Institut de mathématiques

Modules d'endo-permutation

Thèse de doctorat

présentée à la

Faculté des Sciences de
l'Université de Lausanne

par

Nadia Mazza

Diplômée en Mathématiques
Université de Lausanne

Jury

M. le Professeur Gervais Chapuis, Président
M. le Professeur Jacques Thévenaz, Directeur de thèse
M. le Professeur Serge Bouc, Expert
M. le Professeur Jon Carlson, Expert
Mme. le Professeur Donna Testerman, Expert

Lausanne
2003

«J'étais assis, un peu voûté, la tête basse,
seul en face de cette masse
noire et noueuse entièrement brute
et qui me faisait peur.
Et puis j'ai eu cette illumination.»

Jean-Paul Sartre, La nausée.

Table des matières

0.1 Résumé

Dans la théorie des représentations modulaires des groupes finis, les modules d'endo-permutation occupent une place importante. En effet, c'est le rôle joué par ces modules dans l'analyse de la structure de certains modules simples pour des groupes finis p-nilpotents, qui a amené E. Dade à en introduire le concept, en 1978. Quelques années plus tard, L. Puig a démontré que la source de n'importe quel module simple pour un groupe fini p-résoluble quelconque est un module d'endo-permutation. Plus récemment, on s'est rendu compte que ces modules interviennent aussi dans l'analyse locale des catégories dérivées et dans l'étude des systèmes de fusion.

La situation que l'on considère est la suivante. On se donne un nombre premier p, un p-groupe fini P, un corps algébriquement clos k de caractéristique p et on veut déterminer tous les kP-modules d'endo-permutation couverts indécomposables de type fini, c'est-à-dire tous les kP-modules indécomposables de type fini, tels que leur algèbre d'endomorphismes est un kP-module de permutation ayant un facteur direct trivial. On définit une relation d'équivalence sur l'ensemble de ces kP-modules et le produit tensoriel des modules induit une structure de groupe abélien sur l'ensemble des classes d'équivalence. On appelle ce groupe, le groupe de Dade de P. Ainsi, classifier les modules d'endo-permutation couverts revient à déterminer le groupe de Dade de P.

Le groupe de Dade d'un p-groupe fini arbitraire est encore inconnu, bien qu'E. Dade, en 1978, était déjà parvenu à la classification dans le cas où P est abélien. La première partie de ce travail de thèse est consacrée au problème de la classification dans le cas général et résoud la question dans le cas de deux familles de p-groupes finis, à savoir celle des p-groupes métacycliques, pour un nombre premier p impair, et celle des 2-groupes extraspéciaux, de la forme $D_8 * \cdots * D_8$. Ces deux choix ont été motivés par le fait que ces groupes sont "presque" abéliens. De plus, certains résultats sur la structure du groupe de Dade d'un p-groupe fini quelconque rendent le groupe de Dade des groupes de ces deux familles plus simple à étudier.

Dans un deuxième temps, nous nous sommes intéressés à deux occurrences de ces modules dans la théorie de la représentation des groupes finis, c'est-à-dire à deux raisons qui motivent leur étude. Ainsi, nous avons réalisé des modules d'endo-permutation comme sources de modules simples. En particulier, il s'avère que, dans le cas d'un nombre premier p impair, tout module d'endo-permutation indécomposable dont la classe est un élément de torsion dans le groupe de Dade est la source d'un module simple. Finalement, nous avons déterminé, parmi tous les modules d'endo-permutation connus actuellement, lesquels possèdent une résolution de permutation endo-scindée. Nous sommes arrivés à la conclusion que les seuls modules d'endo-permutation qui n'ont pas de résolution de permutation endo-scindée sont les modules "exceptionnels" apparaissant pour un 2-groupe de quaternions généralisés.

0.2 Abstract

This dissertation is concerned with the classification of endo-permutation modules. These modules were first introduced by E. Dade, in 1978, and their study is motivated by the important role they play in some areas of representation theory of finite groups.

For instance, they appear as sources of simple modules for finite p-solvable groups, as it has been proved by L. Puig. They also occur in the local analysis of splendid derived equivalences between blocks. Indeed, J. Rickard noticed that some of them have an endo-split permutation resolution inducing this equivalence. At present, it turns out that they are also of relevant importance in the study of fusion systems, considered in topology, as well as in group theory. Let us give an outline of the situation.

Given a prime number p, a finite p-group P and an algebraically closed field k of characteristic p, we say that a finitely generated module M is an endo-permutation module if its endomorphism algebra $End_k M$ is a permutation kP-module. We say that an endo-permutation module is capped if it has an indecomposable direct summand with vertex P.

We can define an equivalence relation on the set of (isomorphism classes of) capped endo-permutation kP-modules and the set of all equivalence classes is a finitely generated abelian group for the associative law induced by the tensor product. We call this group the Dade group of P.

Hence, the question of the classification of all endo-permutation kP-modules reduces to the computation of the Dade group of P.

In 1978, Dade solved this problem in case P is an abelian p-group. More than twenty years later, the general case is still open and we only have some partial results on the group structure.

Our contribution to the classification of endo-permutation modules consists in determining the Dade group of two families of finite p-groups, namely metacyclic p-groups for an odd prime number p, and extraspecial 2-groups of the shape D_8^{*n}, for an integer $n \geq 2$.

We also consider some aspects of the theory where these modules occur. More precisely, we give an explicit realization of "many" endo-permutation modules as sources of simple modules and, following a recent result of J. Carlson, this proves that all torsion endo-permutation modules effectively occur as sources of simple modules, for an odd prime number p.

Finally, using work of S. Bouc and J. Rickard, we prove that among all endo-permutation modules we know at present, the only ones which don't have an endo-split permutation resolution are the "exceptional" modules occuring for a generalized quaternion 2-group.

0.3 Introduction

Le sujet de ce travail de thèse s'inscrit dans le cadre de la théorie de la représentation des groupes finis. Cette branche des mathématiques dérive de l'étude des groupes finis et a pour objectif d'obtenir des informations sur la structure d'un groupe fini à partir de ses représentations. Autrement dit, elle a pour but de classifier les modules (à isomorphisme près) sur des algèbres de groupes finis.

Les débuts de cette théorie se situent vers la fin du XIX$^{\text{ème}}$ siècle et on les associe surtout aux travaux de Frobenius et de Burnside. Elle continue à se développer dans la première partie du XX$^{\text{ème}}$, grâce notamment à Schur et à Brauer. Ce dernier a révolutionné l'approche des représentations d'un groupe fini, en quittant le corps des complexes, pour considérer des corps dont la caractéristique divise l'ordre du groupe. Il est à l'origine de ce que l'on appelle aujourd'hui la théorie des représentations modulaires.

En ce début de XXI$^{\text{ème}}$ siècle, cette ramification de la théorie des groupes finis continue à occuper une place d'honneur dans le domaine de la recherche en algèbre. En fait, elle a pris tellement d'ampleur que depuis quelques années elle suscite également l'intérêt de nos confrères topologues. En effet, de nos jours, on utilise souvent des méthodes cohomologiques (et donc issues de la topologie) pour résoudre des problèmes concernant les groupes. Et réciproquement, les topologues emploient des résultats purement algébriques des représentations des groupes dans leurs travaux.

On connaît depuis bien longtemps les représentations ordinaires d'un groupe fini G, c'est-à-dire les $\mathbb{C}G$-modules. En effet, par le théorème de Maschke, on sait que toute représentation se décompose comme somme directe de représentations irréductibles, et celles-ci sont en nombre fini et "résumées" par leur table des caractères. Celle-ci nous fournit d'ailleurs des informations fort intéressantes concernant le groupe G, bien qu'elle ne le caractérise pas, car deux groupes distincts peuvent avoir la même table des caractères.

Ce résultat se généralise pour un corps K "assez gros" et dont la caractéristique ne divise pas l'ordre du groupe G. Par contre, la situation devient plus chaotique lorsqu'on quitte ce cadre idyllique pour considérer un corps K dont la caractéristique (nécessairement première) divise l'ordre de G. Dans ce cas, il n'est plus vrai que toute représentation se décompose comme somme directe de représentations irréductibles. Par le théorème de Krull-Schmidt, on a alors un certain contrôle de la situation si on remplace la notion d'irréductibilité par celle d'indécomposabilité. Toutefois, on n'a pas un nombre fini de KG-modules indécomposables, en général, et leur classification complète se révèle passablement ardue, pour ne pas dire impossible. C'est la raison pour laquelle il est préférable de focaliser notre attention sur des familles de modules satisfaisant certaines propriétés.

C'est ce que nous avons fait, en considérant la famille des modules d'endopermutation, que l'on définit comme suit. Etant donné un nombre premier p, un p-groupe fini P et un corps k "assez gros" et de caractéristique p, on dit

qu'un kP-module M est d'endo-permutation si son algèbre d'endomorphismes $\mathrm{End}_k M$ est un kP-module de permutation.

Ces modules ont été introduits en 1978 par E. Dade et on lui doit leur classification dans le cas où P est abélien. La méthode qu'il a utilisée pour en faire la classification est la suivante. Parmi tous les modules d'endo-permutation, il suffit de regarder ceux qui ont un facteur direct indécomposable de vortex P. On dit qu'ils sont couverts ("*capped*", en anglais). Comme chaque kP-module d'endo-permutation couvert possède un unique facteur direct indécomposable de vortex P, appelé chapeau ("*cap*", en anglais), on peut définir une relation d'équivalence sur l'ensemble de ces modules en considérant les classes d'isomorphismes des chapeaux. L'ensemble des classes d'équivalence est stable pour le produit tensoriel (sur k) des modules, et en fait, cela induit une structure de groupe sur cet ensemble. C'est le groupe de Dade de P. Ainsi, la classification des kP-modules d'endo-permutation se ramène à l'étude du groupe de Dade de P.

Contrairement au cas abélien, résolu aussitôt la notion de module d'endo-permutation définie, on essaie de résoudre le cas général, depuis plus de vingt ans, en vain. Seuls des résultats partiels ont été obtenus concernant la structure du groupe de Dade. On sait, en particulier, que c'est un groupe abélien de type fini.

Décrivons à présent comment nous avons organisé la présentation de notre travail.

La première partie de cet ouvrage est consacrée à l'étude du groupe de Dade. Dans le premier chapitre, nous exposons les notions de base dont nous avons besoin pour notre analyse. Dans le deuxième, nous traçons un bref historique du groupe de Dade. Ensuite, dans les deux chapitres suivants, nous déterminons le groupe de Dade des p-groupes métacycliques, pour un nombre premier p impair, et le groupe de Dade des 2-groupes extraspéciaux de la forme D_8^{*n}, pour un nombre entier n valant au moins 2.

La seconde partie de l'ouvrage est consacrée aux occurrences des modules d'endo-permutation dans la théorie de la représentation des groupes finis. Dans le cinquième chapitre, nous réalisons les modules d'endo-permutation comme sources de modules simples. Cette application est motivée par un résultat que L. Puig a démontré dans les années 80, à savoir que les sources de modules simples pour des groupes finis p-résolubles sont des modules d'endo-permutation d'une certaine forme. Nous avons donc abordé cette question sous un autre angle, en nous demandant si chacun des modules de cette forme donnée apparaissaît effectivement comme source d'un module simple.

Grâce aux récents résultats de J. Carlson et J. Thévenaz, il s'avère en particulier que, pour p impair, tous les modules indécomposables dont la classe est un élément de torsion dans le groupe de Dade sont des sources de modules simples.

Finalement, nous avons fait un petit détour du côté des équivalences dérivées et nous avons considéré une remarque de J. Rickard. Il a constaté que si un module possède une résolution de permutation endo-scindée, alors le module

en question est d'endo-permutation. Comme pour la question précédente, nous avons regardé le problème d'un autre point de vue, en déterminant, parmi tous les modules d'endo-permutation connus actuellement, lesquels possèdent une résolution de permutation endo-scindée. En emboîtant, comme s'il s'agissait des pièces d'un puzzle, les travaux de S. Bouc et de J. Rickard, nous sommes arrivés à la conclusion que les seuls modules d'endo-permutation qui n'ont pas de résolution de permutation endo-scindée sont les modules "exceptionnels" apparaissant pour un groupe quaternionien.

Ce travail de thèse est loin de résoudre toutes les questions concernant la classification des modules d'endo-permutation. Les résultats qu'il contient ne constituent en fait que quelques briques supplémentaires pour l'édification de cette classification. Relevons également le fait que les résultats des chapitres 3 et 5 sont publiés (cf. [Ma1] et [Ma2] respectivement).

Terminons ce paragraphe introductif avec la remarque suivante. Les différentes techniques développées dans les récents travaux de S. Bouc, d'une part, et de J. Carlson et J. Thévenaz, d'autre part, ont permis d'obtenir des résultats très prometteurs quant au succès de la classification des modules d'endo-permutation. Les moyens mis en oeuvre par S. Bouc donnent une vision fonctorielle du groupe de Dade, alors que ceux utilisés par J. Carlson et J. Thévenaz font intervenir, entre autres, la cohomologie des groupes.

Première partie

Le groupe de Dade

Chapitre 1

Notions de base

1.1 Représentations des groupes finis

L'objectif de ce premier chapitre est de définir et donner les principales propriétés des objets que nous allons utiliser par la suite. Sauf mention expresse, les preuves des affirmations que nous avançons dans cette section se trouvent dans [CR].

Convention. Si A est un anneau (par exemple $A = R$ ou $A = RG$ dans la définition suivante), nous allons supposer que tous les A-modules sont des A-modules à gauche de type fini. De plus, nous allons toujours considérer les A-modules à isomorphisme près. Autrement dit, lorsque nous dirons qu'un module est unique, nous sous-entendrons qu'il est unique *à isomorphisme près.*

Définition 1.1.1. *Soient R un anneau commutatif et G un groupe fini.*

1. *L'***algèbre du groupe** *G est la R-algèbre RG définie comme suit.*

$$RG = \Big\{ \sum_{g\in G} a_g g \mid a_g \in R,\ \forall\, g \in G \Big\},\ \textit{où on définit}$$

$$\Big(\sum_{g\in G} a_g g\Big) + \Big(\sum_{g\in G} b_g g\Big) = \sum_{g\in G} (a_g + b_g) g \ \textit{et}$$

$$\Big(\sum_{g\in G} a_g g\Big) \cdot \Big(\sum_{h\in G} b_h h\Big) = \sum_{g\in G}\sum_{h\in G} (a_g b_h)(gh) = \sum_{g\in G} \big(\sum_{h\in G} a_{gh^{-1}} b_h\big) g,$$

   pour tous $\sum_{g\in G} a_g g$ et $\sum_{g\in G} b_g g \in RG$.
   En général, RG est un anneau non commutatif.

2. *Soit n un entier avec $n \geq 1$. Une* **représentation** *(***linéaire***)* **de** *G* **sur** *R* **de degré** *n est un homomorphisme de groupes $\rho : G \longrightarrow \mathrm{Aut}_R(V)$, où V est un R-module libre de rang n et $\mathrm{Aut}_R(V)$ est le groupe des automorphismes R-linéaires de V. Rappelons qu'un R-module V est dit* **libre**

si V possède une R-base, i.e. s'il existe un sous-ensemble X de V tel que tout élément de V s'écrive de manière unique comme une combinaison R-linéaire d'éléments de X. Dans cette situation, on appelle **rang** *de V la cardinalité de X.*

La donnée d'une représentation ρ de G sur R de degré n est équivalente à la donnée d'un RG-module V libre comme R-module et de rang n sur R, l'action de G sur V étant donnée par $g \cdot v = \rho(g)(v)$, $\forall\, g \in G$ et $\forall\, v \in V$.

Dorénavant, soit $\rho : G \longrightarrow \mathrm{Aut}_R(V)$ une représentation de G.

3. *Le* **caractère** *de ρ est l'application R-linéaire $\chi_\rho : G \longrightarrow R$, définie par $\chi_\rho(g) = \mathrm{Tr}(\rho(g))$, $\forall\, g \in G$, où $\mathrm{Tr}(\rho(g))$ est la trace de l'homomorphisme $\rho(g)$.*
4. *Une* **sous-représentation** *de ρ est la donnée d'un homomorphisme de groupes $\rho' : G \longrightarrow \mathrm{Aut}_R(W)$, où W est un RG-***sous-module** *de V, c'est-à-dire un R-sous-module de V tel que $g \cdot w \in W$, $\forall\, g \in G$ et $\forall\, w \in W$.*
5. *On dit que ρ est* **irréductible** *si ρ ne possède pas de sous-représentation propre non triviale, c'est-à-dire si V n'est pas nul et ne possède pas de sous-module propre non nul. On dit alors que V est un RG-***module simple**.
6. *On dit qu'une représentation ρ de G est* **indécomposable** *si V est un RG-***module indécomposable**, c'est-à-dire si V n'est pas nul et ne peut s'exprimer comme la somme directe de deux RG-sous-modules propres. En particulier, une représentation irréductible est indécomposable. Rappelons qu'une somme $M + N$ de deux modules est* **directe**, *et on note alors $M \oplus N$, si tout élément x de $M + N$ s'écrit de manière unique sous la forme $x = m + n$, avec $m \in M$ et $n \in N$.*

Définition et proposition 1.1.2. *Soient K un corps et G un groupe fini.*

1. *On dit que K est* **suffisamment gros** *pour G si K possède une racine n-ième de l'unité, où n est l'exposant de G.*
2. *On dit que KG est* **semi-simple** *si toute représentation se décompose comme somme directe de représentations irréductibles. C'est le cas si et seulement si la caractéristique de K ne divise pas l'ordre de G.*

   Si, de plus, K est suffisamment gros pour G, alors le nombre de représentations irréductibles est égal au nombre de classes de conjugaison des éléments de G et donc on a un nombre fini de classes d'isomorphisme de KG-modules simples.

   C'est le cas, en particulier, si $K = \mathbb{C}$ et on parle alors de **représentations ordinaires** *de G.*
3. *Soient p un nombre premier et $\mathcal{O}$ un anneau de valuation discrète (et donc $\mathcal{O}$ est un anneau local), complet, d'unique idéal maximal $\wp$, tels que les deux conditions suivantes soient satisfaites.*
   (a) *Le corps résiduel $k = \mathcal{O}/\wp$ est algébriquement clos et de caractéristique p.*
   (b) *Le corps des fractions K de $\mathcal{O}$ est de caractéristique 0 et suffisamment gros pour tous les groupes que nous allons considérer.*

Un tel triple $(K, \mathcal{O}, k)$ existe pour tout nombre premier p et pour tout groupe fini G. On l'appelle un **système p-modulaire suffisamment gros**. *Comme tous les systèmes p-modulaires que nous allons considérer sont supposés suffisamment gros, nous allons simplement les appeler des systèmes p-modulaires.*

4. *On parle de* **représentations modulaires** *de G, si on considère les RG-modules avec $R = \mathcal{O}$ ou bien k, pour un système p-modulaire $(K, \mathcal{O}, k)$. Si la caractéristique p de k divise l'ordre de G, alors une représentation indécomposable n'est pas nécessairement irréductible. De plus, si un p-sous-groupe de Sylow de G n'est pas cyclique, on a une infinité de représentations (et donc de classes d'isomorphisme de RG-modules) indécomposables.*

Le théorème de Krull-Schmidt (appelé parfois le théorème de Krull-Schmidt-Azumaya ou encore le théorème de Krull-Remak-Schmidt) ramène, dans notre contexte, le problème de la classification de tous les RG-modules à celle des RG-modules indécomposables.

Théorème 1.1.3. *[Krull-Schmidt] Soit A une R-algèbre de type fini comme R-module, où R est un anneau commutatif local, complet et noethérien (par exemple $R = \mathcal{O}$ ou $R = k$), et soit M un A-module de type fini.*

1. *Il existe une décomposition $M = \oplus_{i=1}^{r} M_i$, où r est un entier positif et M_i est un A-module indécomposable, pour tout $1 \leq i \leq r$.*
2. *Si $M = \oplus_{i=1}^{s} N_i$ est une autre telle décomposition de M, alors $r = s$ et il existe une permutation $\sigma \in S_r$, telle que $M_{\sigma(i)} \cong N_i$, $\forall\, 1 \leq i \leq r$, où S_r désigne le groupe symétrique de degré r.*

Dorénavant, p désigne un nombre premier et $(K, \mathcal{O}, k)$ un système p-modulaire. L'intérêt principal des systèmes p-modulaires réside dans le fait que, par l'intermédiaire des $\mathcal{O}G$-modules, on peut passer des représentations modulaires en caractéristique p, c'est-à-dire des kG-modules, aux représentations en caractéristique 0, c'est-à-dire aux KG-modules.

Convention. Comme la plupart des résultats que nous allons obtenir dans ce chapitre sont valables aussi bien pour l'anneau $\mathcal{O}$ que pour k, nous allons simplement noter R l'anneau commutatif $\mathcal{O}$ ou k. De plus, nous allons supposer que tous les $\mathcal{O}G$-modules sont libres sur $\mathcal{O}$.

Terminons cette section en rappelant que pour tout groupe fini G, l'algèbre de groupe RG est symétrique et donc les notions de RG-modules projectifs et injectifs coïncident, et si, de plus, G est un p-groupe, alors les RG-modules projectifs (et donc injectifs) sont libres.

1.2 Modules d'endo-permutation et groupe de Dade

Définition 1.2.1. *Soient P un p-groupe fini et M un RP-module.*

1. *Un ensemble X est un P-**ensemble** s'il existe une application*

$$P \times X \to X, \quad (u, x) \mapsto u \cdot x, \ \forall\, u \in P \quad et \quad \forall\, x \in X,$$

appelée **action de P sur X** *et satisfaisant*

$$1 \cdot x = x \quad et \quad (uv) \cdot x = u \cdot (v \cdot x), \quad \forall\, u, v \in P \quad et \quad \forall\, x \in X.$$

2. *M est un RP-module de* **permutation** *si M possède une R-base P-invariante, c'est-à-dire, s'il existe un P-ensemble fini $X \subset M$, tel que tout élément de M s'écrive de manière unique comme combinaison R-linéaire d'éléments de X (i.e. X est une R-base de M), et tel que $g \cdot x \in X$, $\forall\, g \in P$ et $\forall\, x \in X$ (i.e. X est P-invariant).*
En particulier, RP est un RP-module de permutation de base P et donc tout RP-module libre est un module de permutation.
3. *M est un RP-module d'***endo-permutation** *si $\mathrm{End}_R M$ est un RP-module de permutation pour l'action de P suivante.*

$$(u \cdot f)(x) = u \cdot f(u^{-1} \cdot x), \ \forall\, x \in M, \ \forall\, u \in P \quad et \quad \forall\, f \in \mathrm{End}_R M.$$

4. *M est un RP-module* **endo-trivial** *s'il existe un RP-module projectif (et donc libre) L tel que $\mathrm{End}_R M \cong R \oplus L$ comme RP-modules.*

Exemples.

1. R est un RP-module de permutation, d'endo-permutation et endo-trivial.
2. RP est un RP-module d'endo-permutation qui n'est pas endo-trivial.
3. Tout module de permutation est d'endo-permutation.
4. Tout module endo-trivial est d'endo-permutation.

Lemme 1.2.2. *Soient P un p-groupe fini et M et N deux RP-modules de permutation.*

1. *On a un isomorphisme de RP-modules entre M et son dual $\mathrm{Hom}_R(M, R)$.*
2. *Les RP-modules $M \oplus N$, $M \otimes N$, $\mathrm{Hom}_R(M, N)$ et tout facteur direct de M sont des modules de permutation.*

Preuve. Si X est une R-base P-invariante de M, alors la base duale,

$$\{\hat{x} \mid x \in X \ : \hat{x}(y) = \delta_{x,y}, \ \forall\, y \in X\}\ , \text{ où } \quad \delta_{x,y} = \begin{cases} 1\ , & \text{si } x = y \\ 0\ , & \text{sinon} \end{cases}$$

est une R-base P-invariante de $\mathrm{Hom}_R(M, R)$. D'où la première assertion. La seconde est prouvée dans la section 1 de [Da2]. □

Pour des raisons qui seront motivées par la suite, nous allons focaliser notre attention sur une classe particulière de modules d'endo-permutation. Avant cela, nous allons avoir besoin d'introduire quelques définitions supplémentaires.

Notations. Soient G un groupe fini, H un sous-groupe de G et $g, h \in G$.

1. On note ${}^g h$ l'élément ghg^{-1} de G, et ${}^g H$ le sous-groupe gHg^{-1} de G.
2. Si M est un RG-module, on note $M^* = \mathrm{Hom}_R(M, R)$ son dual.
3. Le symbole "$\otimes$" désigne le produit tensoriel "$\otimes_R$", s'il n'y a aucune ambiguïté sur R.

Utilisons immédiatement ces notations dans le lemme suivant.

Lemme 1.2.3. *Soient G un groupe fini et M et N deux RG-modules. Alors, les RG-modules $\mathrm{Hom}_R(M, N)$ et $M^* \otimes N$ sont isomorphes.*

Preuve. Cf. proposition 10.30 de [CR]. □

Définition 1.2.4. *Soient G un groupe fini, H un sous-groupe de G, M un RG-module et N un RH-module.*

1. *Pour tout $g \in G$, on définit le* **module conjugué** ${}^g N$ **de** N **par** g. *C'est l'ensemble $\{ {}^g n \mid n \in N\}$ et on le munit d'une structure de $R[{}^g H]$-module pour l'action de ${}^g H$ donnée par ${}^g h \cdot {}^g n = {}^g(h \cdot n)$, $\forall\, h \in H$ et $\forall\, n \in N$. Parfois, il convient de noter ce module $g \otimes N$, auquel cas on note ses éléments $g \otimes n$, au lieu de ${}^g n$, et l'action de ${}^g H$ s'écrit alors ${}^g h \cdot g \otimes n = g \otimes (h \cdot n)$.*
2. *Le* **module induit** $\mathrm{Ind}_H^G N$ *de H à G de N est le RG-module $RG \otimes_{RH} N$. L'action de G est donnée par $g \cdot h \otimes n = gh \otimes n$, $\forall\, g, h \in G$ et $\forall\, n \in N$. On note parfois $N{\uparrow}_H^G$ au lieu de $\mathrm{Ind}_H^G N$.*
3. *On dit que M est* **projectif relativement à** *H s'il existe un RH-module L tel que M est isomorphe à un facteur direct de $\mathrm{Ind}_H^G L$.*

Ouvrons une brève parenthèse historique, afin de mentionner que la théorie des vortex et sources, que nous abordons ci dessous, a été introduite et développée par J. A. Green, dans les années 50.

Définition et proposition 1.2.5. *Soient G un groupe fini et M un RG-module indécomposable.*

1. *Soit S un p-sous-groupe de Sylow de G. Alors M est projectif relativement à S.*
2. *Il existe un unique p-sous-groupe P de G, à conjugaison près, et un unique RP-module indécomposable N, à conjugaison près, tels que M est isomorphe à un facteur direct de $\mathrm{Ind}_P^G N$ et M n'est projectif relativement à aucun p-sous-groupe ne contenant pas P ou un de ses conjugués. On dit alors que P est un* **vortex** *de M et N est une* **source** *de M.*
3. *Si P est un vortex de M et S un p-sous-groupe de Sylow de G contenant P, alors le rang (sur R) de M est divisible par l'indice de P dans S.*

Preuve. Cf. respectivement proposition 19.5 (alinea ix), théorème 19.8 et proposition 19.13, et théorème 19.26 de [CR]. □

Revenons-en aux modules d'endo-permutation et exhibons leur principale caractéristique concernant la théorie des vortex et sources.

