\tau$ est symétrique, i.e. $\tau(x, y) = \tau(y, x)$ pour tout $x, y \in H$.*

*Démonstration.*

L'assertion concernant la commutativité de $A_m(H, \theta, a, \tau)$ est claire en considérant la relation du lemme 4.1.3 : $ge_x = e_{\theta(x)}g, \forall x \in H$. Ainsi $A_m(H, \theta, a, \tau)$ est commutative si et seulement si pour tout $x \in H$, $\theta(x) = x$ i.e. $\theta = \mathrm{id}_H$.

Comme $\Delta(g) = \sum_{y,z \in H} \tau(y, z)e_yg \otimes e_zg$, la cocommutativité de $A_m(H, \theta, a, \tau)$ est obtenue si et seulement si $H$ est abélien et $\tau$ est symétrique.

Un morphisme d'algèbres $\chi : A_m(H, \theta, a, \tau) \to k$ correspond à une paire $(x, \lambda) \in H \times k^\times$, où $\chi(\phi) = \phi(x)$ pour tout $\phi \in \mathcal{O}(H)$ et $\chi(g) = \lambda$. La compatibilité de $\chi$ avec les relations qui

définissent $A_m(H,\theta,a,\tau)$ est équivalente à demander que $\lambda^m = a$ et que $\theta(x) = x$ c'est-à-dire $x \in H^\theta$, ce qui revient à écrire que $(x,\lambda) \in G(H,\theta,a,\tau)$.

Un calcul immédiat montre que la loi de groupe de $\mathrm{Alg}(A_m(H,\theta,a,\tau),k)$ coïncide avec la loi de groupe de $G(H,\theta,a,\tau)$. Par conséquent, $\mathrm{Alg}(A_m(H,\theta,a,\tau),k)$ est isomorphe à $G(H,\theta,a,\tau)$.

Ainsi l'abélianisé de $A_m(H,\theta,a,\tau)$, qui est l'algèbre des fonctions sur $\mathrm{Alg}(A_m(H,\theta,a,\tau),k)$, est isomorphe à $\mathcal{O}(G(H,\theta,a,\tau))$. □

Discutons maintenant du cas où le groupe graduateur universel de $A_m(H,\theta,a,\tau)$ est cyclique.

**Proposition 4.2.9.** *Soit $(H,\theta,a,\tau)$ un $m$-datum.*

1. *L'algèbre de Hopf $A_m(H,\theta,a,\tau)$ possède un groupe graduateur universel cyclique si et seulement si le groupe $G_0(H,\theta,a,\tau)$ est cyclique et la restriction de $\theta$ à $Z_{\tau,\theta}(H)$ est triviale.*
2. *Le morphisme naturel d'algèbres de Hopf cocentral $p : A_m(H,\theta,a,\tau) \to k\mathbb{Z}_m$ est universel si et seulement si le groupe $Z_{\tau,\theta}(H)$ est trivial.*

*Démonstration.*

Supposons que $A_m(H,\theta,a,\tau)$ possède un groupe graduateur universel cyclique. D'après la proposition 4.2.7, on obtient que $A_m(Z_{\tau,\theta}(H),\theta,a,\tau)$ est l'algèbre d'un groupe cyclique, et en particulier qu'elle est commutative. Ainsi, d'après l'assertion (1) de la proposition 4.2.8, on a $\theta_{|Z_{\tau,\theta}(H)} = \mathrm{id}_{Z_{\tau,\theta}(H)}$ c'est-à-dire que la restriction de $\theta$ à $Z_{\tau,\theta}(H)$ est triviale et $G_0(H,\theta,a,\tau) = G(Z_{\tau,\theta}(H),\theta,a,\tau)$ est cyclique.

Réciproquement, si la restriction de $\theta$ à $Z_{\tau,\theta}(H)$ est triviale, d'après l'assertion (1) de la proposition 4.2.8, l'algèbre de Hopf $A_m(Z_{\tau,\theta}(H),\theta,a,\tau)$ est commutative donc elle coïncide avec son abélianisé et ainsi elle est isomorphe à $\mathcal{O}(G(Z_{\tau,\theta}(H),\theta,a,\tau))$. Si l'on suppose de plus que $G_0(H,\theta,a,\tau) = G(Z_{\tau,\theta}(H),\theta,a,\tau)$ est cyclique, on obtient que $A_m(Z_{\tau,\theta}(H),\theta,a,\tau)$ est l'algèbre de groupe d'un groupe cyclique, et enfin, la proposition 4.2.7 assure que $A_m(H,\theta,a,\tau)$ possède un groupe graduateur universel. Ceci conclut la preuve de la première équivalence.

Démontrons à présent la deuxième équivalence :

La surjection canonique $A_m(Z_{\tau,\theta}(H),\theta,a,\tau) \to k\mathbb{Z}_m$ est un isomorphisme si et seulement si $Z_{\tau,\theta}(H)$ est trivial, car $\dim(A_m(Z_{\tau,\theta}(H),\theta,a,\tau)) = m|Z_{\tau,\theta}(H)|$. Ainsi, d'après la proposition 4.2.7, on obtient le résultat attendu. □

Le résultat précédent nous amène à introduire du vocabulaire supplémentaire.

**Définition 4.2.10.** Un $m$-datum $(H, \theta, a, \tau)$ est dit *cyclique* (resp. *réduit*) si le groupe $G_0(H, \theta, a, \tau)$ est cyclique et la restriction de $\theta$ à $Z_{\tau,\theta}(H)$ est triviale (resp. si le groupe $Z_{\tau,\theta}(H)$ est trivial).

On obtient alors notre résultat le plus utile pour la classification des algèbres de Hopf du type $A_m(H, \theta, a, \tau)$.

**Proposition 4.2.11.** *Soient $(H, \theta, a, \tau)$ et $(H', \theta', a', \tau')$ des $m$-data cycliques. Les assertions suivantes sont équivalentes :*

1. *les algèbres de Hopf $A_m(H, \theta, a, \tau)$ et $A_m(H', \theta', a', \tau')$ sont isomorphes ;*
2. *les $m$-data $(H, \theta, a, \tau)$ et $(H', \theta', a', \tau')$ sont équivalents.*

*Démonstration.*

L'implication (2)⇒(1) est donnée par la proposition 4.2.2.

Réciproquement, supposons que $A_m(H, \theta, a, \tau) \simeq A_m(H', \theta', a', \tau')$. D'après la proposition 4.2.9, on obtient que les algèbres de Hopf $A_m(H, \theta, a, \tau)$ et $A_m(H', \theta', a', \tau')$ possèdent chacune un groupe graduateur universel cyclique car les $m$-data qui les conditionnent sont supposés cycliques.

Dans cette situation, on peut alors utiliser le lemme 2.1.3 qui nous donne l'existence de l'automorphisme $u$ permettant d'être dans les conditions d'application de l'assertion (1) de la proposition 4.2.2 pour rendre le diagramme commutatif. Finalement, on obtient l'équivalence des $m$-data, ce qui conclut la preuve. □

Finalement, voici le résultat principal de cette partie.

**Théorème 4.2.12.** *Soient $H$ un groupe fini et $m \geq 1$. L'application $(H, \theta, a, \tau) \mapsto A_m(H, \theta, a, \tau)$ induit une bijection entre les ensembles suivants :*

1. *les classes d'équivalence de $m$-data cycliques (resp. réduits) ayant $H$ comme groupe sous-jacent ;*
2. *les classes d'isomorphisme d'algèbres de Hopf $A$ qui s'insèrent dans une extension abélienne cocentrale*

$$k \to \mathcal{O}(H) \to A \to k\mathbb{Z}_m \to k$$

*et possèdent un groupe graduateur universel cyclique (resp. ayant $\mathbb{Z}_m$ comme groupe graduateur universel).*

*Démonstration.*

Ce théorème est une combinaison des résultats obtenus à travers les propositions 4.1.6 et 4.2.11.

Cette application est bien définie : en effet, on a vu que si $(H, \theta, a, \tau)$ est un $m$-datum cyclique alors $A_m(H, \theta, a, \tau)$ est une algèbre de Hopf qui s'insère dans une extension abélienne cocentrale et possédant un groupe graduateur universel.

Respectivement, si $(H, \theta, a, \tau)$ est un $m$-datum réduit alors $A_m(H, \theta, a, \tau)$ est une algèbre de Hopf qui s'insère dans une extension abélienne cocentrale et ayant $\mathbb{Z}_m$ comme groupe graduateur universel.

Par ailleurs, la proposition 4.1.6 permet de dire que toute algèbre de Hopf de dimension finie s'insérant dans une extension cocentrale abélienne est à isomorphisme près de la forme $A_m(H, \theta, a, \tau)$ où $(H, \theta, a, \tau)$ est un $m$-datum.

Enfin, les résultats d'équivalence obtenus dans la proposition 4.2.11 permettent d'obtenir la bijection d'ensembles souhaitée. □

**Corollaire 4.2.13.** *Soient $H$ un groupe fini tel que $Z(H) = \{1\}$ et $m \geq 2$. L'application $(H, \theta, a, \tau) \mapsto A_m(H, \theta, a, \tau)$ induit une bijection entre les ensembles suivants :*

1. *les classes d'équivalence de $m$-data ayant $H$ comme groupe sous-jacent ;*
2. *les classes d'isomorphisme d'algèbres de Hopf $A$ s'insérant dans une extension abélienne cocentrale*
$$k \to \mathcal{O}(H) \to A \to k\mathbb{Z}_m \to k.$$

*Démonstration.*

L'hypothèse que $Z(H) = \{1\}$ permet d'obtenir que tous les $m$-data $(H, \theta, a, \tau)$ sont réduits, et que toutes les extensions cocentrales abéliennes correspondantes $k \to \mathcal{O}(H) \to A \to k\mathbb{Z}_m \to k$ sont universelles. On peut donc appliquer le théorème 4.2.12, ce qui amène au résultat du corollaire. □

## 4.3 Résultats de classification

Appliquons à présent le théorème 4.2.12 et le corollaire 4.2.13 pour obtenir un résultat de classification effectif pour les algèbres de Hopf qui s'insèrent dans une extension abélienne cocentrale, sous diverses hypothèses.

L'ensemble des classes d'équivalence des $m$-data possède une description simple en faisant des hypothèses fortes sur $H$, et ainsi le résultat précédent devient plus simple en utilisant les notations suivantes : si $G$ est un groupe et $m \geq 1$, l'ensemble $\mathrm{CC}_m^\bullet(G)$ est l'ensemble des éléments de $G$ tels que $x^m = 1$ et $x \neq 1$, modulo la relation d'équivalence définie par $x \sim y$ si et seulement si il existe $l$ premier avec $m$ tel que $x^l$ soit conjugué à $y$. Lorsque $m = 2$, $\mathrm{CC}_2^\bullet(G)$ est simplement l'ensemble des classes de conjugaison des éléments d'ordre 2 de $G$.

**Théorème 4.3.1.** *Soit $H$ un groupe fini avec $\widehat{H} = \{1\} = Z(H)$ et $H^2(H, k^\times) \simeq \mathbb{Z}_2$. Alors pour tout $m \geq 2$, il y a une bijection entre l'ensemble des classes d'isomorphisme d'algèbres de Hopf $A$ non commutatives s'insérant dans une extension abélienne cocentrale*

$$k \to \mathcal{O}(H) \to A \to k\mathbb{Z}_m \to k$$

*et*

1. *si $m$ est impair, l'ensemble $\mathrm{CC}_m^\bullet(\mathrm{Aut}(H))$ ;*
2. *si $m$ est pair, l'ensemble $\mathrm{CC}_m^\bullet(\mathrm{Aut}(H)) \times H^2(H, k^\times)$.*

*Démonstration.*

Puisque $Z(H) = \{1\}$, le corollaire 4.2.13 entraîne une bijection entre l'ensemble des classes d'isomorphisme d'algèbres de Hopf non commutatives s'insérant dans une extension comme demandé dans l'énoncé, et l'ensemble des classes d'équivalence de $m$-data $(H, \theta, a, \tau)$ avec $\theta \neq \mathrm{id}$ pour répondre au caractère non commutatif.

Le point clé est que, puisque $H^2(H, k^\times) \simeq \mathbb{Z}_2$, pour tout $\theta \in \mathrm{Aut}(H)$ et $\tau \in Z^2(H, k^\times)$, on a $[\tau] = [\tau \circ (\theta \times \theta)]$ et $[\tau][\tau \circ (\theta \times \theta)] = 1$ dans $H^2(H, k^\times)$.

Plaçons nous tout d'abord dans le cas où $m$ est impair. Soit $(H, \theta, a, \tau)$ un $m$-datum tel que $\theta \neq \mathrm{id}$. Alors $[\tau]^m = 1$ et ainsi $[\tau] = 1$ puisque $m$ est impair. Donc $(H, \theta, a, \tau)$ est équivalent à un $m$-datum du type $(H, \theta, a', 1)$ avec $a' = \mathbb{1}$ puisque $\widehat{H} = \{1\}$. Ce $m$-datum n'est conditionné que par $\theta \in \mathrm{Aut}(H)$ donc on obtient une bijection entre l'ensemble des $m$-data du type $(H, \theta, \mathbb{1}, 1)$ avec $\theta \neq \mathrm{id}$ et l'ensemble $\mathrm{CC}_m^\bullet(\mathrm{Aut}(H))$, la relation d'équivalence de cet ensemble étant directement liée à la condition (1) d'équivalence de $m$-datum de la définition 4.2.1. Finalement, on a démontré la bijection d'ensembles souhaitée pour le cas où $m$ est impair.

À présent, plaçons nous dans le cas où $m$ est pair. On considère une paire $(\theta, \tau)$ avec $\theta \in \mathrm{Aut}(H)$ satisfaisant $\theta^m = \mathrm{id}$, $\theta \neq \mathrm{id}$, et $\tau \in Z^2(H, k^\times)$. L'hypothèse que $H^2(H, k^\times) \simeq \mathbb{Z}_2$ implique qu'il existe $a : H \to k^\times$ tel que $\prod_{k=0}^{m-1} \tau \circ (\theta^k \times \theta^k) = \partial(a^{-1})$. Par ailleurs, l'hypothèse que $\widehat{H} = \{1\}$ entraîne qu'une telle application $a$ est unique et vérifie $a \circ \theta = a$. Ainsi, on peut associer sans ambiguïté un $m$-datum $(H, \theta, a, \tau)$ à la paire $(\theta, \tau)$.

Considérons à présent une autre paire $(\theta', \tau')$ telle que $a'$ soit l'application permettant à $(H, \theta', a', \tau')$ d'être un $m$-datum.

Si les $m$-data $(H, \theta, a, \tau)$ et $(H, \theta', a', \tau')$ sont équivalents, alors il existe $l$ premier avec $m$ (ainsi $l$ est impair), tel que $\theta'^l$ soit conjugué à $\theta$ et $[\tau] = [\tau']^l = [\tau']$ car $\tau \circ (f^{-1} \times f^{-1})$ est cohomologue à $\tau$ toujours d'après l'hypothèse $H^2(H, k^\times) \simeq \mathbb{Z}_2$.

Inversement, si $\theta' = f \circ \theta^l \circ f^{-1}$, pour $f \in \mathrm{Aut}(H)$ et $l$ premier avec $m$, alors on a, d'après le corollaire 4.2.3 :

$$(H, \theta, a, \tau) \sim (H, f \circ \theta^l \circ f^{-1}, (a \circ f^{-1})^l, \prod_{k=0}^{l-1} \tau \circ (\theta^k \times \theta^k) \circ (f^{-1} \times f^{-1})$$
$$\sim (H, \theta', (a \circ f^{-1})^l, \prod_{k=0}^{l-1} \tau \circ (\theta^k \circ f^{-1} \times \theta^k \circ f^{-1}).$$

Le cocycle de droite est cohomologue à $\tau^l$, et par conséquent cohomologue à $\tau$, et si on suppose que $\tau'$ est cohomologue à $\tau$, on obtient (toujours d'après le corollaire 4.2.3)

$$(H, \theta, a, \tau) \sim (H, \theta', b, \tau) \sim (H, \theta', c, \tau')$$

pour des applications $b, c$, avec nécessairement $c = a'$ en raison de la discussion en début de preuve. Ainsi, la relation d'équivalence définie sur les $m$-data est compatible avec la relation d'équivalence définie sur les paires $(\theta, \tau)$, donc on obtient une bijection entre l'ensemble des $m$-data $(H, \theta, a, \tau)$ avec $\theta \neq \mathrm{id}$ et l'ensemble des classes d'équivalence de paires $(\theta, \tau)$. Ce dernier ensemble coïncidant avec $\mathrm{CC}^\bullet_m(\mathrm{Aut}(H)) \times H^2(H, k^\times)$, on obtient finalement la bijection souhaitée dans le cas où $m$ est pair, concluant ainsi la démonstration. □

Toujours sous des hypothèses fortes, voici une autre conséquence utile du théorème 4.2.12.

**Théorème 4.3.2.** *Soit $H$ un groupe fini tel que $|\widehat{H}| \leq 2$, et $Z(H) = \{1\} = H^2(H, k^\times)$. Alors pour tout $m \geq 1$, il y a une bijection entre l'ensemble des classes d'isomorphisme d'algèbres de Hopf non commutatives $A$ s'insérant dans une extension abélienne cocentrale*

$$k \to \mathcal{O}(H) \to A \to k\mathbb{Z}_m \to k$$

*et*

1. *si $m$ est impair, l'ensemble $\mathrm{CC}^\bullet_m(\mathrm{Aut}(H))$ ;*
2. *si $m$ est pair, l'ensemble $\mathrm{CC}^\bullet_m(\mathrm{Aut}(H)) \times \widehat{H}$.*

*Démonstration.*

Le corollaire 4.2.13 permet d'obtenir une bijection entre l'ensemble des classes d'isomorphisme d'algèbres de Hopf non commutatives s'insérant dans une extension comme souhaitée dans l'énoncé, et l'ensemble des classes d'équivalence de $m$-data $(H, \theta, a, \tau)$ avec $\theta \neq \mathrm{id}$ pour respecter l'hypothèse de non commutativité.

Par ailleurs, puisque $H^2(H, k^\times) = \{1\}$, le corollaire 4.2.3 assure que de tels data sont équivalents à des data du type $(H, \theta, a, 1)$ (par conséquent avec $a \in \widehat{H}$).

En utilisant à présent, le fait que $|\widehat{H}| \leq 2$, $\mathrm{Aut}(H)$ agit trivialement sur $\widehat{H}$, et on peut voir que deux $m$-data $(H, \theta, a, 1)$ et $(H, \theta', a', 1)$ sont équivalents si et seulement si il existe $f \in \mathrm{Aut}(H)$, $\varphi \in \widehat{H}$ et $l$ premier à $m$ tels que :

$$\theta'^l = f \circ \theta \circ f^{-1}, \qquad \varphi^m a'^l = a.$$

Si $m$ est pair, comme $|\widehat{H}| \leq 2$, $\varphi$ est d'ordre 1 ou 2, donc $\varphi^m = 1$. Ainsi la dernière condition donne que $a' = a$ car $l$ est nécessairement impair donc $a'^l = a'$ ($a'$ est d'ordre 1 ou 2 également). Ainsi, l'ensemble des classes d'équivalence de $m$-data $(H, \theta, a, 1)$ avec $\theta \neq \mathrm{id}$ est en bijection avec l'ensemble des classes d'équivalence des $m$-data $(H, \theta, \mathbb{1}, 1)$ avec $\theta \neq \mathrm{id}$ étant lui-même en bijection avec l'ensemble $\mathrm{CC}_m^\bullet(\mathrm{Aut}(H))$, ce qui démontre la première assertion.

Si $m$ est impair, on a alors $\varphi^m = \varphi$, et un tel $\varphi$ existe toujours si $l$ existe. Ainsi l'ensemble des classes d'équivalence de $m$-data $(H, \theta, a, 1)$ avec $\theta \neq \mathrm{id}$ est en bijection avec l'ensemble $\mathrm{CC}_m^\bullet(\mathrm{Aut}(H)) \times \widehat{H}$, ce qui achève la preuve. □

Pour démontrer notre prochain résultat de classification, on utilisera le lemme suivant.