Définition et proposition 1.2.6. *Soient P un p-groupe, M un RP-module d'endo-permutation et $M = \oplus_{i=0}^{r} M_i$ une décomposition de M en une somme directe de RP-modules indécomposables.*

S'il existe un facteur direct M_i de vortex P, alors tous les autres facteurs M_j de vortex P sont isomorphes à M_i. En d'autres termes, si M n'est pas somme directe de modules projectifs relativement à des sous-groupes propres de P, alors M possède un unique facteur direct indécomposable de vortex P. Dans ce cas, on dit que M est **couvert** *(***capped** *en anglais) et on appelle* **chapeau** *de M (le* **cap***, en anglais) l'unique facteur direct indécomposable de M de vortex P.*

En particulier, tout RP-module endo-trivial est un RP-module d'endo-permutation couvert.

De plus, si M et N sont deux RP-modules d'endo-permutation couverts, de chapeaux M_0 et N_0 respectivement, on a les propriétés suivantes :

1. *$M \oplus N$ est d'endo-permutation si et seulement si M_0 est isomorphe à N_0. Dans ce cas, $M \oplus N$ est couvert, de chapeau M_0.*
2. *$M \otimes N$ est un RP-module d'endo-permutation couvert, de chapeau égal au chapeau de $M_0 \otimes N_0$.*
3. *M^* est d'endo-permutation couvert, de chapeau M_0^*.*

Preuve. Cf. section 3 de [Da2]. □

Ajoutons à cette liste de propriétés le théorème de la classification des modules de permutation, afin de déterminer quels sont les modules de permutation qui sont des modules d'endo-permutation couverts.

Théorème 1.2.7. *Soit P un p-groupe fini et M un RP-module de permutation. Alors M est indécomposable si et seulement s'il existe un sous-groupe Q de P tel que M est isomorphe à $\mathrm{Ind}_Q^P R$. De plus, dans ce cas, M est de vortex Q et de source triviale R.*

Par conséquent, un RP-module de permutation est couvert si et seulement s'il possède un facteur direct trivial.

Preuve. Cf. section 1 de [Da2]. □

Nous allons maintenant introduire des outils qui vont nous permettre de construire des modules d'endo-permutation couverts à partir des exemples susmentionnés.

Notations. Soit G un groupe fini.

1. Soient H et K deux sous-groupes de G.

   On pose $H \leq K$ (respectivement $H < K$) si H est contenu (respectivement contenu strictement) dans K.

   On pose $H \leq_G K$ (respectivement $H <_G K$), si H est contenu (respectivement contenu strictement) dans un conjugué de K.

   On pose $H \lhd K$, si H est un sous-groupe normal de K.

2. Soient X un G-ensemble, $x \in X$ et H un sous-groupe de G. Alors X est aussi un H-ensemble et on note :
   $|X|$ la cardinalité de X,
   $X^H = \{x \in X \mid h \cdot x = x, \forall\, h \in H\}$ les points fixes de X par H,
   $H_x = \{h \in H \mid h \cdot x = x\}$ le stabilisateur de x dans H, pour tout $x \in X$.

Définition 1.2.8. *Soit G un groupe fini.*

1. *Un* **complexe de RG-modules** *est une suite de RG-modules et d'homomorphismes de RG-modules, appelés* **différentielles**,

$$(C.,\ \partial.) = \left(\dots \xrightarrow{\partial_{n+2}} C_{n+1} \xrightarrow{\partial_{n+1}} C_n \xrightarrow{\partial_n} C_{n-1} \xrightarrow{\partial_{n-1}} \dots \right),$$

   satisfaisant $\partial_n \circ \partial_{n+1} = 0$, $\forall\, n \in \mathbb{Z}$. On pose simplement $C.$ au lieu de $(C.,\ \partial.)$, s'il n'y a aucune ambiguïté sur les différentielles.
   On dit que $C.$ est **borné** *si $C_n = 0$, sauf pour un nombre fini d'entiers n.*
   On dit que $C.$ est **exact**, *ou que $C.$ est une* **suite exacte** *si on a l'égalité $\mathrm{Ker}(\partial_n) = \mathrm{Im}(\partial_{n+1})$, $\forall\, n \in \mathbb{Z}$.*
   On dit que $C.$ est **scindé** *s'il existe une* **section**, *c'est-à-dire une famille $\{s_n \mid n \in \mathbb{Z}\}$ d'homomorphismes de RG-modules tels que*

$$s_n : C_n \longrightarrow C_{n+1}, \quad et \quad \partial_{n+1} \circ s_n \circ \partial_{n+1} = \partial_{n+1},\ \forall\, n \in \mathbb{Z}.$$

   *Pour tout entier n, on définit le n-***ième groupe d'homologie** *de $C.$ comme le groupe quotient $H_n(C.) = \mathrm{Ker}(\partial_n) \big/ \mathrm{Im}(\partial_{n+1})$.*
   Un complexe $C.$ est une **résolution projective** *d'un RG-module M si tous les termes de $C.$ sont des RG-modules projectifs tels que*
   (a) $C_n = 0$, $\forall\, n < 0$ *et*
   (b) $H_n(C.) \cong \begin{cases} M\ , & si\ n = 0 \\ 0\ , & sinon\ . \end{cases}$

2. *Soient P un p-groupe fini et X un P-ensemble fini. Alors RX est un RP-module de permutation, de même que le RP-module trivial R. Le noyau $\Omega^1_X(R)$ de l'homomorphisme $RX \to R, x \mapsto 1$, $\forall\, x \in X$ est un RP-module, appelé* **syzygy relatif** *(de R, relativement à X).*

3. *Les* **translatés de Heller** *d'un RG-module M sont les RG-modules indécomposables $\Omega(M)$ et $\Omega^{-1}(M)$ apparaissant dans les suites exactes courtes suivantes, pour des RG-modules projectifs L et L' de rang (sur R) minimal.*

$$0 \to \Omega(M) \to L \to M \to 0 \quad et \quad 0 \to M \to L' \to \Omega^{-1}(M) \to 0.$$

   *En itérant le procédé ci-dessus, on définit pour tout entier n le n-***ième syzygy** *de M par*

$$\Omega^n(M) = \begin{cases} \Omega(\Omega^{n-1}(M))\ , & si\ n \geq 0 \\ \Omega^{-1}(\Omega^{n+1}(M)), & si\ n < 0. \end{cases}$$

Par conséquent, si

$$\ldots \longrightarrow P_n \xrightarrow{\partial_n} P_{n-1} \xrightarrow{\partial_{n-1}} \ldots \xrightarrow{\partial_1} P_0 \xrightarrow{\partial_0} M \longrightarrow 0$$

est une résolution projective minimale de M (i.e. les P_i sont projectifs et de rang minimal pour tout i), alors $\Omega^n(M) = \mathrm{Ker}(\partial_{n-1})$, $\forall\, n > 0$.

Si on supprime l'hypothèse de minimalité, alors il existe un RP-module projectif L, tel que $\mathrm{Ker}(\partial_{n-1}) \cong \Omega^n(M) \oplus L$.

Par symétrie, on obtient les n-ièmes syzygies de M pour n négatif en considérant une résolution injective minimale de M.

Ainsi, si on décompose M en une somme directe $M_s \oplus M_l$, avec M_l projectif et M_s sans facteur direct projectif, alors $\Omega^0(M)$ est isomorphe à M_s.

Proposition 1.2.9. *Soit P un p-groupe fini.*

1. *Soit $0 \longrightarrow N \longrightarrow L \longrightarrow M \longrightarrow 0$ une suite exacte courte de RP-modules avec L projectif. Alors M est d'endo-permutation (resp. endo-permutation couvert) si et seulement si N est d'endo-permutation (resp. endo-permutation couvert).*
   En particulier, les syzygies d'un RP-module d'endo-permutation (couvert) sont aussi d'endo-permutation (couverts).
2. *Pour tout P-ensemble fini X, le syzygy relatif $\Omega^1_X(R)$ et ses syzygies sont d'endo-permutation. De plus, $\Omega^1_X(R)$ est indécomposable si et seulement si aucune orbite de P sur X n'est l'image, par un homomorphisme de P-ensembles, d'une autre orbite de P sur X, et $\Omega^1_X(R)$ est couvert si et seulement si $|X^P| \neq 1$.*
3. *Si $|X^P| = 1$, alors $\Omega^1_X(R)$ est un RP-module de permutation non couvert.*
4. *Pour tout RG-module M, il existe un RP-module projectif L tel que $\Omega^n(R) \otimes M \cong \Omega^n(M) \oplus L$, $\forall\, n \in \mathbb{Z}$.*

Preuve.

1. Cf. proposition 28.2 [Th1].
2. Cf. théorème 2 [Al3] et section 3.2 de [Bo1].
3. Si $|X^P| = 1$, on peut écrire X comme une réunion disjointe $X = \{*\} \coprod Y$ de P-ensembles, avec $|Y^P| = 0$. D'où un isomorphisme de RP-modules entre RX et $R \oplus RY$, et donc la suite exacte

   $$0 \longrightarrow \Omega^1_X(R) \longrightarrow RX \longrightarrow R \longrightarrow 0$$

   est scindée. Par suite, $\Omega^1_X(R)$ est un module de permutation, car il est isomorphe au facteur direct RY de RX. Mais RY n'a pas de facteur direct trivial par hypothèse, i.e. RY n'est pas couvert.
4. Si $n = 0$, on peut décomposer M en une somme directe $\Omega^0(M) \oplus M_l$, avec M_l projectif (cf. définition 1.2.8). On prend alors $L = M_l$.
   Prouvons l'assertion pour $n > 0$. Soit

   $$\ldots \longrightarrow P_n \xrightarrow{\partial_n} P_{n-1} \xrightarrow{\partial_{n-1}} \ldots \xrightarrow{\partial_1} P_0 \xrightarrow{\partial_0} R \longrightarrow 0$$

une résolution projective minimale de R et appliquons-lui le foncteur exact covariant $\big(_- \otimes M\big)$. On obtient ainsi une résolution projective de M (où 1_M désigne l'identité de M) :

$$\ldots \overset{\partial_n\otimes 1_M}{\longrightarrow} P_{n-1}\otimes M \overset{\partial_{n-1}\otimes 1_M}{\longrightarrow} \ldots \overset{\partial_1\otimes 1_M}{\longrightarrow} P_0\otimes M \overset{\partial_0\otimes 1_M}{\longrightarrow} \underbrace{R\otimes M}_{\cong M} \longrightarrow 0.$$

Mais cette dernière n'est pas minimale en général. D'où l'existence d'un RP-module projectif L satisfaisant :

$$\Omega^n(R)\otimes M = \mathrm{Ker}(\partial_{n-1})\otimes M = \mathrm{Ker}(\partial_{n-1}\otimes \mathrm{Id}) \cong \Omega^n(M)\oplus L.$$

Pour $n<0$, on applique le même raisonnement à une résolution injective de M.

□

Il résulte des deux dernières propositions que l'on peut obtenir beaucoup de modules d'endo-permutation à partir des exemples mentionnés. Mais finalement, par le théorème de Krull-Schmidt, seuls les modules d'endo-permutation couverts indécomposables nous intéressent vraiment.

On aboutit ainsi à la définition du groupe abélien qu'E. Dade avait appelé $\mathrm{Cap}(RP)$ et qu'aujourd'hui on appelle groupe de Dade (cf. [Da1]).

Définition et proposition 1.2.10 (Dade). *Soient M et N deux RP-modules d'endo-permutation couverts.*

On dit que M et N sont **équivalents** *si leurs chapeaux sont isomorphes et on note $D_R(P)$ l'ensemble des classes d'équivalence.*

Le produit tensoriel induit une structure de groupe abélien sur $D_R(P)$ en posant

$$[M]+[N]=[M\otimes N], \quad \forall\,[M],\ [N]\in D_R(P).$$

L'élément neutre est la classe du RP-module trivial R et l'opposé de la classe $[M]$ de M est la classe du dual $[M^*]$, $\forall\,[M]\in D_R(P)$.

On appelle $D_R(P)$ le **groupe de Dade de** P.

Soit $T(P)$ le sous-ensemble de $D(P)$ formé des classes d'équivalences contenant un module endo-trivial. Alors $T(P)$ est un sous-groupe de $D_R(P)$, appelé le **groupe des RP-modules endo-triviaux**.

Preuve. Si M et N sont deux RP-modules d'endo-permutation couverts, de chapeaux M_0 et N_0 respectivement, alors, par la proposition 1.2.5, la relation binaire $\big(M\sim N \Longleftrightarrow M_0\cong N_0\big)$ est une relation d'équivalence.

Par la proposition 1.2.6, le RP-module $M\otimes N$ est encore d'endo-permutation couvert. Par suite, l'ensemble des classes d'équivalence des RP-modules d'endo-permutation couverts est stable pour l'addition

$$[M]+[N]=[M\otimes N],\ \forall\,[M],\ [N]\in D_R(P).$$

Comme $M\otimes N\cong N\otimes M$ et $(M\otimes N)\otimes L\cong M\otimes(N\otimes L)$, pour tout RP-module L, cette loi de composition est associative et commutative.

On a $R \otimes M \cong M$ pour tout RP-module M, et donc $[R]$ est un élément neutre pour l'addition.

Or $[R]$ est formée de tous les RP-modules de permutation couverts (cf. lemme 2.5.1 [Ur]). Par conséquent, si M est d'endo-permutation couvert, le RP-module de permutation $\mathrm{End}_R M \cong M^* \otimes M$ est couvert (par la proposition 1.2.6), et donc $[M] + [M^*] = [R]$, $\forall\, [M] \in D_R(P)$. Ainsi, $D_R(P)$ est un groupe abélien.

Si M et N sont deux RP-modules endo-triviaux, alors, par la proposition 1.2.6, $M \otimes N$ et M^* sont aussi endo-triviaux et tous ces modules sont d'endo-permutation couverts. De plus, comme R est endo-trivial, on en déduit que le sous-ensemble $T_R(P)$ de $D_R(P)$ est un sous-groupe de $D_R(P)$. □

Terminons cette section en donnant un critère fort utile pour savoir si un module est endo-trivial.

Lemme 1.2.11. *Soit M un kP-module. Si $M\downarrow_E^P$ est un kE-module endo-trivial, pour tout sous-groupe abélien élémentaire E de P, alors M est un kP-module endo-trivial.*

Preuve. Cf. lemme 2.9 de [CaTh1]. □

1.3 P-algèbres de Dade et groupe de Dade

Reprenant les travaux d'E. Dade, L. Puig a donné une définition équivalente du groupe de Dade qui fait intervenir des algèbres au lieu de modules. C'est l'approche que nous expliquons dans cette section. La théorie concernant les G-algèbres mériterait à elle seule un chapitre entier, que nous n'allons pas lui concéder car nous n'avons qu'"effleuré" ce point de vue pour notre travail personnel. Nous allons donc nous limiter à définir les objets qui vont nous être utiles par la suite, et nous allons en donner les propriétés dont nous avons besoin pour établir le lien avec les modules d'endo-permutation et le groupe de Dade, renvoyant le lecteur intéressé aux sections 7, 10, 11, 13, 21, 28 et 29 de [Th1] pour plus de détails.

Soient G un groupe fini et A une R-algèbre de type fini, où $R = \mathcal{O}$ ou k, comme dans la section précédente.

1. A est **R-simple** s'il existe un R-module libre V, tel que $A \cong \mathrm{End}_R V$. Autrement dit, A est isomorphe à l'algèbre de matrices $M_n(R)$, où n est le rang de V (comme R-module libre). Par le lemme 7.1 de [Th1], V est un A-module projectif indécomposable et c'est l'unique A-module indécomposable (et libre comme R-module).
2. A est une **G-algèbre** s'il existe $\psi : G \longrightarrow \mathrm{Aut}(A)$ un homomorphisme de groupes. On note ${}^g a = \psi(g)(a)$ l'action de g sur a, $\forall\, g \in G$ et $\forall\, a \in A$.
3. A est une **G-algèbre intérieure** s'il existe un homomorphisme de groupes $\phi : G \longrightarrow A^*$, où A^* est le groupe formé des éléments inversibles de A. On note $g \cdot a = \phi(g)(a)$ l'action de g sur a, $\forall\, g \in G$ et $\forall\, a \in A$.
4. A est une **G-algèbre de permutation** si A est une G-algèbre qui est aussi un RG-module de permutation.

5. Soient $K \leq H \leq G$ et A une G-algèbre (sur R). La **trace relative de H à K** est l'application R-linéaire

$$\begin{array}{rccc} \mathrm{tr}_K^H : & A^K & \longrightarrow & A^H \\ & a & \longmapsto & \sum_{h\in[H/K]} {}^h a, \qquad \forall\, a \in A^H, \end{array}$$

où $[H/K]$ est un système de représentants des classes à gauche de H/K. L'image A_K^H de A^K est un idéal bilatère de A^H.

6. Soient P un p-sous-groupe de G et A une G-algèbre (sur R).
Le **quotient de Brauer** $\bar{A}(P)$ est la k-algèbre quotient

$$A^P/\big(\sum_{Q<P} A_Q^P + \wp A^P\big).$$

La surjection canonique $\mathrm{br}_P : A^P \longrightarrow \bar{A}(P)$ est appelée **homomorphisme de Brauer**.

7. Si P est un p-groupe fini et A une P-algèbre, on dit que A est une **P-algèbre de Dade** si A est une P-algèbre R-simple de permutation telle que $\bar{A}(P) \neq 0$.

La relation entre les P-algèbres de Dade et les RP-modules d'endo-permutation est la suivante.

Proposition 1.3.1. *Soient P un p-groupe fini et $R = \mathcal{O}$ ou $R = k$.*

1. *$\mathrm{End}_R M$ est une P-algèbre de Dade si et seulement si M est un RP-module d'endo-permutation couvert.*
2. *Le produit tensoriel $A \otimes B$ de deux P-algèbres de Dade A et B est une P-algèbre de Dade.*
3. *Si A est une P-algèbre de Dade, alors $\bar{A}(Q)$ est une $N_P(Q)/Q$-algèbre de Dade (sur k), $\forall\, Q \leq P$, et il existe un unique $k[N_P(Q)/Q]$-module d'endo-permutation couvert M tel que $\bar{A}(Q) = \mathrm{End}_k M$.*
4. *Si $A = \mathrm{End}_R M$ est une P-algèbre de Dade telle que $A^P = \mathrm{End}_{RP} M$ est un anneau local, alors M est un RP-module d'endo-permutation couvert indécomposable et le rang de A sur R est congru à 1 modulo p. Par conséquent, le rang de M sur R est congru à ± 1 modulo p.*

Preuve. Cf. paragraphe 28 de [Th1] et proposition 2.5.5 de [Ur]. □

Qu'en est-il de la relation d'équivalence définie sur l'ensemble des RP-modules d'endo-permutation couverts en termes de P-algèbres ?

Afin de répondre à cette question, nous introduisons les concepts suivants.

Définition 1.3.2. *Soit A une P-algèbre de Dade.*

1. *On dit que A est* **neutre** *s'il existe un RP-module de permutation couvert M tel que $A = \mathrm{End}_R M$.*
Autrement dit, A est neutre si A est l'algèbre des endomorphismes d'un RP-module équivalent au RP-module trivial.

2. *On dit que deux P-algèbres de Dade A et B sont* **équivalentes**, *et on le note $A \sim B$, s'il existe deux P-algèbres de Dade neutres S et T telles qu'on ait un isomorphisme de P-algèbres $A \otimes S \cong B \otimes T$.*
   Par le lemme 28.5 de [Th1], $A \sim B$ si et seulement si $A \otimes B^o$ est neutre, où B^o est l'algèbre opposée de B, i.e. le R-module B muni de la multiplication opposée $a \cdot b = ba$, $\forall\, a, b \in B$.

3. *On définit le* **groupe $D'_R(P)$ des P-algèbres de Dade** *comme l'ensemble des classes d'équivalence des P-algèbres de Dade, muni de la loi de composition*

$$[A] + [B] = [A \otimes B], \quad \forall\, [A],\ [B] \in D'_R(P),$$

   C'est un groupe abélien. L'élément neutre est la classe des P-algèbres de Dade neutres et l'opposé de $[A]$ est la classe $[A^o]$ de l'algèbre opposée.

On a un homomorphisme surjectif de groupes abéliens :

$$\begin{array}{rcl} a_R : D_R(P) & \longrightarrow & D'_R(P) \\ [M] & \longrightarrow & [\mathrm{End}_R\, M]\ . \end{array}$$

L'homomorphisme a_k est bijectif. Par contre, si $R = \mathcal{O}$, alors il existe plusieurs $\mathcal{O}P$-modules correspondant à la même P-algèbre. Plus précisément, deux $\mathcal{O}P$-modules M et M' produisent la même P-algèbre si et seulement s'il existe un $\mathcal{O}P$-module N de rang 1 tel que $M' \cong N \otimes M$ (pour l'action diagonale de P sur le membre de droite). Il s'ensuit qu'on a un isomorphisme entre le noyau de $a_{\mathcal{O}}$ et le groupe des $\mathcal{O}\mathcal{P}$-modules de rang 1 (cf. paragraphe 2.5 de [Ur]).

1.4 Changement de caractéristique

Intéressons-nous à une question cruciale dans l'étude des représentations modulaires, à savoir le passage des représentations en caractéristique première p (sur k) aux représentations en caractéristique 0 (sur K). Autrement dit, examinons les relations entre $D_k(P)$ et $D_{\mathcal{O}}(P)$, i.e. entre les kP- et $\mathcal{O}P$-modules d'endo-permutation couverts, et les relations entre $D'_k(P)$ et $D'_{\mathcal{O}}(P)$, i.e. entre les P-algèbres de Dade sur k et sur $\mathcal{O}$.

L'objectif de cette analyse est de déterminer dans quelle mesure on peut relever une représentation en caractéristique première p en une représentation en caractéristique 0, et, si un tel relèvement existe, alors on peut se demander s'il est unique.

Considérons en premier lieu le point de vue des modules et utilisons les résultats de la section 16 de [CR] et ceux de la section 4 de [Da2]. Si M est un $\mathcal{O}P$-module, on note $\overline{M} = M/\wp M$ son image par la réduction modulo $\wp$. C'est un kP-module isomorphe à $k \otimes_{\mathcal{O}} M$. Si, de plus, M est un $\mathcal{O}P$-module d'endo-permutation couvert, alors $\overline{M}$ est un kP-module d'endo-permutation couvert et son chapeau est isomorphe à $k \otimes_{\mathcal{O}} M_0$, où M_0 est le chapeau de M. Par

conséquent, on a un homomorphisme de groupes abéliens

$$\begin{array}{rccl} q & : & D_{\mathcal{O}}(P) & \longrightarrow & D_k(P) \\ & & [M] & \longmapsto & [\overline{M}], \quad \forall\, [M] \in D_{\mathcal{O}}(P), \end{array}$$

car $\overline{M \otimes N} \cong \overline{M} \otimes \overline{N}$. Le noyau de q est isomorphe au groupe formé par les $\mathcal{O}P$-modules de rang 1. En d'autres termes, étant donné un kP-module d'endo-permutation couvert M, s'il existe un $\mathcal{O}P$-module $M_{\mathcal{O}}$ (d'endo-permutation couvert) tel que $\overline{M}_{\mathcal{O}} \cong M$, alors un $\mathcal{O}P$-module $M'_{\mathcal{O}}$ relève M si et seulement s'il existe un $\mathcal{O}P$-module $N_{\mathcal{O}}$ de rang 1 sur $\mathcal{O}$ tel que $M'_{\mathcal{O}} \cong N_{\mathcal{O}} \otimes_{\mathcal{O}} M_{\mathcal{O}}$ (cf. corollaire 2.4.3 et proposition 2.4.4 de [Ur]).

Ayant ainsi répondu à la question concernant l'unicité du relèvement, penchons-nous à présent sur le problème de l'existence de celui-ci. Etant donné un kP-module d'endo-permutation couvert M, existe-t-il un $\mathcal{O}P$-module (d'endo-permutation couvert) $M_{\mathcal{O}}$ qui relève M, i.e. tel que $\overline{M_{\mathcal{O}}} \cong M$? Autrement dit, est-ce que l'homomorphisme q est surjectif ?

On ne connaît pas la réponse en toute généralité. Cependant, dans les cas que nous allons traiter par la suite, nous allons pouvoir répondre par l'affirmative à cette question, et si l'on croit les conjectures actuelles, alors il s'ensuit que q est toujours surjective.

Cessons de spéculer et considérons le point de vue des P-algèbres. Par le théorème 2.6 de [Ur], la réduction modulo $\wp$ induit un homomorphisme de groupes $q' : D'_{\mathcal{O}}(P) \longrightarrow D'_k(P)$ injectif. En effet, on a un diagramme commutatif de groupes abéliens et homomorphismes de groupes abéliens :

$$\begin{array}{ccc} D_{\mathcal{O}}(P) & \xrightarrow{a_{\mathcal{O}}} & D'_{\mathcal{O}}(P) \\ {\scriptstyle q}\downarrow & & \downarrow{\scriptstyle q'} \\ D_k(P) & \xrightarrow{a_k} & D'_k(P)\ . \end{array}$$

L'injectivité de q' est alors immédiate, car a_k est un isomorphisme, $a_{\mathcal{O}}$ est surjectif et les noyaux de q et de $a_{\mathcal{O}}$ coïncident tous deux avec le groupe des $\mathcal{O}P$-modules de rang 1.

1.5 Syzygies, morphismes et compositions

Dans les chapitres 3 et 4, nous allons déterminer la structure de $D_R(P)$ et $D'_R(P)$ pour certains p-groupes finis P. Pour arriver à nos fins, nous allons commencer par analyser $D_k(P)$ en utilisant les homomorphismes de groupes que nous définissons dans cette section.

Soit P un p-groupe fini. Commençons par une définition préliminaire.

Définition 1.5.1. *Soient Q un p-groupe fini, $\varphi : Q \longrightarrow P$ un homomorphisme de groupes, M un RP-module et A une P-algèbre. On définit la* **restriction par** *φ de M, respectivement de A, comme le RQ-module $\mathrm{Res}_\varphi M$, respectivement la Q-algèbre $\widetilde{\mathrm{Res}}_\varphi A$ comme suit.*

1. $\mathrm{Res}_\varphi M$ *est isomorphe à* M *comme* R*-module et l'action de* Q *est donnée par*
$$u \cdot x = \varphi(u) \cdot x, \ \forall\, u \in P \ et \ \forall\, x \in M.$$

2. $\mathrm{Res}_\varphi A$ *est isomorphe à* A *comme* R*-algèbre et, si* $\psi_P : P \longrightarrow \mathrm{Aut}(A)$ *est l'homomorphisme de groupes définissant la structure de* P*-algèbre sur* A*, alors on pose*
$$\begin{array}{rcl} \psi_Q : Q & \longrightarrow & \mathrm{Aut}(\widetilde{\mathrm{Res}}_\varphi A) \\ u & \longmapsto & \psi(\varphi(u)), \ \forall\, u \in Q. \end{array}$$

En considérant les trois homomorphismes de groupes que sont l'inclusion, le passage au quotient par un sous-groupe normal et un isomorphisme, on obtient par restriction les trois homomorphismes de groupes abéliens suivants.

1. Restriction. Soient Q un sous-groupe de P, M un RP-module et A une P-algèbre. L'inclusion $i : Q \longrightarrow P$ induit par restriction une structure de RQ-module sur M, respectivement de Q-algèbre sur A. On l'appelle la **restriction** de P à Q et on note $\mathrm{Res}^P_Q M$, ou $M{\downarrow}^P_Q$, respectivement $\widetilde{\mathrm{Res}}^P_Q A$, ou $A{\downarrow}^P_Q$, les objets restreints correspondants.

En particulier, si M est d'endo-permutation couvert, alors $M{\downarrow}^P_Q$ aussi. De même, si $A = \mathrm{End}_R M$ est une P-algèbre de Dade, alors $A{\downarrow}^P_Q \cong \mathrm{End}_R(M{\downarrow}^P_Q)$ est une Q-algèbre de Dade.

Ainsi, comme les RQ-modules $(M \otimes N){\downarrow}^P_Q$ et $(M{\downarrow}^P_Q) \otimes (N{\downarrow}^P_Q)$ sont isomorphes, de même que les Q-algèbres $\mathrm{End}_R(M \otimes N)$ et $\mathrm{End}_R M \otimes \mathrm{End}_R N$, pour tous RP-modules M et N, on a des homomorphismes de groupes abéliens :

$$\begin{array}{rcl} \mathrm{Res}^P_Q : D_R(P) & \to & D_R(Q) \\ [M] & \mapsto & [M{\downarrow}^P_Q] \end{array} \quad \text{et} \quad \begin{array}{rcl} \widetilde{\mathrm{Res}}^P_Q : D'_R(P) & \to & D'_R(Q) \\ [A] & \mapsto & [A{\downarrow}^P_Q]. \end{array}$$

2. Inflation. Soient Q un sous-groupe normal de P, M un $R[P/Q]$-module et A une P/Q-algèbre. La restriction par le passage au quotient $P \to P/Q$ définit un RP-module $\mathrm{Inf}^P_{P/Q} M$, et une P-algèbre $\widetilde{\mathrm{Inf}}^P_{P/Q} A$. Cette opération est appelée **inflation** de P/Q à P.

Si M est d'endo-permutation couvert, alors $\mathrm{Inf}^P_{P/Q} M$ aussi. De même, si $A = \mathrm{End}_R M$ est une P/Q-algèbre de Dade, alors $\widetilde{\mathrm{Inf}}^P_{P/Q} A \cong \mathrm{End}_R(\mathrm{Inf}^P_{P/Q} M)$ est une P-algèbre de Dade. Comme, pour tous $R[P/Q]$-modules M et N, les RP-modules $\mathrm{Inf}^P_{P/Q}(M \otimes N)$ et $(\mathrm{Inf}^P_{P/Q} M) \otimes (\mathrm{Inf}^P_{P/Q} N)$ sont isomorphes, on obtient des homomorphismes de groupes abéliens :

$$\begin{array}{rcl} \mathrm{Inf}^P_{P/Q} : D_R(P/Q) & \to & D_R(P) \\ [M] & \mapsto & [\mathrm{Inf}^P_{P/Q} M] \end{array} \quad \text{et} \quad \begin{array}{rcl} \widetilde{\mathrm{Inf}}^P_{P/Q} : D'_R(P/Q) & \to & D'_R(P) \\ [A] & \mapsto & [\widetilde{\mathrm{Inf}}^P_{P/Q} A]. \end{array}$$

3. Isomorphisme. Soient $\varphi : Q \longrightarrow P$ un isomorphisme de groupes, M un RP-module et A une P-algèbre. Les restrictions $\mathrm{Res}_\varphi M$ et $\widetilde{\mathrm{Res}}_\varphi A$, notées $\mathrm{Iso}^Q_P M$

et respectivement $\widetilde{\mathrm{Iso}}_P^Q A$, définissent un RQ-module et respectivement une Q-algèbre. Cette opération est appelée **isomorphisme** de P à Q.

Si M est d'endo-permutation couvert, alors $\mathrm{Iso}_P^Q M$ aussi, et, si $A = \mathrm{End}_R M$ est une P-algèbre de Dade, alors $\widetilde{\mathrm{Iso}}_P^Q A \cong \mathrm{End}_R(\mathrm{Iso}_P^Q M)$ est une Q-algèbre de Dade. Comme précédemment, on obtient des homomorphismes de groupes abéliens, nécessairement bijectifs :

$$\begin{array}{rcl} \mathrm{Iso}_P^Q : D_R(P) & \to & D_R(Q) \\ [M] & \mapsto & [\mathrm{Iso}_P^Q M] \end{array} \quad \text{et} \quad \begin{array}{rcl} \widetilde{\mathrm{Iso}}_P^Q : D'_R(P) & \to & D'_R(Q) \\ [A] & \mapsto & [\widetilde{\mathrm{Iso}}_P^Q A]. \end{array}$$

Construisons à présent des homomorphismes de groupes allant dans le sens opposé des restrictions et des inflations définies ci-dessus.

4. Induction tensorielle. Soient Q un sous-groupe de P, M un RQ-module et A une Q-algèbre.

Une opération "naturelle" qui permet de passer d'un RQ-module à un RP-module est l'induction. Or, en général, l'induction ordinaire d'un RQ-module d'endo-permutation n'est pas un RP-module d'endo-permutation et donc ce n'est pas la "bonne" construction à considérer dans notre cas.

Par contre, l'**induction tensorielle** de Q à P satisfait nos exigences. En effet, l'induite tensorielle $\mathrm{Ten}_Q^P M$ de M est le R-module

$$\bigotimes_{s \in [P/Q]} s \otimes M,$$

où $[P/Q]$ est un système de représentants des classes à gauche de P/Q (et $s \otimes M$ est le $R[{}^sQ]$-module conjugué de M, cf. définition 1.2.4). On munit $\mathrm{Ten}_Q^P M$ d'une structure de RP-module comme suit. Pour tout $u \in P$, il existe une unique permutation σ de $[P/Q]$ (qui dépend de u) et des éléments uniques $v_s \in Q$ tels que $us = \sigma(s)v_s$, $\forall\, s \in [P/Q]$. L'action de P sur $\mathrm{Ten}_Q^P M$ est alors donnée par

$$u \cdot \bigotimes_{s \in [P/Q]} s \otimes x_s = \bigotimes_{s \in [P/Q]} s \otimes v_{\sigma^{-1}(s)} \cdot x_{\sigma^{-1}(s)}, \ \forall\, u \in P, \ \forall \bigotimes_{s \in [P/Q]} s \otimes x_s \in \mathrm{Ten}_Q^P M.$$

De même, A est un RQ-module et on peut donc lui appliquer cette construction pour obtenir un RP-module, noté $\mathrm{Ten}_Q^P A$, qui est aussi une R-algèbre.

Si M est un RQ-module d'endo-permutation couvert et $A = \mathrm{End}_R M$ la P-algèbre de Dade correspondante, alors $\mathrm{Ten}_Q^P M$ est un RP-module d'endo-permutation couvert et $\mathrm{Ten}_Q^P A \cong \mathrm{End}_R(\mathrm{Ten}_Q^P M)$ est une P-algèbre de Dade (cf. lemme 2.1 de [BoTh]).

De plus, pour tous RQ-modules M et N, par définition de l'action (diagonale) de P sur $M \otimes N$, on a un isomorphisme $\mathrm{Ten}_Q^P(M \otimes N) \cong \mathrm{Ten}_Q^P M \otimes \mathrm{Ten}_Q^P N$ de RP-modules. Il s'ensuit des homomorphismes de groupes abéliens :

$$\begin{array}{rcl} \mathrm{Ten}_Q^P : D_R(Q) & \to & D_R(P) \\ [M] & \mapsto & [\mathrm{Ten}_Q^P M] \end{array} \quad \text{et} \quad \begin{array}{rcl} \widetilde{\mathrm{Ten}}_Q^P : D'_R(Q) & \to & D'_R(P) \\ [A] & \mapsto & [\widetilde{\mathrm{Ten}}_Q^P A]. \end{array}$$

5. Déflation. Construisons maintenant une application allant dans le sens opposé de l'inflation. Contrairement aux quatre opérations précédentes, définies indifféremment pour les modules et pour les algèbres, et aussi bien pour $R = \mathcal{O}$ que pour $R = k$, l'homomorphisme que nous allons considérer n'est défini, à l'origine du moins, que pour les P-algèbres et pour $R = k$, car il nécessite la construction de quotients de Brauer.

Soient Q un sous-groupe normal de P et A une P-algèbre. La **déflation** de P à P/Q est la P/Q-algèbre $\mathrm{Def}_{P/Q}^{P}(A) = \bar{A}(Q)$. Comme $R = k$, on a $\wp A^Q = 0$ et donc $\bar{A}(Q)$ est le quotient $A^Q/\big(\sum_{S<Q} A_S^Q\big)$.

Par la proposition 1.3.1, si A est une P-algèbre de Dade, alors $A = \mathrm{End}_k M$ pour un kP-module d'endo-permutation couvert M et $\bar{A}(Q)$ est une P/Q-algèbre de Dade. De plus, il existe un unique $k[P/Q]$-module d'endo-permutation couvert N, à isomorphisme près, tel que $\bar{A}(Q) = \mathrm{End}_k N$. On pose alors $[N] = \mathrm{Def}_{P/Q}^{P}[M]$. On définit ainsi deux applications :

$$\begin{array}{rcl} \mathrm{Def}_{P/Q}^{P} : D_R(Q) & \to & D_R(P) \\ [M] & \mapsto & [N] \end{array} \quad \text{et} \quad \begin{array}{rcl} \widetilde{\mathrm{Def}}_{P/Q}^{P} : D'_R(Q) & \to & D'_R(P) \\ [A] & \mapsto & [\bar{A}(Q)]. \end{array}$$

La proposition 28.3 de [Th1] prouve que $(\overline{A \otimes_k B})(Q) \cong \bar{A}(Q) \otimes_k \bar{B}(Q)$, pour toutes P-algèbres de Dade A et B, et donc cela implique que ces deux applications sont des homomorphismes de groupes.

Remarque 1.5.2. *Dans la section 2 de [BoTh], S. Bouc et J. Thévenaz définissent ces cinq homomorphismes comme cinq applications d'un unique procédé fonctoriel.*

Nous allons maintenant donner quelques propriétés de ces morphismes. Etant donné que dans les chapitres suivants nous allons nous concentrer sur la structure de $D_k(P)$, nous n'énonçons les résultats que pour $D_k(P)$ (ou éventuellement aussi pour $D_{\mathcal{O}}(P)$), laissant le soin au lecteur de les adapter à $D'_k(P)$ (respectivement $D'_{\mathcal{O}}(P)$) s'il le souhaite. En effet, les divers résultats que nous allons donner pour $D_R(P)$ se traduisent plus ou moins aisément en termes d'algèbres.

Lemme 1.5.3. *Tous ces morphismes sont* transitifs.

On a, par exemple, $\mathrm{Def}_{P/Q}^{P} = \mathrm{Def}_{P/Q}^{P/S} \circ \mathrm{Def}_{P/S}^{P}$, *pour tous sous-groupes normaux S et Q de P, avec $S \leq Q$.*

Lemme 1.5.4. *Soient S et Q deux sous-groupes normaux de P. Alors les applications*

$$\mathrm{Def}_{P/S}^{P} \circ \mathrm{Inf}_{P/Q}^{P} \quad \textit{et} \quad \mathrm{Inf}_{P/QS}^{P/S} \circ \mathrm{Def}_{P/QS}^{P/Q}$$

de $D_k(P/Q)$ vers $D_k(P/S)$ sont égales. Par suite, la déflation est une rétraction de l'inflation et donc la déflation est surjective et l'inflation est injective.

Preuve. Soient M un $k[P/Q]$-module d'endo-permutation couvert et notons $A = \mathrm{End}_k M$ la P/Q-algèbre de Dade correspondante. Omettons d'écrire les

inflations, pour alléger les notations. Il suffit de montrer que les (P/QS)-algèbres $\bar{A}(S)$ et $\bar{A}(QS)$ sont isomorphes.

Remarquons tout d'abord que $A^S = A^{QS}$, car $A = A^Q$. Ainsi, on a des inclusions

$$\sum_{T<S} A_T^S \subseteq \sum_{T<QS} A_T^{QS} \subseteq A^S.$$

Si $T < QS$, on a $A^T = A^{QT}$. De plus, tr_T^{QT} est nulle si $T < QT$, i.e. si $Q \not\leq T$. Dans ce cas, on a $\mathrm{tr}_T^{QS} = \mathrm{tr}_{QT}^{QS} \circ \mathrm{tr}_T^{QT} = 0$.

Si $Q \leq T$, alors $T = QT$. Par suite, on a $\mathrm{tr}_T^{QS} = \mathrm{tr}_{QT}^{QS}$ et pour calculer A_T^{QS} on peut prendre $[QS/QT] = [S/T \cap S]$ comme système de représentants, car $QS = QTS = TS$. Comme $T < QS$, il s'ensuit que $T \cap S < S$ et donc on a $A_T^{QS} \subseteq A_{T\cap S}^S \subseteq \sum_{R<S} A_R^S$. Ainsi, on a l'égalité cherchée

$$\sum_{T<S} A_T^S = \sum_{T<QS} A_T^{QS} \quad \text{et donc} \quad \bar{A}(QS) = \bar{A}(S).$$

En particulier, si $Q = S$, on a $\mathrm{Def}_{P/S}^P \circ \mathrm{Inf}_{P/S}^P = \mathrm{Inf}_{P/S}^{P/S} \circ \mathrm{Def}_{P/S}^{P/S} = \mathrm{Id}$. D'où la dernière affirmation du lemme. □

La plupart des autres propriétés que nous allons utiliser ne se démontrent pas aussi aisément. Nous allons donc nous contenter de les énoncer en mentionnant les références des articles où elles sont prouvées. Afin de simplifier l'écriture, introduisons les notations suivantes.

Notations. Soient Q et S deux sous-groupes d'un p-groupe fini P avec $S \triangleleft Q$ et X un P-ensemble fini. Rappelons que le quotient Q/S est appelé une **section** de P.

1. Pour tout entier n, on note Ω_X^n la classe de $\Omega_X^n(R)$ dans $D_R(P)$, ou simplement Ω_X, si $n = 1$.
   En particulier, on a $n\Omega_P = [\Omega^n(R)]$, $\forall\, n \in \mathbb{Z}$.
2. On note $\mathrm{Defres}_{Q/S}^P$ la composée $\mathrm{Def}_{Q/S}^Q \circ \mathrm{Res}_Q^P$.
3. On note $\mathrm{Teninf}_{Q/S}^P$ la composée $\mathrm{Ten}_Q^P \circ \mathrm{Inf}_{Q/S}^Q$.
4. On note $D_R^t(P)$ le sous-groupe de torsion de $D_R(P)$.

Théorème 1.5.5. *Soient p un nombre premier et P un p-groupe fini.*

1. *Le sous-groupe $T_k(P)$ de $D_k(P)$ coïncide avec le sous-groupe*

$$\bigcap_{1<Q\leq P} \mathrm{Ker}\left(\mathrm{Defres}_{N_P(Q)/Q}^P\right).$$

Par suite, si M est un kP-module d'endo-permutation couvert indécomposable, alors M est endo-trivial si et seulement si $\mathrm{Defres}_{N_P(Q)/Q}^P[M] = 0$ dans $D_k(N_P(Q)/Q)$, pour tout sous-groupe non trivial Q de P.

2. *Si P n'est pas cyclique et $\mathcal{A}$ désigne l'ensemble des sous-groupes de P qui sont des p-groupes abéliens élémentaires de rang 2, ou aussi quaternioniens d'ordre 8, si $p = 2$, alors l'application*

$$\prod_{E\in\mathcal{A}} \mathrm{Res}^P_E : T_k(P) \longrightarrow \prod_{E\in\mathcal{A}} T_k(E)$$

est injective.

3. *Si n est le nombre de classes de conjugaison de sous-groupes abéliens élémentaires maximaux de rang 2 de P, alors la dimension du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}\otimes_{\mathbb{Z}} T(P)$ vaut :*
   (a) *0, si P est cyclique,*
   (b) *n, si P n'est pas cyclique et si P ne contient aucun sous-groupe abélien élémentaire de rang 3,*
   (c) *$n+1$, sinon.*

4. *Soit $\mathcal{Y}$ l'ensemble des sections de P qui sont des p-groupes abéliens élémentaires de rang 1 ou 2, ou aussi cycliques d'ordre 4 ou quaternioniens d'ordre 8, si $p = 2$. L'application*

$$\prod_{Q/R\in[\mathcal{Y}/P]} \mathrm{Defres}^P_{Q/R} : D_k(P) \longrightarrow \prod_{Q/R\in[\mathcal{Y}/P]} D_k(Q/R) \quad \textit{est injective.}$$

5. *Soit $[\mathcal{S}/P]$ un système de représentants des classes de conjugaison des sous-groupes non cycliques de P. Choisissons pour tout $Q \in [\mathcal{S}/P]$ un sous-groupe $Q_0 \lhd Q$ tel que le p-groupe Q/Q_0 soit abélien élémentaire de rang 2. Alors l'application*

$$\prod_{Q\in[\mathcal{S}/P]} \mathrm{Id}\otimes \mathrm{Defres}^P_{Q/Q_0} : \mathbb{Q}\otimes_{\mathbb{Z}} D_k(P) \longrightarrow \prod_{Q\in[\mathcal{S}/P]} \mathbb{Q}\otimes_{\mathbb{Z}} D_k(Q/Q_0)$$

est un isomorphisme de groupes abéliens.

6. *Si p est impair et P est un p-groupe abélien élémentaire de rang 2, alors*

$$\prod_{1<R<P} \mathrm{Res}^P_R : D^t_k(P) \longrightarrow \prod_{1<R<P} D^t_k(R)$$

est une application injective.

7. *Si p est impair et $[\mathcal{C}/P]$ désigne un système de représentants des classes de conjugaison des sous-groupes cycliques non triviaux de P, alors l'application*

$$\prod_{C\in[\mathcal{C}/P]} \mathrm{Defres}^P_{C/\Phi(C)} : D^t_k(P) \longrightarrow \prod_{C\in[\mathcal{C}/P]} D_k(C/\Phi(C)) \ ,$$

où $\Phi(C)$ est le sous-groupe de Frattini de C, est un isomorphisme de groupes. De plus, $D^t_k(P)$ est un $\mathbb{F}_2$-espace vectoriel et on peut prendre l'ensemble $\{\mathrm{Teninf}^P_{C/\Phi(C)}\,\Omega_{c/\Phi(c)} \mid C \in [\mathcal{C}/P]\}$ comme base.

Preuve. La première affirmation est la proposition 2.1.2 de [Pu2]. Les points suivants sont obtenus en actualisant, selon le théorème principal de [CaTh2], respectivement, le théorème 2.7 de [CaTh1], le théorème 4 de [Al3], le théorème 10.1 de [CaTh1], le théorème 4.1 de [BoTh], le lemme 6.1 de [BoTh] et le théorème 6.2 de [BoTh]. □

Il convient de préciser que dans l'énoncé du théorème, nous avons pris la liberté d'actualiser les résultats originaux, en tenant compte des progrès effectués depuis leur parution (cf. chapitre 2).

Comme la dernière assertion du théorème le laisse entrevoir, les syzygies (relatifs) jouent un rôle prépondérant dans la structure du groupe de Dade. Donnons-en alors les propriétés qui vont nous être utiles.

Lemme 1.5.6. [Relèvements.] *Pour tout P-ensemble fini X et pour tout entier n, on a $\Omega^n_X(k) \cong k \otimes_{\mathcal{O}} \Omega^n_X(\mathcal{O})$, i.e. $\Omega^n_X(\mathcal{O})$ relève $\Omega^n_X(k)$.*

Preuve. On a $\overline{\Omega^n_X(\mathcal{O})} \cong \Omega^n_X(\bar{\mathcal{O}}) = \Omega^n_X(k)$, où $\bar{\cdot}$ désigne le passage au quotient modulo l'idéal maximal $\wp$ de $\mathcal{O}$. □

Lemme 1.5.7. *Soient P un p-groupe fini et X et Y deux P-ensembles finis non vides. Si, pour tout sous-groupe Q de P, l'ensemble X^Q n'est pas vide si et seulement si l'ensemble Y^Q n'est pas vide, alors $\Omega_X = \Omega_Y$ dans $D_R(P)$.*

En particulier, pour tout P-ensemble fini X, on a $\Omega_{X \amalg X} = \Omega_X$.

Preuve. Cf. Lemme 3.2.7 de [Bo1]. □

Lemme 1.5.8. [Lemme de Thévenaz.] *Soient P un p-groupe fini et X et Y deux P-ensembles finis. On a*

$$\Omega_{X \amalg Y} + \Omega_{X \times Y} = \Omega_X + \Omega_Y \quad \textit{dans } D_R(P).$$

Plus généralement, soient $n \geq 1$, $\mathcal{X}_n = \{X_i,\ 1 \leq i \leq n\}$ une famille de P-ensembles finis et $Y = \coprod_{i=1}^n X_i$. Alors on a dans $D_R(P)$

$$\Omega_Y = \sum_{s=1}^{n} (-1)^{s-1} \Big(\sum_{1 \leq i_1 < \cdots < i_s \leq n} \Omega_{Y_{i_1,\ldots,i_s}} \Big)\ , \quad \textit{où}$$

$$Y_{i_1,\ldots,i_s} = \prod_{1 \leq j \leq s} X_{i_j}, \quad \forall\, 1 \leq i_1 < \cdots < i_s \leq n \quad \textit{et} \quad \forall\, 1 \leq s \leq n.$$

Preuve. Le cas $n = 1$ est banal et le cas $n = 2$ est le lemme de Thévenaz, démontré dans [Bo1], dans la preuve du théorème 5.1.2.

Soit $n > 2$ et supposons l'assertion prouvée pour toute famille $\mathcal{X}_m$ de P-ensembles finis, avec $1 \leq m < n$. Posons $Z = \coprod_{i=1}^{n-1} X_i$ et considérons les mêmes notations que dans la donnée. Par le cas $n = 2$ et associativité de la réunion disjointe, on a

$$\Omega_Y = \Omega_Z + \Omega_{X_n} - \Omega_{(Z \times X_n)}.$$

Or, les P-ensembles $Z \times X_n$ et $\coprod_{i=1}^{n-1}(X_i \times X_n)$ sont isomorphes (cf. sections 2 et 3 de [Bo2]) et, par hypothèse de récurrence, on a

$$\Omega_Z = \sum_{s=1}^{n-1}(-1)^{s-1}\Big(\sum_{1\le i_1<\cdots<i_s\le n-1}\Omega_{Y_{i_1,\ldots,i_s}}\Big) \quad \text{et}$$

$$\Omega_{\{Z\times X_n\}} = \sum_{s=1}^{n-1}(-1)^{s-1}\Big(\sum_{1\le i_1<\cdots<i_s\le n-1}\Omega_{Z_{i_1,\ldots,i_s}}\Big),$$

$$\text{où} \quad Z_{i_1,\ldots,i_s} = \prod_{1\le j\le s}(X_{i_j}\times X_n).$$

Comme on a $\big(\prod_{i=1}^{r-1}(X_i\times X_r)\big)^Q \neq \emptyset \iff (\prod_{i=1}^{r} X_i)^Q \neq \emptyset$, $\forall\, Q \le P$ et $\forall\, 1 \le r \le n$, le lemme 1.5.7 implique l'égalité

$$\Omega_{Z_{i_1,\ldots,i_s}} = \Omega_{(Z'_{i_1,\ldots,i_s}\times X_n)}\ , \quad \text{où}$$

$$Z'_{i_1,\ldots,i_s} = \prod_{1\le j\le s} X_{i_j}\ ,\ \forall\, 1\le i_1<\cdots<i_s\le n-1 \quad \text{et} \quad \forall\, 1\le s\le n-1.$$

Finalement on obtient

$$\Omega_Y = \sum_{s=1}^{n-1}(-1)^{s-1}\Big(\sum_{1\le i_1<\cdots<i_s\le n}\Omega_{Y_{i_1,\ldots,i_s}}\Big)+$$

$$+\,\Omega_{X_n} - \sum_{s=1}^{n-1}(-1)^{s-1}\Big(\sum_{1\le i_1<\cdots<i_s\le n-1}\Omega_{(Z'_{i_1,\ldots,i_s}\times X_n)}\Big) =$$

$$=\sum_{s=1}^{n-1}(-1)^{s-1}\Big(\sum_{1\le i_1<\cdots<i_s\le n}\Omega_{Y_{i_1,\ldots,i_s}}\Big)+\Omega_{X_n}+\sum_{s=1}^{n-1}(-1)^{s}\Big(\sum_{1\le i_1<\cdots<i_s\le n-1}\Omega_{Z''_{i_1,\ldots,i_s}}\Big),$$

où $Z''_{i_1,\ldots,i_s} = (Z'_{i_1,\ldots,i_s}\times X_n)$. En particulier, la parité de s n'est pas la parité du nombre de facteurs X_i dans $Z''_{i_1,\ldots,i_s}$. D'où l'égalité cherchée.

□

Le lemme suivant décrit le comportement des classes d'équivalence des syzygies relatifs lorsqu'on leur applique un des morphismes définis précédemment.

Lemme 1.5.9. *Soient $\varphi : Q \longrightarrow P$ un homomorphisme de groupes et X un P-ensemble fini. Notons $\mathrm{Res}_\varphi \Omega_X$ la classe de $\mathrm{Res}_\varphi \Omega^1_X(k)$ et considérons la convention $\Omega_\emptyset = 0$ dans $D_R(Q)$. La restriction par φ induit une structure de Q-ensemble $\mathrm{Res}_\varphi X$ sur X.*

1. *On a $\mathrm{Res}_\varphi \Omega_X = \Omega_{\mathrm{Res}_\varphi X}$ dans $D_R(Q)$.*
   En particulier, on a $\mathrm{Res}^P_Q \Omega_P = \Omega_Q$ dans $D_R(Q)$.
2. *Supposons $Q \lhd P$. Alors $\mathrm{Def}^P_{P/Q}\Omega_X = \Omega_{X^Q}$ dans $D_k(P/Q)$.*
   En particulier, on a $\mathrm{Def}^P_{P/Q}\Omega_P = 0$ dans $D_k(P/Q)$.

Preuve. Cf. section 4 de [Bo1]. □

Précisons que pour les preuves des deux dernières égalités, S. Bouc a utilisé la convention de son article, qui consiste à identifier la classe d'un syzygy avec la classe de son algèbre d'endomorphismes. En effet, on a un isomorphisme entre $\mathrm{Ten}_Q^P(\mathrm{End}_R M)$ et $\mathrm{End}_R(\mathrm{Ten}_Q^P M)$, pour tout RQ-module M et pour tout $Q \leq P$ (cf. lemme 2.1 de [BoTh]). Autrement dit, on peut identifier Ω_X dans $D_R(P)$ avec $\mathrm{End}_R \Omega_X$ dans $D'_R(P)$, car $\mathrm{Ten}_Q^P(\mathrm{End}_R \Omega_X) = \mathrm{End}_R(\mathrm{Ten}_Q^P \Omega_X)$ est alors identifié avec $\mathrm{Ten}_Q^P \Omega_X$.