**Lemme 4.3.3.** *Soit $H$ un groupe fini dans lequel tous les automorphismes sont intérieurs et tel que $Z(H) = \{1\}$ et $|\widehat{H}| \leq 2$. Si $(H, \theta, a, \tau)$ et $(H, \theta, a', \tau)$ sont des 2-data équivalents, alors $a = a'$.*

*Démonstration.*

Tout d'abord, supposons que nos 2-data sont normalisés : $\tau \cdot \tau \circ (\theta \times \theta) = 1$ (on sait également que $a, a' \in \widehat{H}$, voir la remarque 4.2.4).

Comme $(H, \theta, a, \tau) \sim (H, \theta, a', \tau)$ , il existe $f \in \mathrm{Aut}(H)$ et $\varphi : H \to k^\times$ tels que

$$f \circ \theta = \theta \circ f, \ \varphi \cdot \varphi \circ \theta \cdot a' = a \circ f^{-1}, \ \tau = \partial(\varphi)\tau \circ (f^{-1} \times f^{-1}).$$

Notons $\theta = \mathrm{ad}(x)$ et $f^{-1} = \mathrm{ad}(y)$, puisque tous les automorphismes de $H$ sont supposés intérieurs. On a $xy = yx$ grâce à la relation $f \circ \theta = \theta \circ f$ et à l'hypothèse que $Z(H) = \{1\}$. De plus, en utilisant le lemme 2.4.3 avec $\tau \circ (f^{-1} \times f^{-1}) \in Z^2(H, k^\times)$ et $y^{-1} \in H$, on a : $\tau \circ (f^{-1} \times f^{-1}) = \partial(\mu_y^{-1})\tau \circ (f^{-1} \times f^{-1}) \circ (f \times f) = \partial(\mu_y^{-1})\tau$, avec $\mu_y$ définie comme dans le lemme. Donc on a :

$$\varphi \cdot \varphi \circ \theta \cdot a' = a \circ f^{-1}, \ \tau = \partial(\varphi)\tau \circ (f^{-1} \times f^{-1}) = \partial(\varphi)\partial(\mu_y^{-1})\tau.$$

Ainsi, il existe $\chi \in \widehat{H}$ tel que $\varphi = \chi\mu_y$ et $\varphi \cdot \varphi \circ \theta = \chi \cdot \chi \circ \theta \cdot \mu_y \cdot \mu_y \circ \theta$.

Puisque $|\widehat{H}| \leq 2$ et que $\theta$ est intérieur, on a : $\chi \cdot \chi \circ \theta = \mathbb{1}$ et donc on obtient que $\varphi \cdot \varphi \circ \theta = \mu_y \cdot \mu_y \circ \theta = \mu_y \cdot \mu_y \circ \mathrm{ad}(x)$. En utilisant le fait que notre datum est normalisé et que $xy = yx$, pour $z \in H$, on a alors :

$$\begin{aligned}
\mu_y \circ \mathrm{ad}(x)(z) &= \tau(yxzx^{-1}, y^{-1})\tau(y, xzx^{-1})\tau(y, y^{-1})^{-1} \\
&= \tau(xyzx^{-1}, xy^{-1}x^{-1})\tau(xyx^{-1}, xzx^{-1})\tau(xyx^{-1}, xy^{-1}x^{-1})^{-1} \\
&= \tau(yz, y^{-1})^{-1}\tau(y, z)^{-1}\tau(y, y^{-1}) \\
&= \mu_y(z)^{-1}.
\end{aligned}$$

Ainsi $\varphi \cdot \varphi \circ \theta = \mathbb{1}$, et $a = a'$.

Généralisons à présent lorsque nos data ne sont pas normalisés. D'après la remarque 4.2.4, nos 2-data $(H, \theta, a, \tau)$ et $(H, \theta, a', \tau')$ sont respectivement équivalents à deux 2-data normalisés $(H, \theta, b, \tau')$ et $(H, \theta, b', \tau')$. Ainsi, grâce au raisonnement précédent, on obtient que $b = b'$ et par conséquent, $a = a'$ en raison de la construction de $b$ et $b'$ à partir de $a$ et $a'$ (voir la preuve du corollaire 4.2.3). □

**Théorème 4.3.4.** *Soit $H$ un groupe fini dont tous les automorphismes sont intérieurs et tel que $|\widehat{H}| \leq 2$, $Z(H) = \{1\}$ et $|H^2(H, k^\times)| \leq 2$. Alors il y a une bijection entre l'ensemble des classes d'isomorphisme d'algèbres de Hopf non commutatives $A$ s'insérant dans une extension abélienne cocentrale $k \to \mathcal{O}(H) \to A \to k\mathbb{Z}_2 \to k$ et l'ensemble $\mathrm{CC}_2^\bullet(H) \times \widehat{H} \times H^2(H, k^\times)$.*

*Démonstration.*

Comme avant, grâce à l'hypothèse $Z(H) = \{1\}$, d'après le corollaire 4.2.13, il s'agit de classifier les 2-data $(H, \theta, a, \tau)$ avec $\theta \neq \mathrm{id}$ pour respecter le caractère non commutatif, à équivalence près.

On peut supposer que $H^2(H, k^\times) \simeq \mathbb{Z}_2$, car le cas où $H^2(H, k^\times) \simeq \{1\}$ est traité dans le théorème 4.3.2 en prenant $m = 2$.

Fixons un ensemble de représentants $\{\theta_1, \ldots, \theta_r\}$ des éléments de $\mathrm{CC}_2^\bullet(\mathrm{Aut}(H)) \simeq \mathrm{CC}_2^\bullet(H)$, et fixons pour tout $i \in \{1, ..., r\}$, un 2-cocycle non trivial $\tau_i \in H^2(H, k^\times)$ tel que $\tau_i \cdot \tau_i \circ (\theta_i \times \theta_i) = 1$ (grâce à l'hypothèse $H^2(H, k^\times) \simeq \mathbb{Z}_2$, l'existence de ces cocycles est assurée).

Le corollaire 4.2.3 assure que tout 2-datum dont l'automorphisme sous-jacent est non trivial, est équivalent à un 2-datum de la liste

$$\{(H, \theta_i, a, 1),\ i = 1, \ldots, r,\ a \in \widehat{H}\}, \quad \{(H, \theta_i, a, \tau_i),\ \ i = 1, \ldots, r,\ a \in \widehat{H}\}.$$

D'après le lemme 4.3.3, dans le premier ensemble, si $\theta_i$ est fixé, alors les data non équivalents sont conditionnés par les choix possibles de $a \in \widehat{H}$. C'est également le cas pour le deuxième ensemble avec $\theta_i$ et $\tau_i$ fixés.

Finalement, on obtient une bijection entre $\mathrm{CC}_2^\bullet(H) \times \widehat{H} \times H^2(H, k^\times)$ et l'ensemble des 2-data non équivalents issus des deux ensembles ci-dessus, ce qui conclut la preuve. □

## 4.4 Retour au twist gradué

Pour terminer ce chapitre, revenons aux twists gradués.

**Proposition 4.4.1.** *Soit $(i, \alpha)$ une action cocentrale de $\mathbb{Z}_m$ sur un groupe fini $G$. Posons $H = G/i(\widehat{\mathbb{Z}_m})$, et fixons un 2-cocycle $\tau_0 : H \times H \to \widehat{\mathbb{Z}_m}$ tel que $G \simeq H \times_{\tau_0} \widehat{\mathbb{Z}_m}$ et un générateur $g$ de $\mathbb{Z}_m$. On définit un 2-cocycle $\tau : H \times H \to \mu_m$ par $\tau(x, y) = \tau_0(x, y)(g)$, et soit $\theta$ l'automorphisme de $H$ induit par $\alpha = \alpha_g$. Alors il existe $a : H \to \mu_m$ tel que $(H, \theta, a, \tau)$ soit un $m$-datum et $\mathcal{O}(G)^{i,\alpha} \simeq A_m(H, \theta, a, \tau)$.*

*Démonstration.*

On peut supposer sans perte de généralité que $G = H \times_{\tau_0} \widehat{\mathbb{Z}_m}$ et que $i$ est l'injection canonique. En effet, considérons l'isomorphisme $F : G \to H \times_{\tau_0} \widehat{\mathbb{Z}_m}$ rendant le diagramme suivant commutatif :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \widehat{\mathbb{Z}_m} & \xrightarrow{i} & G & \xrightarrow{\pi} & H & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle F} & & \| & & \\ 1 & \longrightarrow & \widehat{\mathbb{Z}_m} & \xrightarrow{i_0} & H \times_{\tau_0} \widehat{\mathbb{Z}_m} & \xrightarrow{\pi_0} & H & \longrightarrow & 1 \end{array}$$

où $\pi$ est la surjection canonique, et $i_0$ et $\pi_0$ désignent l'injection et la surjection canonique.

En utilisant l'isomorphisme d'algèbres de Hopf $\mathcal{O}(G) \simeq \mathcal{O}(H \times_{\tau_0} \widehat{\mathbb{Z}_m})$ induit par $F$, on obtient un isomorphisme $\mathcal{O}(G)^{i,\alpha} \simeq \mathcal{O}(H \times_{\tau_0} \widehat{\mathbb{Z}_m})^{i_0, F\alpha F^{-1}}$.

Rappelons de la partie 2.4, en particulier de la preuve du lemme 2.4.1, que $\alpha = \alpha_g$ est de la forme $\alpha = (\theta, \mu)$ avec $\theta \in \mathrm{Aut}(H)$ et $\mu : H \to \widehat{\mathbb{Z}_m}$ vérifiant :

$$\theta^m = \mathrm{id}, \ \prod_{i=0}^{m-1} \mu \circ \theta^i = 1, \ \tau_0 = \partial(\mu) \cdot (\tau_0 \circ (\theta \times \theta)).$$

Définissons à présent une application $a_0 : H \to \widehat{\mathbb{Z}_m}$ :

$$a_0 = \prod_{k=1}^{m-1} (\mu \circ \theta^{-k})^k.$$

On a alors :

$$\prod_{i=0}^{m-1} \tau_0 \circ (\theta^i \times \theta^i) = \prod_{i=0}^{m-1} \tau_0 \circ (\theta^{-i} \times \theta^{-i}) = \partial(a_0^{-1}) \text{ et } a_0 \circ \theta = a_0.$$

Définissons maintenant $a : H \to \mu_m$ par $a(x) = a_0(x)(g)$. On obtient les relations :

$$\theta^m = \mathrm{id},\ a \circ \theta = a,\ \prod_{i=0}^{m-1} \tau \circ (\theta^i \times \theta^i) = \partial(a^{-1}).$$

Ainsi, $(H, \theta, a, \tau)$ est un $m$-datum. Il reste à voir que $A_m(H, \theta, a, \tau) \simeq \mathcal{O}(H \times_{\tau_0} \widehat{\mathbb{Z}_m})^{i,\alpha}$.

Pour cela, notons en premier que la graduation de $\mathbb{Z}_m$ sur $\mathcal{O}(H \times_{\tau_0} \widehat{\mathbb{Z}_m})^{i,\alpha}$ est donnée par :

$$\mathcal{O}(H \times_{\tau_0} \widehat{\mathbb{Z}_m})_h^{i,\alpha} = \{\phi \in \mathcal{O}(H \times_{\tau_0} \widehat{\mathbb{Z}_m}) \mid \phi(x, \chi) = \chi(h)\phi(x, 1),\ \forall (x, \chi) \in H \times \hat{\mathbb{Z}}_m\}.$$

Posons :

$$u_g = \sum_{x \in H} \sum_{\chi \in \widehat{\mathbb{Z}_m}} \chi(g) e_{x,\chi} \in \mathcal{O}(H \times_{\tau_0} \widehat{\mathbb{Z}_m})_g^{i,\alpha}, \quad \text{et pour } x \in H,\ e'_x = \sum_{\chi \in \widehat{\mathbb{Z}_m}} e_{x,\chi} \in \mathcal{O}(H \times_{\tau_0} \widehat{\mathbb{Z}_m})_e^{i,\alpha}.$$

En utilisant le produit de $\mathcal{O}(H \times_{\tau_0} \widehat{\mathbb{Z}_m})^{i,\alpha}$, on voit que :

$$u_g e'_x = e'_{\theta(x)} u_g, \qquad u_g^m = a.$$

Ainsi, il existe un morphisme d'algèbres $A_m(H, \theta, a, \tau) \to \mathcal{O}(H \times_{\tau_0} \widehat{\mathbb{Z}_m})^{i,\alpha}$ qui envoie $e_x$ sur $e'_x$ et $g$ sur $u_g$, qui est, comme dans la preuve de la proposition 4.1.6, un isomorphisme d'algèbres de Hopf. □

*Remarque* 4.4.2. On dit qu'un $m$-datum $(H, \theta, a, \tau)$ est de type twist gradué si $\tau$ prend ses valeurs dans $\mu_m$ et si il existe $\mu : H \to \mu_m$ tel que

$$\prod_{i=0}^{m-1} \mu \circ \theta^i = 1, \qquad \tau = \partial(\mu) \cdot (\tau \circ (\theta \times \theta)), \qquad a = \prod_{k=1}^{m-1} (\mu \circ \theta^{-k})^k.$$

Le résultat précédent (et sa preuve) nous donne que si $(i, \alpha)$ est une action cocentrale de $\mathbb{Z}_m$ sur un groupe fini $G$, alors en posant $H = G/i(\widehat{\mathbb{Z}_m})$, on a $\mathcal{O}(G)^{i,\alpha} \simeq A_m(H, \theta, a, \tau)$ pour tout $m$-datum $(H, \theta, a, \tau)$ de type twist gradué.

Inversement, il n'est pas difficile de voir que si $(H, \theta, a, \tau)$ est un $m$-datum de type twist gradué, alors $A_m(H, \theta, a, \tau)$ est un twist gradué de $\mathcal{O}(H \times_\tau \mu_m)$.

Utilisons maintenant les considérations précédentes pour obtenir un nouveau résultat d'isomorphisme pour les twists gradués d'algèbres de fonctions des groupes finis $\mathbb{Z}_p$, où $p$ est un nombre premier. Commençons par un lemme.

**Lemme 4.4.3.** *Soit $(H, \theta, a, \tau)$ un $p$-datum, avec $p$ un nombre premier. Supposons que $H^2(H, k^\times) \simeq \mathbb{Z}_p$. Alors on a $[\tau] = [\tau \circ (\theta \times \theta)]$ dans $H^2(H, k^\times)$. Si de plus $\tau$ est à valeurs dans $\mu_p$ et $\mathrm{Hom}(H, \mathbb{Z}_p) = \{1\}$, alors on a également $[\tau] = [\tau \circ (\theta \times \theta)]$ dans $H^2(H, \mu_p)$.*

*Démonstration.*

On peut supposer que $\tau$ est non trivial, ainsi $[\tau]$ est un générateur de $H^2(H, k^\times)$. Le groupe $\mathrm{Aut}(H)$ agit par automorphisme sur le groupe cyclique $H^2(H, k^\times)$. Ainsi, il existe $l$ premier avec $p$ tel que $[\tau]^l = [\tau \circ (\theta \times \theta)]$.

L'hypothèse que $(H, \theta, a, \tau)$ est un $p$-datum nous donne :

$$[1] = \prod_{k=0}^{p-1} [\tau \circ (\theta^k \times \theta^k)] = \prod_{k=0}^{p-1} [\tau]^{l^k} = [\tau]^{\sum_{k=0}^{p-1} l^k}.$$

Puisque $p$ est premier et que $[\tau]$ est d'ordre $p$, on obtient que $l \equiv 1[p]$, et ainsi $[\tau] = [\tau \circ (\theta \times \theta)]$ dans $H^2(H, k^\times)$.

Avec les hypothèses supplémentaires que $\tau$ est à valeurs dans $\mu_p$ et que $\mathrm{Hom}(H, \mathbb{Z}_p) = \{1\}$, par le théorème des coefficients universels, on obtient que $H^2(H, \mathbb{Z}_p) \simeq \mathbb{Z}_p$ et la suite exacte induite par l'application $k^\times \to k^\times$ définie par $x \mapsto x^p$

$$1 \to \mathrm{Hom}(H, \mu_p) \to \mathrm{Hom}(H, k^\times) \to \mathrm{Hom}(H, k^\times) \to H^2(H, \mu_p) \to H^2(H, k^\times) \to H^2(H, k^\times)$$

assure que l'application naturelle $H^2(H, \mu_p) \to H^2(H, k^\times)$ est un isomorphisme, ce qui donne $[\tau] = [\tau \circ (\theta \times \theta)]$ dans $H^2(H, \mu_p)$. □

Nous arrivons enfin au résultat tant attendu suivant.

**Théorème 4.4.4.** *Soient $G$ un groupe fini de centre cyclique, $(i, \alpha)$ et $(j, \beta)$ des actions cocentrales de $\mathbb{Z}_p$ sur $G$, où $p$ est un nombre premier, et posons $H = G/i(\widehat{\mathbb{Z}_p}) = G/j(\widehat{\mathbb{Z}_p})$. Supposons que $\mathrm{Hom}(H, \mathbb{Z}_p) = \{1\}$ et que $H^2(H, k^\times)$ est trivial ou cyclique d'ordre $p$. Alors les assertions suivantes sont équivalentes :*

1. *les algèbres de Hopf $\mathcal{O}(G)^{i,\alpha}$ et $\mathcal{O}(G)^{j,\beta}$ sont isomorphes ;*
2. *les actions cocentrales $(i, \alpha)$ et $(j, \beta)$ sont équivalentes.*

*Démonstration.*

Tout d'abord, comme $Z(G)$ est cyclique, il possède un unique sous-groupe d'ordre donné, donc nécessairement $i(\widehat{\mathbb{Z}_p}) = j(\widehat{\mathbb{Z}_p})$. L'implication (2) $\Rightarrow$ (1) découle du lemme 2.2.5. Il reste donc à démontrer que (1) $\Rightarrow$ (2).

Supposons donc que les algèbres de Hopf $\mathcal{O}(G)^{i,\alpha}$ et $\mathcal{O}(G)^{j,\beta}$ soient isomorphes. Pour démontrer l'assertion (2), on peut se placer dans le cadre où $G = H \times_{\tau_0} \widehat{\mathbb{Z}_p}$ pour un 2-cocycle $\tau_0 : H \times H \to \widehat{\mathbb{Z}_p}$ et $i, j$ les injections canoniques. En effet, rappelons comme dans le début de la preuve de la proposition 4.4.1, dont nous garderons les notations, qu'en fixant un isomorphisme $F : G \to H \times_{\tau_0} \widehat{\mathbb{Z}_p}$, on obtient les isomorphismes suivants :

$$\mathcal{O}(G)^{i,\alpha} \simeq \mathcal{O}(H \times_{\tau_0} \widehat{\mathbb{Z}_m})^{i_0, F\alpha F^{-1}}, \qquad \mathcal{O}(G)^{j,\beta} \simeq \mathcal{O}(H \times_{\tau_0} \widehat{\mathbb{Z}_m})^{i_0, F\beta F^{-1}}$$

où $i_0$ est l'injection canonique.

Les actions cocentrales $(i, \alpha)$ et $(j, \beta)$ sont alors équivalentes si et seulement si les actions cocentrales $(i_0, F\alpha F^{-1})$ et $(i_0, F\beta F^{-1})$ le sont.

D'après la proposition 4.4.1, on a $\mathcal{O}(G)^{i,\alpha} \simeq A_p(H, \theta, a, \tau)$ et $\mathcal{O}(G)^{j,\beta} \simeq A_p(H, \theta', a', \tau)$, pour $\theta = \overline{\alpha_g}$, $\theta' = \overline{\beta_g}$ (on notera là encore par $f \mapsto \overline{f}$ le morphisme de groupes du lemme 2.4.1 de $\mathrm{Aut}_{i(\widehat{\Gamma})}(G)$ vers $\mathrm{Aut}(H)$), et $a, a' : H \to \mu_p$ tels que $(H, \theta, a, \tau)$ et $(H, \theta', a', \tau)$ soient des $p$-data, car $\tau$ est à valeurs dans $\mu_p$.

Puisque l'on a supposé que $A_p(H, \theta, a, \tau) \simeq A_p(H, \theta', a', \tau)$, et grâce au lemme 2.2.3, le théorème 4.2.12 fournit un automorphisme de groupes $f \in \mathrm{Aut}(H)$, $\varphi : H \to k^\times$ et $l$ premier avec $p$ tels que :

$$\theta'^l = f \circ \theta \circ f^{-1}, \qquad \prod_{k=0}^{l-1} \tau \circ (\theta'^{-k} \times \theta'^{-k}) = \tau \circ (f^{-1} \times f^{-1}) \cdot \partial(\varphi).$$

Le lemme précédent 4.4.2 assure que $[\tau \circ (\theta' \times \theta')] = [\tau]$, et ainsi on a $[\tau]^l = [\tau \circ (f^{-1} \times f^{-1})]$ dans $H^2(H, k^\times)$ et dans $H^2(H, \mu_p)$.

Ainsi, d'après le lemme 2.4.2, il existe $F \in \mathrm{Aut}(G)$ tel que $\beta_g^l = F^{-1} \circ \alpha_g \circ F$ et $F_{|\widehat{\mathbb{Z}_p}} = (-)^l$, ce qui signifie également que nos actions cocentrales sont équivalentes. On a ainsi montré l'implication (1) $\Rightarrow$ (2) et donc l'équivalence souhaitée. □

*Remarque* 4.4.5. Soit $(i, \alpha)$ une action cocentrale de $\mathbb{Z}_m$ (pour lequel on fixe un générateur $g$) sur un groupe fini $G$. Alors l'algèbre de Hopf $\mathcal{O}(G)^{i,\alpha}$ est non commutative si et seulement si $\theta$, l'automorphisme de $H = G/i(\mathbb{Z}_m)$ induit par $\alpha_g$, est non trivial. Ceci découle de la combinaison de la proposition 4.4.1 et de la proposition 4.2.8 (mais peut être démontré plus

directement en analysant les représentations de dimension 1 de $\mathcal{O}(G)^{p,\alpha}$). Par conséquent, dans le cadre du théorème 3.0.1 (ou du théorème 3.0.3 pour $m = 2$), il y a une bijection entre :

1. l'ensemble des classes d'isomorphisme d'algèbres de Hopf étant des twists gradués non commutatifs de $\mathcal{O}(G)$ par $\mathbb{Z}_m$,
2. l'ensemble des classes d'équivalence d'actions cocentrales de $\mathbb{Z}_m$ sur $G$ qui n'induisent pas l'identité sur $H$, où $H$ est le quotient de $G$ par son unique sous-groupe central d'ordre $m$,
3. l'ensemble des classes de faible équivalence d'actions cocentrales de $\mathbb{Z}_m$ sur $G$ qui ne sont pas faiblement équivalentes à l'action triviale.

Le deuxième ensemble est en bijection avec $\mathbb{X}_m^\bullet(G)$ (voir la fin de la partie 2.3) et pour $m = 2$, est aussi en bijection avec $\mathrm{CC}_2^\bullet(\mathrm{Aut}(H))$ (voir le lemme 2.4.1).

Sous les hypothèses du théorème 4.4.4, on obtient, pour $p$ premier, une bijection entre :

1. l'ensemble des classes d'isomorphisme d'algèbres de Hopf étant des twists gradués non commutatifs de $\mathcal{O}(G)$ par $\mathbb{Z}_p$,
2. l'ensemble des classes d'équivalence d'actions cocentrales de $\mathbb{Z}_p$ sur $G$ qui ne sont pas équivalentes à l'action triviale.

Le dernier ensemble est, d'après le lemme 2.3.1, en bijection avec $\mathbb{X}_p^\bullet(G)$ (voir la fin de la partie 2.3).

# Chapitre 5

# Exemples

Dans cette partie, nous utilisons les résultats de classification obtenus précédemment sur les exemples concrets cités dans l'introduction.

## 5.1 Groupes spéciaux linéaires sur un corps fini

On commence par examiner les twists gradués des groupes linéaires sur un corps fini.

**Théorème 5.1.1.** *Soit $q = p^\alpha$, avec $p \geq 3$ un nombre premier et $\alpha \geq 1$. Soit $n \geq 2$ un entier pair. L'ensemble des classes d'isomorphisme d'algèbres de Hopf non commutatives étant des twists gradués de $\mathcal{O}(\mathrm{SL}_n(\mathbb{F}_q))$ par $\mathbb{Z}_2$ est en bijection avec l'ensemble $\mathbb{X}_2^\bullet(\mathrm{SL}_n(\mathbb{F}_q))$.*

*Démonstration.*

D'après le théorème 3.0.3 et la remarque 4.4.5, l'ensemble des classes d'isomorphisme d'algèbres de Hopf non commutatives étant des twists gradués de $\mathcal{O}(\mathrm{SL}_n(\mathbb{F}_q))$ par $\mathbb{Z}_2$ est en bijection avec l'ensemble des classes d'équivalence d'actions cocentrales de $\mathbb{Z}_2$ sur $\mathrm{SL}_n(\mathbb{F}_q)$ n'induisant pas l'identité sur $H$ où $H$ est le quotient de $\mathrm{SL}_n(\mathbb{F}_q)$ par son unique sous-groupe central d'ordre 2. Ce dernier ensemble est lui même en bijection avec $\mathbb{X}_2^\bullet(\mathrm{SL}_n(\mathbb{F}_q))$.

Sous réserve de pouvoir appliquer le théorème 3.0.3, on aura donc le résultat annoncé. Il s'agit donc de voir que le centre de $\mathrm{SL}_n(\mathbb{F}_q)$ est cyclique, que $\mathrm{Hom}(H, \mathbb{Z}_2) = \{\mathbb{1}\}$ et que $H^2(H, k^\times)$ est cyclique.

La première condition est toujours vérifiée puisque le centre de $\mathrm{SL}_n(\mathbb{F}_q)$ est isomorphe au sous-groupe des racines n-ième de l'unité dans $\mathbb{F}_q$, que l'on note $\mu_n(\mathbb{F}_q)$, qui est cyclique d'ordre $\mathrm{PGCD}(n, q-1)$. Comme $n$ et $q-1$ sont pairs, ce sous-groupe est d'ordre pair. Il possède donc un unique sous-groupe d'ordre 2. On pose alors $H := \mathrm{SL}_n(\mathbb{F}_q)/\{\pm 1\}$.

On considère à partir de maintenant, le cas où $n = 2$ et $q = 3$ de manière isolé, car le raisonnement diffère.

Dans ce cas, $\mu_2(\mathbb{F}_3)$ est d'ordre 2 donc $\mu_2(\mathbb{F}_3) \simeq \{\pm 1\}$. Ainsi, $H = \mathrm{SL}_2(\mathbb{F}_3)/\mu_2(\mathbb{F}_3) = \mathrm{PSL}_2(\mathbb{F}_3) \simeq A_4$.

Si $f$ est un morphisme de $A_4$ dans $\mathbb{Z}_2$, alors $Ker(f)$ est un sous-groupe distingué de $A_4$. Comme $A_4$ contient les 3-cycles qui sont d'ordre 3 et que $\mathbb{Z}_2$ ne contient pas d'éléments d'ordre 3, $Ker(f)$ contient ces 3-cycles. Donc $|Ker(f)| \geq 9$. Par ailleurs, $Ker(f)$ est un sous-groupe de $A_4$ donc $|Ker(f)| \mid 12$, ainsi on obtient que $Ker(f) = A_4$ et donc $\mathrm{Hom}(A_4, \mathbb{Z}_2) = \{\mathbb{1}\}$.

Pour la dernière condition, on sait que $H_2(\mathrm{PSL}_2(\mathbb{F}_3), \mathbb{Z}) \simeq \mathbb{Z}_2$. En utilisant le théorème des coefficients universels, on obtient que $H^2(\mathrm{PSL}_2(\mathbb{F}_3), \mathbb{Z}_2) \simeq \mathbb{Z}_2$ qui est donc bien cyclique.

Plaçons nous à présent dans le cas où $n > 2$ et $q \neq 3$. Le groupe $\mathrm{SL}_n(\mathbb{F}_q)$ est parfait, c'est-à-dire que son groupe dérivé est également $\mathrm{SL}_n(\mathbb{F}_q)$. Or on sait que l'indice de $D(\mathrm{SL}_n(\mathbb{F}_q))$ dans $\mathrm{SL}_n(\mathbb{F}_q)$ correspond au nombre de représentations irréductibles de dimension 1 de $\mathrm{SL}_n(\mathbb{F}_q)$. Comme cet indice vaut 1 ici, et que $\mathbb{Z}_2$ s'injecte dans $k^\times$, on obtient que $\mathrm{Hom}(H, \mathbb{Z}_2) = \{\mathbb{1}\}$.

Par ailleurs, sous nos hypothèses, $H^2(\mathrm{PSL}_n(\mathbb{F}_q), k^\times)$ est cyclique (voir par exemple la référence [14, chapitre 7]). Comme $\mathrm{PSL}_n(\mathbb{F}_q)$ est un quotient de $H$, en appliquant le théorème d'Iwahori et Matsumoto [15], on obtient que $H^2(H, k^\times)$ est aussi cyclique.

Grâce au raisonnement détaillé en début de preuve, on obtient la bijection d'ensemble souhaitée en appliquant le théorème 3.0.3 et la remarque 4.4.5. □

**Théorème 5.1.2.** *Soit $q = p^\alpha$, avec $p$ un nombre premier et $\alpha \geq 1$. Soit un entier $n \geq 2$ et supposons que $m = \mathrm{PGCD}(n, q-1)$ est un nombre premier et que $(n, q) \notin \{(2, 9), (3, 4)\}$. Alors l'ensemble des classes d'isomorphisme d'algèbres de Hopf étant des twists gradués de $\mathcal{O}(\mathrm{SL}_n(\mathbb{F}_q))$ par $\mathbb{Z}_m$ est en bijection avec l'ensemble $\mathbb{X}^\bullet_m(\mathrm{SL}_n(\mathbb{F}_q))$.*

*Démonstration.*

Comme dans la preuve précédente, on rappelle que le centre de $\mathrm{SL}_n(\mathbb{F}_q)$ correspond au sous-groupe $\mu_n(\mathbb{F}_q)$, cyclique d'ordre $m = \mathrm{PGCD}(n, q-1)$.

On a toujours $\mathrm{Hom}(\mathrm{PSL}_n(\mathbb{F}_p), \mathbb{Z}_m)$ trivial, et $H^2(\mathrm{PSL}_n(\mathbb{F}_q), k^\times) \simeq \mathbb{Z}_m$ sous nos hypothèses (voir par exemple la référence [14, chapter 7]). Par conséquent, le théorème 4.4.4 et la remarque 4.4.5 donnent la bijection annoncée. □

Précisons maintenant pour $n = 2$, les résultats obtenus dans le cas d'extensions abéliennes cocentrales.

**Théorème 5.1.3.** *Soit $p \geq 3$ un nombre premier.*

1. *Il y a exactement 2 classes d'isomorphisme d'algèbres de Hopf non commutatives étant des twists gradués de $\mathcal{O}(\mathrm{SL}_2(\mathbb{F}_p))$ par $\mathbb{Z}_2$.*
2. *Si $p \geq 5$, il y a exactement 4 classes d'isomorphisme d'algèbres de Hopf non commutatives s'insérant dans une extension abélienne cocentrale $k \to \mathcal{O}(\mathrm{PSL}_2(\mathbb{F}_p)) \to A \to k\mathbb{Z}_2 \to k$.*

*Démonstration.*

Le théorème 5.1.1 assure qu'il y a une bijection entre l'ensemble des classes d'isomorphisme d'algèbres de Hopf non commutatives étant des twists gradués de $\mathcal{O}(\mathrm{SL}_2(\mathbb{F}_p))$ par $\mathbb{Z}_2$ et $\mathbb{X}_2^\bullet(\mathrm{SL}_2(\mathbb{F}_p))$. Il s'agit donc de déterminer le cardinal de l'ensemble $\mathbb{X}_2^\bullet(\mathrm{SL}_2(\mathbb{F}_p))$.

Tous les automorphismes de $\mathrm{SL}_2(\mathbb{F}_p)$ sont obtenus comme conjugaison par une matrice de $\mathrm{GL}_2(\mathbb{F}_p)$ : si $\theta \in \mathrm{Aut}(\mathrm{SL}_2(\mathbb{F}_p))$ alors il existe $M \in \mathrm{GL}_2(\mathbb{F}_p)$ tel que $\theta = \mathrm{ad}(M)$ (voir par exemple la référence [8]).

On constate qu'il y a deux classes d'équivalence dans $\mathbb{X}_2^\bullet(\mathrm{SL}_2(\mathbb{F}_p))$, représentées par les automorphismes :

$$\mathrm{ad}\left(\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right), \qquad \mathrm{ad}\left(\begin{pmatrix} 0 & \lambda \\ 1 & 0 \end{pmatrix}\right)$$

où $\lambda$ est un élément fixé de $\mathbb{F}_p^*$ tel que $\lambda \notin (\mathbb{F}_p^*)^2$. Ceci démontre la première assertion.

Pour $p \geq 5$, on a $\widehat{\mathrm{PSL}_2(\mathbb{F}_p)} = \{1\}$.

De plus, $Z(\mathrm{PSL}_2(\mathbb{F}_p)) = \{1\}$ et $H^2(\mathrm{PSL}_2(\mathbb{F}_p), k^\times) \simeq \mathbb{Z}_2$.

On peut donc appliquer le théorème 4.3.1 dans le cas où $m = 2$.

Ainsi, l'ensemble des classes d'isomorphisme d'algèbres de Hopf non commutatives s'insérant dans une extension comme dans l'énoncé, est en bijection avec l'ensemble :

$$\mathrm{CC}_2^\bullet(\mathrm{Aut}(\mathrm{PSL}_2(\mathbb{F}_p))) \times H^2(\mathrm{PSL}_2(\mathbb{F}_p), k^\times).$$

On sait que dans le cas $m = 2$ les ensembles $\mathrm{CC}_2^\bullet(\mathrm{Aut}(\mathrm{PSL}_2(\mathbb{F}_p)))$ et $\mathbb{X}_2^\bullet(\mathrm{SL}_2(\mathbb{F}_p))$ sont en bijection. En réutilisant les résultats montrés dans la première assertion, on a :

$$|\mathbb{X}_2^\bullet(\mathrm{SL}_2(\mathbb{F}_p))| = 2,$$

et donc $|\mathrm{CC}_2^\bullet(\mathrm{Aut}(\mathrm{PSL}_2(\mathbb{F}_p))) \times H^2(\mathrm{PSL}_2(\mathbb{F}_p), k^\times)| = 2 \times 2 = 4$. D'où le résultat. □

## 5.2 Groupes symétriques et alternés

Discutons à présent d'exemples liés aux groupes symétriques et aux groupes alternés. Commençons par le cas des groupes alternés et de leurs revêtements de Schur (voir par exemple [14]).

**Théorème 5.2.1.** *Soient $n \geq 4$ et $\widetilde{A_n}$ l'unique revêtement de Schur du groupe alterné $A_n$.*

1. *L'ensemble des classes d'isomorphisme d'algèbres de Hopf non commutatives étant des twists gradués de $\mathcal{O}(\widetilde{A_n})$ par $\mathbb{Z}_2$ est en bijection avec $\mathrm{CC}_2^\bullet(\mathrm{Aut}(A_n))$. Pour $n \neq 6$, il y en a exactement $\lfloor \frac{n}{2} \rfloor$.*
2. *Pour $n = 5$ ou $n \geq 8$, l'ensemble des classes d'isomorphisme d'algèbres de Hopf non commutatives s'insérant dans une extension abélienne cocentrale $k \to \mathcal{O}(A_n) \to A \to k\mathbb{Z}_2 \to k$ est en bijection avec l'ensemble $\mathrm{CC}_2^\bullet(\mathrm{Aut}(A_n)) \times \mathbb{Z}_2$. Il y en a exactement $2\lfloor \frac{n}{2} \rfloor$.*

*Démonstration.*

Dans tous les cas $\mathbb{Z}_2 \subset Z(\widetilde{A_n})$, le centre $Z(\widetilde{A_n})$ est cyclique, et $H^2(A_n, k^\times)$ est cyclique (isomorphe à $\mathbb{Z}_6$ pour $n = 6, 7$ et à $\mathbb{Z}_2$ dans les autres cas).

De plus, on a $\mathrm{Hom}(A_n, \mathbb{Z}_2) = \{1\}$, ainsi, la première assertion est une conséquence directe de la remarque 4.4.5.

En effet, nous sommes dans la situation du théorème 3.0.3. On a donc une bijection entre :

1. l'ensemble des classes d'isomorphisme d'algèbres de Hopf non commutatives étant des twists gradués de $\mathcal{O}(\widetilde{A_n})$ par $\mathbb{Z}_2$,
2. l'ensemble des classes d'équivalence d'actions cocentrales de $\mathbb{Z}_2$ sur $\widetilde{A_n}$ qui n'induisent pas l'identité sur $A_n$, le quotient de $\widetilde{A_n}$ par son unique sous-groupe central d'ordre 2.

Le second ensemble est en bijection avec $\mathbb{X}_2^\bullet(\widetilde{A_n})$, et dans le cas $m = 2$, également en bijection avec $\mathrm{CC}_2^\bullet(\mathrm{Aut}(A_n))$. D'où le premier résultat.

On a $\mathrm{CC}_2^\bullet(\mathrm{Aut}(A_n)) = \mathrm{CC}_2^\bullet(\mathrm{Aut}(S_n))$, et lorsque $n \neq 6$, tous les automorphismes de $S_n$ sont intérieurs et on sait que $\mathrm{Int}(S_n) \simeq S_n$. Ainsi, $\mathrm{CC}_2^\bullet(\mathrm{Aut}(A_n)) \simeq \mathrm{CC}_2^\bullet(S_n)$.

On rappelle également pour déterminer $\mathrm{CC}_2^\bullet(S_n)$ les faits connus suivants :

— Les éléments de $S_n$ d'ordre 2 sont les produits de transpositions à supports disjoints.

— Une permutation $\sigma$ de $S_n$ est conjuguée à toute permutation dont la décomposition en produit de cycles à supports disjoints a la même structure que celle de $\sigma$ (même nombre de cycles de chaque longueur).

Finalement les classes de conjugaison d'ordre 2 correspondent à la classe des transpositions, la classe des produits de deux transpositions à supports disjoints, la classe des produits de trois transpositions à supports disjoints... suivant la valeur de $n$. D'où $|\mathrm{CC}_2^\bullet(S_n)| = \lfloor \frac{n}{2} \rfloor$.

Pour $n = 5$ ou $n \geq 8$, on a de plus que $H^2(A_n, k^\times) \simeq \mathbb{Z}_2$, et $\widehat{A_n} = \{1\}$, et puisque $Z(A_n) = \{1\}$, le résultat découle du théorème 4.3.1. L'ensemble étudié est alors isomorphe à $\mathrm{CC}_2^\bullet(\mathrm{Aut}(A_n)) \times H^2(A_n, k^\times) \simeq \mathrm{CC}_2^\bullet(\mathrm{Aut}(A_n)) \times \mathbb{Z}_2$, de cardinal $2\lfloor \frac{n}{2} \rfloor$. Ce qui termine la preuve de la deuxième assertion. □

**Théorème 5.2.2.** *Supposons que $n \neq 6$.*

1. *Il y a exactement $4\lfloor \frac{n}{2} \rfloor$ classes d'isomorphisme d'algèbres de Hopf non commutatives s'insérant dans une extension abélienne cocentrale $k \to \mathcal{O}(S_n) \to A \to k\mathbb{Z}_2 \to k$.*
2. *Soit $G$ un groupe s'insérant dans une extension cocentrale $1 \to \mathbb{Z}_2 \to G \to S_n \to 1$. Il y a exactement $2\lfloor \frac{n}{2} \rfloor$ classes d'isomorphisme d'algèbres de Hopf non commutatives étant des twists gradués de $\mathcal{O}(G)$ par $\mathbb{Z}_2$.*

*Démonstration.*

Rappelons que lorsque $n \neq 6$, tous les automorphismes de $S_n$ sont intérieurs. De plus, on a : $\widehat{S_n} \simeq \mathbb{Z}_2 \simeq H^2(S_n, k^\times)$ et $Z(S_n) = \{1\}$.

Ainsi en appliquant le théorème 4.3.4, on obtient une bijection entre l'ensemble des classes d'isomorphisme d'algèbres de Hopf $A$ non commutatives s'insérant dans une extension abélienne cocentrale $k \to \mathcal{O}(S_n) \to A \to k\mathbb{Z}_2 \to k$, et l'ensemble $\mathrm{CC}_2^\bullet(S_n) \times \widehat{S_n} \times H^2(S_n, k^\times)$.