Contrairement aux quatre autres opérations, l'induction tensorielle d'un syzygy relatif Ω_X ne s'exprime pas comme syzygy relatif d'un ensemble dépendant de X. Par contre, on a le résultat suivant, dû également à S. Bouc.

Lemme 1.5.10. [Formule de Bouc.] *Soient Q un sous-groupe de P et X un Q-ensemble fini. Alors,*

$$\mathrm{Ten}_Q^P \Omega_X = \sum_{\substack{U,V \in [s_P] \\ U \leq_P V}} \mu_P(U,V) |\{a \in V \backslash P/Q \mid X^{V^a \cap Q} \neq \emptyset\}| \ \Omega_{P/U},$$

où $[s_P]$ est un ensemble de représentants des classes de conjugaison des sous-groupes de P et $\mu_P(U,V)$ la fonction de Möbius de l'ensemble partiellement ordonné $[s_P]$, définie récursivement comme suit. Pour tous sous-groupes U et S dans $[s_P]$, on pose :

$$\mu_P(U,U) = 1 \ ; \qquad \mu_P(U,S) = 0, \text{ si } U \not\leq_P S \quad \text{et}$$

$$\mu_P(U,S) = \sum_{\substack{T \in [s_P] \\ U \leq_P T <_P S}} -\mu_P(U,T), \quad \text{si } U \leq_P S.$$

Preuve. Cf. théorème 5.1.2 de [Bo1]. □

Considérons à présent certaines compositions de ces différents morphismes. Ce sujet est développé dans la section 3 de [BoTh] et nécessite une définition préalable (que nous avons simplifiée afin de l'adapter à nos besoins).

Définition 1.5.11. *Soit p un nombre premier et P un p-groupe fini.*

1. *Soit $Perm(P)$ la catégorie dont les objets sont les P-ensembles finis et les morphismes m entre deux objets Y et X sont des matrices à coefficients dans k, indexées par $X \times Y$ et telles que $m_{gx,gy} = m_{x,y}$, $\forall\, g \in P$, $\forall\, x \in X$ et $\forall\, y \in Y$.*
2. *Soit q une puissance de p. On définit le foncteur γ_q de $Perm(P)$ vers $Perm(P)$ comme étant l'identité sur les objets de $Perm(P)$ et faisant correspondre à un morphisme $m : Y \to X$ de $Perm(P)$ le morphisme $\gamma_q(m) : Y \to X$, donné par $\big(\gamma_q(m)\big)_{x,y} = (m_{x,y})^q$, $\forall\, x \in X$ et $\forall\, y \in Y$.*

Ce foncteur induit un endomorphisme, toujours noté γ_q, sur $D'_R(P)$ (cf. section 3 de [BoTh]) et celui-ci est un automorphisme si k est un corps parfait,

puisque l'endomorphisme de k qui consiste à élever à la puissance p est bijectif dans ce cas. Ce foncteur intervient lorsqu'on étudie la composition des opérations $\widetilde{\mathrm{Def}}$ et $\widetilde{\mathrm{Ten}}$. En effet, la proposition 3.10 de [BoTh] démontre que si Q et R sont des sous-groupes de P avec R normal dans P et $q = |R : Q \cap R|$, alors les applications

$$\widetilde{\mathrm{Def}}^P_{P/R} \circ \widetilde{\mathrm{Ten}}^P_Q \quad \text{et} \quad \gamma_q \circ \widetilde{\mathrm{Ten}}^{P/R}_{QR/R} \circ \widetilde{\mathrm{Iso}}^{QR/R}_{Q/Q\cap R} \circ \widetilde{\mathrm{Def}}^Q_{Q/Q\cap R}$$

de $D'_k(Q)$ vers $D'_k(P/R)$ coïncident.

Or, en ce qui nous concerne, nous nous intéressons uniquement à la composition correspondante pour les syzygies relatifs, et ceux-ci sont définis sur le corps $\mathbb{F}_p$, qui est parfait. En fait, comme l'élévation à la puissance p est l'identité sur $\mathbb{F}_p$, le morphisme induit par γ_q sur $D_k(P)$ est l'identité sur les syzygies relatifs (cf. exemple 3.3 de [BoTh]). Ceci simplifie l'expression ci-dessus, comme nous le mettons en évidence dans la seconde affirmation du lemme suivant, la première égalité correspondant à la formule de Mackey dans le cas de l'induction tensorielle.

Lemme 1.5.12. *Soient S et Q deux sous-groupes de P et X un Q-ensemble fini. On a :*

$$\mathrm{Res}^P_S \circ \mathrm{Ten}^P_Q(\Omega_X) = \sum_{u\in[S\backslash P/Q]} \mathrm{Ten}^S_{S\cap {}^uQ} \circ \mathrm{Res}^{{}^uQ}_{S\cap {}^uQ} \circ \mathrm{Iso}^{{}^uQ}_Q(\Omega_X) \text{ dans } D_R(S).$$

Si, de plus, $S \lhd P$, alors on a, dans $D_k(P/S)$,

$$\mathrm{Def}^P_{P/S} \circ \mathrm{Ten}^P_Q(\Omega_X) = \mathrm{Ten}^{P/S}_{QS/S} \circ \mathrm{Iso}^{QS/S}_{Q/Q\cap S} \circ \mathrm{Def}^Q_{Q/Q\cap S}(\Omega_X),$$

Preuve. La première égalité est démontrée dans la proposition 3.15.2 de [Be], et elle est valable pour tous les RP-modules. La seconde découle de la proposition 3.10 de [BoTh]. □

Nous allons clore ce premier chapitre en fixant quelques notations supplémentaires. Nous allons noter $D^\Omega_R(P)$ le sous-groupe de $D_R(P)$ engendré par les syzygies relatifs, c'est-à-dire le groupe constitué des combinaisons $\mathbb{Z}$-linéaires des éléments Ω_X, où X est un P-ensemble fini. De plus, dorénavant, nous allons appeler $D_k(P)$ **le** groupe de Dade de P, respectivement $T_k(P)$ **le** groupe des modules endo-triviaux et nous noterons ces groupes $D(P)$, respectivement $T(P)$. On notera aussi $D^\Omega(P)$ au lieu de $D^\Omega_k(P)$. C'est en effet sur les classes d'équivalence des kP-modules d'endo-permutation couverts que nous avons choisi de concentrer nos efforts.

Les deux raisons principales qui ont motivé cette décision sont, en premier lieu, la nécessité d'utiliser la déflation comme outil d'analyse du groupe de Dade, ce qui implique qu'il nous faut travailler sur k au lieu de $\mathcal{O}$. D'ailleurs, il va se révéler plus aisé de travailler sur k, puis de relever les modules sur $\mathcal{O}$, que d'essayer de déterminer directement $D_\mathcal{O}(P)$.

En second lieu, nous avons fait le choix de considérer des modules au lieu d'algèbres pour satisfaire une question de goût personnel. Soulignons, pour terminer, que ce choix ne nous a pas pénalisé dans notre étude du groupe de Dade, comme nous allons le constater par la suite.

Chapitre 2

1978-2002 : L'Odyssée du groupe de Dade

Ce chapitre ne prétend pas être un exposé exhaustif de tous les résultats concernant le groupe de Dade d'un p-groupe fini depuis ses premiers balbutiements. Toutefois, nous avons voulu retracer son histoire dans les grandes lignes, pour justifier l'intérêt que nous lui avons porté.

Commençons avec la première apparition du terme *endo-permutation* dans la littérature. Elle remonte à 1978, lorsque E. Dade, motivé par l'étude des extensions de modules simples pour des groupes finis p-nilpotents, a introduit le concept de module d'endo-permutation dans le domaine des représentations modulaires des groupes finis (cf. [Da2]). D'emblée, il est parvenu à la classification des modules d'endo-permutation couverts (à équivalence près) dans le cas d'un p-groupe fini abélien. Voici, dans les mêmes notations qu'au chapitre 1, ce qu'il a démontré.

Théorème 2.0.13. *Soit P un p-groupe abélien fini.*

1. *$T_R(P)$ est engendré par Ω_P. Donc $T_R(P)$ est trivial si $|P| = 2$, cyclique d'ordre 2, si P est cyclique d'ordre ≥ 3, et cyclique infini sinon.*
2. *$D_R(P)$ est isomorphe à la somme directe des groupes $T_R(P/Q)$, où Q parcourt l'ensemble des sous-groupes propres de P.*

La première assertion est le théorème 10.1 de [Da2]. La seconde est le théorème 12.5 de ce même article, où E. Dade prouve que si P est abélien, alors tout RP-module d'endo-permutation couvert indécomposable est le chapeau d'un produit tensoriel M de modules d'endo-permutation couverts obtenus par inflation depuis des quotients de P et, si $R = \mathcal{O}$, d'un unique $\mathcal{O}P$-module de rang 1. De plus, il montre que la multiplicité du chapeau dans M vaut 1.

A cette époque, E. Dade n'était pas le seul à s'intéresser à ces modules. En effet, pratiquement en même temps, et de manière totalement indépendante, J. Alperin et aussi J. Carlson s'étaient penchés sur des problèmes semblables. Plus exactement, précédant les travaux d'E. Dade, J. Alperin avait déjà considéré les

modules endo-triviaux, qu'il avait alors appelé **modules inversibles** (cf. [Al1]). De son côté, J. Carlson a décrit les kP-modules endo-triviaux pour un p-groupe abélien élémentaire de rang 2, prouvant d'une autre manière le théorème 2.0.13 dans ce cas particulier (cf. [Ca]), et son article est paru deux ans après celui d'E. Dade. Soulignons encore que J. Carlson et E. Dade étaient au courant des travaux de J. Alperin, comme ils le mentionnent dans leurs articles.

Au début des années 1980, L. Puig a annoncé des résultats concernant le groupe de Dade d'un p-groupe fini arbitraire, où le problème majeur réside dans le fait que l'argument utilisé par E. Dade ne s'applique pas, car en général les sous-groupes ne sont pas normaux. Mais ce n'est qu'en 1990 qu'il a publié une partie de ses recherches sur le groupe de Dade (cf. [Pu2]), introduisant ainsi "officiellement" la notion de P-algèbre de Dade qu'il avait déjà utilisée dans ses notes non publiées de 1988 (cf. [Pu1]).

Détaillons sa démarche. Comme l'application de déflation de P à P/Q n'a aucun sens pour un sous-groupe Q non normal dans P, L. Puig a considéré la composition de la restriction au normalisateur $N_P(Q)$ de Q, suivie de la déflation à $N_P(Q)/Q$. Finalement, il a étudié l'homomorphisme

$$\prod_{1<Q\leq P} \mathrm{Defres}^P_{N_P(Q)/Q} : D(Q) \longrightarrow \prod_{1<Q\leq P} D(N_P(Q)/Q).$$

Il a appelé **groupe des classes d'équivalences des P-algèbres de source quasi triviale** le noyau de cette application et il a démontré qu'il coïncide avec le groupe $T(P)$ des modules endo-triviaux. Il en a déduit, en particulier, qu'un kP-module d'endo-permutation couvert indécomposable est endo-trivial si et seulement si sa classe est dans le noyau de $\prod_{1<Q\leq P} \mathrm{Defres}^P_{N_P(Q)/Q}$ (cf. [Pu1] ou l'assertion 1 du théorème 1.5.5).

Dans [Pu1], L. Puig a aussi montré que les sources de modules simples pour des groupes finis p-résolubles sont des modules d'endo-permutation d'une certaine forme (utilisant le produit tensoriel, l'induction tensorielle et l'inflation de translatés de Heller). Comme on reviendra sur ce sujet dans la deuxième partie de ce travail, nous n'allons pas donner plus de détails sur la structure de ces modules dans ce chapitre.

Ce qui résulte des travaux présentés ci-dessus, c'est qu'on peut séparer les sujets d'étude du groupe de Dade en deux parties. D'une part, on s'intéresse à la structure du groupe :

1. Est-il de type fini ?
2. Peut-on trouver des générateurs aussi simplement que dans le cas abélien ?
3. Que peut-on dire de son sous-groupe de torsion ? Du sous-groupe des modules endo-triviaux ?
4. Est-ce que tout kP-module d'endo-permutation se relève en un $\mathcal{O}P$-module d'endo-permutation ? Etc...

Et d'autre part, on peut se demander quelles en sont les applications :

1. Dans quelles circonstances, dans la théorie des représentations, voit-on apparaître des modules d'endo-permutation ?

2. Et des modules endo-triviaux ?

Nous avons décidé de suivre le même principe pour présenter notre travail et donc nous avons divisé ce texte en deux : la première partie est dédiée à l'étude de la structure du groupe de Dade de certaines familles de p-groupes finis, et la seconde se concentre sur certaines occurrences de ces modules dans la théorie des représentations.

Pour l'instant, revenons-en à l'exposition des principaux résultats connus, avant le début de cette thèse.

Dans [Pu2], L. Puig démontre que le noyau de la restriction

$$\prod_{E\in\mathcal{A}} \mathrm{Res}_E^P \ : \ T(P) \longrightarrow \prod_{E\in\mathcal{A}} T(E)$$

est fini, où $\mathcal{A}$ est un système de représentants des classes de conjugaison des sous-groupes abéliens élémentaires de P. En particulier, cela implique que le groupe des classes d'équivalence des P-algèbres de Dade d'un p-groupe fini P quelconque est de type fini et donc $D(P)$ aussi.

Un an plus tard paraît un nouvel article de L. Puig concernant les P-algèbres de Dade d'un p-groupe fini abélien, où il démontre le fait suivant. Pour chaque sous-groupe Q de P, il se donne une P/Q-algèbre de Dade A_Q satisfaisant certaines conditions de compatibilité. Il est alors en mesure de les "recoller" en une P-algèbre de Dade A, telle que la déflation $\mathrm{Def}_{P/Q}^P(A)$ soit équivalente à A_Q, pour tout sous-groupe Q (cf. [Pu3]).

Ce "petit jeu" de recollement, qui peut sembler anodin au premier abord, se révèle en fait d'une grande importance dans l'analyse locale des blocs. Et aujourd'hui, cela intéresse également les topologues qui étudient les systèmes de fusion. Ceci constitue donc une motivation supplémentaire pour parvenir à une classification complète des modules d'endo-permutation.

Les points de vue d'E. Dade et de L. Puig sont très différents, et cela peut prêter à confusion. C'est probablement une des raisons qui a convaincu J. Thévenaz de reprendre leurs travaux afin de les présenter en parallèle dans les paragraphes 28 à 30 de son livre [Th1], créant ainsi un dictionnaire entre les terminologies des P-algèbres de Dade et des RP-modules d'endo-permutation. Il redémontre, avec d'autres arguments, un certain nombre de résultats connus. Entre autres, il donne une preuve du résultat (toujours non publié) de L. Puig affirmant que les sources de modules simples pour des groupes finis p-résolubles sont des modules d'endo-permutation.

Les faits que nous souhaitons relever à présent, sans entrer dans les détails, concernent les occurrences des modules d'endo-permutation et endo-triviaux dans les équivalences de catégories (stables et dérivées).

En 1986, paraît un article de M. Linckelmann dans lequel il démontre que les modules endo-triviaux sont intimement liés aux équivalences stables induites par une équivalence dérivée (cf. [Li]). Puis, en 1997, M. Harris et M. Linckelmann publient un article commun (cf. [HL]), dont on retiendra essentiellement le rôle prépondérant joué par les modules d'endo-permutation dans l'analyse locale

des blocs et dans les équivalences dérivées splendides introduites par J. Rickard quelques années auparavant.

En parlant de J. Rickard, il nous faut mentionner son article de 1996 traitant des équivalences dérivées splendides (cf. [Ri]), puisqu'il est à l'origine du jeu auquel nous nous sommes prêtés au chapitre 6. Dans cet article, J. Rickard remarque que certains modules d'endo-permutation ont une résolution de permutation endo-scindée et démontre, en particulier, que si P est abélien, alors tout module d'endo-permutation possède une telle résolution. L'importance de l'existence d'une résolution de permutation endo-scindée réside dans le fait qu'on a alors un complexe basculant splendide qui induit une équivalence splendide entre deux blocs donnés (et donc ceux-ci ont la même structure locale).

Beaucoup d'articles sont parus depuis, mettant en évidence l'importance des modules d'endo-permutation et les équivalences stables et dérivées notamment. Il serait prétentieux de vouloir tous les exposer ici. Nous allons donc conclure cette parenthèse catégorique en mentionnant encore le "bon comportement" des modules endo-triviaux dans les équivalences stables. Si on a une équivalence entre les sous-catégories épaisses engendrées par le module trivial des catégories stables de deux groupes, alors cette équivalence fait correspondre un module endo-trivial à un module endo-trivial. Ce fait a été prouvé par J. Carlson et R. Rouquier dans [CaRo].

Venons-en, à présent, aux résultats publiés après le début de ce travail de thèse, c'est-à-dire parus (ou à paraître) depuis septembre 1999.

L'année 2000 a été riche en publications concernant les modules d'endo-permutation. Commençons par citer deux articles de J. Alperin. Dans le premier (cf. [Al3]), il démontre que les syzygies relatifs sont des modules d'endo-permutation, il calcule leur image par l'homomorphisme de déflation et il donne un critère d'indécomposabilité de ces modules. Il détermine également le rang "sans torsion" du groupe des modules endo-triviaux, i.e. la dimension du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}\otimes_{\mathbb{Z}} T_R(P)$. Nous avons explicité celui-ci au point 3 du théorème 1.5.5.

Dans l'article suivant (cf. [Al4]), J. Alperin démontre que tout kP-module endo-trivial se relève sur $\mathcal{O}$, pour tout p-groupe fini P.

Poursuivons avec les travaux de S. Bouc et J. Thévenaz. Dans [BoTh], ils démontrent que le rang "sans torsion" du groupe de Dade d'un p-groupe fini P est égal au nombre de classes de conjugaison de sous-groupes non cycliques de P (théorème 4.1 de [BoTh] et assertion 5 du théorème 1.5.5).

Ils obtiennent aussi des résultats partiels concernant le sous-groupe de torsion $D^t(P)$ de $D(P)$. Ils démontrent que si p est un nombre premier impair, alors un certain quotient $\overline{D^t}(P)$ de $D^t(P)$ est un $\mathbb{F}_2$-espace vectoriel, de base

$$\left\{ \operatorname{Teninf}_{\overline{C}}^{P} \Omega_{\overline{C}} \mid \overline{C} = C/\phi(C), C \in [\mathcal{C}/P] \right\},$$

où $\phi(C)$ est le sous-groupe de Frattini de C et $[\mathcal{C}/P]$ un système de représentants des classes de conjugaison de sous-groupes cycliques non triviaux de P. Par la suite, il va s'avérer que $\overline{D^t}(P)$ est égal à $D^t(P)$ (cf. [CaTh2] ou assertion 7 du théorème 1.5.5).

Finalement, ils développent une approche fonctorielle du problème concernant $D(P)$, en considérant, d'une certaine manière, $\mathbb{Q}\otimes_{\mathbb{Z}} D(\cdot)$ et $D^t(\cdot)$ comme des foncteurs. Comme nous n'avons pas utilisé ce point de vue, nous ne développons pas plus cet aspect du groupe de Dade.

Encore en 2000, J. Carlson et J. Thévenaz publient un article synonyme de nouvelle avancée dans l'analyse du groupe de Dade (cf. [CaTh1]). En effet, ils parviennent à réduire la question concernant la structure du groupe des modules endo-triviaux de n'importe quel p-groupe fini au groupe des modules endo-triviaux de p-groupes finis appartenant à une famille "détectrice". C'est le l'assertion 2 du théorème 1.5.5, auquel il faut ajouter à la famille détectrice les groupes extraspéciaux d'exposant p, si p est impair, ou (quasi-)extraspéciaux sauf D_8, si $p = 2$ (cf. théorème 2.7 [CaTh1]). En effet, l'assertion 2 du théorème 1.5.5 est la conjecture 2.6 de [CaTh1] et celle-ci a été démontrée depuis dans [CaTh2].

Dans [CaTh1], J. Carlson et J. Thévenaz déterminent aussi le groupe de Dade des 2-groupes diédraux, quaternioniens et semi-diédraux, sur lesquels nous reviendrons plus en détail dans le chapitre 5.

Toujours durant cette prolifique année 2000, S. Bouc a travaillé sur les syzygies relatifs (cf. [Bo1]), et a obtenu, entre autres, les résultats que nous avons déjà mentionnés dans le chapitre précédent.

Il a également démontré que le sous-groupe $D^{\Omega}_{\mathcal{O}}(P) + K_{\mathcal{O}}(P)$ du groupe de Dade engendré par les syzygies relatifs $(D^{\Omega}_{\mathcal{O}}(P))$ et le noyau des restrictions-déflations aux sections abéliennes élémentaires $(K_{\mathcal{O}}(P))$ est d'indice fini dans $D_{\mathcal{O}}(P)$ et l'exposant du quotient divise l'ordre de P. Autrement dit, à un multiple de p près et à un élément de $K_{\mathcal{O}}(P)$ près, les classes des modules d'endo-permutation sont des combinaisons linéaires des classes des syzygies relatifs. Par ailleurs, grâce aux résultats obtenus [CaTh2], il s'avère que $K_{\mathcal{O}}(P)$ est trivial si p est impair (cf. assertion 4 du théorème 1.5.5).

Finalement, il montre que si X est un P-ensemble fini, alors Ω_X est un élément de torsion dans $D_{\mathcal{O}}(P)$ si et seulement si $\Omega_X = \Omega_{P/Q}$ pour un sous-groupe Q de P tel que le quotient est cyclique ou quaternionien et tel que Q contient le stabilisateur de tout $x \in X$, avec égalité pour certains $x \in X$.

Actuellement, il est conjecturé que les classes des syzygies relatifs engendrent toujours le groupe de Dade d'un p-groupe fini P, excepté si $p = 2$ et P possède une section qui est un groupe quaternionien (cf. [CaTh1]). Si cette conjecture est vraie, alors cela implique, en particulier, que tout module d'endo-permutation se relève en caractéristique 0.

Maintenant, nous allons brièvement exposer des résultats qui ne sont pas encore publiés. Commençons avec ceux de S. Bouc, qui a obtenu un résultat d'injectivité concernant le sous-groupe de torsion $T^t(P)$ du groupe des modules endo-triviaux. Il a considéré les sections isométriques d'un p-groupe fini P, c'est-à-dire les sections U/V de P satisfaisant les conditions suivantes :

1. le groupe U/V est de p-rang normal 1, i.e. U/V est cyclique, diédral d'ordre au moins 16, quaternionien ou semi-diédral ;
2. si M est l'unique $\mathbb{Q}[U/V]$-module simple fidèle, c'est-à-dire tel que le sous-groupe $\{\bar{u} \in U/V \mid \bar{u} \cdot x = x,\ \forall\, x \in M\}$ de U/V est trivial, alors le $\mathbb{Q}P$-

module induit $\widetilde{M} = \mathrm{Ind}_U^P \mathrm{Inf}_{U/V}^U M$ vérifie un isomorphisme d'algèbres entre $\mathrm{End}_{\mathbb{Q}P} \widetilde{M}$ et $\mathrm{End}_{\mathbb{Q}P} M$. On dit alors que le $\mathbb{Q}P$-module (a fortiori simple) $\widetilde{M}$ est de **type** U/V.

L'ensemble des sections isométriques de P est muni d'une relation d'équivalence. En considérant alors la somme directe F des groupes $T^t(U/V)$, où U/V parcourt un système de représentants des classes d'équivalences des sections isométriques de P, S. Bouc prouve que F s'injecte dans le sous-groupe de torsion $D^t(P)$ du groupe de Dade, et que cette injection (donnée par $\mathrm{Teninf}_{U/V}^P$) admet une rétraction. En d'autres termes, F est isomorphe à un facteur direct de $D^t(P)$. De plus, S. Bouc conjecture qu'en fait cette injection est un isomorphisme. C'est en effet vérifié dans tous les cas connus, et, en particulier, c'est vrai pour tout nombre premier p impair, en tenant compte du résultat suivant.

Comme nous l'avons déjà mentionné, J. Carlson et J. Thévenaz ont démontré la conjecture 2.6 de [CaTh1]. Autrement dit, si P est un p-groupe fini alors l'application

$$\mathrm{Res} : T(P) \longrightarrow \prod_{Q \in \mathcal{X}} T(Q),$$

où $\mathcal{X}$ est l'ensemble des sous-groupes abéliens élémentaires de rang 2 ou aussi quaternioniens d'ordre 8, si $p = 2$, est injective (cf. [CaTh2]).

En fait, comme tient à le préciser J. Thévenaz, la conjecture 2.6 pour p impair est due essentiellement à J. Carlson, qui a analysé la variété d'un certain quotient d'un hypothétique module endo-trivial de torsion pour aboutir à une contradiction et montrer ainsi que le sous-groupe de torsion du groupe des modules endo-triviaux pour un p-groupe extraspécial d'exposant p est trivial.

L'injectivité de l'application Res ci-dessus (i.e. l'élimination des groupes extraspéciaux de la famille détectrice) s'avère capitale dans l'étude du sous-groupe de torsion du groupe de Dade d'un p-groupe fini quelconque. En effet, une des conséquences majeures de ceci est que le sous-groupe de torsion $D^t(P)$ de $D(P)$ se détecte à l'aide de l'application $\prod_{1<Q\leq P} \mathrm{Defres}_{N_P(Q)/Q}^P$ pour les sections $N_P(Q)/Q$ qui sont des groupes cycliques d'ordre au moins 3, quaternioniens ou semi-diédraux.

Sans entrer dans les détails, et selon les notations précédentes, l'injectivité de l'application Res entraîne aussi, pour p impair, $D^t(P) = \overline{D^t}(P)$ et donc $D^t(P)$ est un $\mathbb{F}_2$-espace vectoriel de dimension égale au nombre de classes de conjugaison de sous-groupes cycliques non triviaux de P, engendré par les classes des syzygies relatifs.

Nous allons maintenant apporter notre contribution à ce travail autour du groupe de Dade en traitant deux exemples particuliers. Le premier concerne un p-groupe métacyclique pour un nombre premier p impair et le second traite le cas d'un 2-groupe extraspécial du type D_8^{*n}, pour un entier $n \geq 1$.

La motivation d'étudier le groupe de Dade d'un p-groupe métacyclique pour un nombre premier p impair est due au fait qu'un tel groupe ne possède pas de section extraspéciale d'exposant p. En effet, au début de ce travail de thèse le dernier résultat démontré par J. Carlson et J. Thévenaz n'était encore qu'une

conjecture, et donc, pour espérer pouvoir classifier tous les modules d'endo-permutation pour un p-groupe fini P, il nous fallait choisir une famille de groupes n'ayant pas de section extraspéciale d'exposant p.

L'idée pour le deuxième exemple a été motivée par le fait que parmi les 2-groupes (quasi-)extraspéciaux, ce sont les seuls pour lesquels le sous-groupe de torsion du groupe de Dade est trivial, puisqu'un tel 2-groupe P ne contient aucun sous-groupe Q produisant une section de la forme $N_P(Q)/Q$ qui soit un groupe cyclique d'ordre 4, quaternionien ou semi-diédral. Ils apparaissent donc parmi les groupes (quasi-)extraspéciaux les "plus faciles" à aborder.