Rappelons que $\mathrm{CC}_2^\bullet(S_n)$ correspond à l'ensemble des classes de conjugaison d'éléments d'ordre 2 de $S_n$. On a déjà effectué ce calcul dans la preuve du théorème 5.2.1. Donc $|\mathrm{CC}_2^\bullet(S_n)| = \lfloor \frac{n}{2} \rfloor$.

Pour conclure la preuve de l'assertion (1), l'ordre de $\mathrm{CC}_2^\bullet(S_n) \times \widehat{S_n} \times H^2(S_n, k^\times)$ vaut $\lfloor \frac{n}{2} \rfloor \times 2 \times 2 = 4\lfloor \frac{n}{2} \rfloor$, d'où le résultat.

Soit $G$ un groupe s'insérant dans une extension cocentrale $1 \to \mathbb{Z}_2 \to G \to S_n \to 1$. D'après la proposition 4.4.1, un twist gradué de $\mathcal{O}(G)$ est isomorphe à l'algèbre $A_2(S_n, \theta, a, \tau)$ où $\tau : S_n \times S_n \to \mathbb{Z}_2$ est un 2-cocycle construit canoniquement à partir de l'extension centrale $1 \to \mathbb{Z}_2 \to G \to S_n \to 1$.

Le lemme 4.3.3 s'applique ici d'après les rappels fait au-dessus. Comme $\tau$ est fixé, que l'on a deux possibilités pour $a$ et $\lfloor \frac{n}{2} \rfloor$ pour $\theta$ comme décrit ci-dessus, à équivalence près, on obtient au plus $2\lfloor \frac{n}{2} \rfloor$ classes d'isomorphisme de twists gradués non commutatifs de $\mathcal{O}(G)$.

Inversement, si l'on considère un 2-datum $(S_n, \theta, a, \tau)$, avec $\tau$ comme précédemment, il faut vérifier que l'algèbre de Hopf $A_2(S_n, \theta, a, \tau)$ est bien isomorphe à un twist gradué de $\mathcal{O}(G)$.

Comme tous les automorphismes de $S_n$ sont intérieurs, il existe $x \in S_n$ tel que $\theta = ad(x)$. D'après le lemme 2.4.3, il existe $\mu : S_n \to \mu_2$ tel que $\tau \cdot \tau \circ (\theta \times \theta) = \partial(\mu)$.

Comme $a$ est tel que $\tau \cdot \tau \circ (\theta \times \theta) = \partial(a^{-1})$, alors $a^{-1}$ et $\mu$ différent d'un élément de $\widehat{S_n}$ donc $\mu a \in \widehat{S_n}$. Ainsi $\mu^2 a^2 = \mathbb{1}$ donc $a^2 = \mathbb{1}$ (et $\mu^2 = \mathbb{1}$).

Ainsi notre 2-datum $(S_n, \theta, a, \tau)$ est du type twist gradué comme expliqué dans la remarque 4.4.2. On sait donc que $A_2(S_n, \theta, a, \tau)$ est un twist gradué de $\mathcal{O}(S_n \times_\tau \mu_2) \simeq \mathcal{O}(G)$. Ce qui conclut la preuve. □

## 5.3 Le groupe alterné $A_5$

Le groupe alterné $A_5$ fait parti des cas d'étude précédents, mais le résultat de [3] cité ci-dessous lui confère un intérêt particulier :

Toute algèbre de Hopf $A$ co-semisimple, de dimension finie, ayant un comodule $V$ fidèle de dimension 2 avec $V \otimes V^* \simeq V^* \otimes V$, s'insère dans une extension abélienne cocentrale

$$k \to \mathcal{O}(H) \to A \to k\mathbb{Z}_m \to k$$

pour $m \geq 2$ et un groupe polyédral $H \in \{A_4,\ S_4,\ A_5,\ D_{2n}\}$. En utilisant le théorème 4.3.1 et la description simple des classes de conjugaison de $S_5 \simeq \mathrm{Aut}(A_5)$, nous contribuons à cette situation par le théorème suivant.

**Théorème 5.3.1.** *Soit $m \geq 2$ et posons $N$ le nombre de classes d'isomorphisme d'algèbres de Hopf non commutatives $A$ s'insérant dans une extension abélienne cocentrale $k \to \mathcal{O}(A_5) \to A \to k\mathbb{Z}_m \to k$. Selon la valeur de* $\mathrm{PGCD}(m, 120)$*, la valeur de $N$ est la suivante :*

1. $N = 0$ *si* $\mathrm{PGCD}(m, 120) = 1$.
2. $N = 4$ *si* $\mathrm{PGCD}(m, 120) = 2$.
3. $N = 1$ *si* $\mathrm{PGCD}(m, 120) = 3, 5$.
4. $N = 6$ *si* $\mathrm{PGCD}(m, 120) = 4, 8$.
5. $N = 8$ *si* $\mathrm{PGCD}(m, 120) = 6, 20, 40$.
6. $N = 6$ *si* $\mathrm{PGCD}(m, 120) = 10$.
7. $N = 10$ *si* $\mathrm{PGCD}(m, 120) = 12, 24$.
8. $N = 2$ *si* $\mathrm{PGCD}(m, 120) = 15$.
9. $N = 10$ *si* $\mathrm{PGCD}(m, 120) = 30$.
10. $N = 12$ *si* $\mathrm{PGCD}(m, 120) = 60, 120$.

*Démonstration.*

On sait que $H^2(A_5, k^\times) \simeq \mathbb{Z}_2$, et $\widehat{A_5} = \{1\} = Z(A_5)$. En appliquant le théorème 4.3.1, on obtient que l'ensemble des classes d'isomorphisme d'algèbres de Hopf $A$ non commutatives s'insérant dans une extension comme dans l'énoncé est en bijection avec :

— $\mathrm{CC}_m^\bullet(\mathrm{Aut}(A_5)) \times H^2(A_5, k^\times)$ si $m$ est pair,

— $\mathrm{CC}_m^\bullet(\mathrm{Aut}(A_5))$ si $m$ est impair.

Ainsi $N$ vaut :

— $|\mathrm{CC}_m^\bullet(\mathrm{Aut}(A_5))| \times 2 = |\mathrm{CC}_m^\bullet(S_5)| \times 2$ si $m$ est pair,

— $|\mathrm{CC}_m^\bullet(\mathrm{Aut}(A_5))| = |\mathrm{CC}_m^\bullet(S_5)|$ si $m$ est impair.

Il s'agit donc de déterminer le nombre d'éléments de $\mathrm{CC}_m^\bullet(S_5)$ suivant les valeurs de $m$. On rappelle que $S_5$ possède 7 classes de conjugaison dont les représentants sont :

$$\mathrm{id}, (12), (123), (12)(34), (1234), (123)(45), (12345).$$

1. Si $\mathrm{PGCD}(m, 120) = 1$ alors $m$ est impair. De plus, pour tout $x \in S_5$ non trivial, on ne peut pas avoir $x^m = 1$. Donc l'ensemble $\mathrm{CC}_m^\bullet(S_5)$ est vide donc $N = 0$.
2. Si $\mathrm{PGCD}(m, 120) = 2$, alors $m$ est pair et n'est pas un multiple de 4 ou 6. Les deux seuls éléments de $\mathrm{CC}_m^\bullet(S_5)$ sont $(12)$ et $(12)(34)$. Donc $N = 2 \times 2 = 4$.
3. Si $\mathrm{PGCD}(m, 120) = 3, 5$, alors $m$ est impair. Il n'y a qu'un seul élément dans $\mathrm{CC}_m^\bullet(S_5)$ étant $(123)$ si $\mathrm{PGCD}(m, 120) = 3$ et $(12345)$ si $\mathrm{PGCD}(m, 120) = 5$. Donc $N = 1$.
4. Si $\mathrm{PGCD}(m, 120) = 4, 8$, alors $m$ est pair. Il y a 3 éléments dans $\mathrm{CC}_m^\bullet(S_5)$ qui sont dans les deux cas : $(12), (12)(34), (1234)$. Donc $N = 2 \times 3 = 6$.
5. Si $\mathrm{PGCD}(m, 120) = 6, 20, 40$ alors $m$ est pair. Dans le cas où $\mathrm{PGCD}(m, 120) = 6$ il y a 4 éléments : $(12), (12)(34), (123), (123)(45)$. Dans le cas où $\mathrm{PGCD}(m, 120) = 20$ ou 40, il y a 4 éléments : $(12), (12)(34), (1234), (12345)$. Dans tous les cas, $N = 2 \times 4 = 8$.
6. Si $\mathrm{PGCD}(m, 120) = 10$, alors $m$ est pair. Il y a 3 éléments : $(12), (12)(34), (12345)$. Donc $N = 2 \times 3 = 6$.
7. Si $\mathrm{PGCD}(m, 120) = 12, 24$, alors $m$ est pair. Il y a 5 éléments : $(12), (12)(34), (123), (1234), (123)(45)$. Donc $N = 2 \times 5 = 10$.
8. Si $\mathrm{PGCD}(m, 120) = 15$, alors $m$ est impair. Il y a 2 éléments : $(123), (12345)$. Donc $N = 2$.
9. Si $\mathrm{PGCD}(m, 120) = 30$, alors $m$ est pair. Il y a 5 éléments : $(12), (12)(34), (123), (123)(45), (12345)$. Donc $N = 2 \times 5 = 10$.
10. Si $\mathrm{PGCD}(m, 120) = 60, 120$, alors $m$ est pair. Il y a 6 éléments : $(12), (12)(34), (123), (123)(45), (12345), (1234)$. Donc $N = 2 \times 6 = 12$.

□

Bien sûr, le théorème précédent ne donne aucune information à propos de la possibilité pour une algèbre de Hopf issue du théorème de posséder un comodule fidèle de dimension 2.

## 5.4 Groupes diédraux $D_n$

On considère dans cette partie le cas des algèbres de Hopf s'insérant dans une extension abélienne cocentrale

$$k \to \mathcal{O}(D_n) \to A \to k\mathbb{Z}_2 \to k$$

avec $D_n$ le groupe diédral d'ordre $2n$. La structure de groupe de $D_n$ est moins riche que celle des groupes des paragraphes précédents, mais la situation avec les extensions d'algèbres de Hopf comme ci-dessus est dans ce cas beaucoup plus complexe.

**Notation**

Comme à l'habitude, le groupe $D_n$ est défini par une présentation : des générateurs $r$, $s$ et des relations $r^n = 1 = s^2$, $sr = r^{n-1}s$. De plus, ses automorphismes sont tous de la forme $\Psi_{k,l}$, $(k,l) \in \mathbb{Z}/n\mathbb{Z} \times U(\mathbb{Z}/n\mathbb{Z})$, défini par :

$$\Psi_{k,l}(r) = r^l, \quad \Psi_{k,l}(s) = sr^k.$$

Un tel automorphisme $\Psi_{k,l}$ est d'ordre 2 exactement lorsque $(k,l) \neq (0,1)$, $k(l+1) = 0$ (dans $\mathbb{Z}/n\mathbb{Z}$) et $l^2 = 1$. Rappelons les résultats bien connus suivants :

$$\text{Si } n \text{ est impair, alors } Z(D_n) = \{1\}, \qquad H^2(D_n, k^\times) = \{1\}, \qquad \widehat{D_n} \simeq \mathbb{Z}_2.$$

$$\text{Si } n \text{ est pair, alors } Z(D_n) = \{1, r^{n/2}\}, \qquad H^2(D_n, k^\times) \simeq \mathbb{Z}_2, \qquad \widehat{D_n} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2.$$

On introduit également un lemme qui sera utile dans plusieurs démonstrations.

**Lemme 5.4.1.** *Soient $p$ et $q$ des nombres premiers distincts, et $r, s \in \mathbb{Z}$. Alors il existe $a, b \in \mathbb{Z}$ inversibles dans $\mathbb{Z}/p^r q^s\mathbb{Z}$ tels que $ap^r + bq^s = 1$.*

*Démonstration.*

Comme $p$ et $q$ sont premiers et distincts, $\mathrm{PGCD}(p^r, q^s) = 1$. D'après le théorème de Bézout, il existe $a_0, b_0 \in \mathbb{Z}$ tels que $a_0 p^r + b_0 q^s = 1$.

On cherche $a, b \in \mathbb{Z}$, inversibles dans $\mathbb{Z}/p^r q^s\mathbb{Z}$, solutions de l'équation $ap^r + bq^s = 1$.

Ainsi $a$ et $b$ sont de la forme : $a = a_0 + lp^r$ et $b = b_0 - lq^s$, avec $l \in \mathbb{Z}$.

On cherche $l \in \mathbb{Z}$ tel que $\mathrm{PGCD}(a, p^r q^s) = 1$ et $\mathrm{PGCD}(b, p^r q^s) = 1$. Le théorème de Bézout fournit également que $\mathrm{PGCD}(a_0, q^s) = 1$ et $\mathrm{PGCD}(b_0, q^s) = 1$. Cela revient donc à chercher $a, b$ tels que $\mathrm{PGCD}(a, p^r) = 1$ et $\mathrm{PGCD}(b, q^s) = 1$, c'est-à-dire tels que $\mathrm{PGCD}(a, p) = 1$ et $\mathrm{PGCD}(b, q) = 1$.

Distinguons les différents cas de figure.

— Si $p \nmid a_0$ et $q \nmid b_0$ : alors les $a_0$ et $b_0$ trouvés via le théorème de Bézout conviennent. On prend $a = a_0$ et $b = b_0$.

— Si $p \mid a_0$ et $q \nmid b_0$ : alors $b_0 \in U(\mathbb{Z}/p^r q^s \mathbb{Z})$. Prenons $l = q$. Alors $a = a_0 + q^{s+1}$ et $b = b_0 - qp^r$. Il est facile de vérifier que $p \nmid a$ et $q \nmid b$.

— Si $p \mid a_0$ et $q \mid b_0$ : alors prenons $l = 1$. Dans ce cas, $a = a_0 + q^s$ et $b = b_0 - p^r$. De même, il est facile de vérifier que $p \nmid a$ et $q \nmid b$.

— Si $p \nmid a_0$ et $q \mid b_0$ : alors $a_0 \in U(\mathbb{Z}/p^r q^s \mathbb{Z})$. Prenons $l = p$. Dans ce cas, $a = a_0 + pq^s$ et $b = b_0 - p^{r+1}$. De même, il est facile de vérifier que $p \nmid a$ et $q \nmid b$.

Ainsi, il est toujours possible de trouver $a, b \in \mathbb{Z}$ inversibles dans $\mathbb{Z}/p^r q^s \mathbb{Z}$ tels que $ap^r + bq^s = 1$. □

### 5.4.1 Le cas où $n$ est impair.

Ici la situation est très simple, puisque nous sommes dans le cadre du corollaire 4.3.2 : en effet, pour $m \geq 1$, on a une bijection entre l'ensemble des classes d'isomorphisme d'algèbres de Hopf non commutatives $A$ s'insérant dans une extension abélienne cocentrale

$$k \to \mathcal{O}(D_n) \to A \to k\mathbb{Z}_m \to k$$

et

— si $m$ est impair, l'ensemble $\mathrm{CC}_m^\bullet(\mathrm{Aut}(D_n))$ ;

— si $m$ est pair, l'ensemble $\mathrm{CC}_m^\bullet(\mathrm{Aut}(D_n)) \times \widehat{D_n}$.

Comme conséquence immédiate, on obtient le théorème suivant.

**Théorème 5.4.2.** *Soit $n \geq 3$ un entier impair et définissons $e_n$ comme le nombre de classes d'isomorphisme d'algèbres de Hopf $A$ non commutatives, s'insérant dans une extension abélienne cocentrale $k \to \mathcal{O}(D_n) \to A \to k\mathbb{Z}_2 \to k$.*

— *Si $n = p^r$ avec $p$ premier impair et $r \geq 1$, alors $e_n = 2$.*

— *Si $n = p^r q^s$, avec $p, q$ deux nombres premiers impairs distincts et $r, s \geq 1$, alors $e_n = 6$.*

*Démonstration.*

L'introduction de ce paragraphe implique que $e_n$ est le double du nombre de classes de conjugaison d'éléments d'ordre 2 de $\mathrm{Aut}(D_n)$, que l'on va calculer dans chacun des deux cas.

**Cas 1 : $n = p^r$** On commence par déterminer les éléments d'ordre 2 de $\mathrm{Aut}(D_n)$, c'est-à-dire les $\Psi_{k,l}$ tels que $(k, l) \in \mathbb{Z}/p^r\mathbb{Z} \times U(\mathbb{Z}/p^r\mathbb{Z})$, $(k, l) \neq (0, 1)$, $l^2 = 1$ et $k(l+1) = 0$ (dans $\mathbb{Z}/p^r\mathbb{Z}$).

Les éléments d'ordre 2 de $U(\mathbb{Z}/p^r\mathbb{Z})$ sont 1 et $-1$.

Si $l = 1$ alors $k(l+1) = 2k$. Il faut donc que $p^r \mid 2k$ avec $\mathrm{PGCD}(p^r, 2) = 1$. Donc $k = 0[p^r]$, ce qui est impossible. Donc $l \neq 1$.

Ainsi $l = -1$. La condition $k(l+1) = 0$ est vérifiée pour tout $k \in Z/p^r\mathbb{Z}$. Les $\Psi_{k,l}$ d'ordre 2 sont donc de la forme $\Psi_{k,-1}$ avec $k \in Z/p^r\mathbb{Z}$.

Il reste à déterminer les représentants à équivalence près.

Or on a : $\mathrm{cl}(\Psi_{0,-1}) = \{\Psi_{2i,-1} \mid i \in Z/p^r\mathbb{Z}\}$. Comme $n$ est impair, 2 est inversible, et donc il n'y a qu'une seule classe de conjugaison : $\mathrm{cl}(\Psi_{0,-1})$.

Finalement, $e_{p^r} = 2 \times 1 = 2$.

**Cas 2 : $n = p^r q^s$** De même, on cherche les $\Psi_{k,l}$ d'ordre 2. Comme $p$ et $q$ sont des nombres premiers distincts, on a $\mathrm{PGCD}(p^r, q^s) = 1$. D'après le lemme 5.4.1, il existe $a, b \in \mathbb{Z}$ inversibles dans $\mathbb{Z}/p^r q^s\mathbb{Z}$ tels que $ap^r + bq^s = 1$. Grâce au théorème chinois, l'application $f : \mathbb{Z}/p^r\mathbb{Z} \times \mathbb{Z}/q^s\mathbb{Z} \to \mathbb{Z}/p^r q^s\mathbb{Z}$ définie par $f(k,l) = alp^r + bkq^s$ est un isomorphisme. On trouve alors 3 éléments d'ordre 2 dans $U(\mathbb{Z}/p^r q^s\mathbb{Z})$ : $-1$ ; $2q^s b - 1$ ; $2p^r a - 1$. Testons la compatibilité de ces valeurs de $l$ avec la condition $k(l+1) = 0$.

— Si $l = -1$, tous les $k \in \mathbb{Z}/p^r q^s\mathbb{Z}$ conviennent.

— Si $l = 2q^s b - 1$, alors $k \in \{0; p^r; 2p^r; ...; (q^s - 1)p^r\}$.

— Si $l = 2p^r a - 1$, alors $k \in \{0; q^s; 2q^s; ...; (p^r - 1)q^s\}$.

Enfin, étudions les classes de conjugaison.

Comme 2 est inversible, $\mathrm{cl}(\Psi_{0,-1}) = \{\Psi_{k,-1} \mid k \in Z/p^r\mathbb{Z}\}$ est la seule classe de conjugaison pour $l = -1$. Il en est de même pour les deux autres valeurs de $l$ qui fournissent chacune une seule classe de conjugaison car $a$ et $b$ sont eux aussi inversibles : $\mathrm{cl}(\Psi_{0,2q^s b-1})$ et $\mathrm{cl}(\Psi_{0,2p^r a-1})$.

Ainsi, $e_{p^r q^s} = 3 \times 2 = 6$. □

*Remarque* 5.4.3. Pour $n = 3$, les deux algèbres de Hopf non isomorphes du théorème précédent, sont les deux algèbres de Hopf non isomorphes, non commutatives, et non cocommutatives de dimension 12 classifiées par Fukuda [10].