Chapitre 3

Les p-groupes métacycliques

3.1 Structure des p-groupes métacycliques

Définition 3.1.1. *Un groupe G est dit métacyclique si G est une extension d'un groupe cyclique par un groupe cyclique. En d'autres termes, on peut insérer G dans une suite exacte courte*

$$1 \longrightarrow C_n \longrightarrow G \longrightarrow C_m \longrightarrow 1,$$

où C_n et C_m sont des groupes cycliques d'ordre $n \geq 1$ et $m \geq 1$ respectivement.

Soient P un p-groupe métacyclique (pour un nombre premier p impair) et deux entiers n et m, tels que la suite

$$1 \longrightarrow C_{p^n} \longrightarrow P \longrightarrow C_{p^m} \longrightarrow 1$$

est exacte. Autrement dit, selon les notations de [Di], on peut choisir $u, v \in P$ tels que $u^{p^n} = 1$, $v^{p^m} \in < u >$ (avec $m = 0$ si P est cyclique) et ${}^v u = u^{p^l+1}$, pour un certain $0 < l \leq n$ (le groupe P est abélien si $l = n$).

En particulier, P est d'ordre p^{m+n}, $< u > \cong C_{p^n}$ est un sous-groupe normal dans P et tout élément de P s'écrit de manière unique $u^a v^b$, avec $0 \leq a < p^n$ et $0 \leq b < p^m$.

Remarquons aussi que les sous-groupes et les quotients de P sont eux aussi métacycliques, et donc toute section de P est un p-groupe métacyclique.

De plus, on a $<u^{p^{n-1}}> \leq Z(P)$. En effet, l'action par conjugaison de v sur $u^{p^{n-1}}$ est un automorphisme de $<u^{p^{n-1}}>$ d'ordre une puissance de p (car $v^{p^m} \in < u >$). Mais $\mathrm{Aut}(<u^{p^{n-1}}>)$ est cyclique d'ordre $p-1$. Donc v agit trivialement sur $u^{p^{n-1}}$, i.e. v et $u^{p^{n-1}}$ commutent.

D'autre part, si P n'est pas cyclique, alors P contient au moins un sous-groupe abélien élémentaire E de rang 2, car p est impair (cf. théorème 4.10 de [Go]). Nous allons montrer qu'en fait, P possède *au plus* un sous-groupe abélien élémentaire de rang 2, mais avant cela, introduisons la convention et la notation suivante.

Convention. Dorénavant, p désigne un nombre premier impair.

Notation. On note $\Phi(G)$ le sous-groupe de Frattini d'un groupe fini G. Par définition, $\Phi(G)$ est l'intersection des sous-groupes maximaux de G (cf. section 5.1 de [Go]).

Lemme 3.1.2. *Soit P un p-groupe métacyclique non cyclique. Alors il existe un unique sous-groupe abélien élémentaire de rang 2.*

A fortiori, celui-ci est normal dans P.

Preuve. Soit E un sous-groupe abélien élémentaire de rang 2 d'un p-groupe métacyclique non cyclique $P = <u, v>$. Alors $E \cap <u> \neq \{1\}$ car le quotient $E/(E \cap <u>)$ est cyclique, isomorphe au sous-groupe non trivial $E<u>/<u>$ du groupe cyclique $P/<u>$. Donc E contient $u^{p^{n-1}}$.

L'image de E dans $P/<u>$ n'est pas triviale et donc E contient un élément de la forme $u^a v^{p^{m-1}}$. En fait, $E = <u^{p^{n-1}}, u^a v^{p^{m-1}}>$, car $<u^{p^{n-1}}>$ est un sous-groupe propre du sous-groupe $<u^{p^{n-1}}, u^a v^{p^{m-1}}>$ de E.

Posons $w = v^{p^{m-1}}$. L'action de w sur $<u>$ est donnée par ${}^w u = u^r$, où $r = sp^{n-1} + 1$ pour un entier $s > 0$. En particulier, si w et u commutent, on prend $s = p$. C'est le cas si $n = 1$, car cela force $l = n = 1$ (dans les notations de début de section) et donc P est abélien.

Comme P est métacyclique, il existe un unique entier d tel que $0 \leq d < p^n$ et $w^p = u^d$. On a $p|d$ si et seulement si P n'est pas cyclique. En effet, p et d sont premiers entre eux si et seulement s'il existe un entier e avec $de \equiv 1 \,(\mod p^n)$. Mais alors on a $u = u^{de} = w^{pe} \in <v>$. Par hypothèse, P n'est pas cyclique et donc d est un multiple de p et on a

$$(u^a\ w)^p = u^a({}^w u)^a({}^{w^2} u)^a \cdots ({}^{w^{p-1}} u)^a w^p = u^{a(r+r^2+\cdots+r^{p-1})+d} = u^{a\frac{r^p-1}{r-1}+d}.$$

Or,

$$\frac{r^p-1}{r-1} = (sp^{n-1})^{p-1} + \binom{p}{1}(sp^{n-1})^{p-2} + \cdots + \binom{p}{p-2} sp^{n-1} + \binom{p}{p-1}.$$

Comme $(sp^{n-1})^{p-1} \equiv 0 \,(\mod p^n)$ (même si $n = 1$, car on a alors $s = p$), et comme, pour p impair, les coefficients binomiaux sont tous des multiples de p, on en déduit que $\frac{r^p-1}{r-1} \equiv p \,(\mod p^n)$.

Donc $(u^a w)^p = u^{ap+d}$ et ceci est égal à 1 si et seulement si $ap + d$ est un multiple de p^n. Or, $ap + d \equiv 0 \,(\mod p^n)$ si et seulement si $a \equiv -\frac{d}{p} \,(\mod p^{n-1})$ et donc $E = <u^{p^{n-1}}, u^{-\frac{d}{p}} v^{p^{m-1}}>$.

Réciproquement, l'argument précédent prouve que le groupe E défini par cette formule est abélien élémentaire de rang 2. Donc P a un unique sous-groupe abélien élémentaire de rang 2.

□

Remarque 3.1.3. *Le lemme ne se généralise pas pour $p = 2$. En effet, le groupe diédral d'ordre 8 est métacyclique non cyclique. Mais il possède 2 sous-groupes abéliens élémentaires de rang 2.*

Du lemme 3.1.2 découle immédiatement une conséquence, fondamentale pour la motivation de ce travail, comme nous l'avons mentionné au chapitre précédent.

Corollaire 3.1.4. *Soit P un p-groupe métacyclique. Alors P ne possède aucune section extra-spéciale d'exposant p.*

Preuve. Tout p-groupe (non trivial) extra-spécial d'exposant p possède plusieurs p-sous-groupes abéliens élémentaires de rang 2. Or, toute section de P est un p-groupe métacyclique et ne peut donc pas être extra-spéciale d'exposant p. □

Par ailleurs, si P n'est pas cyclique, nous pouvons caractériser les sous-groupes non cycliques de P par les propriétés suivantes.

Lemme 3.1.5. *Supposons P non cyclique et soit H un sous-groupe non cyclique de P.*

1. *Alors H est déterminé de manière unique par $\Phi(H)$.*
   En d'autres termes, si H et K sont deux sous-groupes non cycliques de P, avec $\Phi(K) = \Phi(H)$, alors $K = H$.
2. *On a $N_P(H) = N_P(\Phi(H))$.*

Preuve.

1. Considérons $N = N_P(\Phi(H))$. Le quotient $N/\Phi(H)$ est un p-groupe métacyclique, car c'est une section d'un p-groupe métacyclique, et il est non cyclique, car il contient $H/\Phi(H)$ qui est abélien élémentaire de rang 2 (car H n'est pas cyclique).
   Donc, par le lemme 3.1.2, $N/\Phi(H)$ possède un unique sous-groupe abélien élémentaire de rang 2. Autrement dit, il existe un unique sous-groupe de N contenant $\Phi(H)$ et dont le quotient par $\Phi(H)$ est abélien élémentaire de rang 2. A fortiori, H est cet unique sous-groupe. En effet, s'il existe un sous-groupe K non cyclique de P, avec $\Phi(K) = \Phi(H)$, alors, de $\Phi(H) \triangleleft K$, il s'ensuit que $K \leq N$ et par unicité, cela force $K = H$.
2. On a $N_P(H) \leq N_P(\Phi(H))$, car $\Phi(H)$ est un sous-groupe caractéristique de H.
   D'autre part, si $u \in N_P(\Phi(H))$, alors le sous-groupe de Frattini de ${}^uH$ est $\Phi({}^uH) = {}^u(\Phi(H)) = \Phi(H)$. On a donc $H = {}^uH$, par le point précédent. Ainsi, on a $u \in N_P(H)$, pour tout $u \in N$. D'où $N_P(\Phi(H)) = N_P(H)$.

□

3.2 Groupe de Dade

Soient p un nombre premier impair et P un p-groupe métacyclique. Considérons l'homomorphisme de groupes abéliens

$$\Psi_P = \prod_{Q \in [\mathcal{X}/P]} \mathrm{Defres}^P_{Q/\Phi(Q)} : D(P) \to \prod_{Q \in [\mathcal{X}/P]} D(Q/\Phi(Q)),$$

où $\mathcal{X}$ est l'ensemble des sous-groupes non triviaux de P et $[\mathcal{X}/P]$ un système de représentants des classes de conjugaison par P des éléments de $\mathcal{X}$.

Notons $\mathcal{S}$ l'ensemble des sous-groupes non cycliques de P, $\mathcal{C}$ l'ensemble des sous-groupes cycliques non triviaux de P, et $[\mathcal{S}/P]$ et $[\mathcal{C}/P]$ pour les systèmes de représentants des classes de conjugaison par P correspondants.

Proposition 3.2.1. *L'application Ψ_P, définie ci-dessus, est injective.*

Preuve. Nous savons que tout $Q \in [\mathcal{X}/P]$ est un p-groupe métacyclique. Ainsi, on a $Q/\Phi(Q) \cong C_p$, si Q est cyclique, et $Q/\Phi(Q) \cong C_p \times C_p$, sinon. D'où, respectivement,

$$D(Q/\Phi(Q)) = T(Q/\Phi(Q)) \cong \mathbb{Z}/2\mathbb{Z}\ , \quad \text{si } Q \text{ est cyclique,}$$

$$D(Q/\Phi(Q)) \cong \bigoplus_{R<Q} T(Q/R) \cong \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{p+1}, \quad \text{si } Q \text{ n'est pas cyclique.}$$

Par le théorème 1.5.5, l'application

$$\prod_{H/K \in [\mathcal{Y}/P]} \mathrm{Defres}^P_{H/K} : D(P) \longrightarrow \prod_{H/K \in [\mathcal{Y}/P]} D(H/K) \quad \text{est injective,}$$

où $[\mathcal{Y}/P]$ est un système de représentants des classes de conjugaison des sections de P qui sont des p-groupes abéliens élémentaires de rang 1 ou 2.

Raisonnons par récurrence sur $|P|$.

Supposons $|P| = p$. On a alors $\mathcal{S} = \emptyset$ et $\mathcal{C} = \{P\}$, et donc $\Psi_P = \mathrm{Id}_{D(P)}$ est injective.

Supposons maintenant $|P| > p$ et Ψ_Q injective pour tout groupe Q d'ordre strictement plus petit que celui de P. Soit $a \in \mathrm{Ker}(\Psi_P)$. Par le théorème 1.5.5, il suffit de prouver que $\mathrm{Defres}^P_{H/K}(a) = 0$ pour toute section H/K abélienne élémentaire de rang 1 ou 2. On distingue deux cas :

1. Si $H < P$, on a $\mathrm{Res}^P_H(a) \in \mathrm{Ker}(\Psi_H)$, où $\Psi_H = \prod_{Q \in [\mathcal{X}_Q/H]} \mathrm{Defres}^H_{Q/\Phi(Q)}$, et où $\mathcal{X}_Q$ est l'ensemble des sous-groupes non triviaux de Q. En effet, par transitivité de la restriction, on a

   $$\mathrm{Defres}^P_{Q/\Phi(Q)} = \mathrm{Defres}^H_{Q/\Phi(Q)} \circ \mathrm{Res}^P_H,\ \forall\, Q \leq H \leq P.$$

   De plus, si Q et ${}^gQ$ sont deux sous-groupes de H conjugués dans P, alors on a $\mathrm{Defres}^P_{{}^gQ/\Phi({}^gQ)} = \mathrm{conj}(g) \circ \mathrm{Defres}^P_{Q/\Phi(Q)}$, où $\mathrm{conj}(g)$ est la conjugaison par g. Par suite, $\mathrm{Ker}(\mathrm{Defres}^P_{{}^gQ/\Phi({}^gQ)}) = \mathrm{Ker}(\mathrm{Defres}^P_{Q/\Phi(Q)})$.

   Donc $\mathrm{Res}^P_H(a) = 0$, car, par hypothèse de récurrence, Ψ_H est injective.

   Ainsi, pour toute section abélienne élémentaire H/K de P de rang 1 ou 2, avec $H < P$, on a $\mathrm{Defres}^P_{H/K}(a) = 0$.

2. Si $H = P$, alors on a deux sous-cas à traiter :
   (a) Si K est un sous-groupe normal d'indice p^2 dans P tel que le quotient est abélien élémentaire de rang 2, alors $K = \Phi(P)$, puisque $P/\Phi(P)$ est l'unique quotient abélien élémentaire de rang 2 de P. Donc, par hypothèse, $a \in \mathrm{Ker}(\mathrm{Def}^P_{P/\Phi(P)})$.

(b) Si K est un sous-groupe normal d'indice p dans P, alors K est maximal dans P. Donc P/K est une section de $P/\Phi(P)$, car K contient $\Phi(P)$ comme sous-groupe (a fortiori normal). D'où, par transitivité de la déflation et par hypothèse, on a

$$\mathrm{Def}_{P/K}^{P}(a) = \mathrm{Def}_{P/K}^{P/\Phi(P)}\left(\mathrm{Def}_{P/\Phi(P)}^{P}(a)\right) = \mathrm{Def}_{P/K}^{P/\Phi(P)}(0) = 0.$$

□

Les deux lemmes suivants vont nous permettre d'améliorer ce résultat d'injectivité.

Lemme 3.2.2. *Soient p un nombre premier impair et P un p-groupe métacyclique non cyclique. Alors, l'application*

$$\prod_{1<Q<P} \mathrm{Res}_{Q}^{P} : D^t(P) \longrightarrow \prod_{1<Q<P} D^t(Q) \quad \textit{est injective.}$$

Preuve. Par la proposition 3.2.1, nous savons que

$$\prod_{1<Q\leq P} \mathrm{Defres}_{Q/\Phi(Q)}^{P} : D^t(P) \longrightarrow \prod_{1<Q\leq P} D^t(Q/\Phi(Q))$$

est injective (en fait nous savons même que nous pouvons considérer les sous-groupes Q à conjugaison près).

D'autre part, le théorème 1.5.5 implique que si Q est un sous-groupe non cyclique de P, alors la restriction

$$\prod_{\Phi(Q)<R<Q} \mathrm{Res}_{R/\Phi(Q)}^{Q/\Phi(Q)} : D^t(Q/\Phi(Q)) \longrightarrow \prod_{\Phi(Q)<R<Q} D^t(R/\Phi(Q))$$

est injective, pour tout sous-groupe non cyclique Q de P. En effet, $Q/\Phi(Q)$ est abélien élémentaire de rang 2 et les sous-groupes propres de $Q/\Phi(Q)$ sont de la forme $R/\Phi(Q)$, pour des sous-groupes R de P, tels que $\Phi(Q) < R < Q$.

On obtient ainsi un diagramme commutatif de groupes abéliens et homomorphismes de groupes abéliens

$$\begin{array}{ccc} D^t(P) & \xrightarrow{\varphi_1} & \prod_{1<S<P} D^t(S) \\ {\scriptstyle\varphi_2}\downarrow & & \downarrow \\ \prod_{1<Q\leq P} D^t(Q/\Phi(Q)) & \xrightarrow{\varphi_3} & \prod_{\Phi(Q)<R<Q} D^t(R/\Phi(Q)), \end{array}$$

où les applications $\varphi_3 = \prod_{\Phi(Q)<R<Q} \mathrm{Res}_{R/\Phi(Q)}^{Q/\Phi(Q)}$ et $\varphi_2 = \prod_{1<Q\leq P} \mathrm{Defres}_{Q/\Phi(Q)}^{P}$ sont injectives, par le théorème 1.5.5 et, respectivement, par la proposition précédente. Par suite, l'application $\varphi_1 = \prod_{1<S<P} \mathrm{Res}_{S}^{P}$ est injective. □

Lemme 3.2.3. *Soit P un p-groupe métacyclique. L'application*

$$\prod_{[C\in\mathcal{C}/P]} \mathrm{Defres}_{C/\Phi(C)}^{P} : D^t(P) \longrightarrow \prod_{C\in[\mathcal{C}/P]} T(C/\Phi(C))$$

est injective.

Preuve. Cette application est bien définie, puisque $C/\Phi(C)$ est cyclique d'ordre p et donc $D(C/\Phi(C)) = T(C/\Phi(C))$, $\forall\, C \in \mathcal{C}$.

Prouvons l'assertion par récurrence sur $|P|$ et commençons par supposer $|P| = p$. Alors on a $T(P) = D(P)$ et $\mathcal{C} = \{P\}$. Par suite, on a

$$\prod_{C\in[\mathcal{C}/P]} \mathrm{Defres}^P_{C/\Phi(C)} = \mathrm{Id}_{T(P)}$$

est injective.

Supposons maintenant $|P| > p$ et le lemme vérifié pour tout p-groupe métacyclique d'ordre strictement inférieur à $|P|$. Distinguons deux cas.

1. Si P est cyclique, alors le lemme est la version cyclique de la proposition 3.2.1, et donc il n'y a rien à démontrer.
2. Si P n'est pas cyclique, alors, par le lemme 3.2.2 et par hypothèse de récurrence, la composition

$$D^t(P) \xrightarrow{\alpha} \prod_{1<Q<P} D^t(Q) \xrightarrow{\beta} \prod_{1<Q<P} \Big(\prod_{C\in\mathcal{C}_Q} T(C/\Phi(C))\Big)$$

est injective, où $\alpha = \prod_{1<Q<P} \mathrm{Res}^P_Q$, $\beta = \prod_{1<Q<P} \big(\prod_{C\in\mathcal{C}_Q} \mathrm{Defres}^Q_{C/\Phi(C)} \big)$ et $\mathcal{C}_Q$ est l'ensemble des sous-groupes cycliques non triviaux de Q, pour tout sous-groupe Q de P.

Or, $\forall\, C \in \mathcal{C}$ et $\forall\, Q, Q' < P$ tels que $C \in \mathcal{C}_Q \cap \mathcal{C}_{Q'}$, on a

$$\mathrm{Defres}^Q_{C/\Phi(C)} \circ \mathrm{Res}^P_Q = \mathrm{Defres}^P_{C/\Phi(C)} = \mathrm{Defres}^{Q'}_{C/\Phi(C)} \circ \mathrm{Res}^P_{Q'}\,.$$

De plus, on a $\mathrm{Ker}\big(\mathrm{Defres}^P_{Q/\Phi(Q)}\big) = \mathrm{Ker}\big(\mathrm{Defres}^P_{{}^gQ/\Phi({}^gQ)}\big)$, pour tout sous-groupe Q de P (par un argument déjà vu).

Par suite, on peut se restreindre aux classes de conjugaison de sous-groupes cycliques (non triviaux), sans perdre l'injectivité de l'application. Ainsi, $\prod_{C\in[\mathcal{C}/P]} \mathrm{Defres}^P_{C/\Phi(C)} : D^t(P) \longrightarrow \prod_{C\in[\mathcal{C}/P]} T(C/\Phi(C))$ est injective.

□

Ce dernier résultat nous donne une "borne supérieure" en ce qui concerne le rang du sous-groupe de torsion du groupe de Dade d'un p-groupe métacyclique P (pour p impair). En effet, nous savons désormais qu'il ne peut excéder le nombre de classes de conjugaison de sous-groupes cycliques non triviaux de P. Nous allons à présent montrer que le rang en question est égal à cette borne supérieure.

Remarquons que nous pouvons encore améliorer ce résultat d'injectivité. En effet, pour toute section abélienne élémentaire H de P, de rang inférieur ou égal à 2, nous pouvons considérer l'application surjective $\rho_H : D(H) \to T(H)$, définie comme la composition de l'isomorphisme

$$\bigoplus_{1\le K<H} \mathrm{Def}^H_{H/K} : D(H) \longrightarrow \bigoplus_{1\le K<H} T\big(H/K\big)$$

du théorème 1.2.10 (dont l'inverse est $\oplus_{K<H} \mathrm{Inf}_{H/K}^{H}$), avec la projection sur la composante correspondant à $K = 1$. En particulier, si $H \cong C_p$, alors $\rho_H = \mathrm{Id}$.

Considérons l'homomorphisme de groupes abéliens

$$\alpha_P = \Big(\prod_{Q \in [\mathcal{X}/P]} \rho_{Q/\Phi(Q)} \Big) \circ \Psi_P.$$

Théorème 3.2.4. *L'application*

$$\alpha_P : D(P) \longrightarrow \prod_{Q \in [\mathcal{S}/P]} T\big(Q/\Phi(Q)\big) \times \prod_{C \in [\mathcal{C}/P]} T\big(C/\Phi(C)\big) \quad \textit{est injective.}$$

Preuve. L'homomorphisme injectif Ψ_P de la proposition 3.2.1, composé avec l'isomorphisme du théorème 2.0.13 donne un homomorphisme injectif

$$\Psi'_P : D(P) \longrightarrow \prod_{Q \in [\mathcal{S}/P]} \big(\oplus_{\Phi(Q) \leq R < Q} T(Q/R) \big) \times \prod_{C \in [\mathcal{C}/P]} T\big(C/\Phi(C)\big).$$

Soit $x \in \mathrm{Ker}(\alpha_P)$. Alors $\Psi'_P(x) = (x_Q)_{Q \in [\mathcal{X}/P]}$ vérifie $x_Q = 0$, si Q est cyclique, ou $x_Q \in \oplus_{\Phi(Q) < R < Q} T(Q/R)$, sinon. D'où, $2x \in \mathrm{Ker}(\Psi'_P) = \mathrm{Ker}(\Psi_P)$ et donc $x \in D^t(P)$, par injectivité de Ψ_P.

Par le lemme précédent, $D^t(P)$ s'injecte dans $\prod_{C \in [\mathcal{C}/P]} T\big(C/\Phi(C)\big)$ par le produit des déflations-restrictions, c'est-à-dire par la restriction de α_P à $D^t(P)$. Par hypothèse, $x \in \mathrm{Ker}(\alpha_P)$ et donc $x = 0$. Il s'ensuit que α_P est injective.

□

Il nous reste à prouver que cette injection est un isomorphisme. Pour y parvenir, nous allons exhiber un sous-ensemble de $D(P)$ qui est envoyé par α_P sur le système de générateurs $\mathcal{E} = \{\Omega_{Q/\Phi(Q)} \mid Q \in [\mathcal{X}/P]\}$ du groupe abélien d'arrivée. En fait, $\mathcal{E}$ est la réunion d'une base du $\mathbb{Z}$-module libre $\prod_{Q \in [\mathcal{S}/P]} T\big(Q/\Phi(Q)\big)$ et d'une base du $\mathbb{F}_2$-espace vectoriel $\prod_{Q \in [\mathcal{C}/P]} T\big(Q/\Phi(Q)\big)$. On fait de $\mathcal{E}$ une base ordonnée du groupe abélien d'arrivée, pour l'ordre sur $[\mathcal{X}/P]$ défini comme suit.

Considérons séparément les représentants des classes de conjugaison des sous-groupes cycliques non triviaux et celles des sous-groupes non cycliques, respectivement $[\mathcal{C}/P]$ et $[\mathcal{S}/P]$. On a $\mathcal{S} = \emptyset$ si et seulement si P est cyclique et $\mathcal{C} \neq \emptyset$, $\forall P \neq \{1\}$.

Sur chacun de ces ensembles, il existe un ordre "naturel" induit par l'inclusion $\leq_P$, que nous pouvons prolonger en un ordre total $\preceq$ sur $[\mathcal{C}/P]$, respectivement sur $[\mathcal{S}/P]$.

Soient maintenant H et K deux éléments de $[\mathcal{X}/P]$. Nous posons $H \preceq K$ si exactement une des conditions suivantes est réalisée.

1. $H \in [\mathcal{C}/P]$ et $K \in [\mathcal{S}/P]$.
2. $H, K \in [\mathcal{C}/P]$ et $H \preceq K$ selon l'ordre total sur $[\mathcal{C}/P]$.
3. $H, K \in [\mathcal{S}/P]$ et $H \preceq K$ selon l'ordre total sur $[\mathcal{S}/P]$.

En d'autres termes, les sous-groupes cycliques sont "plus petits" que les non cycliques et chaque catégorie de sous-groupes de P est elle-même totalement ordonnée. On vérifie aisément que cette relation est une relation d'ordre total sur $[\mathcal{X}/P]$.

Posons maintenant

$$\mathcal{B} = \left\{ \mathrm{Teninf}^P_{C/\Phi(C)} \Omega_{C/\Phi(C)},\, C \in [\mathcal{C}/P] \right\} \bigcup \left\{ \Omega_{P/\Phi(Q)},\, Q \in [\mathcal{S}/P] \right\}$$

et ordonnons cet ensemble selon l'ordre $\preceq$ croissant des sous-groupes C, respectivement Q, apparaissant dans les indices.

Remarquons, tout d'abord, que ces éléments sont bien dans $D(P)$. En effet, ceux du premier ensemble le sont par définition de l'application

$$\mathrm{Teninf}^P_{C/\Phi(C)} : D(C/\Phi(C)) \to D(P),$$

et par le fait que $\Omega_{C/\Phi(C)} \in T(C/\Phi(C)) = D(C/\Phi(C))$, pour tout $C \in [\mathcal{C}/P]$. Quant à ceux du second, ce sont les classes d'équivalences des syzygies relatifs des P-ensembles transitifs $P/\Phi(Q)$, où Q parcourt les sous-groupes non cycliques de P (à conjugaison près). Donc, par la proposition 1.2.9 ces syzygies sont des modules d'endo-permutation couverts indécomposables.

Montrons que $\mathcal{B}$ est une base du groupe de Dade $D(P)$, dans le sens suivant :

1. $\left\{ \mathrm{Teninf}^P_{C/\Phi(C)} \Omega_{C/\Phi(C)},\, C \in [\mathcal{C}/P] \right\}$ forme une base du $\mathbb{F}_2$-espace vectoriel $D^t(P)$, de dimension $|[\mathcal{C}/P]|$.
2. $\left\{ \Omega_{P/\Phi(Q)},\, Q \in [\mathcal{S}/P] \right\}$ forme une base d'un sous-module $\mathbb{Z}$-libre facteur direct de $D(P)$, de rang $|[\mathcal{S}/P]|$.

Déterminons les images des éléments de torsion. Soit $C \in [\mathcal{C}/P]$ et calculons les composantes de $\alpha_P(\mathrm{Teninf}^P_{C/\Phi(C)} \Omega_{C/\Phi(C)})$ dans $\{\Omega_{Q/\Phi(Q)} \mid Q \in [\mathcal{X}/P]\}$. L'image sur chaque $T(Q/\Phi(Q))$ pour $Q \in [\mathcal{S}/P]$ est nulle puisque ceux-ci sont des groupes sans torsion.