*Remarque* 5.4.4. Nous avons également tenté de généraliser le théorème précédent pour une décomposition de $n$ en facteurs premiers impairs : $n = p_1^{r_1}...p_s^{r_s}$ avec $p_1, ...p_s$ des nombres premiers impairs distincts et $r_1, ...r_s \in \mathbb{N}^*$. Il est possible d'obtenir le nombre d'élément $l \in U(\mathbb{Z}/n\mathbb{Z})$ d'ordre 2, néanmoins nous n'avons pas pu les obtenir explicitement et donc nous ne pouvons pas poursuivre le travail de classification avec la condition $k(l+1) = 0$ et la recherche des classes de conjugaison...

### 5.4.2 Le cas où $n$ est pair.

Supposons maintenant dans cette partie que $n$ est pair. Aucun des résultats de classification précédents ne s'applique ici et nous devons donc effectuer une analyse spécifique.

On obtient les résultats assez satisfaisants énoncés dans le tableau 5.1. Il indique d'autre part, qu'en général, il est difficile d'envisager obtenir des résultats de classification synthétiques comme dans les théorèmes 4.3.1, 4.3.2, 4.3.4.

Commençons par un résultat utile pour déterminer si un 2-cocycle de $D_n$ est trivial ou non, et dans le cas où il est trivial, pour le décrire explicitement grâce à un cobord.

**Lemme 5.4.5.** *Soit $\beta \in Z^2(D_n, k^\times)$. Les assertions suivantes sont équivalentes :*

1. *$[\beta] = 1$ dans $H^2(D_n, k^\times)$ ;*
2. *Il existe $x, y \in k^\times$ tels que*

$$x^n = \beta(r,r)\beta(r,r^2)\cdots\beta(r,r^{n-1}), \quad y^2 = \beta(s,s), \quad x^2 = \beta(r,r^{n-1})\beta(r^{n-1},s)^{-1}\beta(s,r);$$

3. *On a $(\beta(r,r^{n-1})\beta(r^{n-1},s)^{-1}\beta(s,r))^{n/2} = \beta(r,r)\beta(r,r^2)\cdots\beta(r,r^{n-1})$.*

*De plus, lorsque $[\beta] = 1$ dans $H^2(D_n, k^\times)$, en prenant $x, y \in k^\times$ comme ci-dessus, l'application $\mu : D_n \to k^\times$ définie par, pour $0 \leq i \leq n-1$, $0 \leq j \leq 1$,*

$$\mu(r^i s^j) = \beta(r^i, s^j)^{-1}\beta(r,r)^{-1}\beta(r,r^2)^{-1}\cdots\beta(r,r^{i-1})^{-1}\beta(s,s^j)^{-1}x^i y^j$$

*est telle que $\beta = \partial(\mu)$.*

*Démonstration.*

On utilise le fait connu suivant : $\beta = \partial(\phi)$ si et seulement si il existe un morphisme d'algèbres $\chi : k_\beta D_n \to k$ où $k_\beta D_n$ est l'algèbre du groupe $D_n$, de base $[g]$, $g \in D_n$, twistée, c'est à dire munie du produit $[g][h] = \beta(g,h)[gh]$. De plus, si $\beta = \partial(\phi)$, le morphisme d'algèbres $\chi$ est défini par : $\chi([g]) = \phi(g)$ pour tout $g \in D_n$.

Dans $k_\beta D_n$, on a les relations suivantes :
— $[r]^n = \beta(r,r)\beta(r,r^2)\cdots\beta(r,r^{n-1})[1]$
— $[s]^2 = \beta(s,s)[1]$
— $[s][r] = \beta(s,r)\beta(r,r)^{-1}...\beta(r,r^{n-2})^{-1}\beta(r^{n-1},s)^{-1}[r]^{n-1}[s]$.

Ainsi $[\beta] = 1$ dans $H^2(D_n, k^\times)$ si et seulement si il existe $\phi : D_n \to k$ tel que $\beta = \partial(\phi)$. D'après le rappel précédent, si et seulement si il existe un morphisme d'algèbres $\chi : k_\beta D_n \to k$.

Il faut donc montrer que : il existe un morphisme d'algèbres $\chi : k_\beta D_n \to k$ si et seulement si il existe $x, y \in k^\times$ vérifiant les relations de (2).

Si $\chi : k_\beta D_n \to k$ est un morphisme d'algèbres, il suffit de définir $x = \chi([r])$ et $y = \chi([s])$. On vérifie par un simple calcul, en utilisant les relations décrites au dessus et le produit twisté de $k_\beta D_n$, que $x$ et $y$ satisfont les relations de (2).

Réciproquement, si il existe $x, y \in k^\times$ vérifiant les relations (2), alors on définit le morphisme d'algèbres $\chi : k_\beta D_n \to k$ par $\chi([r]) = x$ et $\chi([s]) = y$.

D'où l'équivalence des deux premières assertions.

Montrons à présent que (2) implique (3) :

$\beta(r,r)\beta(r,r^2)\cdots\beta(r,r^{n-1}) = x^n = (x^2)^{n/2} = (\beta(r,r^{n-1})\beta(r^{n-1},s)^{-1}\beta(s,r))^{n/2}$. D'où la relation.

Réciproquement, si on définit $x$ tel que $x^2 = \beta(r,r^{n-1})\beta(r^{n-1},s)^{-1}\beta(s,r)$, et $y$ tel que $y^2 = \beta(s,s)$ alors on obtient bien la relation souhaitée pour $x^n$. D'où l'équivalence.

Enfin, si $[\beta] = 1$ dans $H^2(D_n, k^\times)$, on écrit $\beta = \partial(\phi)$. Ainsi on définit $\chi : k_\beta D_n \to k$ tel que $\chi([g]) = \phi(g)$. On pose $x = \chi([r])$ et $y = \chi([s])$ qui vérifient les relations (2). Ainsi on définit maintenant $\mu(g) = \chi([g])$ pour tout $g \in D_n$. Donc $\mu(g) = \phi(g)$ et comme $\beta = \partial(\phi)$, on a bien $\beta = \partial(\mu)$.

Pour terminer, on obtient l'expression de $\mu$ sur les éléments $r^i s^j$ par un simple calcul, en utilisant les relations sur $k_\beta D_n$ et le fait que $\mu(r) = \phi(r) = \chi([r]) = x$, $\mu(s) = \phi(s) = \chi([s]) = y$. □

Explicitons à présent un 2-cocycle non trivial de $D_n$.

**Lemme 5.4.6.** *Soit $\omega \in k^\times$ tel que $\omega^n = 1$. Alors l'application :*

$$\begin{aligned} \tau_\omega : D_n \times D_n &\longrightarrow k^\times \\ (r^i s^j, r^k s^l) &\longmapsto \omega^{jk} \ (j,l \in \{0,1\}) \end{aligned}$$

*est un 2-cocycle, et $[\tau_\omega] = 1 \iff \omega^{n/2} = 1$. Lorsque $\omega^{n/2} = -1$, $\tau_\omega$ est l'unique représentant non trivial des classes de cohomologie de $H^2(D_n, k^\times)$.*

*Démonstration.*

En utilisant la définition de $\tau_\omega$, on montre facilement avec le calcul, que cette application remplie les propriétés d'un 2-cocycle.

La condition de trivialité provient de l'équivalence des assertions (1) et (3) du lemme 5.4.5.

Enfin, comme $H^2(D_n, k^\times) \simeq \mathbb{Z}_2$, il y a un unique représentant non trivial des 2-cocycles à équivalence près. D'après les faits précédents, dans le cas où $\omega^{n/2} \neq 1$, c'est à dire $\omega^{n/2} = -1$ (car $\omega^n = 1$ donc $\omega^{n/2} = 1$ ou $-1$), on a mis en évidence $\tau_\omega$ comme un 2-cocycle non trivial, c'est donc l'unique représentant recherché. □

Poursuivons par un lemme préliminaire, dans le but de décrire les 2-data possibles dans le cas de $D_n$.

**Lemme 5.4.7.** *Soient $\theta \in \mathrm{Aut}(D_n)$ et $\tau \in Z^2(D_n, k^\times)$ tels que $[\tau] = 1$ et $\tau \circ (\theta \times \theta) = \tau$, et soit $a : D_n \to k^\times$ vérifiant $\tau = \partial(a)$. Si $a(\theta(r)) = a(r)$ et $a(\theta(s)) = a(s)$, alors $a \circ \theta = a$.*

*Démonstration.*

Pour tout $g, h \in D_n$, on a :

$$a(g)a(h)a(gh)^{-1} = \tau(g,h) = \tau(\theta(g),\theta(h)) = a(\theta(g))a(\theta(h))a(\theta(gh))^{-1}.$$

Ainsi, si $a(g) = a(\theta(g))$ et $a(h) = a(\theta(h))$, alors $a(\theta(gh)) = a(gh)$.

Puisque $D_n$ est engendré par $r$ et $s$, la relation précédente donne que pour tout $x \in D_n$,

$$a \circ \theta(x) = a(x).$$

D'où le résultat. □

**Lemme 5.4.8.** *Soit $\Psi_{u,v} \in \mathrm{Aut}(D_n)$. Soit $\omega \in k^\times$ avec $\omega = -1$ si $n/2$ est impair, et avec $\omega$ une racine primitive $n$-ième de l'unité si $n/2$ est pair. Soit $\tau_\omega \in Z^2(D_n, k^\times)$ le 2-cocycle non trivial du lemme 5.4.6. Soient $x, y \in k^\times$ tels que $x^n = 1$, $y^2 = \omega^u$ et $x^2 = \omega^{-v-1}$ ($x^2 = 1$ si $n/2$ est impair). L'application $a_{x,y} : D_n \to k^\times$ définie par*

$$a_{x,y}(r^i s^j) = \omega^{-uj} x^i y^j, \qquad 0 \leq i \leq n-1,\ 0 \leq j \leq 1$$

*est telle que $\tau_\omega^{-1}(\tau_\omega \circ (\Psi_{u,v} \times \Psi_{u,v}))^{-1} = \partial(a_{x,y})$, et toute application satisfaisant cette identité est de la forme $a_{\pm x, \pm y}$. De plus, on a $a_{x,y} \circ \Psi_{u,v} = a_{x,y}$ si et seulement si $x^u = 1 = x^{v-1}$.*

*Si l'on suppose également que $\Psi_{u,v}$ est d'ordre 2, alors $a_{x,y} \circ \Psi_{u,v} = a_{x,y}$ si et seulement si l'on est dans l'une des situations suivantes :*

1. *$n/2$ est impair, $u$ est pair, $x = \pm 1$ et $y = \pm 1$.*
2. *$n/2$ est impair, $u$ est impair, $x = 1$ et $y = \pm\xi$, avec $\xi$ une racine primitive quatrième de l'unité.*
3. *$n/2$ est pair, $u$ est pair, $v^2 = 1 + kn$, $u(1+v) = ln$ avec $k, l$ pairs, et $x = \pm\omega^{\frac{-v-1}{2}}$, $y = \pm\omega_0^u$, avec $\omega_0^2 = \omega$.*
4. *$n/2$ est pair, $u$ est impair, $v^2 = 1 + kn$, $u(1+v) = ln$ avec $k, l$ pairs, et $x = \omega^{\frac{-v-1}{2}}$, $y = \pm\omega_0^u$, avec $\omega_0^2 = \omega$.*
5. *$n/2$ est pair, $u$ est impair, $v^2 = 1 + kn$, $u(1+v) = ln$ avec $k$ pair et $l$ impair, et $x = -\omega^{\frac{-v-1}{2}}$, $y = \pm\omega_0^u$, avec $\omega_0^2 = \omega$.*

*Démonstration.*

Comme $[\tau_\omega] \neq 1$, et que $H^2(D_n, k^\times)$ est d'ordre 2, le cocycle $\tau_\omega^{-1}(\tau_\omega \circ (\Psi_{u,v} \times \Psi_{u,v}))^{-1}$ est trivial.

Ainsi, d'après le lemme 5.4.5, en posant $\beta := \tau_\omega^{-1}(\tau_\omega \circ (\Psi_{u,v} \times \Psi_{u,v}))^{-1}$, il existe $x, y \in k^\times$ tels que

$$x^n = \beta(r,r)\beta(r,r^2)\cdots\beta(r,r^{n-1}), \quad y^2 = \beta(s,s), \quad x^2 = \beta(r,r^{n-1})\beta(r^{n-1},s)^{-1}\beta(s,r).$$

Après calculs, en utilisant la définition de $\tau_\omega$, on obtient que :

$$x^n = 1, \quad y^2 = \omega^u, \quad x^2 = \omega^{-v-1}.$$

De plus, l'application $\mu$ définie dans le lemme 5.4.5 coïncide avec $a_{x,y}$.
Donc $\tau_\omega^{-1}(\tau_\omega \circ (\Psi_{u,v} \times \Psi_{u,v}))^{-1} = \partial(a_{x,y})$.

Réciproquement, toute application $a$ satisfaisant l'identité $\tau_\omega^{-1}(\tau_\omega \circ (\Psi_{u,v} \times \Psi_{u,v}))^{-1} = \partial(a)$ est de la forme $\mu$ comme dans le lemme 5.4.5, au signe près de $x$ et de $y$ (voir dans la preuve du lemme, les choix possibles pour $x$ et $y$). Donc $a$ est du type $a_{\pm x,\pm y}$.

Par ailleurs, le lemme 5.4.7 assure que :
$a_{x,y} \circ \Psi_{u,v} = a_{x,y}$ si et seulement si $a_{x,y}(\Psi_{u,v}(r)) = a_{x,y}(r)$ et $a_{x,y}(\Psi_{u,v}(s)) = a_{x,y}(s)$.
Or on a : $a_{x,y}(r) = x,\ a_{x,y}(\Psi_{u,v}(r)) = x^v,\ a_{x,y}(s) = \omega^{-u}y,\ a_{x,y}(\Psi_{u,v}(s)) = \omega^{-u}x^{-u}y$.

Ainsi, $a_{x,y} \circ \Psi_{u,v} = a_{x,y}$ si et seulement si $x^{v-1} = 1$ et $x^u = 1$.

Les résultats suivants sont obtenus par une étude au cas par cas.

**Cas 1 : $n/2$ est impair, $u$ est pair**

Alors $\omega = -1$. Ainsi $x, y \in k^\times$ sont tels que $x^n = 1$, $y^2 = (-1)^u = 1$ et $x^2 = (-1)^{-v-1} = 1$. Donc $x = \pm 1$ et $y = \pm 1$. Par ailleurs, les conditions $x^u = 1 = x^{v-1}$ sont vérifiées puisque $u$ est pair, et $v \in U(\mathbb{Z}/n\mathbb{Z})$ est impair.

**Cas 2 : $n/2$ est impair, $u$ est impair**

Alors $\omega = -1$. Ainsi $x, y \in k^\times$ vérifient $x^n = 1$, $y^2 = (-1)^u = -1$ et $x^2 = (-1)^{-v-1} = 1$. Donc $x = \pm 1$ et $y = \pm\xi$ avec $\xi$ une racine primitive quatrième de l'unité. Seule la valeur $x = 1$ permet d'obtenir les conditions $x^u = 1 = x^{v-1}$ dans le cas où $u$ est impair.

**Remarque** : dans les trois cas suivants on fait apparaître des conditions particulières : pour que $\Psi_{u,v}$ soit dans $\mathrm{Aut}(D_n)$, on sait que $v^2 \equiv 1[n]$ et $u(1+v) \equiv 0[n]$. On écrit donc $v^2 = 1+kn$ et $u(1+v) = ln$ avec $k, l \in \mathbb{Z}$. $l$ peut être pair ou impair, mais $k$ est obligatoirement pair. En effet, comme $n$ est pair et $v \in U(\mathbb{Z}/n\mathbb{Z})$, $v$ est impair, donc $v^2 - 1$ est pair. Donc $k$ doit être pair.

**Cas 3 : $n/2$ est pair, $u$ est pair, $v^2 = 1 + kn$, $u(1+v) = ln$ avec $k, l$ pairs**

Alors $\omega$ est une racine primitive n-ième de l'unité. Ainsi $x, y \in k^\times$ tels que $x^n = 1$, $y^2 = \omega^u$ et $x^2 = \omega^{-v-1}$. Comme $-v-1$ est pair, la troisième condition donne $x = \pm\omega^{\frac{-v-1}{2}}$. Comme $n/2$ est pair, on a $\omega^{n/2} = -1$ et donc ces valeurs de $x$ vérifient bien l'équation $x^n = 1$. D'autre part, on a $y = \pm\omega_0^u$, avec $\omega_0^2 = \omega$. La parité de $u$ et les conditions sur $k, l$ permettent d'obtenir $x^u = 1 = x^{v-1}$ pour les deux valeurs de $x$.

**Cas 4 : $n/2$ est pair, $u$ est impair, $v^2 = 1 + kn$, $u(1 + v) = ln$ avec $k, l$ pairs**

Alors $\omega$ est une racine primitive n-ième de l'unité. Ainsi $x, y \in k^\times$ tels que $x^n = 1$, $y^2 = \omega^u$ et $x^2 = \omega^{-v-1}$. Le raisonnement pour les valeurs de $x$ est le même que dans le cas 3, donc $x = \pm\omega^{\frac{-v-1}{2}}$. Néanmoins, avec ces conditions, les équations $x^u = 1 = x^{v-1}$ ne sont valides que pour $x = \omega^{\frac{-v-1}{2}}$. D'autre part, $y = \pm\omega_0^u$, avec $\omega_0^2 = \omega$.

**Cas 5 : $n/2$ est pair, $u$ est impair, $v^2 = 1 + kn$, $u(1 + v) = ln$ avec $k$ pair et $l$ impair**

Alors $\omega$ est une racine primitive n-ième de l'unité. Ainsi $x, y \in k^\times$ tels que $x^n = 1$, $y^2 = \omega^u$ et $x^2 = \omega^{-v-1}$. Le raisonnement pour les valeurs de $x$ est le même que dans le cas 3, donc $x = \pm\omega^{\frac{-v-1}{2}}$. Néanmoins, avec ces conditions, les équations $x^u = 1 = x^{v-1}$ ne sont valides que pour $x = -\omega^{\frac{-v-1}{2}}$. D'autre part, $y = \pm\omega_0^u$, avec $\omega_0^2 = \omega$.

Ceci conclut la preuve. □

Le lemme 5.4.8 décrit les automorphismes $\Psi_{u,v}$ qui peuvent s'insérer dans un 2-datum $(D_n, \Psi_{u,v}, a, \tau_\omega)$ associés à la description des applications $a$ compatibles. À présent, classifions les à équivalence près. On commencera par un lemme pour l'une des conditions d'équivalence, puis le lemme suivant donnera la classification de ces data à équivalence près.

**Lemme 5.4.9.** *Soient $(H, \theta, a, \tau)$ et $(H, \theta', a', \tau')$ des 2-data tels qu'il existe $f \in Aut(H)$ et $\varphi : H \to k^\times$ vérifiant $\theta' = f \circ \theta \circ f^{-1}$ et $\tau' = \partial(\varphi).\tau \circ (f^{-1} \times f^{-1})$. Si il existe $x, y \in H$ tels que $(\varphi.\varphi\circ\theta'.a')(x) = a\circ f^{-1}(x)$ et $(\varphi.\varphi\circ\theta'.a')(y) = a\circ f^{-1}(y)$, alors $(\varphi.\varphi\circ\theta'.a')(xy) = a\circ f^{-1}(xy)$.*

*Démonstration.*

Soient $(H, \theta, a, \tau)$ et $(H, \theta', a', \tau')$ comme dans l'énoncé.

$(H, \theta, a, \tau)$ est un 2-datum donc $a \circ \theta = a$ et $\tau.\tau \circ (\theta \times \theta) = \partial(a^{-1})(*)$.

De même, $(H, \theta', a', \tau')$ est un 2-datum donc $a' \circ \theta' = a'$ et $\tau'.\tau' \circ (\theta' \times \theta') = \partial(a'^{-1})(**)$.

D'autre part, $\tau' = \partial(\varphi).\tau \circ (f^{-1} \times f^{-1})$ donc pour tout $x, y \in H$ on a :

$$\tau'(\theta'(x), \theta'(y)) = \partial(\varphi)(\theta'(x), \theta'(y)).\tau(f^{-1}(\theta'(x)), f^{-1}(\theta'(y))).$$

Or $f^{-1} \circ \theta' = \theta \circ f$, donc l'équation devient :

$$\tau'(\theta'(x), \theta'(y)) = \partial(\varphi)(\theta'(x), \theta'(y)).\tau(\theta(f^{-1}(x)), \theta(f^{-1}(y))).$$

et on a également $\tau'(x, y) = \partial(\varphi)(x, y).\tau(f^{-1}(x), f^{-1}(y))$.

En multipliant ces deux dernières équations, on a :

$$\tau'(\theta'(x), \theta'(y))\tau'(x, y) = \partial(\varphi)(\theta'(x), \theta'(y)).\partial(\varphi)(x, y).\tau(\theta(f^{-1}(x)), \theta(f^{-1}(y))).\tau(f^{-1}(x), f^{-1}(y)).$$

En appliquant $(*), (**)$, les équations faites comme hypothèses dans l'énoncé et après simplification, on obtient :

$$a'(xy) = a \circ f^{-1}(xy)\varphi(xy)^{-1}\varphi(\theta'(xy))^{-1}.$$

C'est-à-dire : $(\varphi.\varphi \circ \theta'.a')(xy) = a \circ f^{-1}(xy)$. D'où le résultat. □

*Remarque* 5.4.10. — L'intérêt de ce lemme est que lorsque les conditions (a) et (c) d'équivalence de deux data sont déjà vérifiées, et que $H$ est engendré par deux éléments $x$ et $y$, il suffit de vérifier la condition (b) sur chacun de ces éléments seulement.

— Dans le cas où $H = D_n$, comme ce groupe est engendré par $r$ et $s$, si $(\varphi.\varphi \circ \theta'.a')(r) = a \circ f^{-1}(r)$ et $(\varphi.\varphi \circ \theta'.a')(s) = a \circ f^{-1}(s)$ alors $(\varphi.\varphi \circ \theta'.a')(x) = a \circ f^{-1}(x)$ pour tout $x \in D_n$.

**Lemme 5.4.11.** *Soit $\Psi_{u,v} \in \mathrm{Aut}(D_n)$ un élément d'ordre 2, et utilisons les notations du lemme 5.4.8.*

1. *Pour $n/2$ impair, $u$ pair, les 2-data $(D_n, \Psi_{u,v}, a_{1,1}, \tau_\omega)$ et $(D_n, \Psi_{u,v}, a_{1,-1}, \tau_\omega)$ sont équivalents, alors que les 2-data $(D_n, \Psi_{u,v}, a_{1,1}, \tau_\omega)$, $(D_n, \Psi_{u,v}, a_{-1,1}, \tau_\omega)$ et $(D_n, \Psi_{u,v}, a_{-1,-1}, \tau_\omega)$ sont deux à deux non équivalents. Ainsi, il y a exactement 3 classes d'équivalence de 2-data de $D_n$ ayant $\Psi_{u,v}$ comme automorphisme sous-jacent.*
2. *Pour $n/2$ impair et $u$ impair, les 2-data $(D_n, \Psi_{u,v}, a_{1,\xi}, \tau_\omega)$ et $(D_n, \Psi_{u,v}, a_{1,-\xi}, \tau_\omega)$ sont équivalents. Ainsi, il y a exactement 1 classe d'équivalence de 2-data de $D_n$ ayant $\Psi_{u,v}$ comme automorphisme sous-jacent.*
3. *Pour $n/2$ pair et $u$ impair satisfaisant les conditions des cas 4 et 5 du lemme 5.4.8, et pour $x, y$ compatibles, les 2-data $(D_n, \Psi_{u,v}, a_{x,y}, \tau_\omega)$ et$(D_n, \Psi_{u,v}, a_{x,-y}, \tau_\omega)$ sont équivalents. Ainsi, il y a exactement 1 classe d'équivalence de 2-data de $D_n$ ayant $\Psi_{u,v}$ comme automorphisme sous-jacent.*
4. *Pour $n \equiv 0[8]$ et $u$ pair satisfaisant les conditions du cas 3 du lemme 5.4.8, et pour $x, y$ compatibles, les 2-data $(D_n, \Psi_{u,v}, a_{x,y}, \tau_\omega)$ et $(D_n, \Psi_{u,v}, a_{x,-y}, \tau_\omega)$ sont équivalents, alors que les 2-data $(D_n, \Psi_{u,v}, a_{x,y}, \tau_\omega)$ et $(D_n, \Psi_{u,v}, a_{-x,y}, \tau_\omega)$ ne le sont pas. Ainsi, il y a exactement 2 classes d'équivalence de 2-data de $D_n$ ayant $\Psi_{u,v}$ comme automorphisme sous-jacent.*
5. *Pour $n \equiv 4[8]$, $u$ pair et $v \equiv 3[4]$ satisfaisant les conditions du cas 3 du lemme 5.4.8, et pour $x, y$ compatibles, les 2-data $(D_n, \Psi_{u,v}, a_{x,y}, \tau_\omega)$ et $(D_n, \Psi_{u,v}, a_{x,-y}, \tau_\omega)$ sont équivalents, alors que les 2-data $(D_n, \Psi_{u,v}, a_{x,y}, \tau_\omega)$ et $(D_n, \Psi_{u,v}, a_{-x,y}, \tau_\omega)$ ne le sont pas. Ainsi, il y a exactement 2 classes d'équivalence de 2-data de $D_n$ ayant $\Psi_{u,v}$ comme automorphisme sous-jacent.*
6. *Pour $n \equiv 4[8]$, $u$ pair et $v \equiv 1[4]$ satisfaisant les conditions du cas 3 du lemme 5.4.8, et pour $x, y$ compatibles, il y a exactement 3 classes d'équivalence de 2-data de $D_n$ ayant $\Psi_{u,v}$ comme automorphisme sous-jacent.*

*Démonstration.*

Rappelons tout d'abord que deux 2-data $(H, \theta, a, \tau)$ et $(H, \theta, a', \tau)$ sont équivalents si il existe une paire $(f, \varphi)$ avec $f \in \mathrm{Aut}(H)$ et $\varphi : H \to k^\times$ tels que :

$$\text{(a)} \quad f \circ \theta = \theta \circ f, \ \text{(b)} \quad \varphi \cdot \varphi \circ \theta \cdot a' = a \circ f^{-1}, \quad \text{(c)} \ \tau = \partial(\varphi) \cdot \tau \circ (f^{-1} \times f^{-1}).$$

On démontrera ce lemme en considérant d'abord le cas où $u$ est impair, ce qui permettra de prouver les assertions (2) et (3). Ensuite, nous ferons l'étude du cas où $u$ est pair qui nécessite plus de détails et de conditions pour démontrer les autres assertions.

On remarquera également que d'après la remarque précédente, si les conditions (a) et (c) sont déjà vérifiées, il suffit alors de démontrer la condition (b) sur les éléments $r$ et $s$ seulement.

Dans le cas où $u$ est impair (cas (2) et (3) du lemme), prenons $\varphi \in \widehat{H}$ tel que $\varphi(r) = -1$. On constate que la paire $(\mathrm{id}, \varphi)$ réalise l'équivalence entre les 2-data $(D_n, \Psi_{u,v}, a_{x,y}, \tau_\omega)$ et $(D_n, \Psi_{u,v}, a_{x,-y}, \tau_\omega)$. En effet, si $\varphi \in \widehat{H}$ alors $\partial(\varphi) = \mathbb{1}$ et donc la condition (c) est validée. La condition (a) l'est également avec $f = \mathrm{id}$. Enfin, on a d'une part : $\varphi(r)\varphi(\Psi_{u,v}(r)) = (-1)^{v+1}$, avec $v$ impair donc $\varphi(r)\varphi(\Psi_{u,v}(r)) = 1$. La condition (b) est donc vérifiée sur $r$. D'autre part, $\varphi(s)\varphi(\Psi_{u,v}(s)) = \varphi(s)\varphi(sr^u) = \varphi(s)^2(-1)^u = -1$ car $u$ est supposé impair. Donc la condition (b) est aussi vérifiée sur $s$. Finalement $\varphi \cdot \varphi \circ \theta \cdot a_{x,y} = a_{x,-y}$, d'où l'équivalence.

Comme dans chacun des cas (2) et (3) du lemme il n'y a qu'une seule valeur de $x$ (voir le lemme 5.4.8), on obtient les résultats annoncés.

On se place à présent dans le cas où $u$ est pair. Soit $f \in \mathrm{Aut}(D_n)$ tel que l'on note $f^{-1} = \Psi_{\alpha,\beta}$. De manière similaire à la preuve du lemme 5.4.8, on montre à partir de la condition (c), que l'application $\varphi : D_n \to k^\times$ est définie par

$$\varphi_{z,t}(r^i s^j) = \omega^{-j\alpha} z^i t^j$$

où $z = \pm\omega^{\frac{1-\beta}{2}}$, $t = \pm(\omega_0)^\alpha$, avec $\omega_0^2 = \omega$.

On extrait alors une partie du calcul de la condition (b) pour plus de facilité :

$$\varphi_{z,t}(r^i s^j)\varphi_{z,t}(\Psi_{u,v}(r^i s^j)) = \omega^{-2j\alpha} z^{i(1+v)-ju} t^{2j}$$

et en particulier :

$$\varphi_{z,t}(r)\varphi_{z,t}(\Psi_{u,v}(r)) = z^{1+v} = \omega^{\frac{(1-\beta)(1+v)}{2}}, \quad \varphi_{z,t}(s)\varphi_{z,t}(\Psi_{u,v}(s)) = \omega^{-\alpha}z^{-u}.$$

L'équation (b), pour $a_{x,y}$ et $a_{x',y'} = \varepsilon a_{x,y}$ où $\varepsilon \in \widehat{D_n}$ (avec $x' = \varepsilon(r)x$, $y' = \varepsilon(s)y$), devient :

$$z^{1+v} = \varepsilon(r)x^{\beta-1}, \quad z^{-u} = \varepsilon(s)\omega^{\alpha}x^{-\alpha}.$$

La première équation donne :

$$\omega^{\frac{(1-\beta)(v+1)}{2}} = \varepsilon(r)\omega^{\frac{(-v-1)(\beta-1)}{2}},$$

ce qui amène que $\varepsilon(r) = 1$.

Par conséquent, si les 2-data $(D_n, \Psi_{u,v}, a_{x,y}, \tau_\omega)$ et $(D_n, \Psi_{u,v}, a_{x',y'}, \tau_\omega)$ sont équivalents, alors nécessairement $x = x'$.

Puisque $u$ est pair, la seconde équation devient :

$$\omega^{\frac{(\beta-1)u}{2}-\alpha} = \varepsilon(s)x^{-\alpha}. \tag{5.4.1}$$

Cette équation permet d'obtenir une équivalence de data si $\varepsilon(s) = -1$. C'est ce que l'on cherche à voir selon différents cas.

Supposons que $n/2$ est impair. Dans ce cas, $\omega = -1$. Puisque $\beta$ est impair, la seconde équation devient : $(-1)^{\alpha} = \varepsilon(s)x^{\alpha}$. Or on est dans le cas (1) du lemme 5.4.8 donc $x = \pm 1$. On constate que pour $x = -1$, aucune valeur de $\alpha$ ne permet d'obtenir $\varepsilon(s) = -1$. Ainsi, on constate que les 2-data $(D_n, \Psi_{u,v}, a_{-1,1}, \tau_\omega)$ et $(D_n, \Psi_{u,v}, a_{-1,-1}, \tau_\omega)$ ne sont pas équivalents.

D'autre part, en prenant $f = f^{-1} = \Psi_{n/2,1}$ (qui commute avec $\Psi_{u,v}$) et $\varphi_{z,t}$ défini comme ci-dessus, on voit que la paire $(\Psi_{n/2,1}, \varphi_{z,t})$ donne l'équivalence entre les 2-data $(D_n, \Psi_{u,v}, a_{1,1}, \tau_\omega)$ et $(D_n, \Psi_{u,v}, a_{1,-1}, \tau_\omega)$ dans le cas où $x = 1$. En effet, la condition (a) est vérifiée, la condition (c) aussi grâce à la définition de $\varphi_{z,t}$ et la condition (b) sur $s$ avec $\varepsilon(s) = -1$ donne :

$$(-1)^{0-(n/2)} = (-1)1^{-n/2} \iff (-1)^{n/2} = -1$$

ce qui est vrai puisque l'on a supposé que $n/2$ est impair. La condition (b) sur $r$ est automatique puisque $x = x' = 1$.

D'où l'équivalence. Ceci conclut la preuve de l'assertion (1).

Il reste à prouver les assertions (4), (5) et (6).

Supposons maintenant que $n/2$ est pair. Alors $n \equiv 0[8]$ ou $n \equiv 4[8]$ sont les deux cas de figure possibles.

On écrit $x = \nu\omega^{\frac{-v-1}{2}}$ avec $\nu = \pm 1$ pour décrire les valeurs possibles de $x$ dans chaque cas. L'équation 5.4.1 devient :

$$\varepsilon(s) = \nu^{\alpha}\omega^{\frac{(\beta-1)u-\alpha(v+3)}{2}} = \nu^{\alpha}\omega^{\frac{(\beta-1)u-\alpha(v-1)}{2}}\omega^{-2\alpha}. \tag{5.4.2}$$

Par ailleurs, on sait que $v$ est impair, donc soit $v \equiv 3[4]$, soit $v \equiv 1[4]$.

Si $v \equiv 3[4]$, prenons $\alpha = n/2$ et $\beta = 1$. L'équation 5.4.2 est réalisée avec $\varepsilon(s) = -1$.

En effet, on a alors :

$$-1 = \nu^{n/2}\omega^{0-\frac{n}{2}\frac{v-1}{2}}\omega^{-n}.$$

Comme $\nu = \pm 1$ et $n/2$ pair, $\nu^{n/2} = 1$. De plus, $\omega^n = 1$ et $\omega^{n/2} = -1$, donc on a :

$$-1 = (\omega^{-\frac{n}{2}})^{\frac{v-1}{2}} \iff -1 = (-1)^{\frac{v-1}{2}}.$$

Comme $v \equiv 3[4]$, $\frac{v-1}{2}$ est impair, d'où l'égalité.

Finalement, la paire $(\Psi_{n/2,1},\varphi_{z,t})$ permet d'obtenir que les 2-data $(D_n, \Psi_{u,v}, a_{x,y}, \tau_\omega)$ et $(D_n, \Psi_{u,v}, a_{x,-y}, \tau_\omega)$ sont équivalents lorsque $v \equiv 3[4]$. (Les calculs ci-dessus montrent que (b) sur $s$ est vraie. (b) sur $r$ l'est aussi car $x = x'$. (a) est vérifiée puisque $\Psi_{n/2,1}$ et $\Psi_{u,v}$ commutent. Enfin (c) l'est également grâce à la définition de $\varphi_{z,t}$.) Ceci prouve l'assertion (5).

Supposons maintenant que $v \equiv 1[4]$. Dans ce cas, on a deux possibilités : soit $v \equiv 1[8]$, soit $v \equiv 5[8]$.

Si $n/4$ est pair i.e. $n \equiv 0[8]$, il est facile de vérifier que la condition $v^2 \equiv 1[2n]$ (due au lemme 5.4.8) implique que $v \equiv 1[8]$.

En effet, supposons par l'absurde que $v \equiv 5[8]$. Alors on écrit $v = 8k+5$ avec $k \in \mathbb{Z}$. Dans ce cas, $v^2 = (8k+5)^2 = 64k^2 + 40k + 25$. Donc $v^2 - 1 = 64k^2 + 40k + 24 = 8(8k^2 + 5k + 3)$. On doit alors avoir : $8(8k^2 + 5k + 3) \equiv 0[2.4.\frac{n}{4}]$ i.e. $(8k^2 + 5k + 3) \equiv 0[\frac{n}{4}]$. Ce qui est absurde car $n/4$ est pair et $8k^2 + 5k + 3$ est impair. Donc forcément dans le cas où $n \equiv 0[8]$, on a $v \equiv 1[8]$.

Par ailleurs, on voit que la condition 5.4.2 est réalisée avec $\varepsilon(s) = -1$ en prenant $\beta = 1$ et $\alpha = n/4$, et donc en choisissant $f = \Psi_{n/4,1}$ (qui commute avec $\Psi_{u,v}$).

En effet, on a :

$$-1 = \nu^{n/4}\omega^{0-\frac{n}{4}\frac{v-1}{2}}\omega^{-n/2}.$$

Comme $\nu = \pm 1$ et $n/4$ pair, $\nu^{n/4} = 1$. De plus, $\omega^{n/2} = -1$, donc on a :

$$-1 = \omega^{-\frac{n}{4}\frac{v-1}{2}}(-1) \iff 1 = \omega^{-\frac{n}{2}\frac{v-1}{4}} \iff 1 = (\omega^{-\frac{n}{2}})^{\frac{v-1}{4}} \iff 1 = (-1)^{\frac{v-1}{4}}.$$

Comme $v \equiv 1[8]$, $\frac{v-1}{4}$ est pair, d'où l'égalité.

On obtient finalement que les 2-data $(D_n, \Psi_{u,v}, a_{x,y}, \tau_\omega)$ et $(D_n, \Psi_{u,v}, a_{x,-y}, \tau_\omega)$ sont équivalents. Ceci conclut la preuve de l'assertion (4).

Enfin, supposons que $n/4$ est impair i.e. $n \equiv 4[8]$ (toujours avec $v \equiv 1[4]$). On rappelle l'écriture précédente : $x = \nu\omega^{\frac{-v-1}{2}}$ avec $\nu = \pm 1$. Prenons $\alpha = n/4$ et $\beta = 1$. L'équation 5.4.2 avec $\varepsilon(s) = -1$ donne :

$$-1 = \nu^{n/4}\omega^{0-\frac{n}{4}\frac{v-1}{2}}\omega^{-n/2} \iff -1 = \nu^{n/4}(\omega^{-\frac{n}{2}})^{\frac{v-1}{4}}(-1) \iff 1 = \nu^{n/4}(-1)^{\frac{v-1}{4}}.$$

Comme $\nu = \pm 1$, $n/4$ est impair, cette équation est réalisée dans les deux situations suivantes :

$$\nu = 1,\ v \equiv 1[8]\ ; \quad \nu = -1,\ v \equiv 5[8].$$

En posant $f = \Psi_{n/4,1}$, pour $v \equiv 5[8]$, on obtient que les 2-data $(D_n, \Psi_{u,v}, a_{-\omega^{\frac{-v-1}{2}},y}, \tau_\omega)$ et $(D_n, \Psi_{u,v}, a_{-\omega^{\frac{-v-1}{2}},-y}, \tau_\omega)$ sont équivalents.

Pour voir que ce sont les seuls cas d'équivalence, supposons que l'équation 5.4.2 soit réalisée avec $\varepsilon(s) = -1$, et $(\beta-1)u \equiv \alpha(v-1)[n]$ (cette condition correspond à la commutativité de $\Psi_{u,v}$ et de $f$ donné par (a)). Alors on obtient :

$$-1 = \nu^{\alpha}\omega^{\frac{(\beta-1)u-\alpha(v-1)}{2}}\omega^{-2\alpha}.$$

En élevant au carré cette identité, on obtient :

$$1 = \omega^{(\beta-1)u-\alpha(v-1)}\omega^{-4\alpha} \iff \omega^{4\alpha} = 1.$$

Donc $\omega^{2\alpha} = \pm 1$. Si $\omega^{2\alpha} = 1$ alors $n \mid 2\alpha$ donc $2\alpha = 0 \Leftrightarrow \alpha = 0$ ou $2\alpha = n \Leftrightarrow \alpha = n/2$.

D'autre part, si $\omega^{2\alpha} = -1 = \omega^{n/2}$ alors $\omega^{2\alpha - n/2} = 1$. Donc $n \mid 2\alpha - n/2$.
Ainsi, $2\alpha - n/2 = 0 \iff \alpha = n/4$ ou $2\alpha - n/2 = n \iff \alpha = 3n/4$.
Finalement, $\alpha \in \{0, n/4, n/2, 3n/4\}$.

La condition $u(v+1) \equiv 0[2n]$ implique qu'il n'existe pas de $\beta$ tel que $(\beta - 1)u \equiv n[2n]$.