D'autre part, par le théorème 1.5.5, nous savons que

$$\mathrm{Defres}^P_{C'/\Phi(C')}(\mathrm{Teninf}^P_{C/\Phi(C)} \Omega_{C/\Phi(C)}) = \delta_{C,C'} \Omega_{C/\Phi(C)},$$

où δ est le symbole de Kronecker. Autrement dit,

$$\alpha_P(\mathrm{Teninf}^P_{C/\Phi(C)} \Omega_{C/\Phi(C)}) = \left(\delta_{C,X} \Omega_{X/\Phi(X)}\right)_{X \in [\mathcal{X}/P]},\ \forall\, C \in [\mathcal{C}/P].$$

Passons maintenant aux éléments qui ne sont pas de torsion (et supposons donc P non cyclique, sinon $\mathcal{S} = \emptyset$) et prouvons que pour tous $H, K \in [\mathcal{S}/P]$ avec $H \preceq K$ on a $\mathrm{Defres}^P_{K/\Phi(K)} \Omega_{P/\Phi(H)} = \delta_{H,K} \Omega_{H/\Phi(H)}$.

La condition $H \preceq K$ implique que $K \in \mathcal{S}$, par définition de l'ordre. On veut exprimer

$$\mathrm{Defres}^P_{K/\Phi(K)} \left(\Omega_{P/\Phi(H)}\right) = \mathrm{Def}^K_{K/\Phi(K)} \left(\mathrm{Res}^P_K \left(\Omega_{P/\Phi(H)}\right) \right)$$

comme combinaison linéaire des $\Omega_{Q/\Phi(Q)}$, pour Q parcourant $[\mathcal{X}/P]$. Rappelons d'abord les deux conséquences du lemme 1.5.9 suivantes.

1. Si X est un P-ensemble, K et N des sous-groupes de P, avec $N \lhd K$, on a $\mathrm{Res}^P_K \Omega_X = \Omega_Z \in D(K)$, où $Z = \mathrm{Res}^P_K X$ et
2. $\mathrm{Def}^K_{K/N} \Omega_X = \Omega_Y \in D(K/N)$, où $Y = X^N$ est l'ensemble des points fixes de X sous l'action de N.

Rappelons également que, pour tout sous-groupe K de P, on a un isomorphisme de P-ensembles $\mathrm{Ind}^P_K\{*\} \cong P/K$, où $\{*\}$ désigne un singleton, i.e. un ensemble constitué d'un point.

Considérons alors $X = P/\Phi(H) \cong \mathrm{Ind}^P_{\Phi(H)}\{*\}$ comme P-ensemble. On doit calculer sa restriction à K, puis déterminer les points fixes de X sous l'action de $\Phi(K)$. En appliquant la formule de Mackey, on obtient :

$$\mathrm{Res}^P_K X = \coprod_{g\in[K\backslash P/H]} \mathrm{Ind}^K_{K\cap {}^g\Phi(H)} \mathrm{Res}^{{}^g\Phi(H)}_{K\cap {}^g\Phi(H)}\{*\} = \coprod_{g\in[K\backslash P/H]} K/(K\cap {}^g\Phi(H)) =$$

$$= \left(\coprod_{\substack{g\in[K\backslash P/\Phi(H)]\\ g\in N}} \underbrace{K/(K\cap\Phi(H))}_{(I)} \right) \coprod \left(\coprod_{\substack{g\in[K\backslash P/\Phi(H)]\\ g\notin N}} \underbrace{K/(K\cap {}^g\Phi(H))}_{(II)} \right),$$

où $N = N_P(\Phi(H)) = N_P(H)$, par le lemme 3.1.5. Distinguons les cas suivants.

1. Supposons $H = K$.
   On veut montrer que $\mathrm{Defres}^P_{H/\Phi(H)} \Omega_{P/\Phi(H)} = \Omega_{H/\Phi(H)}$.
   Clairement, tous les éléments de (I) sont fixes par $\Phi(H)$. Par contre, on n'a aucun point fixe dans (II). En effet, on a
   $$\big(H/H\cap {}^g\Phi(H)\big)^{\Phi(H)} \neq \emptyset \iff \Phi(H) \leq H\cap {}^g\Phi(H)$$
   $$\iff \Phi(H) = {}^g\Phi(H) \iff g \in N.$$
   D'où $\mathrm{Defres}^P_{H/\Phi(H)} \Omega_{P/\Phi(H)} = \Omega_{H/\Phi(H)} \in D(H/\Phi(H))$, car $\Omega^1_{H/\Phi(H)}(k)$ est un facteur direct du noyau de l'application $\left(\bigoplus_{g\in[N/H]} k[H/\Phi(H)] \to k\right)$ (par unicité, c'est donc le chapeau du noyau).
2. Supposons $|H| < |K|$. Alors $\Phi(K) \not\leq \Phi(H)$ et donc $X^{\Phi(K)} = \emptyset$. Par suite, on a bien $\mathrm{Defres}^P_{K/\Phi(K)} \Omega_{P/\Phi(K)} = 0$.
3. Il nous reste à traiter le cas $H \preceq K$ et $|H| = |K|$. En d'autres termes, H et K sont deux sous-groupes de P de même ordre, non cycliques et non conjugués dans P. On a $|\Phi(K)| = |\Phi(H)|$ car ils sont tous deux d'indice p^2 dans K, respectivement H. Ainsi,
   $$X^{\Phi(K)} \neq \emptyset \iff \exists\, g \in P \text{ tel que } \Phi(K) = {}^g\Phi(H).$$
   Mais, par le lemme 3.1.5, les sous-groupes de Frattini de deux sous-groupes non cycliques et non conjugués de P sont eux aussi non conjugués dans P. En effet, s'il existe $g \in P$ tel que $\Phi(K) = {}^g\Phi(H)$, alors $K = {}^gH$, puisque $\Phi({}^gH) = {}^g\Phi(H)$. On en conclut donc, comme ci-dessus, que $X^{\Phi(K)} = \emptyset$. Ainsi, $\mathrm{Defres}^P_{K/\Phi(K)} \Omega_{P/\Phi(H)} = 0$ dans $D(K/\Phi(K))$.

En résumé, on a montré que $\mathrm{Defres}^P_{K/\Phi(K)}\,\Omega_{P/\Phi(H)} = \delta_{H,K}\Omega_{K/\Phi(K)}$, pour tous $H, K \in [\mathcal{S}/P]$ avec $H \preceq K$.

Par conséquent, les images par α_P des éléments de $\mathcal{B}$, exprimés dans la base $\mathcal{E}$ du groupe abélien d'arrivée, forment une matrice triangulaire, à coefficients entiers et dont les éléments diagonaux valent 1 (et donc une matrice inversible dans $\mathbb{Z}$).

Autrement dit, nous avons démontré le théorème suivant.

Théorème 3.2.5. *Soient p un nombre premier impair et P un p-groupe métacyclique. Alors,*

$$\alpha_P = \prod_{H\in[\mathcal{X}/P]} \left(\rho_{H/\Phi(H)} \circ \mathrm{Defres}^P_{H/\Phi(H)}\right) : D(P) \longrightarrow \prod_{H\in[\mathcal{X}/P]} T(H/\Phi(H))$$

est un isomorphisme de groupes abéliens.

En particulier, tout élément de $D(P)$ s'écrit de manière unique comme une combinaison linéaire à coefficients entiers d'éléments de l'ensemble

$$\{\Omega_{P/\Phi(H)},\ H \in [\mathcal{S}/P]\}$$

et une combinaison linéaire à coefficients dans $\mathbb{Z}/2\mathbb{Z}$ d'éléments de l'ensemble

$$\{\mathrm{Teninf}^P_{H/\Phi(H)}\,\Omega_{H/\Phi(H)},\ H \in [\mathcal{C}/P]\}.$$

Corollaire 3.2.6. *Soient p un nombre premier impair et P un p-groupe métacyclique. Alors,*

$$D(P) = D^\Omega(P) \quad \textit{et} \quad \mathcal{B}' = \{\Omega_{P/H} \mid H \in [\mathcal{X}/P] \setminus \{P\}\} \cup \{\Omega_P\}$$

forme un système de générateurs de cardinalité minimale du $\mathbb{Z}$-module $D(P)$.

Preuve. Par le lemme 1.5.10, tous les $\mathrm{Teninf}^P_{H/\Phi(H)}\,\Omega_{H/\Phi(H)}$ apparaissant dans $\mathcal{B}$ sont des combinaisons $\mathbb{Z}$-linéaires des classes des syzygies relatifs $\Omega_{P/Q}$, pour les sous-groupes (propres) Q de P.

Si M est un $\mathbb{Z}$-module et X un sous-ensemble de M, notons $\mathrm{vect}(X)$ le sous-module de M engendré par X. Par le théorème 3.2.5 et par définition de $D^\Omega(P)$ on a ainsi

$$D(P) = \mathrm{vect}(\mathcal{B}) \subseteq \mathrm{vect}(\mathcal{B}') = D^\Omega(P) \subseteq D(P).$$

Par suite, $D^\Omega(P) = D(P)$ et $\mathcal{B}'$ est un système de générateurs du $\mathbb{Z}$-module $D(P)$.

Par ailleurs, $\mathcal{B}$ et $\mathcal{B}'$ ont le même nombre d'éléments et, par le théorème 3.2.5, $\mathcal{B}$ est un système de générateurs de $D(P)$ de cardinalité minimale. Donc $\mathcal{B}'$ aussi. □

Nous avons ainsi déterminé la structure du groupe de Dade (sur k) d'un p-groupe métacyclique, pour un nombre premier p impair. On va maintenant répondre aux questions suivantes, avant de traiter un exemple.

1. Qu'en est-il de $T(P)$?
2. Qu'en est-il de $D_{\mathcal{O}}(P)$?

Si P est abélien, les réponses à ces questions sont connues depuis plus de vingt ans et nous les avons déjà rappelées (cf. [Da2] ou chapitre 1). Pour le cas général, le corollaire suivant répond à ces questions.

Corollaire 3.2.7. *Soient p un nombre premier impair et P un p-groupe métacyclique.*

1. *$T(P)$ est cyclique, engendré par Ω_P. On a donc*

$$T(P) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & , \quad \textit{si } P \textit{ est cyclique} \\ \mathbb{Z} & , \quad \textit{sinon .} \end{cases}$$

2. *Dans les notations de la section 1.4, la réduction $q' : D'_{\mathcal{O}}(P) \cong D'_k(P)$ modulo l'idéal $\wp$ est un isomorphisme.*

Preuve.

1. Si P n'est pas cyclique, alors par le théorème 1.5.5 et le lemme 3.1.2, on a que $T(P)$ est cyclique infini, engendré par Ω_P. En effet, il existe alors un unique sous-groupe abélien élémentaire de rang 2, a fortiori maximal, car un groupe métacyclique ne peut pas avoir de sous-groupe abélien élémentaire de rang supérieur.
2. Par le lemme 1.5.6, $\Omega^n_X(\mathcal{O})$ relève $\Omega^n_X(k)$, $\forall\, n \in \mathbb{Z}$ et pour tout P-ensemble fini X. Donc la réduction modulo l'idéal $\wp$ induit un isomorphisme entre les groupes abéliens $D^{\Omega}_{\mathcal{O}}(P)$ et $D^{\Omega}_k(P)$.
   Par le corollaire 3.2.6, on a $D^{\Omega}_k(P) = D_k(P)$. Par suite, dans le diagramme

$$\begin{array}{ccc} D_{\mathcal{O}}(P) & \xrightarrow{a_{\mathcal{O}}} & D'_{\mathcal{O}}(P) \\ {\scriptstyle q}\downarrow & & \downarrow{\scriptstyle q'} \\ D_k(P) & \xrightarrow{a_k} & D'_k(P)) \end{array}$$

   de la section 1.4, l'homomorphisme $q : D_{\mathcal{O}}(P) \longrightarrow D_k(P)$ est surjectif. A fortiori, q' l'est aussi. Comme q' est injectif, q' est un isomorphisme.

□

3.3 Le plus petit exemple non abélien

Nous allons maintenant illustrer les résultats de la section précédente avec un exemple de p-groupe métacyclique, pour un nombre premier p impair. Le cas que nous allons traiter est celui du plus petit de ces p-groupes qui ne soit pas abélien. Autrement dit, nous allons déterminer explicitement le groupe de Dade d'un 3-groupe métacyclique non abélien, d'ordre 27.

Avant de commencer les calculs, remarquons que jusqu'à présent, nous avons supposé que k était algébriquement clos. Or, le seul groupe de Dade connu

actuellement qui dépend de k concerne $p = 2$ et le groupe quaternion Q_8 d'ordre 8. En effet, si k possède une racine cubique non triviale de l'unité, alors $D(Q_8) \cong \mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$, et dans le cas contraire (par exemple si $k = \mathbb{F}_2$), alors $D(Q_8) \cong \mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ (cf. théorème 10.3 de [CaTh1]). En fait, par la remarque précedant le lemme 1.5.12, si on a $D^\Omega(P) = D(P)$, alors on peut prendre $k = \mathbb{F}_p$, car les syzygies sont définis sur le corps $\mathbb{F}_p$.

Posons alors $p = 3$, $k = \mathbb{F}_3$ et $P = <u, v \mid u^9 = v^3 = 1, {}^v u = u^4>$. Autrement dit, P est un 3-groupe métacyclique d'ordre 27 non abélien et il s'insère dans une suite exacte courte scindée

$$1 \longrightarrow <u> \longrightarrow P \longrightarrow <\bar{v}> \longrightarrow 1,$$

où $\bar{v}$ est l'image de v dans le quotient $P/<u>$.

Structure de P. Le groupe P possède 4 sous-groupes maximaux, d'ordre 9. Plus précisément, on a un unique sous-groupe abélien élémentaire $E = <u^3, v>$ de rang 2 et trois sous-groupes cycliques $A_i = <uv^i>$, $0 \leq i \leq 2$ d'ordre 9. On a donc

$$A_0 = \{1, u, u^2, \ldots, u^8\};$$

$$A_1 = \{1, uv, u^5v^2, u^3, u^4v, u^8v^2, u^6, u^7v, u^2v^2\};$$

$$A_2 = \{1, uv^2, u^8v, u^3, u^4v^2, u^2v, u^6, u^7v^2, u^5v\}.$$

L'intersection de ces sous-groupes (maximaux) est le sous-groupe de Frattini $\Phi = <u^3>$ de P. Il est cyclique d'ordre 3 et coïncide avec le centre de P et avec le sous-groupe des commutateurs de P. De plus Φ est aussi le sous-groupe de Frattini de A_i, $0 \leq i \leq 2$.

Il y a trois autres sous-groupes cycliques $<v>$, $<u^3v>$ et $<u^6v>$ d'ordre 3 et ils sont tous conjugués. En effet, ${}^u<v> = <u^6v>$ et ${}^{u^2}<v> = <u^3v>$.

Notons $\overline{Q}$ l'image de Q dans le quotient $\overline{P} = P/\Phi$, pour tout sous-groupe Q de P et identifions $<v>$ avec $\overline{<v>}$ et E avec $\overline{E}$. Posons $V = <v>$. On a

$$[\mathcal{S}/P] = \{E, P\}, \qquad [\mathcal{C}/P] = \{A_0,\ A_1,\ A_2,\ \Phi,\ V\},$$

$$\mathcal{B} = \{\mathrm{Ten}_V^P\,\Omega_V,\ \mathrm{Ten}_\Phi^P\,\Omega_\Phi,\ \mathrm{Teninf}_{\overline{A}_0}^P\,\Omega_{\overline{A}_0},\ \mathrm{Teninf}_{\overline{A}_1}^P\,\Omega_{\overline{A}_1},\ \mathrm{Teninf}_{\overline{A}_2}^P\,\Omega_{\overline{A}_2},\ \Omega_P,\ \Omega_{\overline{P}}\},$$

$$\text{et} \quad \mathcal{E} = \{\Omega_V,\ \Omega_\Phi,\ \Omega_{\overline{A}_0},\ \Omega_{\overline{A}_1},\ \Omega_{\overline{A}_2},\ \Omega_E,\ \Omega_{\overline{P}}\},$$

selon un ordre choisi, satisfaisant les conditions de la section précédente.

Groupe de Dade. Déterminons le groupe de Dade de P et commençons par le sous-groupe des modules endo-triviaux. Par le corollaire 3.2.7, on sait que $T(P)$ est cyclique infini, engendré par Ω_P, i.e. la classe du $\mathbb{F}_3P$-module de dimension 26 défini comme le noyau de l'homomorphisme

$$\begin{array}{rcl} \varepsilon : \mathbb{F}_3P & \longrightarrow & \mathbb{F}_3 \\ x & \longmapsto & 1\ ,\ \forall\, x \in P. \end{array}$$

L'isomorphisme α_P de la section précédente donne

$$\alpha_P : D(P) \xrightarrow{\cong} T(V) \times T(\Phi) \times \prod_{i=0}^{2} T(\overline{A}_i) \times T(E) \times T(\overline{P}) \cong \left(\mathbb{Z}/2\mathbb{Z}\right)^5 \times \mathbb{Z}^2,$$

et consiste en l'application

$$\mathrm{Res}_V^P \times \mathrm{Res}_\Phi^P \times \prod_{i=0}^{2} \mathrm{Defres}_{\overline{A}_i}^P \times \mathrm{Res}_E^P \times \mathrm{Def}_{\overline{P}}^P .$$

Exprimons dans $\mathcal{E}$ les images des éléments de $\mathcal{B}$ et écrivons ces vecteurs en ligne dans une matrice 7×7 :

$$(\alpha_P)_{\mathcal{B}}^{\mathcal{E}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

En particulier, si l'on cherche un système de générateurs de $D(P)$ qui soit envoyé canoniquement sur $\mathcal{E}$, alors on peut prendre l'ensemble

$$\tilde{\mathcal{B}} = \{e_1,\ e_2,\ e_3,\ e_4,\ e_5,\ e_6 - e_1 - e_2,\ e_7 - e_1 - e_3 - e_4 - e_5\},$$

où e_i désigne le i-ème élément de $\mathcal{B}$, pour $1 \leq i \leq 7$.

Par ailleurs, on vérifie aisément que :

$$\mathrm{Defres}_{N_P(Q)/Q}^P \left(2\Omega_{P/V}\right) = 2\,\mathrm{Defres}_{N_P(Q)/Q}^P \left(\Omega_{P/V}\right) = 0 \ ,\ \forall\, 1 < Q \leq P \ .$$

D'où $2\Omega_{P/V} \in T(P)$. Mais, $\Omega^1_{P/V}(\mathbb{F}_3) \otimes \Omega^1_{P/V}(\mathbb{F}_3)$ n'est pas endo-trivial. En effet, il est de dimension $(\frac{27}{3} - 1)^2 = 64 \not\equiv \pm 1(\bmod 27)$. On a donc un exemple d'un module non endo-trivial, appartenant à la classe d'un module endo-trivial.

Syzygies relatifs. Par le corollaire 3.2.6, on sait que

$$\mathcal{B}' = \{\Omega_{P/H} \mid H \in [\mathcal{X}/P] \setminus \{P\}\} \cup \{\Omega_P\} =$$

$$= \{\Omega_P,\ \Omega_{P/V},\ \Omega_{\overline{P}},\ \Omega_{P/A_0},\ \Omega_{P/A_1},\ \Omega_{P/A_2},\ \Omega_{P/E}\}$$

forme un système de générateurs de cardinalité minimale du $\mathbb{Z}$-module $D(P)$. Calculons alors dans $\mathcal{E}$ les images des éléments de $\mathcal{B}'$:

$$(\alpha_P)_{\mathcal{B}'}^{\mathcal{E}} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & -2 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Explicitons le calcul qui nous a donné $\alpha_P(\Omega_{P/V})_E = -2$.

On a $\mathrm{Res}^P_E\,\Omega_{P/V} = \Omega_X$, où

$$X = \mathrm{Res}^P_E\,P/V = \coprod_{g\in[E\backslash P/V]} \{*\}\uparrow^P_V\downarrow^P_E = \coprod_{i=0}^{2} E/{}^{u^i}V = \coprod_{i=0}^{2} E/<u^{3i}v>.$$

Par le lemme 1.5.8, on a

$$\Omega_X = \sum_{i=0}^{2} \Omega_{E/<u^{3i}v>} - \sum_{0\le i<j\le 2} \Omega_{Y_{ij}} + \Omega_Y,$$

où $Y_{ij} = E/<u^{3i}v> \times E/<u^{3j}v>$, $\forall\, 0 \le i < j \le 2$ et $Y = \prod_{i=0}^{2} E/<u^{3i}v>$.

Ainsi, pour tous les indices i et j avec $0 \le i < j \le 2$, le E-ensemble Y_{ij} est isomorphe à

$$\big(\{*\}\uparrow^E_{<u^{3i}v>}\big) \times \big(\{*\}\uparrow^E_{<u^{3j}v>}\big) \cong \big(\{*\}\uparrow^E_{<u^{3i}v>}\downarrow^E_{<u^{3j}v>} \times\{*\}\big)\uparrow^E_{<u^{3j}v>} \cong E,$$

par la proposition 2.2.1 de [Bo2] (communément appelée "**formule de réciprocité de Frobenius**"). De même, on obtient $Y \cong E^3$. On en déduit

$$\Omega_X = \sum_{i=0}^{2} \Omega_{E/<u^{3i}v>} - 3\Omega_E + \Omega_E \overset{\sigma}{\longmapsto} -2\Omega_E,$$

où $\sigma = \rho_E \circ \mathrm{Res}^P_E$. Pour ce dernier calcul, on a utilisé l'égalité $\Omega_{X\amalg X} = \Omega_X$ du lemme 1.5.7.

Formule de Bouc et changement de base. Terminons cet exemple en appliquant la formule de Bouc (cf. lemme 1.5.10) aux éléments de torsion de $\mathcal{B}$, afin de comparer les deux systèmes de générateurs $\mathcal{B}$ et $\mathcal{B}'$ de $D(P)$. On a pour tout P-ensemble fini X et pour tout sous-groupe Q :

$$\mathrm{Ten}^P_Q\,\Omega_X = \sum_{\substack{S,T\in[s_P]\\ S\le_P T}} \mu_P(S,T)\big|\{a\in T\backslash P/Q \mid X^{T^a\cap Q}\neq\emptyset\}\big|\;\Omega_{P/S},$$

où $[s_P]$ est l'ensemble partiellement ordonné (pour l'inclusion $\le_P$) des classes de conjugaison des sous-groupes de P. Pour notre exemple, $[s_P]$ contient 8 éléments, représentés par $1,\ V,\ \Phi,\ A_0,\ A_1,\ A_2,\ E$ et P, où 1 désigne le groupe trivial.

Par suite, on a

$$\mu_P(S,T) = \begin{cases} 1 & , \text{ si } S = T \text{ , ou si } (S,T) = (1,\ E);\\ -1 & , \text{ si } S \lhd T \text{ et si } T/S \cong C_p;\\ 3 & , \text{ si } (S,T) = (\Phi, P);\\ 0 & , \text{ sinon.}\end{cases}$$

On calcule ainsi

$$\begin{array}{l} \mathrm{Ten}^P_V\Omega_V = 4\Omega_P + 2\Omega_{P/V} + \sum_{i=0}^{2}\Omega_{P/A_i};\\ \mathrm{Ten}^P_\Phi\,\Omega_\Phi = 6\Omega_P + 3\Omega_{P/<v>};\\ \mathrm{Teninf}^P_{A_i}\,\Omega_{\overline{A}_i} = \sum_{\substack{0\le j\le 2\\ i\neq j}}\Omega_{P/A_j} + \Omega_{P/E}\ ,\ \forall\, 0\le i\le 2.\end{array}$$

On peut vérifier l'exactitude de ces calculs en appliquant α_P des deux côtés des égalités. Les résultats doivent coïncider dans $D(P)$ (isomorphe à $(\mathbb{Z}/2\mathbb{Z})^5 \times \mathbb{Z}^2$).

Ce calcul montre, par exemple, que les chapeaux de $\mathrm{Ten}_\Phi^P\, \Omega^1_\Phi(\mathbb{F}_3)$ et de $(\Omega^1_P(\mathbb{F}_3))^{\otimes 6} \otimes (\Omega^1_{P/V}(\mathbb{F}_3))^{\otimes 3}$ sont isomorphes.

Exprimons ceci matriciellement, les lignes correspondant aux éléments de $\mathcal{B}$ exprimés dans $\mathcal{B}'$.

$$\begin{pmatrix} 4 & 2 & 0 & 1 & 1 & 1 & 0 \\ 6 & 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Chapitre 4

Groupes extraspéciaux

Les p-groupes extraspéciaux apparaissaient dans la famille détectrice déterminée par J. Carlson et J. Thévenaz dans leur article [CaTh1]. Désormais, ils n'en font plus partie (cf. [CaTh2]). Néanmoins, déterminer la structure du groupe de Dade de ces groupes constitue une étape successive "naturelle" quant à la classification des modules d'endo-permutation. En effet, les p-groupes extraspéciaux sont proches des p-groupes abéliens, dans le sens que le quotient d'un p-groupe extraspécial par son centre (cyclique d'ordre p) est un p-groupe abélien (et même abélien élémentaire). Or, rappelons-le, la classification est connue pour les p-groupes abéliens depuis plus de vingt ans, et le but du jeu consiste à résoudre la question pour un p-groupe fini arbitraire. Une façon de parvenir à obtenir des résultats est de compliquer petit à petit les groupes considérés. C'est ce que nous avons fait dans le chapitre précédent, en traitant le cas des p-groupes métacycliques. Dans ce chapitre, nous allons donner quelques propriétés des groupes de Dade des p-groupes extraspéciaux et nous allons ensuite traiter en détail le cas d'un 2-groupe extraspécial du type D_8^{*n}, pour $n \geq 2$.

4.1 Généralités sur les p-groupes extraspéciaux

Notation. Soit G un groupe. On note $Z(G)$ son centre, $\Phi(G)$ son sous-groupe de Frattini et G' son sous-groupe des commutateurs.

Définition 4.1.1. *Soient p un nombre premier et P un p-groupe fini. On dit que P est un p-***groupe extraspécial** *si les conditions suivantes sont satisfaites :*

1. *Les sous-groupes $Z(P)$, $\Phi(P)$ et P' coïncident. Notons Z ce sous-groupe.*
2. *Le groupe Z est cyclique d'ordre p.*

En particulier, si P est un p-groupe extraspécial, alors le groupe quotient P/Z est abélien élémentaire, car $Z = \Phi(P)$.

On dispose d'un théorème de classification des p-groupes extraspéciaux, qui les décrit en utilisant le produit central.

Définition 4.1.2. *Soient H, K et M des groupes tels que $M \leq Z(H)$ et tel qu'il existe un homomorphisme injectif $\theta : M \longrightarrow Z(K)$. Alors, si on identifie M avec son image $\theta(M)$, il existe un groupe G de la forme $G = HK$ avec $M = H \cap K \leq Z(G)$ et tel que H centralise K.*

Un groupe G satisfaisant ces propriétés est appelé le **produit central** *de H et K et on le note $G = H * K$. En particulier, si $|M| = 1$, alors on a un produit direct de groupes (cf. théorème 2.5.3 de [Go]).*

Notation. Dans le cas particulier où on considère le produit central d'un groupe G avec G lui-même, on note simplement G^{*2}, au lieu de $G * G$. Plus généralement, on note G^{*r} le produit central de r copies du groupe G, pour tout entier $r \geq 0$, avec les conventions que $G^{*0} = Z(G)$ et que $G^{*1} = G$.