En effet, si on suppose qu'il existe $\beta$ tel que $(\beta - 1)u \equiv n[2n]$. Comme $v \equiv 1[4]$, on écrit $v = 4v_0 + 1$, alors $u(1+v) \equiv 0[2n] \iff 2u(2v_0+1) \equiv 0[2n] \iff u(2v_0+1) \equiv 0[n]$. Comme $4 \mid n$, on doit avoir $4 \mid u(2v_0 + 1)$. Or $2v_0 + 1$ est impair, donc $4 \mid u$.

Dans ce cas, $(\beta - 1)u \equiv n[2n] \iff (\beta - 1)4u_0 \equiv n[2n] \iff (\beta - 1)u_0 \equiv \frac{n}{4}[\frac{n}{2}]$. Pour des raisons de parité, on aboutit à une contradiction ($\beta - 1$ pair, $n/2$ pair et $n/4$ impair).

Ainsi $(\beta - 1)u \not\equiv n[2n]$. La conséquence de ce résultat est que $\omega^{\frac{(\beta-1)u}{2}} \neq -1$.

En supposant donc que $\nu = 1$ et $v \equiv 5[8]$ ou que $\nu = -1$ et $v \equiv 1[8]$, en examinant toutes les valeurs possibles de $\alpha$, on arrive toujours à l'identité $-1 = 1$ qui fournit une contradiction. Ceci conclut la preuve de l'assertion (6), et par conséquent la preuve du lemme. □

Le lemme 5.4.11 permet de classer les 2-data réduits de $D_n$, dès lors que les représentants des classes de conjugaison dans $\mathrm{Aut}(D_n)$ d'ordre 2 sont trouvés. Nous compilons les résultats dans le tableau 5.1, où $\Psi_{u,v}$ est un automorphisme d'ordre 2 de $D_n$ (par conséquent avec $v^2 \equiv 1[n]$ et $u(v+1) \equiv 0[n]$), et notons $N(u,v)$ le nombre de classe d'équivalence de 2-data réduits de $D_n$ ayant $\Psi_{u,v}$ comme automorphisme sous-jacent.

| Caractéristiques de $n/2$, $u$ et $v$ | $N(u,v)$ |
|---|---|
| $n/2$ impair, $u$ impair | 1 |
| $n/2$ impair, $u$ pair | 3 |
| $n/2$ pair, $u$ impair, $v^2 \equiv 1[2n]$ | 1 |
| $n \equiv 0[8]$, $u$ pair, $v^2 \equiv 1[2n]$, $u(v+1) \equiv 0[2n]$ | 2 |
| $n \equiv 4[8]$, $u$ pair, $v^2 \equiv 1[2n]$, $u(v+1) \equiv 0[2n]$, $v \equiv 3[4]$ | 2 |
| $n \equiv 4[8]$, $u$ pair, $v^2 \equiv 1[2n]$, $u(v+1) \equiv 0[2n]$, $v \equiv 1[4]$ | 3 |

TABLE 5.1 – Nombre de 2-data réduits de $D_n$ ayant $\Psi_{u,v}$ comme automorphisme.

À présent, dans un certain nombre de cas particuliers, dénombrons grâce au tableau 5.1, les algèbres de Hopf s'insérant dans une extension cocentrale universelle $k \to \mathcal{O}(D_n) \to A \to k\mathbb{Z}_2 \to k$.

**Théorème 5.4.12.** *Soit $n \geq 4$ un entier pair et notons $e_n$ le nombre de classe d'isomorphisme d'algèbres de Hopf non commutatives $A$ s'insérant dans une extension universelle cocentrale $k \to \mathcal{O}(D_n) \to A \to k\mathbb{Z}_2 \to k$.*

1. *Si $n = 2^r$ avec $r \geq 2$, alors $e_n = 3$.*
2. *Si $n = 2p^r$, avec $r \geq 1$ et $p$ premier impair, alors $e_n = 5$.*
3. *Si $n = 4p^r$, avec $r \geq 1$ et $p$ premier impair, alors $e_n = 9$.*
4. *Si $n = 2^s p^r$, avec $s \geq 3$, $r \geq 1$ et $p$ premier impair, alors $e_n = 10$.*

*Démonstration.*

Un 2-datum $(D_n, \theta, a, \tau)$ n'est pas réduit si $\tau$ est un cocycle trivial, car $Z(D_n)$ n'est pas trivial, et est réduit si $\tau$ est le 2-cocycle non trivial du lemme 5.4.6.

Par conséquent, d'après le corollaire 4.2.3, le théorème 4.2.12 et la proposition 4.2.8, $e_n$ correspond au nombre de classes d'équivalence de 2-data $(D_n, \theta, a, \tau_\omega)$, tels que $\theta \neq \mathrm{id}$, que l'on peut à présent déterminer à équivalence près grâce au tableau 5.1.

**Cas 1 : $n = 2^r$, $r \geq 2$**

Il faut distinguer le cas $r = 2$ des cas où $r > 2$.

— Pour $r = 2$, c'est-à-dire $n = 4$, il y a 3 classes de conjugaison pour les automorphismes d'ordre 2 de $D_4$ dont les représentants sont : $\Psi_{2,1}$, $\Psi_{0,-1}$ et $\Psi_{1,-1}$.
Le premier automorphisme $\Psi_{2,1}$ ne satisfait pas la condition $u(1+v) \equiv 0[8]$ du lemme 5.4.8, donc ne peut être inséré dans un 2-datum. On est dans le cas où $n/2$ est pair et $n \equiv 4[8]$. L'automorphisme $\Psi_{0,-1}$ remplit les critères de la $5^{ème}$ ligne du tableau 5.1, donc fournit deux data à équivalence près.
De même, $\Psi_{1,-1}$ remplit les critères de la $3^{ème}$ ligne du tableau 5.1, donc fournit 1 datum à équivalence près.
Finalement, on obtient $e_4 = 2 + 1 = 3$.

— Dans le cas où $n = 2^r$ avec $r \geq 3$, il y a 5 classes de conjugaison d'automorphismes d'ordre 2 de $D_n$ dont les représentants sont :

$$\Psi_{2^{r-1},1}, \quad \Psi_{0,2^{r-1}-1}, \quad \Psi_{0,2^{r-1}+1}, \quad \Psi_{0,-1}, \quad \Psi_{1,-1}.$$

Parmi ces automorphismes, seuls $\Psi_{0,-1}$ et $\Psi_{1,-1}$ remplissent les conditions de compatibilité du lemme 5.4.8, et peuvent donc faire parti d'un 2-datum. On est dans le cas où $n/2$ est pair, et $n \equiv 0[8]$. Les lignes concernées dans le tableau 5.1 sont similaires à celles du cas $n = 4$, donc on obtient que $e_n = 2 + 1 = 3$ également.

Finalement, on peut écrire que $e_n = 3$ pour $n = 2^r$ avec $r \geq 2$.

**Cas 2 : $n = 2p^r$ avec $r \geq 1$, $p$ premier impair**

Ici il y a 3 classes de conjugaison d'automorphismes d'ordre 2 de $D_n$ dont les représentants sont $\Psi_{p^r,1}$, $\Psi_{0,-1}$ et $\Psi_{1,-1}$.

On est dans le cas où $n/2$ est impair.

— Pour $\Psi_{p^r,1}$, on obtient 1 datum à équivalence près (ligne 1).

— Pour $\Psi_{0,-1}$, on obtient 3 data à équivalence près (ligne 2).

— Pour $\Psi_{1,-1}$, on obtient 1 datum à équivalence près (ligne 1).

Finalement, $e_n = 1 + 3 + 1 = 5$.

**Cas 3 : $n = 4p^r$, avec $r \geq 1$, $p$ premier impair**

Fixons des entiers $a, b$ tels que $4a + p^r b = 1$. Grâce au lemme 5.4.1, on sait que l'on peut choisir $a, b \in \mathbb{Z}$ inversibles dans $\mathbb{Z}/4p^r\mathbb{Z}$.

On a alors 4 éléments de $\mathbb{Z}/4p^r\mathbb{Z}$ tels que $v^2 \equiv 1[2n]$ : $v = \pm 1$, $v = \pm(4a - p^r b)$.

Après vérification des conditions de compatibilité du lemme 5.4.8, les représentants des classes de conjugaison d'automorphismes d'ordre 2 de $D_n$ satisfaisants sont :

$$\Psi_{0,-1}, \quad \Psi_{1,-1}, \quad \Psi_{0,8a-1}, \quad \Psi_{p^r,8a-1}, \quad \Psi_{0,1-8a}.$$

On est dans le cas où $n/2$ est pair, et $n \equiv 4[8]$.

— Pour $\Psi_{0,-1}$, on a 2 data à équivalence près (ligne 5).

— Pour $\Psi_{1,-1}$, on a 1 datum à équivalence près (ligne 3).

— Pour $\Psi_{0,8a-1}$, on a 2 data à équivalence près (ligne 5).

— Pour $\Psi_{p^r,8a-1}$, on a 1 datum à équivalence près (ligne 3).

— Pour $\Psi_{0,1-8a}$, on a 3 data à équivalence près (ligne 6).

Finalement, le tableau 5.1 nous donne $e_n = 2 + 1 + 2 + 1 + 3 = 9$.

**Cas 4 : $n = 2^s p^r$ avec $s \geq 3$, $r \geq 1$, $p$ premier impair**

Grâce au lemme 5.4.1, fixons $a, b \in \mathbb{Z}$ inversibles dans $\mathbb{Z}/2^s p^r\mathbb{Z}$ tels que $2^s a + p^r b = 1$.

Il y a 8 éléments dans $\mathbb{Z}/2^s p^r\mathbb{Z}$ tels que $v^2 \equiv 1[2n]$ : $v = \pm 1$, $v = \pm(2^s a - p^r b) = \pm(2^{s+1}a - 1)$.

Après vérification des conditions de compatibilité du lemme 5.4.8, les représentants des classes de conjugaison d'automorphismes d'ordre 2 de $D_n$ satisfaisants sont :

$$\Psi_{0,-1}, \quad \Psi_{1,-1}, \quad \Psi_{0,2^{s+1}a-1}, \quad \Psi_{p^r,2^{s+1}a-1}, \quad \Psi_{0,1-2^{s+1}a}, \quad \Psi_{2^s,1-2^{s+1}a}.$$

Nous sommes dans le cas où $n/2$ est pair, et $n \equiv 0[8]$.

— Pour $\Psi_{0,-1}$, on a 2 data à équivalence près (ligne 4).

— Pour $\Psi_{1,-1}$, on a 1 datum à équivalence près (ligne 3).

— Pour $\Psi_{0,2^{s+1}a-1}$, on a 2 data à équivalence près (ligne 4).

— Pour $\Psi_{p^r,2^{s+1}a-1}$, on a 1 datum à équivalence près (ligne 3).

— Pour $\Psi_{0,1-2^{s+1}a}$, on a 2 data à équivalence près (ligne 4).

— Pour $\Psi_{2^s,1-2^{s+1}a}$, on a 2 data à équivalence près (ligne 4).

Finalement, le tableau 5.1 nous donne $e_n = 2 + 1 + 2 + 1 + 2 + 2 = 10$. □

*Remarque* 5.4.13. La première partie de ce théorème contribue à la classification des algèbres de Hopf semisimples de dimension $2^r$, étudiées dans les références [17, 18].

### 5.4.3 Algèbres de Hopf de dimension $p^2q^r$

Étudions à présent un exemple où le groupe $H$ est abélien : $H = \mathbb{Z}_p^2$, avec $p$ premier impair. C'est l'une des situations les plus étudiées dans la littérature [23, 26, 20]. Nous souhaitons démontrer le théorème énoncé ci-dessous. Pour ce faire, un certain nombre de pré-requis sont nécessaires avant de passer à la démonstration du théorème. Le cas où $r = 1$ est obtenu dans la référence [26].

**Théorème 5.4.14.** *Soient $p, q$ des nombres premiers impairs et $r \geq 1$. Supposons que $q^r | p-1$.*

*Le nombre $\mathcal{E}$ de classe d'isomorphisme d'algèbres de Hopf non commutatives et non cocommutatives s'insérant dans une extension cocentrale*

$$k \to \mathcal{O}(\mathbb{Z}_p^2) \to A \to k\mathbb{Z}_{q^r} \to k$$

*est exactement $\mathcal{E} = \frac{1}{2}(\sum_{s=1}^{r} q^s + q^{s-1}) = \frac{(q+1)(q^r-1)}{2(q-1)}$.*

La suite de cette partie est dédiée à la preuve du théorème 5.4.14. Commençons par quelques généralités. Comme décrit dans la partie 4.3, rappelons que si $G$ est un groupe et $m \geq 1$, $\mathrm{CC}_m^\bullet(G)$ est l'ensemble des éléments $x$ de $G$ tels que $x^m = 1$ et $x \neq 1$, modulo la relation d'équivalence définie par : $x \sim y \iff$ il existe $l$ premier avec $m$ tel que $x^l$ soit conjugué à $y$. Pour $d$ un diviseur de $m$, $d > 1$, on note $\mathrm{CC}_{m,d}^\bullet(G)$ l'ensemble des classes d'équivalence d'éléments d'ordre $d$ dans $G$ (évidemment l'ordre d'un élément est bien défini dans $\mathrm{CC}_m^\bullet(G)$). On obtient la décomposition suivante :

$$\mathrm{CC}_m^\bullet(G) = \coprod_{d|m, d>1} \mathrm{CC}_{m,d}^\bullet(G).$$

Pour un tel diviseur $d$ de $m$, l'application $\mathrm{CC}_{m,d}^\bullet(G) \to \mathrm{CC}_{d,d}^\bullet(G)$ est bien définie et est surjective. Elle est injective si $m$ est une puissance d'un nombre premier. Par conséquent, on peut identifier les deux ensembles lorsque $m = q^r$ où $q$ est un nombre premier, et on obtient alors la décomposition :

$$\mathrm{CC}_{q^r}^\bullet(G) = \coprod_{s=1}^{r} \mathrm{CC}_{q^s,q^s}^\bullet(G).$$

Le groupe $G$ auquel nous nous intéressons est $\mathrm{Aut}(\mathbb{Z}_p^2)$, que l'on peut identifier à $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. On obtient alors le résultat suivant.

**Lemme 5.4.15.** *Soient $p, q$ des nombres premiers impairs, et $r \geq 1$ tels que $q^r | (p-1)$. Soit $\xi$ une racine de l'unité d'ordre $q^r$ dans $\mathbb{Z}/p\mathbb{Z}$. L'ensemble*

$$\left\{ \begin{pmatrix} \xi & 0 \\ 0 & \xi^l \end{pmatrix},\ l \in \{1, 2, \ldots, \frac{q^r-1}{2}, q^r - 1\},\ \mathrm{PGCD}(q, l) = 1 \right\} \cup \left\{ \begin{pmatrix} \xi & 0 \\ 0 & \xi^{qu} \end{pmatrix},\ 0 \leq u < q^{r-1} \right\}$$

*est un ensemble de représentants des éléments de* $\mathrm{CC}^{\bullet}_{q^r, q^r}(\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}))$.

*Démonstration.*

Soit $\theta \in \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, d'ordre $q^r$. $\theta$ est racine du polynôme $X^{q^r} - 1 \in \mathbb{Z}/p\mathbb{Z}[X]$ donc son polynôme minimal $\mu_\theta$ divise $X^{q^r} - 1$. $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique d'ordre $p-1$, or par hypothèse $q^r \mid p-1$, donc il existe un unique sous-groupe d'ordre $q^r$ dans $(\mathbb{Z}/p\mathbb{Z})^*$. Ainsi le polynôme $X^{q^r} - 1 \in \mathbb{Z}/p\mathbb{Z}[X]$ est scindé à racines simples. Donc $\theta$ est diagonalisable et on peut ainsi supposer que $\theta$ est diagonal.
On note $\theta = \begin{pmatrix} \eta_1 & 0 \\ 0 & \eta_2 \end{pmatrix}$, avec $\eta_1, \eta_2 \in (\mathbb{Z}/p\mathbb{Z})^*$ tels que $\eta_1^{q^r} = 1 = \eta_2^{q^r}$.

On s'intéresse à présent à la relation d'équivalence :

$$\theta \simeq \theta' \iff \exists\ l \in [\![1, q^r]\!],\ \mathrm{PGCD}(l, q) = 1,\ \exists\ f \in \mathrm{Aut}(\mathbb{Z}_p^2) \text{ tels que } \theta'^l = f \circ \theta \circ f^{-1}.$$

On distingue alors plusieurs cas suivant les valeurs de $\eta_1$ et $\eta_2$. Comme $\theta$ est d'ordre $q^r$, au moins l'une des deux racines de l'unité doit être primitive.

Déterminons dans un premier temps les représentants possibles avec $\eta$ une racine primitive $q^r$-ième de l'unité fixée.

**Cas 1**

Il est clair que $\begin{pmatrix} 1 & 0 \\ 0 & \eta \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & \eta' \end{pmatrix}$ pour $\eta' \neq \eta$ racines primitives $q^r$-ième de l'unité.
Il suffit de prendre $f = \mathrm{id}$ et $l = k$ où $k$ est l'entier tel que $\eta' = \eta^k$.

**Cas 2**

En prenant $f$ la matrice de changement de base et $l = 1$, on obtient que : $\begin{pmatrix} \eta & 0 \\ 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & \eta \end{pmatrix}$, ce qui nous ramène au cas 1 ci-dessus.

**Cas 3**

On regarde à présent les conditions d'équivalence de deux matrices $\begin{pmatrix} \eta & 0 \\ 0 & \eta^k \end{pmatrix}$ et $\begin{pmatrix} \eta & 0 \\ 0 & \eta^{k'} \end{pmatrix}$ pour $k \neq k' \in [\![2, q^r - 2]\!]$ tels que $\mathrm{PGCD}(k, q) = 1 = \mathrm{PGCD}(k', q)$.

Comme $\begin{pmatrix} \eta & 0 \\ 0 & \eta^{k'} \end{pmatrix} \sim \begin{pmatrix} \eta^{k'} & 0 \\ 0 & \eta \end{pmatrix}$, on cherche l'équivalence entre $\begin{pmatrix} \eta & 0 \\ 0 & \eta^{k} \end{pmatrix}$ et $\begin{pmatrix} \eta^{k'} & 0 \\ 0 & \eta \end{pmatrix}$.

Pour obtenir l'équivalence, on doit prendre $f = \mathrm{id}$. Cela revient donc à présent, à trouver $l \in [\![1, q^r]\!]$, avec $\mathrm{PGCD}(l, q) = 1$ tel que :

$$\begin{pmatrix} \eta^{k'} & 0 \\ 0 & \eta \end{pmatrix}^l = \begin{pmatrix} \eta & 0 \\ 0 & \eta^{k} \end{pmatrix}.$$

On a alors : $k'l \equiv 1[q^r]$ et $k \equiv l[q^r]$. En prenant $l = k$, $\mathrm{PGCD}(l, q) = 1$ et l'équivalence n'est réalisée que lorsque $k' = k^{-1}$.

Ainsi les matrices de cette sorte sont groupées par paires dans les classes d'équivalence.

Le cas des matrices $\theta := \begin{pmatrix} \eta & 0 \\ 0 & \eta \end{pmatrix}$ et $\theta' := \begin{pmatrix} \eta & 0 \\ 0 & \eta^{-1} \end{pmatrix}$ est à traiter à part. Ces deux matrices ne sont pas équivalentes, ce qui fournit deux représentants supplémentaires.

En effet, si $\theta \sim \theta'$ alors on a l'existence de $l$ et $f$ tels que $\theta^l = f \circ \theta' \circ f^{-1}$. Or $\det(\theta') = 1$, donc on obtient, en appliquant le déterminant, l'équation : $\eta^{2l} = 1$. Comme $\mathrm{PGCD}(l, q) = 1$ et $\eta$ est une racine primitive $q^r$-ième de l'unité, on arrive à une contradiction.

**Cas 4**

Il reste à traiter les matrices du type $\begin{pmatrix} \eta & 0 \\ 0 & \eta^{k} \end{pmatrix}$ pour $k \in [\![1, q^r - 1]\!]$ tels que $\mathrm{PGCD}(k, q) \neq 1$.

On peut alors écrire $k = qu$ avec $1 \leqslant u < q^{r-1}$.