Théorème 4.1.3. *Soient p un nombre premier et P un p-groupe extraspécial.*

1. *Si $p = 2$ et $|P| = 8$, alors soit P est isomorphe au groupe diédral D_8, soit P est isomorphe au groupe quaternionien Q_8.*
2. *Si p est impair, et $|P| = p^3$, alors P est isomorphe à l'un des deux groupes suivants :*

$$M = <x, y, z \mid x^p = y^p = z^p = 1, [x, z] = [y, z] = 1, [y, x] = z>;$$

$$N = <x, y \mid x^{p^2} = y^p = 1, {}^y x = x^{1+p}>.$$

   Remarquons que M est d'exposant p et de centre $<z>$, et que N est d'exposant p^2 et de centre $<x^p>$ (en fait, N est aussi un p-groupe métacyclique).
3. *Si $p = 2$ et $|P| > 8$, alors il existe un entier $r > 1$ tel que P est d'ordre 2^{2r+1} et isomorphe à l'un des groupes $Q_8 * D_8^{*(r-1)}$ ou bien D_8^{*r}.*

   De plus, les groupes $Q_8 * D_8^{*(r-1)}$ et D_8^{*r} ne sont pas isomorphes. Par contre, si r est pair, alors $D_8^{*r} \cong Q_8^{*r}$.
4. *Si p est impair et $|P| > p^3$, alors il existe un entier $r > 1$ tel que P est d'ordre p^{2r+1} et isomorphe au groupe $N * M^{*(r-1)}$, si P est d'exposant p^2, ou bien M^{*r}, si P est d'exposant p.*

   De plus, les groupes $N * M^{*(r-1)}$ et M^{*r} ne sont pas isomorphes.

Preuve. Cf. théorèmes 5.5.1 et 5.5.2 de [Go]. □

Nous verrons certaines propriétés du groupe des automorphismes de ces groupes dans le chapitre 5. Pour l'instant, concentrons-nous sur leur structure et donnons-nous, pour toute cette section, un nombre premier p, un entier n avec $n \geq 1$ et un p-groupe extraspécial P d'ordre p^{1+2n}.

Lemme 4.1.4. *Soit Q un sous-groupe de P. Les assertions suivantes sont vérifiées.*

1. *$1 < Q \lhd P \iff Z \leq Q$.*
2. *$Q \not\lhd P \implies N_P(Q) = C_P(Q)$ et Q est abélien élémentaire de rang au plus n.*

3. $N_P(Q) \triangleleft P$.

Preuve. Par définition, on a $[x, y] \in Z$, $\forall\, x, y \in P$. Autrement dit,

$$\forall\, x, y \in P \text{ , on a } {}^{y}x = x \text{ , ou bien } \exists\ z \in Z \text{ tel que } {}^{y}x = xz \text{ et } <z> = Z. \quad (4.1)$$

1. Supposons $1 < Q \triangleleft P$. Si $Q = Z$, l'assertion est vérifiée. Si $Q \neq Z$, alors il existe $x \in Q$ et $y \in P$ qui ne commutent pas. Or, par hypothèse, on a ${}^{y}x \in Q$, $\forall\, y \in P$ et $\forall\, x \in Q$ et donc, par 4.1, ${}^{y}x = xz$, avec $<z> = Z$. Par suite, $z = x^{-1}\,{}^{y}x \in Q$ car $Q \triangleleft P$. D'où $Z \leq Q$.
   Réciproquement, supposons $Z \leq Q$. Alors on a $Q/Z \ \triangleleft\ P/Z$, car P/Z est abélien et donc $Q \triangleleft P$.
2. Si $Q \not\triangleleft P$, alors $Z \not\leq Q$. Soient $x \in Q$ et $y \in N_P(Q)$. Supposons ${}^{y}x \neq x$. Alors, par 4.1, il existe un générateur z de Z tel que ${}^{y}x = xz$. Mais alors, $z = x^{-1}\,{}^{y}x \in Q$, car $y \in N_P(Q)$. D'où $Z \leq Q$. Par conséquent, on a nécessairement ${}^{y}x = x$, $\forall\, x \in Q$ et $\forall\, y \in N_P(Q)$. D'où $N_P(Q) = C_P(Q)$.
   Si Q n'est pas abélien, alors il existe x et y dans Q tels que $[x, y]$ engendre Z et donc $Z \leq Q$, ce qui contredit l'hypothèse $Q \not\triangleleft P$. Or, si Q est abélien, alors Q est abélien élémentaire. En effet, si Q contient un élément x d'ordre p^2, alors on a $1 \neq x^p \in \Phi(P)$ et $\Phi(P) = Z$. Donc, x^p engendre Z.
3. On a $Z \leq N_P(Q)$, $\forall\, Q \leq P$ et donc $N_P(Q) \triangleleft P$, par 1.

□

Ce lemme nous permet de répartir les sous-groupes non triviaux d'un p-groupe extraspécial P dans deux classes :

- Les sous-groupes non triviaux normaux de P. Autrement dit, ceux qui contiennent Z.
- Les sous-groupes non normaux de P. Autrement dit, ceux non triviaux qui ne contiennent pas Z.

Examinons les sous-groupes non normaux des deux types de p-groupes extraspéciaux suivants.

Notations. Soient p un nombre premier et n un entier avec $n \geq 0$.

1. Notons P_n, ou simplement P, un p-groupe extraspécial isomorphe à M^{*n}, si p est impair, ou isomorphe à D_8^{*n}, si $p = 2$, où M et D_8 sont définis comme dans le théorème précédent.
2. On note $\mathcal{Q}(P_n)$, ou simplement $\mathcal{Q}$, un système de représentants des classes de conjugaison des sous-groupes non normaux de P_n.
3. Pour tout $1 \leq i \leq n$, on note $\mathcal{Q}_i(P_n)$, ou simplement $\mathcal{Q}_i$, le sous-ensemble de $\mathcal{Q}$ formé des sous-groupes d'ordre p^i.

Corollaire 4.1.5. *Soient Q, $R \in \mathcal{Q}$ et $P = P_n$, pour un entier $n \geq 1$. On a,*

$$Q <_P R \iff Q <_P R < N_P(R) < N_P(Q) < P \quad (\text{et } N_P(R),\ N_P(Q) \triangleleft P).$$

De plus, si $Q <_P R$, alors il existe un unique $u \in [P/N_P(Q)]$ tel que $Q < {}^{u}R$, pour tout choix d'un système de représentants $[P/N_P(Q)]$.

Preuve. Soient Q, $R \in \mathcal{Q}$ et supposons $Q <_P R$. Par le lemme 4.1.4, on a $C_P(S) = N_P(S) < P$, et $N_P(S) \lhd P$, $\forall S \in \mathcal{Q}$. Donc, on a les inclusions $N_P(R) \leq N_P(Q) < P$ et on a aussi $N_P(R),\ N_P(Q) \lhd P$.

Soient $Q, R \in \mathcal{Q}$ avec $Q <_P R$, ou soient Q le groupe trivial et $R \in \mathcal{Q}$. Vérifions, par récurrence sur n, que l'inclusion $N_P(R) < N_P(Q)$ est stricte. Si $n = 1$, alors l'assertion est vraie car $\mathcal{Q}$ ne contient que des sous-groupes cycliques non centraux d'ordre p et donc l'hypothèse $Q <_P R$ n'est satisfaite que si Q est le groupe trivial, auquel cas on a $N_P(Q) = P > N_P(R)$, car $R \not\lhd P$.

Supposons $n > 1$ et l'assertion vraie pour les groupes P_m avec $m < n$. Quitte à remplacer R par un de ses conjugués, on peut supposer $Q < R$, car, comme $N_P(R) \lhd P$, on a $N_P(R) = N_P({}^gR)$, $\forall g \in P$. Si Q est le groupe trivial, alors on a $N_P(Q) = P > N_P(R)$, car $R \not\lhd P$, et donc l'assertion est vérifiée dans ce cas. Supposons $Q, R \in \mathcal{Q}$ avec $Q <_P R$. Soit $x \in Q$ tel que $x \neq 1$. Dans la preuve du théorème de la classification des p-groupes extraspéciaux (cf. théorème 4.18 de [Su]), M. Suzuki démontre que si $x' \in P \setminus Z$, alors il existe $y \in P$ tel que $[x', y] \neq 1$ et tel que le sous-groupe $E = <x', y>$ est extraspécial d'ordre p^3. Il montre ensuite que P est égal au produit central $E * C_P(E)$ et que $C_P(E)$ est un p-groupe extraspécial, d'ordre $\frac{|P|}{p^2}$. Il s'ensuit que $C_P(<x'>) = <x'> \times C_P(E)$, car $x' \notin C_P(E)$ et x' est d'ordre p. En particulier, ceci est vrai pour $x' = x$ et donc le groupe quotient $C_P(<x>)/<x>$ est extraspécial d'ordre $\frac{|P|}{p^2}$. De plus, les images $\bar{Q}$ de Q et $\bar{R}$ de R dans le groupe quotient $P_{n-1} = C_P(<x>)/<x>$ sont des sous-groupes ne contenant pas le centre $Z(P_{n-1})$ de P_{n-1}, car $Z(P_{n-1}) = (Z \cdot <x>)/<x>$ et $\underline{Q, R \not\geq Z}$. Ainsi, par hypothèse de récurrence, l'inclusion des images $\overline{N_P(R)} < \overline{N_P(Q)}$ est stricte. A fortiori, comme $<x> \leq N_P(R) \leq N_P(Q)$, l'inclusion $N_P(R) < N_P(Q)$ est aussi stricte. D'où $Q <_P R \implies Q <_P R < N_P(R) < N_P(Q) < P$ et $N_P(R),\ N_P(Q) \lhd P$. L'implication réciproque est évidente.

Prouvons à présent la seconde affirmation. Soient Q, $R \in \mathcal{Q}$ et $[P/N_P(Q)]$ un système de représentants des classes $P/N_P(Q)$. Supposons $Q <_P R$. Le groupe P agit transitivement (par conjugaison) sur l'ensemble $\mathrm{Conj}(Q)$ des sous-groupes conjugués de Q. Le stabilisateur d'un élément de $\mathrm{Conj}(Q)$ est $N_P(Q)$ (et $N_P(Q) = C_P(Q)$), et donc on a,

$$\mathrm{Conj}(Q) = \{\, {}^gQ \mid g \in [P/N_P(Q)]\} \quad \text{et} \quad |\,\mathrm{Conj}(Q)| = |[P/N_P(Q)]|.$$

Par hypothèse, il existe au moins un $g \in [P/N_P(Q)]$ avec ${}^gQ < R$. Soit alors $h \in [P/N_P(Q)]$ satisfaisant ${}^hQ < R$. Comme R est abélien et comme ${}^gQ$ et ${}^hQ$ sont des sous-groupes de R, l'ensemble ${}^hQ \cdot {}^gQ$ est aussi un sous-groupe de R. Montrons que si ${}^gQ \neq {}^hQ$, alors $Z \leq ({}^hQ \cdot {}^gQ)$. Quitte à conjuguer le tout par g^{-1}, on peut supposer $g = 1$ et on veut donc montrer que si $Q \neq {}^hQ$, alors $Z \leq ({}^hQ \cdot Q)$. Comme Q et ${}^hQ$ ont même ordre, il existe $x \in Q$ tel que $x \notin {}^hQ$. Donc $x \neq {}^hx$ car ${}^hx \in {}^hQ$. Ainsi, ${}^hx = zx$, i.e. $z = {}^hx \cdot x^{-1} \in ({}^hQ \cdot Q)$, pour un générateur z de Z, et donc $Z < ({}^hQ \cdot Q)$. Par suite, si ${}^gQ < R$ pour un $g \in [P/N_P(Q)]$, alors ${}^hQ \not< R$, pour tout $h \in [P/N_P(Q)]$ avec $h \neq g$, car $Z \not\leq R$. En résumé, si $Q <_P R$, alors il existe un unique $g \in [P/N_P(Q)]$ tel que ${}^gQ < R$. De manière équivalente, on a ainsi montré que si $Q <_P R$, alors

il existe un unique $u \in [P/N_P(Q)]$ tel que $Q < {}^uR$, car $\{g^{-1} \mid g \in [P/N_P(Q)]\}$ est aussi un système de représentants des classes $P/N_P(Q)$, car $N_P(Q) \lhd P$.

□

La seconde affirmation du lemme prouve, en particulier, le fait suivant et nous incite à introduire une notation supplémentaire.

Remarque 4.1.6. *Soient $Q, R \in \mathcal{Q}$ avec $Q <_P R$ et $[P/N_P(Q)]$ un système de représentants des classes $P/N_P(Q)$. Alors l'ensemble $\{u \in P \mid Q < {}^uR\}$ est égal à exactement une des classes de $P/N_P(Q)$. Ce fait nous permet de définir la notation $u_{Q,R}$ pour l'unique élément $u_{Q,R} \in [P/N_P(Q)]$ tel que $Q < {}^{u_{Q,R}}R$.*

Remarque 4.1.7. *Soit $P = P_n$ et appliquons les résultats des sections II.9 et III.13 de [Hu1] à notre situation.*

Le groupe quotient P/Z est un $\mathbb{F}_p$-espace symplectique non dégénéré si p est impair, respectivement orthogonal non dégénéré si $p = 2$. L'image des éléments de $\mathcal{Q}$ par le passage au quotient $\pi : P \to P/Z$ correspond à l'ensemble des sous-espaces totalement isotropes de P/Z si p est impair, i.e.

$$\pi(Q) \subseteq \big(\pi(Q)\big)^{\perp \overset{déf}{=}} \{xZ \in P/Z \mid [y,x] = 1,\ \forall\, y \in Q\},\ \forall\, Q \in \mathcal{Q}\ ,$$

respectivement totalement singuliers si $p = 2$ (i.e. $x^2 = 1,\ \forall\, x \in Q$). En particulier, il résulte que l'image du normalisateur $N_P(Q)$ d'un élément $Q \in \mathcal{Q}$ est l'orthogonal de $\pi(Q)$ car $N_P(Q) = C_P(Q)$. Par suite, pour tout sous-groupe $Q \in \mathcal{Q}$, on a l'égalité $|Q| \cdot |N_P(Q)| = |P|$, car $Z \leq N_P(Q)$ et la forme symplectique si p est impair, respectivement orthogonale si $p = 2$, est non dégénérée.

De plus, l'argument de la preuve du théorème 4.18 de [Su] que nous avons utilisé dans la preuve du corollaire précédent implique que si $|Q| = p^i$, pour un entier $1 \leq i \leq n$, alors $N_P(Q)$ est de la forme $Q \times P_{n-i}$ (voir aussi la section 3 de [CaTh2]).

Le lemme suivant va nous être fort utile pour les calculs de la prochaine section.

Lemme 4.1.8. *Soient Q, $R \in \mathcal{Q}$.*

1. *Si $Q \not\leq_P R$, alors* $\mathrm{Defres}^P_{N_P(Q)/Q}\, \Omega_{P/R} = 0$.
2. *Si $Q \leq_P R$, alors* $\mathrm{Defres}^P_{N_P(Q)/Q}\, \Omega_{P/R} = \Omega_{N_P(Q)/\,{}^uR}$ *, où $u = u_{Q,R}$.*

Avant de prouver ce résultat, rappelons un fait général concernant les ensembles munis d'une action de groupe.

Remarque 4.1.9. *Soient G un groupe fini et $H,\ K \leq G$. Considérons le G-ensemble transitif G/H muni de l'action de G induite par la multiplication à gauche. Alors, $\big(G/H\big)^K \neq \emptyset \Longleftrightarrow K \leq_G H$.*

En effet, on a $\big(G/H\big)^K = \{xH \in G/H \mid gxH = xH,\ \forall\, g \in K\}$. Soient alors $xH \in G/H$ et $g \in K$. On a $gxH = xH \Longleftrightarrow g^x \in H \Longleftrightarrow g \in {}^xH$. Donc, $\big(G/H\big)^K = \{xH \in G/H \mid K \leq {}^xH\}$.

Nous pouvons à présent démontrer le lemme 4.1.8.

Preuve. Par le lemme 1.5.9, on a $\mathrm{Defres}^P_{N_P(Q)/Q}\,\Omega_{P/R} = \Omega_{X^Q}$, où X est le $N_P(Q)$-ensemble $\mathrm{Res}^P_{N_P(Q)}(P/R) = \{*\}\uparrow^P_R\downarrow^P_{N_P(Q)}$. La formule de Mackey pour les P-ensembles nous donne

$$X = \coprod_{g\in[N_P(Q)\backslash P/R]} \{*\}\downarrow^{\,{}^gR}_{{}^gR\cap N_P(Q)}\uparrow^{N_P(Q)}_{{}^gR\cap N_P(Q)} = \coprod_{g\in[P/RN_P(Q)]} N_P(Q)/({}^gR\cap N_P(Q)),$$

car $N_P(Q)\lhd P$.

Par la remarque ci-dessus, on a

$$\Big(N_P(Q)/\big({}^gR\cap N_P(Q)\big)\Big)^Q \neq \emptyset \iff Q\leq_{N_P(Q)} {}^gR\ .$$

En particulier, il s'ensuit que $\mathrm{Defres}^P_{N_P(Q)/Q}\,\Omega_{P/R} = 0$, si $Q\not\leq_P R$.

Si $Q\leq_P R$, alors $X = \coprod_{g\in[P/N_P(Q)]} N_P(Q)/\,{}^gR$ et $u_{Q,R}$ est l'unique élément $g\in[P/N_P(Q)]$ tel que $Q\leq {}^gR$, par le corollaire 4.1.5. Par suite,

$$X^Q = \coprod_{g\in[P/N_P(Q)]} \big(N_P(Q)/\,{}^gR\big)^Q = N_P(Q)/\,{}^{u_{Q,R}}R\ ,$$

ce qui démontre le lemme. □

Nous allons à présent étudier le groupe de Dade de P_n (avec $n\geq 1$) en considérant le sous-groupe $E(P_n)$ de $D(P_n)$ défini comme suit.

Définition 4.1.10. *Soient n un entier avec $n\geq 1$ et $P = P_n$. On note $E(P)$ le sous-groupe* $\mathrm{Ker}(\mathrm{Def}^P_{P/Z})$ *de $D(P)$ et on pose $E^\Omega(P) = E(P)\cap D^\Omega(P)$.*

Le lemme 10.2 de [CaTh1] décompose $D(G)$ comme la somme directe de $E(G)$ et de $D(G/Z(G))$, pour un 2-groupe G diédral, quaternionien ou semi-diédral. En fait, ce résultat est aussi valable dans notre situation.

Proposition 4.1.11. *Soient n un entier avec $n\geq 1$ et $P = P_n$. On a une suite exacte courte scindée de groupes abéliens :*

$$0\ \longrightarrow\ E(P)\ \xrightarrow{\ i\ }\ D(P)\ \xrightarrow{\ \mathrm{Def}^P_{P/Z}\ }\ D(P/Z)\ \longrightarrow\ 0\ ,$$

où i est l'inclusion et la section est l'homomorphisme $\mathrm{Inf}^P_{P/Z}$.

Autrement dit, on a un isomorphisme de groupes abéliens :

$$\begin{array}{rcl}\varphi : D(P) & \longrightarrow & D(P/Z)\ \oplus\ E(P)\\ x & \longmapsto & \big(\mathrm{Def}^P_{P/Z}(x)\ ,\ x-\mathrm{Inf}^P_{P/Z}\,\mathrm{Def}^P_{P/Z}(x)\big)\ .\end{array}$$

Preuve. Par définition de $E(P)$, la suite est exacte en $D(P)$. De plus, par le lemme 1.5.4, la déflation est surjective et l'inflation est une section de la déflation. Donc la suite est exacte et scindée et φ est un isomorphisme. □

Remarque 4.1.12. *Le groupe $T(P)$ des modules endo-triviaux est un sous-groupe de $E(P)$. En effet, par l'assertion 1 du théorème 1.5.5, on a*

$$T(P) \;=\; \bigcap_{1<Q\leq P} \left(\mathrm{Ker}\left(\mathrm{Defres}^P_{N_P(Q)/Q} \right) \right) \;\leq\; \mathrm{Ker}(\mathrm{Def}^P_{P/Z}) \;=\; E(P).$$

4.2 Un cas particulier

Soient $p = 2$, $n \geq 1$ et posons $P = P_n$. Dans cette section, nous allons déterminer $D(P)$ et $D_{\mathcal{O}}(P)$.

Notation. Pour tous entiers m et i avec $1 \leq i \leq m$, posons $q_{m,i} = |\mathcal{Q}_i(P_m)|$. Notons q_m, ou simplement q, la cardinalité de $\mathcal{Q}(P_m)$.

Posons $Z = <z>$ et remarquons le fait suivant.

Remarque 4.2.1. *Le nombre de sous-groupes abéliens élémentaires de rang 2 contenant Z est égal à $q_{n,1}$.*

Preuve. Soient $u, v \in P$, avec u d'ordre 2 et $u \neq z$. Alors, ${}^v u = u$, ou bien ${}^v u = uz$. Par suite, tout sous-groupe $<u> = Q \in \mathcal{Q}_1$ possède un unique conjugué, à savoir $<uz>$, et tous deux sont identifiés à $<\bar{u}>$ dans le quotient P/Z. Or, $<\bar{u}>$ se relève en $<u, z>$, lorsqu'on considère la bijection entre les sous-groupes de P/Z et ceux de P contenant Z. Ainsi, on a une bijection entre les classes de conjugaison des sous-groupes cycliques d'ordre 2 non centraux (i.e. les éléments de $\mathcal{Q}_1$) et les sous-groupes abéliens élémentaires de rang 2 contenant Z. □

Continuons avec un petit exercice de comptage.

Lemme 4.2.2. *On a $q_{n,1} = (2^n - 1)(2^{n-1} + 1) = 2^{2n-1} + 2^{n-1} - 1$.*

Preuve. Prouvons le résultat par récurrence sur n. Si $n = 1$, alors $P = D_8$ et $\mathcal{Q} = \mathcal{Q}_1$ est de cardinalité 2. D'où l'assertion car $2 = (2^1 - 1)(2^{1-1} + 1)$.

Supposons $n > 1$ et le résultat prouvé pour tout entier m avec $1 \leq m < n$. Déterminons le nombre $q_{n,1}$ de sous-groupes non centraux d'ordre 2.

On considère le passage au quotient $\pi : P \longrightarrow P/Z$. Comme P/Z est abélien élémentaire de rang $2n$, c'est un $\mathbb{F}_2$-espace vectoriel de dimension $2n$ et donc possède $2^{2n} - 1$ droites. Celles-ci sont les images par π de toutes les classes de conjugaison des sous-groupes cycliques non centraux de P, c'est-à-dire les sous-groupes de $\mathcal{Q}_1$ et les sous-groupes cycliques d'ordre 4 (et normaux dans P car contenant Z).

Par ailleurs, P s'écrit comme un produit central $D_8 * P_{n-1}$. Donc ses éléments d'ordre 2 peuvent s'écrire comme un produit xy, avec $x \in D_8$, $y \in P_{n-1}$ et x et y sont des éléments d'ordre au plus 2, ou bien tous deux d'ordre 4. En effet, par définition du produit central, x et y commutent, et donc s'ils sont tous deux d'ordre 4, alors $(xy)^2 = x^2y^2 = zz = 1$, i.e. leur produit est d'ordre 2. Par récurrence, on obtient ainsi

- Si $x = 1$, alors, à conjugaison près, on a 1 possibilité pour x et $q_{n-1,1}$ possibilités pour y .
- Si x est d'ordre 2, alors, à conjugaison près, on a $q_{1,1} = 2$ possibilités pour x et $q_{n-1,1} + 1$ possibilités pour y .
- Si x est d'ordre 4, alors, à conjugaison près, on a 1 possibilité pour x et $(2^{2(n-1)} - 1) - q_{n-1,1}$ possibilités pour y. En effet, par définition, on a $Z = Z(P_{n-1})$ et P_{n-1}/Z est un $\mathbb{F}_2$-espace vectoriel de dimension $2(n-1)$. Par conséquent, P_{n-1}/Z possède $(2^{2(n-1)}-1)$ sous-groupes cycliques, avec chaque fois deux relevés conjugués, dont $q_{n-1,1}$ se relèvent dans P_{n-1} en sous-groupes d'ordre 2, par la remarque précédente.

D'où, en tout,

$$q_{n,1} = 1\cdot q_{n-1,1} + 2\cdot(q_{n-1,1}+1) + 1\cdot\big((2^{2(n-1)}-1) - q_{n-1,1}\big) = 2q_{n-1,1} + 2^{2(n-1)} + 1 =$$

$$= 2(2^{2n-3} + 2^{n-2} - 1) + 2^{2n-2} + 1 = 2^{2n-1} + 2^{n-1} - 1.$$

□

Poursuivons notre analyse du groupe de Dade et montrons que le sous-groupe de torsion $D^t(P)$ de $D(P)$ est trivial, en utilisant le résultat suivant de la section 12 de [CaTh2].

Théorème 4.2.3. *Soit G un 2-groupe fini et notons $\mathcal{Y}$ un système de représentants des classes de conjugaison des sous-groupes H de G tels que le quotient $N_G(H)/H$ est un groupe cyclique d'ordre au moins 4, ou quaternionien, ou semidiédral.*

Pour tout $H \in \mathcal{Y}$, notons $\rho_{N_G(H)/H} : D^t(N_G(H)/H) \to T^t(N_G(H)/H)$ la projection canonique. Alors l'application

$$\prod_{H\in\mathcal{Y}} \rho_{N_G(H)/H} \circ \mathrm{Defres}^G_{N_G(H)/H} : D^t(G) \longrightarrow \prod_{H\in\mathcal{Y}} T^t(N_G(H)/H)$$

est injective.

Rappelons que si N est un 2-groupe cyclique d'ordre 2^n, avec $n \geq 2$, alors le théorème 2.0.13 implique $D^t(N) = \oplus_{1\leq M<\Phi(N)} T^t(N/M) \cong (\mathbb{Z}/2\mathbb{Z})^{n-2}$. Si N est quaternionien ou semidiédral, alors on a $D(N) \cong T(N) \oplus D(N/Z(N))$, par le lemme 10.2 de [CaTh1], et $T^t(N)$ est isomorphe à $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, respectivement $\mathbb{Z}/2\mathbb{Z}$, par les sections 6, respectivement 7, de [CaTh1].