Dans ce cas, deux matrices $\begin{pmatrix} \eta & 0 \\ 0 & \eta^{qu} \end{pmatrix}$ et $\begin{pmatrix} \eta & 0 \\ 0 & \eta^{qu'} \end{pmatrix}$ avec $1 \leqslant u < q^{r-1}, 1 \leqslant u' < q^{r-1}$, $u \neq u'$, ne sont jamais équivalentes. Cela nous fournit de nouveaux représentants.

Revenons à $\theta = \begin{pmatrix} \eta_1 & 0 \\ 0 & \eta_2 \end{pmatrix}$. On se ramène toujours aux cas précédents :

— Si $\eta_1 = 1$ et $\eta_2$ est une racine primitive $q^r$-ième de l'unité, alors on se ramène au cas 1.

— Si $\eta_1$ est une racine primitive $q^r$-ième de l'unité et $\eta_2 = 1$, alors on se ramène au cas 2.

— Si $\eta_1$ et $\eta_2$ sont deux racines primitives $q^r$-ième de l'unité, alors on se ramène au cas 3.

— Si $\eta_1$ ou $\eta_2$ est primitive et l'autre non, alors on se ramène au cas 4.

Soit $\xi$ une racine primitive $q^r$-ième de l'unité fixée. On obtient alors l'ensemble des représentants à équivalence près des automorphismes de $\mathbb{Z}_p^2$ qui sont :

$$\begin{pmatrix}1 & 0\\ 0 & \xi\end{pmatrix}, \quad \left\{\begin{pmatrix}\xi & 0\\ 0 & \xi^k\end{pmatrix}, k \in [\![2, \frac{q^r-1}{2}]\!], \mathrm{PGCD}(k,q)=1\right\}, \quad \left\{\begin{pmatrix}\xi & 0\\ 0 & \xi^{qu}\end{pmatrix}, 1 \leqslant u < q^{r-1}\right\},$$

$$\begin{pmatrix}\xi & 0\\ 0 & \xi\end{pmatrix}, \quad \begin{pmatrix}\xi & 0\\ 0 & \xi^{-1}\end{pmatrix}.$$

En regroupant les matrices isolées, on obtient bien les deux ensembles de représentants annoncés dans le lemme. □

À présent, discutons des conditions d'appartenance de ces automorphismes à un $q^r$-datum réduit de $\mathbb{Z}_p^2$.

**Lemme 5.4.16.** *Soient $p, q$ des nombres premiers impairs et $r \geq 1$ tels que $q^r | (p-1)$. Soit $\theta$ un automorphisme d'ordre $q^r$ dans $\mathbb{Z}_p^2$, représenté par l'une des matrices du lemme précédent.*

1. *Si $\theta = \begin{pmatrix}\xi & 0\\ 0 & \xi^{-1}\end{pmatrix}$, il n'existe aucun $q^r$-datum réduit ayant $\theta$ comme automorphisme.*
2. *Dans les autres cas, il existe, à équivalence près, un unique $q^r$-datum réduit ayant $\theta$ comme automorphisme.*

*Démonstration.*

Fixons $x_1$, $x_2$ des générateurs de $\mathbb{Z}_p^2$, et pour $\omega \in \mu_p$, on définit $\tau_\omega : \mathbb{Z}_p^2 \times \mathbb{Z}_p^2 \to k^\times$ l'unique bi-caractère tel que

$$\tau_\omega(x_1,x_1) = 1 = \tau_\omega(x_2,x_2) = \tau_\omega(x_2,x_1), \quad \tau_\omega(x_1,x_2) = \omega.$$

Rappelons le résultat connu suivant : tout 2-cocycle de $\mathbb{Z}_p^2$ est cohomologue à $\tau_\omega$ pour $\omega \in \mu_p$. De plus, deux 2-cocycles $\tau_\omega$ et $\tau_{\omega'}$ sont cohomologues si et seulement si $\omega = \omega'$.

D'après le corollaire 4.2.3, on peut supposer que tout $q^r$-datum possède un cocycle sous-jacent du type $\tau_\omega$ avec $\omega \in \mu_p$.

Notons $\theta = \begin{pmatrix}\eta_1 & 0\\ 0 & \eta_2\end{pmatrix}$.

Par un calcul direct, avec $\omega \neq 1$, on obtient :

$$\prod_{k=0}^{q^r-1} \tau_\omega \circ (\theta^k \times \theta^k)(x_1,x_1) = 1, \quad \prod_{k=0}^{q^r-1} \tau_\omega \circ (\theta^k \times \theta^k)(x_2,x_2) = 1,$$

$$\prod_{k=0}^{q^r-1} \tau_\omega \circ (\theta^k \times \theta^k)(x_2,x_1) = 1,$$

$$\prod_{k=0}^{q^r-1} \tau_\omega \circ (\theta^k \times \theta^k)(x_1, x_2) = 1 \text{ si } \eta_1\eta_2 \neq 1 \text{ et } \omega^{q^r} \text{ si } \eta_1\eta_2 = 1.$$

Donc $\prod_{k=0}^{q^r-1} \tau_\omega \circ (\theta^k \times \theta^k)$ vaut $\mathbb{1}$ si $\eta_1\eta_2 \neq 1$ et vaut $\tau_{\omega^{q^r}}$ si $\eta_1\eta_2 = 1$.

On utilise à présent le fait que $\prod_{k=0}^{q^r-1} \tau_\omega \circ (\theta^k \times \theta^k) = \delta(a^{-1})$, et que $H^2(\mathbb{Z}_p^2, \Bbbk^\times)$ est cyclique d'ordre $p$.

Supposons que $\eta_1\eta_2 = 1$. On obtient que $[\tau_{\omega^{q^r}}] = [\mathbb{1}]$ et donc $\omega^{q^r} = 1$. Comme $\omega \in \mu_p$, $\omega \neq 1$, on a alors $p \mid q^r$ ce qui contredit l'hypothèse $q^r \mid p-1$.

Donc $\theta$ tel que $\eta_1\eta_2 = 1$ ne permet pas de créer un datum réduit. Donc nécessairement, on doit avoir $\eta_1\eta_2 \neq 1$.

Parmi les représentants déterminés dans le lemme précédent, le cas où $\theta = \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix}$, ne permet pas d'obtenir un $q^r$-datum réduit ayant $\theta$ comme automorphisme sous-jacent.

Passons à la démonstration de la deuxième assertion.

On a vu que $\eta_1\eta_2 \neq 1$, et donc $\prod_{k=0}^{q^r-1} \tau_\omega \circ (\theta^k \times \theta^k) = 1 = \delta(a^{-1})$ et on obtient alors que $a \in \widehat{\mathbb{Z}_p^2}$.

De plus, pour tout $a \in \widehat{\mathbb{Z}_p^2}$ tel que $a \circ \theta = a$, on obtient un $q^r$-datum réduit $(\mathbb{Z}_p^2, \theta, a, \tau_\omega)$, et inversement tout $q^r$-datum réduit est de cette forme.

Plus précisément, la condition $a \circ \theta = a$ nous donne les équations suivantes :

$$a(x_1)^{\eta_1 - 1} = 1, \quad a(x_2)^{\eta_2 - 1} = 1.$$

Si $a = \mathbb{1}$ alors les deux équations sont vérifiées, peu importe le représentant de $\theta$ choisi (vérifiant tout de même $\eta_1\eta_2 \neq 1$).

Si $a \neq \mathbb{1}$, alors $a(x_1) \neq 1$ ou $a(x_2) \neq 1$.

— Supposons que $a(x_1) = \mu \neq 1$ avec $\mu \in \mu_p$. Ainsi $\eta_1 \equiv 1[p]$ et donc $\theta = \begin{pmatrix} 1 & 0 \\ 0 & \eta_2 \end{pmatrix}$.
Comme $\eta_1\eta_2 \neq 1$, $\eta_2 \neq 1$ donc pour que $a(x_2)^{\eta_2 - 1} = 1$ il faut que $a(x_2) = 1$.

— En inversant les rôles, si on suppose que $a(x_2) = \mu' \neq 1$, alors on obtient par le même raisonnement que $a(x_1) = 1$ et donc $\theta = \begin{pmatrix} \eta_1 & 0 \\ 0 & 1 \end{pmatrix}$.

Il reste à déterminer les cas d'équivalence entre les $q^r$-data obtenus.

Établissons la classification à équivalence près au cas par cas en reprenant les notations du lemme 5.4.15 où $\xi$ est une racine $q^r$-ième primitive de l'unité.

— Si $\theta = \begin{pmatrix} \xi & 0 \\ 0 & 1 \end{pmatrix}$, les $a$ compatibles sont des éléments de $\widehat{\mathbb{Z}_p^2}$ tels que $a(x_1) = 1$ et $a(x_2) \neq 1$. Il existe $k$ avec $0 \leq k \leq p-1$ tel que $a(x_2) = \omega^k$. On note $a_k$ un tel élément dans $\widehat{\mathbb{Z}_p^2}$.
Ainsi pour $0 \leq k_1 \leq p-1$ et $1 \leq k_2 \leq p-1$ ($\omega \neq 1$), les $q^r$-data $(\mathbb{Z}_p^2, \theta, 1, \tau_\omega)$ et $(\mathbb{Z}_p^2, \theta, a_{k_1}, \tau_{\omega^{k_2}})$ sont équivalents, pour $f^{-1} = \begin{pmatrix} k_2 & 0 \\ 0 & 1 \end{pmatrix}$ et $\varphi \in \widehat{\mathbb{Z}_p^2}$ tel que $\varphi(x_1) = 1$ et $\varphi(x_2)^{q^r} = \omega^{-k_1}$, avec les notations de la définition 4.2.1.

— Si $\theta = \begin{pmatrix} \xi & 0 \\ 0 & \xi^i \end{pmatrix}$, avec $\xi^i \neq 1$ alors le seul $a$ compatible est $a = \mathbb{1}$. On peut écrire que, pour $1 \leq k \leq p-1$ ($\omega \neq 1$), les $q^r$-data $(\mathbb{Z}_p^2, \theta, 1, \tau_\omega)$ et $(\mathbb{Z}_p^2, \theta, 1, \tau_{\omega^k})$ sont équivalents, avec les notations de la définition 4.2.1, pour $f^{-1} = \begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix}$ et $\varphi = \mathbb{1}$.

Finalement, dans les autres cas, on a montré qu'il n'y avait qu'un seul datum à équivalence près, ce qui conclut la preuve. □

*Démonstration du théorème 5.4.14.*

Soit $A$ une algèbre de Hopf comme donnée dans le théorème 5.4.14. Alors il existe un $q^r$-datum $(\mathbb{Z}_p^2, \theta, a, \tau)$ tel que $A \simeq A_{q^r}(\mathbb{Z}_p^2, \theta, a, \tau)$, avec $\theta \neq \mathrm{id}$ et $[\tau] \neq 1$ (proposition 4.2.8). De plus, d'après la preuve du lemme précédent, le datum est réduit.

Par conséquent, d'après la proposition 4.2.11 (et le théorème 4.2.12), on a une bijection entre les classes d'isomorphisme d'algèbres de Hopf $A$ ayant les caractéristiques énoncées dans le théorème et les classes d'équivalence de $q^r$-data $(\mathbb{Z}_p^2, \theta, a, \tau)$ avec $\theta \neq \mathrm{id}$ et $[\tau] \neq 1$.

Pour $1 \leq s \leq r$, posons $\mathcal{E}_s$ l'ensemble des classes d'équivalence de $q^r$-data comme ci-dessus, avec $\theta$ d'ordre $q^s$. On obtient ainsi $\mathcal{E} = \coprod_{s=1}^r \mathcal{E}_s$. En utilisant le corollaire 4.2.3, les lemmes 5.4.15 et 5.4.16, on obtient le dénombrement suivant :

— $\theta = \begin{pmatrix} 1 & 0 \\ 0 & \xi \end{pmatrix}$ fournit 1 datum.

— L'ensemble $\left\{ \begin{pmatrix} \xi & 0 \\ 0 & \xi^l \end{pmatrix},\ l \in \{2, \dots, \frac{q^s-1}{2}\},\ \mathrm{PGCD}(q,l) = 1 \right\}$ contient $\frac{q^s - q^{s-1}}{2} - 1$ éléments.

— L'ensemble $\left\{ \begin{pmatrix} \xi & 0 \\ 0 & \xi^{qu} \end{pmatrix},\ 1 \leq u \leq q^{s-1} - 1 \right\}$ contient $q^{s-1} - 1$ éléments.

— $\theta = \begin{pmatrix} \xi & 0 \\ 0 & \xi \end{pmatrix}$ fournit 1 datum.

— $\theta = \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix}$ ne fournit aucun datum.

Au total, pour chaque $1 \leq s \leq r$, on a donc :
$|\mathcal{E}_s| = 1 + (\frac{q^s - q^{s-1}}{2} - 1) + (q^{s-1} - 1) + 1 = \frac{q^s - q^{s-1}}{2} + q^{s-1} = \frac{q^s - q^{s-1} + 2q^{s-1}}{2} = \frac{q^s + q^{s-1}}{2}$.

Finalement, comme $\mathcal{E} = \coprod_{s=1}^{r} \mathcal{E}_s$, on obtient :

$$|\mathcal{E}| = \sum_{s=1}^{r} |\mathcal{E}_s| = \sum_{s=1}^{r} \frac{q^s + q^{s-1}}{2}.$$

Ce qui achève la preuve.
Si $r = 1$, la démonstration a été faite dans [26]. □

Le raisonnement précédent fonctionne également lorsque $q = 2$. La seule différence concerne le comptage des représentants des automorphismes du lemme 5.4.15. Le résultat est le suivant :

**Théorème 5.4.17.** *Soit $p$ un nombre premier impair et $r \geq 1$. Supposons que $2^r | p - 1$. Le nombre de classe d'isomorphisme d'algèbres de Hopf s'insérant dans une extension cocentrale $k \to \mathcal{O}(\mathbb{Z}_p^2) \to A \to k\mathbb{Z}_{2^r} \to k$ vaut 1 si $r = 1$, et vaut $2(3.2^{r-2} - 1)$ si $r \geq 2$.*

*Démonstration.*

Comme déjà indiqué, le raisonnement est similaire à la démonstration du théorème précédent. On ne donnera pas plus de détails ici, si ce n'est dans le calcul final de $|\mathcal{E}|$.

Le cas $r = 1$ est à traiter séparément. En effet, dans ce cas les $\theta$ possibles sont réduit à la seule matrice $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, laquelle fournit un seul 2-datum à équivalence près donc $|\mathcal{E}| = 1$.

D'autre part, si $r \geq 1$, le dénombrement est le même que précédemment et on obtient, en séparant le cas $s = 1$ du reste :

$$\begin{aligned}
|\mathcal{E}| &= 1 + \sum_{s=2}^{r} |\mathcal{E}_s| \\
&= 1 + \sum_{s=2}^{r} \frac{2^s + 2^{s-1}}{2} \\
&= 1 + \frac{1}{2}(\sum_{s=2}^{r} 2^s + \sum_{s=2}^{r} 2^{s-1}) \\
&= 1 + \frac{1}{2}(2^2.\frac{2^{r-1} - 1}{2 - 1} + 2.\frac{2^{r-1} - 1}{2 - 1}) \\
&= 1 + 3(2^{r-1} - 1) \\
&= 2(3.2^{r-2} - 1).
\end{aligned}$$

D'où le résultat. □

Encore une fois si $r = 1$, le résultat a été obtenue dans [26].

Ce dernier résultat achève le travail de classification effectué tout au long de ces trois années de thèse.

# Bibliographie


[1] N. Andruskiewitsch, J. Devoto, Extensions of Hopf algebras, *St. Petersburg Math. J.* **7** (1996), no. 1, 17-52.

[2] N. Andruskiewitsch, M. Müller, Examples of extensions of Hopf algebras, *Rev. Colombiana Mat.* **49** (2015), no. 1, 193-211.

[3] J. Bichon, S. Natale, Hopf algebra deformations of binary polyhedral groups, *Transform. Groups* **16** (2011), no. 2, 339-374.

[4] J. Bichon, S. Neshveyev, M. Yamashita, Graded twisting of categories and quantum groups by group actions, *Ann. Inst. Fourier (Grenoble)* **66** (2016), no. 6, 2299-2338.

[5] J. Bichon, S. Neshveyev, M. Yamashita, Graded twisting of comodule algebras and module categories, *J. Noncommut. Geom.* **12** (2018), no. 1, 331-368.

[6] A. Chirvasitu, Centers, cocenters and simple quantum groups, *J. Pure Appl. Algebra* **218** (2014), no. 8, 1418-1430.

[7] A. Chirvasitu, P. Kasprzak, On the Hopf (co)center of a Hopf algebra, *J. Algebra* **464** (2016), 141-174.

[8] J. A. Dieudonné, La géométrie des groupes classiques. Troisième édition. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 5. Springer-Verlag, Berlin-New York, 1971.

[9] Y. Doi, Braided bialgebras and quadratic bialgebras, *Comm. Algebra* **21** (1993), no. 5, 1731-1749.

[10] N. Fukuda, Semisimple Hopf algebras of dimension 12, *Tsukuba J. Math.* **21** (1997), no. 1, 43-54.

[11] C. Galindo, Y. Morales, A five-term exact sequence for Kac cohomology, *Algebra Number Theory* **13** (2019), no. 5, 1121-1144.

[12] P.J. Hilton, U. Stammbach, A course in homological algebra. Second edition. Graduate Texts in Mathematics, 4. Springer-Verlag, 1997.

[13] G. I. Kac, Extensions of groups to ring groups, *Math. USSR, Sb.* **5** (1969), 451-474.

[14] G. Karpilovsky, The Schur multiplier. London Mathematical Society Monographs. New Series, 2. The Clarendon Press, Oxford University Press, New York, 1987.

[15] G. Karpilovsky, Projective representations of finite groups, Monographs and Textbooks in Pure and Applied Mathematics, 94. Marcel Dekker, Inc., New York, 1985.

[16] Y. Kashina, Classification of semisimple Hopf algebras of dimension 16, *J. Algebra* **232** (2000), no. 2, 617-663.

[17] Y. Kashina, On semisimple Hopf algebras of dimension $2^m$, *Algebr. Represent. Theory* **6** (2003), no. 4, 393-425.

[18] Y. Kashina, On semisimple Hopf algebras of dimension $2^m$, II, *Algebr. Represent. Theory* **19** (2016), no. 6, 1387-1422.

[19] D. Kazhdan, H. Wenzl, Reconstructing monoidal categories, I. M. Gelfand Seminar, 111-136, *Adv. Soviet Math.*, **16**, Part 2, Amer. Math. Soc., Providence, RI, 1993.

[20] L. Krop, On the classification of finite-dimensional semisimple Hopf algebras, *Contemp. Math.* **688** (2017), 181-218.

[21] A. Masuoka, Self-dual Hopf algebras of dimension $p^3$ obtained by extension, *J. Algebra* **178** (1995), no. 3, 791-806.

[22] A. Masuoka, Calculations of some groups of Hopf algebra extensions, *J. Algebra* **191** (1997), no. 2, 568-588.

[23] A. Masuoka, Extensions of Hopf algebras, *Trab. Math. (FAMAF)* **31**, 1999.

[24] A. Masuoka, Y. Doi, Generalization of cleft comodule algebras, *Comm. Algebra* **20** (1992), no. 12, 3703-3721.

[25] S. Montgomery, Hopf algebras and their actions on rings, Amer. Math. Soc. 1993.

[26] S. Natale, On semisimple Hopf algebras of dimension $pq^2$, *J. Algebra* **221** (1999), no. 1, 242-278.

[27] S. Neshveyev, M. Yamashita, Twisting the q-deformations of compact semisimple Lie groups, *J. Math. Soc. Japan* **67** (2015), no. 2, 637-662.

[28] P. Podleś, Symmetries of quantum spaces. Subgroups and quotient spaces of quantum SU(2) and SO(3) groups, *Comm. Math. Phys.* **170** (1995), no. 1, 1-20.

[29] H.J. Schneider, Normal basis and transitivity of crossed products for Hopf algebras. *J. Algebra* **152** (1992), no. 2, 289-312.

[30] J. J. Zhang, Twisted graded algebras and equivalences of graded categories, *Proc. London Math. Soc.* **72** (1996), no. 2, 281-311.