Corollaire 4.2.4. *Le sous-groupe de torsion $D^t(P)$ de $D(P)$ est trivial.*

Preuve. Par le théorème 4.2.3, il suffit de montrer que P ne possède aucun sous-groupe Q tel que le quotient $N_P(Q)/Q$ soit un groupe cyclique d'ordre au moins 4, quaternionien, ou semidiédral. Soit $1 < Q \leq P$ et distinguons les deux cas suivants. Si $Z \leq Q$, alors $Q \lhd P$, par le lemme 4.1.4, et le quotient P/Q est un 2-groupe abélien élémentaire. Par la remarque 4.1.7, si $Z \not\leq Q$, alors $N_P(Q) \cong Q \times P_{n-i}$, où i est l'entier compris entre 1 et n et tel que $|Q| = 2^i$ (avec la convention $P_0 = Z$). Par suite, on a $N_P(Q)/Q \cong P_{n-i}$. D'où le corollaire. □

Remarque 4.2.5. *Le corollaire ci-dessus constitue la raison principale qui nous a incités à étudier le groupe de Dade d'un 2-groupe extraspécial du type D_8^{*n}. En effet, le fait que le groupe de Dade est sans torsion rend son analyse plus aisée. Signalons également que ce résultat est démontré dans la section 12 de [CaTh2]. Toutefois, nous avons tenu à le redémontrer ici, car il nous permet de mettre en évidence d'autres caractéristiques de ces 2-groupes.*

Par la proposition 4.1.11, pour déterminer le groupe de Dade de P, il suffit de déterminer $E(P)$. En effet, P/Z est abélien et donc $D(P/Z)$ est engendré par les syzygies relatifs $\Omega_{P/Q}$, où Q parcourt les sous-groupes de P contenant Z et d'indice au moins 3 dans P (cf. théorème 2.0.13). Afin de déterminer $E(P)$, on retiendra du corollaire 4.2.4 les deux conséquences suivantes :

1. Le sous-groupe $E(P)$ de $D(P)$ est sans torsion.
2. $T(P) = <\Omega_P> \cong \mathbb{Z}$, si $n \geq 2$ (cf. assertions 2 et 3 du théorème 1.5.5).

Comme le groupe de Dade $D(D_8)$ est connu (cf. théorème 10.3 de [CaTh1]), nous allons dorénavant supposer $n \geq 2$.

Par le corollaire 4.2.4, $E(P)$ est un $\mathbb{Z}$-module libre. Calculons son rang r_E. Par la proposition 4.1.11, on a $r_E = r_P - r_{P/Z}$, où r_P et $r_{P/Z}$ sont les rangs de $D(P)$ et $D(P/Z)$ respectivement.

Par l'assertion 5 du théorème 1.5.5, on sait que r_P et $r_{P/Z}$ sont égaux au nombre de sous-groupes non cycliques de P et respectivement P/Z.

Considérons les notations introduites en début de section et notons c le nombre de sous-groupes cycliques d'ordre 4 et d le nombre de sous-groupes normaux d'ordre au moins 4. Le nombre de classes de conjugaisons des sous-groupes non cycliques de P vaut

$$r_P = (d - c) + (q - q_{n,1}) \ .$$

Qu'en est-il de $r_{P/Z}$? L'ensemble des sous-groupes cycliques de P/Z est en bijection avec l'ensemble constitué des sous-groupes cycliques d'ordre 4 et des sous-groupes abéliens élémentaires de rang 2 contenant Z. Ainsi, par la remarque du début de cette section, le nombre de sous-groupes non cycliques de P/Z vaut :

$$r_{P/Z} = d - (c + q_{n,1}) \quad \text{et donc} \quad r_E = r_P - r_{P/Z} = q \ .$$

Autrement dit, on a montré le résultat suivant.

Théorème 4.2.6. *$E(P)$ est un $\mathbb{Z}$-module libre de rang q.*

Remarque 4.2.7. *Il résulte de la section 7 de [Bo1], que le groupe quotient $D(P)/D^{\Omega}(P)$ est fini. Par suite, comme*

$$D(P) \cong E(P) \oplus D(P/Z) \quad \textit{et comme} \quad D(P/Z) = D^{\Omega}(P/Z),$$

on obtient un isomorphisme de groupes

$$D(P)/D^{\Omega}(P) \cong E(P)\big/\big(E(P) \cap D^{\Omega}(P)\big) = E(P)/E^{\Omega}(P),$$

en identifiant $D(P/Z)$ à un sous-groupe de $D^\Omega(P)$, par inflation. Il s'ensuit que $E^\Omega(P)$ est un sous-module libre de $E(P)$ de même rang. Toutefois, nous préférons donner ci-dessous une preuve directe du fait que $E^\Omega(P)$ est un sous-module libre de $E(P)$ de même rang, indépendamment des résultats subtils de la section 7 de [Bo1].

Lemme 4.2.8. *Soit $Q \in \mathcal{Q}$. Alors, $\Omega_{P/Q} \in E(P)$.*

Preuve. Soit $Q \in \mathcal{Q}$. On a $\mathrm{Def}^P_{P/Z}\,\Omega_{P/Q} = \Omega_X$, où $X = (P/Q)^Z$, par le lemme 1.5.9. Or, $Z \not\leq_P Q$ implique $(P/Q)^Z = \emptyset$, par la remarque 4.1.9. Par suite, $\mathrm{Def}^P_{P/Z}\,\Omega_{P/Q} = \Omega_\emptyset = 0$. □

Ce lemme nous incite à nous demander si l'ensemble

$$\{\Omega_{P/Q} \mid Q \in \mathcal{Q}\} \cup \{\Omega_P\}$$

peut former un système de générateurs du $\mathbb{Z}$-module libre $E(P)$, et si l'on peut en extraire "facilement" une base. En effet, cet ensemble est contenu dans $E(P)$ et il est de cardinal $q+1$.

Afin de répondre à cette question, nous définissons l'application β ci-dessous.

Soit $Q \in \mathcal{Q}_1$. On a $N_P(Q)/Q \cong P_{n-1}$ et donc $Z\big(N_P(Q)/Q\big) = ZQ/Q \cong Z$. En identifiant Z avec $Z\big(N_P(Q)/Q\big)$, on peut aussi identifier $N_P(Q)/QZ$ avec $\big(N_P(Q)/Q\big) \,/\, \big(Z(N_P(Q)/Q)\big)$ et donc $E\big(N_P(Q)/Q\big)$ avec $\mathrm{Ker}\,\big(\mathrm{Def}^{N_P(Q)/Q}_{N_P(Q)/QZ}\big)$.

Par conséquent, on peut considérer l'application (bien définie)

$$\begin{array}{rcl} dr_Q : E(P) & \longrightarrow & E(N_P(Q)/Q) \\ x & \longmapsto & \mathrm{Defres}^P_{N_P(Q)/Q}(x)\ . \end{array}$$

Notons dr'_Q la restriction de dr_Q à $E^\Omega(P)$ et posons

$$\beta = \prod_{Q\in\mathcal{Q}_1} dr_Q \qquad \text{et} \qquad \beta' = \prod_{Q\in\mathcal{Q}_1} dr'_Q\ .$$

Proposition 4.2.9. *On a $\mathrm{Ker}(\beta) = \mathrm{Ker}(\beta') = T(P) = <\Omega_P>$.*

Preuve. Comme nous l'avons déjà remarqué ci-dessus, on a $T(P) = <\Omega_P>$, par les assertions 2 et 3 du théorème 1.5.5. De plus, par le lemme 1.5.9, on a :

$$\mathrm{Defres}^P_{N_P(Q)/Q}\,\Omega_P = \mathrm{Def}^{N_P(Q)}_{N_P(Q)/Q}\,\Omega_{N_P(Q)} = \Omega_{(N_P(Q))^Q} = \Omega_\emptyset = 0,\ \forall\, 1 < Q \leq P\ .$$

Donc, on a $T(P) \leq \mathrm{Ker}(\beta)$ et $T(P) \leq \mathrm{Ker}(\beta')$, car $T(P) = <\Omega_P> \leq E^\Omega(P)$.

Comme $E^\Omega(P_m) \leq E(P_m)$, $\forall\, m \geq 1$, on a $\mathrm{Ker}(\beta') \leq \mathrm{Ker}(\beta)$ et donc il nous reste à prouver l'inclusion $\mathrm{Ker}(\beta) \leq T(P)$. On va utiliser l'égalité

$$T(P) = \bigcap_{1<Q\leq P} \mathrm{Ker}\,\big(\mathrm{Defres}^P_{N_P(Q)/Q}\big)\ ,$$

donnée par l'assertion 1 du théorème 1.5.5, pour montrer cette inclusion. En d'autres termes, on doit montrer que

$$\mathrm{Defres}^P_{N_P(Q)/Q}(x) = 0 \ , \ \forall\, x \in \mathrm{Ker}(\beta) \quad \text{et} \quad \forall\, 1 < Q \leq P \ .$$

Par définition de $E(P)$, l'application $\mathrm{Def}^P_{P/Q}$ restreinte à $E(P)$ est nulle pour tout sous-groupe Q contenant Z, c'est-à-dire pour tout sous-groupe normal non trivial Q. Soit alors $R \in \mathcal{Q}$ un sous-groupe non normal de P. Comme, pour tout $1 \leq i \leq n$, on peut toujours choisir l'ensemble $\mathcal{Q}_i$ de telle sorte que chacun de ses éléments contienne au moins un élément de $\mathcal{Q}_1$ comme sous-groupe, il existe $Q \in \mathcal{Q}_1$ tel que $Q \leq R$. D'où, $Q \leq R < N_P(R) \leq N_P(Q)$, par le corollaire 4.1.5, et donc

$$\mathrm{Defres}^P_{N_P(R)/R} = \mathrm{Defres}^{N_P(Q)/Q}_{N_P(R)/R} \circ \mathrm{Defres}^P_{N_P(Q)/Q} \ .$$

En effet, si A est une $N_P(Q)$-algèbre de Dade (sur k) et si on note $(.\downarrow)$ la restriction $\mathrm{Res}^{N_P(Q)}_{N_P(R)}(.)$, on a

$$\mathrm{Def}^{N_P(R)}_{N_P(R)/Q}(A\downarrow) = (A\downarrow)^Q / \sum_{S<Q} (A\downarrow)^Q_S \cong \big(A^Q / \sum_{S<Q} A^Q_S\big)\downarrow^{N_P(Q)/Q}_{N_P(R)/Q} \ ,$$

car Q agit trivialement. Autrement dit, on a, dans $D'_k(N_P(R)/Q)$,

$$\mathrm{Def}^{N_P(R)}_{N_P(R)/Q} \circ \mathrm{Res}^{N_P(Q)}_{N_P(R)} = \mathrm{Res}^{N_P(Q)/Q}_{N_P(R)/Q} \circ \mathrm{Def}^{N_P(Q)}_{N_P(Q)/Q} \ .$$

Par conséquent, l'application $\mathrm{Defres}^P_{N_P(R)/R}$ se factorise comme la composition $\mathrm{Defres}^{N_P(Q)/Q}_{N_P(R)/R} \circ dr_Q$. Or, la restriction de dr_Q à $\mathrm{Ker}(\beta)$ est nulle et donc $\mathrm{Defres}^P_{N_P(R)/R}$ restreinte à $\mathrm{Ker}(\beta)$ est aussi nulle. D'où la proposition. □

On en déduit immédiatement la conséquence suivante.

Corollaire 4.2.10. *Les suites de groupes abéliens*

$$0 \longrightarrow T(P) \xrightarrow{i} E(P) \xrightarrow{\beta} \prod_{Q \in \mathcal{Q}_1} E(N_P(Q)/Q) \xrightarrow{\pi} \mathrm{Coker}(\beta) \longrightarrow 0 \quad \textit{et}$$

$$0 \longrightarrow T(P) \xrightarrow{i'} E^\Omega(P) \xrightarrow{\beta'} \prod_{Q \in \mathcal{Q}_1} E(N_P(Q)/Q) \xrightarrow{\pi'} \mathrm{Coker}(\beta') \longrightarrow 0 \ ,$$

où i et i' sont les inclusions et π et π' les passages aux quotients, sont exactes.

Comme $\mathrm{Ker}(\beta) = T(P)$, le rang de β, c'est-à-dire le rang du $\mathbb{Z}$-module $\mathrm{Im}(\beta)$, vaut au plus $(q-1)$, et de même pour son sous-module $\mathrm{Im}(\beta')$. Nous allons montrer que cette borne maximale est atteinte, et qu'en fait, l'image de β' est un facteur direct de rang $(q-1)$ de $\prod_{Q \in \mathcal{Q}_1} E(N_P(Q)/Q)$.

Définition 4.2.11. *Posons $\mathcal{E} = \{\Omega_{P/Q} \mid Q \in \mathcal{Q}\}$ et $\mathcal{E}' = \mathcal{E} \cup \{\Omega_P\}$. Ce sont des sous-ensembles de $E^\Omega(P)$ de cardinal q et $(q+1)$ respectivement.*

Nous allons à présent montrer que $\mathcal{E}'$ est un système de générateurs du $\mathbb{Z}$-module libre $E(P)$ et on va en extraire une base. Rappelons que notre but est de déterminer $D(P)$. Pour y parvenir, on va procéder par récurrence, selon le plan suivant.

Plan

1. Soit $P = P_2$. On montre que $q = 15$ et que $\mathrm{Im}(\beta)$ est un $\mathbb{Z}$-module libre facteur direct de rang 14 de $\prod_{Q\in\mathcal{Q}_1} E(N_P(Q)/Q)$.
2. On en déduit que $\mathcal{E}'$ engendre $E^\Omega(P)$ et que $E^\Omega(P) = E(P)$. A fortiori, cela implique $D^\Omega(P) = D(P)$.
3. On exhibe l'unique relation non triviale (à multiple entier près) liant les éléments de $\mathcal{E}'$. On en déduit une $\mathbb{Z}$-base de $E(P)$.
4. On suppose $n > 2$ et on applique la récurrence, en commençant par déterminer l'unique relation non triviale (à multiple entier près) liant les éléments de $\mathcal{E}'$.
5. On prouve que $\mathrm{Im}(\beta)$ est un $\mathbb{Z}$-module libre facteur direct de rang $q-1$ de $\prod_{Q\in\mathcal{Q}_1} E(N_P(Q)/Q)$, pour $P = P_n$ et $n > 2$, par récurrence. On en déduit le résultat cherché, à savoir $D^\Omega(P) = D(P)$, et en plus, on va expliciter une base de ce $\mathbb{Z}$-module libre.

Avant de nous lancer dans cette démonstration, il convient de rappeler quelques résultats des sections 5 et 10 de [CaTh1], concernant le groupe de Dade d'un groupe diédral d'ordre 8.

Théorème 4.2.12. *Soit $D_8 = <s,t \mid s^2 = t^2 = (st)^4 = 1>$ un groupe diédral d'ordre 8 et notons $Z = <(st)^2>$ son centre.*

1. $T(D_8) = < \Omega_{D_8},\ \Omega_{D_8/<s>} > \cong \mathbb{Z}^2$. *De plus,* $\Omega_{D_8/<t>} = -\Omega_{D_8/<s>}$.
2. $D(D_8) \cong T(D_8) \oplus D(D_8/Z) \cong \mathbb{Z}^3$.

En particulier, ce théorème implique $T(D_8) = E(D_8)$.

Nous sommes maintenant prêts pour montrer le premier point de notre plan.

Proposition 4.2.13. *Supposons $n = 2$ et notons $P = P_2$. Les assertions suivantes sont vérifiées :*

1. $q = 15$ *;*
2. $\mathrm{Im}(\beta') = \mathrm{Im}(\beta)$ *;*
3. $\mathrm{Im}(\beta)$ *est un $\mathbb{Z}$-module libre facteur direct de $\prod_{Q\in\mathcal{Q}_1} E(N_P(Q)/Q)$ de rang* 14.

Preuve. Ecrivons $P = D * D'$ avec $D = <s,t>$ et $D' = <u,v>$ diédraux d'ordre 8, et notons $z = (st)^2 = (uv)^2$ le générateur de Z. Rappelons que nous considérons toujours les sous-groupes et les éléments de P à conjugaison près.

Par le lemme 4.2.2, on a $q_{n,1} = (2^2-1)(2^1+1) = 9$. Plus précisément, on peut choisir

$$\mathcal{Q}_1 = \{<s>, <t>, <u>, <v>, <su>, <sv>, <tu>, <tv>, <stuv>\}.$$

Déterminons q_2. Un sous-groupe de $\mathcal{Q}_2$ est engendré par deux éléments non centraux x et y, d'ordre 2. Or, x et y engendrent un groupe abélien élémentaire si et seulement si $[x, y] = 1$. Sinon $<x, y>$ est diédral d'ordre 8. Utilisons $\mathcal{Q}_1$ pour dénombrer ces sous-groupes et commençons avec $x = s$. On a

$$<s, y> \in \mathcal{Q}_2 \Longleftrightarrow y \in \{u, v, su, sv\} \quad \text{et}$$

$$<s, y> = D_8 \Longleftrightarrow y \in \{t, tu, tv, stuv\}.$$

Ainsi, quatre éléments engendrent avec s un groupe abélien élémentaire de rang 2 non normal dans P (et les quatre autres un groupe diédral d'ordre 8). Il en va de même pour les huit autres éléments non centraux d'ordre 2. D'où $9 \cdot 4 = 36$ possibilités.

Or, un sous-groupe E abélien élémentaire de rang 2 possède 3 éléments d'ordre 2 et donc on a $3 \cdot 2 = 6$ systèmes de générateurs possibles pour E. Autrement dit, parmi les 36 sous-groupes recensés, on en a $\frac{36}{6} = 6$ distincts. D'où $q_2 = 6$ et donc $q = 9 + 6 = 15$.

Pour tout $Q \in \mathcal{Q}_1$, le quotient $N_P(Q)/Q$ est un groupe diédral d'ordre 8. Ainsi, par le théorème 4.2.12, on a

$$E(N_P(Q)/Q) = T(N_P(Q)/Q) = <\Omega_{N_P(Q)/Q}, \Omega_{N_P(Q)/R}> \cong \mathbb{Z}^2,$$

pour un sous-groupe R abélien élémentaire de rang 2 non normal dans $N_P(Q)$ et tel que $Q \leq R$.

Exprimons l'image de $\mathcal{E}$ par β' matriciellement. Pour ce faire, on définit un ordre total sur l'ensemble $\mathcal{Q}$, afin d'en déduire un ordre sur $\mathcal{E}$ et sur une base du $\mathbb{Z}$-module d'arrivée.

Ordonnons les éléments x_i, $1 \leq i \leq 9$ de $\mathcal{Q}_1$ selon l'ordre dans lequel nous les avons écrits plus haut et prolongeons cet ordre à $\mathcal{Q}$ en posant :

$$x_{10} = <s, u> \ , \ x_{11} = <s, v> \ , \ x_{12} = <t, u> \ ,$$

$$x_{13} = <t, v> \ , \ x_{14} = <su, tv> \quad \text{et} \quad x_{15} = <sv, tu> \ .$$

On ordonne ainsi les "indices" des éléments de $\mathcal{E}$, ce qui induit un ordre sur $\mathcal{E}$.

D'autre part, notons $dr'_i = dr'_{x_i}$, $N_i = N_P(x_i)$ et $\bar{N}_i = N_i/x_i$, et prenons $\{\Omega_{\bar{N}_i}, \Omega_{N_i/x_{j_i}}\}$ comme $\mathbb{Z}$-base de $T(\bar{N}_i)$, où on choisit le plus petit indice j_i avec $10 \leq j_i \leq 15$ et tel que $x_i < x_{j_i}$, $\forall\, 1 \leq i \leq 9$. Remarquons que le choix des $x_{j_i} \in \mathcal{Q}$ est rendu possible par notre choix de $\mathcal{Q}$. Explicitement, on obtient :

$$x_{10} = x_{j_1} = x_{j_3} = x_{j_5} \ , \quad x_{11} = x_{j_4} = x_{j_6} \ ,$$

$$x_{12} = x_{j_2} = x_{j_7} \ , \quad x_{13} = x_{j_8} \quad \text{et} \quad x_{14} = x_{j_9} \ .$$

On considère la base ordonnée

$$\mathcal{F} = \{\Omega_{\bar{N}_1}, \ldots, \Omega_{\bar{N}_9}, \Omega_{N_1/x_{j_1}}, \ldots, \Omega_{N_9/x_{j_9}}\} \quad \text{de} \quad \prod_{i=1}^{9} T(\bar{N}_i).$$

Ecrivons la matrice B de l'image par β' de l'ensemble $\mathcal{E}$ dans $\mathcal{F}$ et écrivons ces images en ligne. Autrement dit, $B = (B_{e,f})$ est une matrice 15×18 à coefficients entiers, où on définit $B_{e,f}$ comme suit. Soit $1 \leq e \leq 15$.

– Si $1 \leq f \leq 9$, alors $B_{e,f}$ est la composante selon $\Omega_{\bar{N}_f}$ de $dr'_f(\Omega_{P/x_e})$.
– Si $10 \leq f \leq 18$, alors $B_{e,f}$ est la composante selon $\Omega_{N_{f-9}/x_{j_{f-9}}}$ de $dr'_{f-9}(\Omega_{P/x_e})$.

Par le lemme 4.1.8, $\forall\, 1 \leq f \leq 9$ et $\forall\, 1 \leq e \leq 15$, on a (selon la notation introduite après le corollaire 4.1.5)

$$dr'_f(\Omega_{P/x_e}) = \begin{cases} \Omega_{N_f/{}^u x_e}\ , & \text{si } x_f \leq_P x_e \text{ et où } u = u_{x_f,x_e} \\ 0\ , & \text{sinon .} \end{cases}$$

On en déduit immédiatement que $B_{e,f} = \delta_{e,f}$, $\forall\, 1 \leq e, f \leq 9$, et que $B_{e,f} = 0$ si x_e et x_f n'ont pas le même ordre (i.e. si $1 \leq e \leq 9$ et $10 \leq f \leq 18$, ou bien si $10 \leq e \leq 15$ et $1 \leq f \leq 9$).

Calculons les coefficients $B_{e,f}$ avec $10 \leq e \leq 15$ et $10 \leq f \leq 18$. On a $B_{e,f} \neq 0$ si et seulement si $x_{f-9} <_P x_e$. Supposons alors $x_{f-9} <_P x_e$ et déterminons la valeur de $B_{e,f}$. Par le corollaire 4.1.5, on a $x_{f-9} <_P x_e$ si et seulement si $x_e < N_{f-9}$. De plus, $N_{f-9} = x_{f-9} \times D_8$, avec $D_8 = <x_{j_{f-9}}, x'>$, pour un unique sous-groupe $x' \in \mathcal{Q}_2$ et où $x_{j_{f-9}}$ joue le rôle du sous-groupe $<s>$ dans la première assertion du théorème 4.2.12. Ainsi, le théorème 4.2.12 implique les égalités $B_{e,f} = 1$, si $x_e = x_{j_{f-9}}$, et $B_{e,f} = -1$, sinon. En effet, comme on a choisi les $x_{j_{f-9}}$ dans $\mathcal{Q}$ et comme $x_e \in \mathcal{Q}$, on a soit $x_e = x_{j_{f-9}}$, soit x_e et $x_{j_{f-9}}$ ne sont pas conjugués. Dans le premier cas, on a $u_{x_f,x_e} = 1$ et $x_e = x_{j_{f-9}}$. D'où, $\mathrm{Defres}^P_{\bar{N}_{f-9}}\, \Omega_{P/x_e} = \Omega_{N_{f-9}/x_{j_{f-9}}} \in \mathcal{F}$. Dans le second cas, x_e est conjugué au sous-groupe x' de N_{f-9} et on a $\mathrm{Defres}^P_{\bar{N}_{f-9}}\, \Omega_{x_e} = \Omega_{N_{f-9}/x_e} = -\Omega_{N_{f-9}/x_{j_{f-9}}}$.

Remarquons aussi que, pour tout $1 \leq f \leq 9$, on a exactement deux sous-groupes x_e avec $10 \leq e \leq 15$ et tels que $x_e < N_f$. Donc on a exactement deux termes non nuls, valant une fois 1 et une fois -1, dans chacune des colonnes 10 à 18 de B. Il s'ensuit que la matrice B est diagonale par blocs :

$$B = \begin{pmatrix} B_1 & 0 \\ 0 & B_2 \end{pmatrix}\ , \quad \text{avec} \quad B_1 = \mathrm{Id}_9\ , \quad \text{et on obtient, par choix de } \mathcal{F}\ ,$$

$$B_2 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & -1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 & -1 & -1 & 0 & -1 \end{pmatrix}\ .$$

En effectuant des opérations élémentaires sur les lignes et les colonnes de B, on se ramène à la matrice $\begin{pmatrix} \mathrm{Id}_{14} & 0 \\ 0 & 0 \end{pmatrix}$. Il s'ensuit que le rang de β' est exactement 14 et que les diviseurs élémentaires de B valent tous 1. Autrement dit, $\mathrm{Im}(\beta')$ est un facteur direct du $\mathbb{Z}$-module libre $A = \prod_{Q \in \mathcal{Q}_1} E(N_P(Q)/Q) \cong \mathbb{Z}^{18}$ de rang 14. En effet, le fait que les diviseurs élémentaires valent 1 implique qu'il existe une $\mathbb{Z}$-base $\{e_1, \ldots, e_{15}\}$ de $E^\Omega(P)$ et une $\mathbb{Z}$-base $\{f_1, \ldots, f_{18}\}$ de A telles que $\beta'(e_i) = f_i$, $\forall\, 1 \leq i \leq 14$ et $\beta'(e_{15}) = 0$ (voir aussi le théorème des facteurs invariants, cf. théorème 4.14 de [CR]).

Par conséquent, l'inclusion $\mathrm{Im}(\beta') \leq \mathrm{Im}(\beta) < A$ et le fait que le rang de $\mathrm{Im}(\beta)$ est au plus 14 force l'égalité $\mathrm{Im}(\beta') = \mathrm{Im}(\beta)$. D'où la proposition.

□

Comme nous l'avions annoncé, cette proposition entraîne le fait suivant.

Théorème 4.2.14. *On a $E^\Omega(P) = E(P)$, et donc, a fortiori, $D(P) = D^\Omega(P)$.*

Preuve. Par définition, on a l'inclusion $E^\Omega(P) \leq E(P)$ et β' est la restriction de β à $E^\Omega(P)$. Réciproquement, si $x \in E(P)$, alors il existe $y \in E^\Omega(P)$ tel que $\beta(x) = \beta'(y) = \beta(y)$ car, par la proposition, on a $\mathrm{Im}(\beta) = \mathrm{Im}(\beta')$. Il s'ensuit qu'il existe un entier n tel que $x = y + n\Omega_P$, car on a $x - y \in \mathrm{Ker}(\beta) = T(P) = <\Omega_P>$. Comme $\Omega_P \in E^\Omega(P)$, on a $x \in E^\Omega(P)$. D'où l'inclusion réciproque.

Par la proposition 4.1.11, on a $D(P) = E(P) \oplus D(P/Z)$ et, comme P/Z est abélien, on a $D(P/Z) = D^\Omega(P/Z)$. D'où la seconde affirmation. □

Avant d'exhiber une $\mathbb{Z}$-base de $D(P)$, calculons son rang, égal au nombre de classes de conjugaison des sous-groupes non cycliques de P (cf. théorème 1.5.5). Déterminons "à la main" tous les sous-groupes de P (à conjugaison près). On obtient :

- 1 sous-groupe d'ordre 32, à savoir P ;
- 15 sous-groupes d'ordre 16 :
  - les centralisateurs des 9 sous-groupes de $\mathcal{Q}_1$, isomorphes à $C_2 \times D_8$;
  - les centralisateurs des $15 - 9 = 6$ sous-groupes cycliques d'ordre 4, isomorphes à $C_4 * Q_8$;
- 35 sous-groupes d'ordre 8, à savoir 18 diédraux, 2 quaternions, 9 isomorphes à $C_4 \times C_2$ et 6 abéliens élémentaires de rang 3 ;
- 21 sous-groupes d'ordre 4, à savoir 6 cycliques et 15 abéliens élémentaires de rang 2 dont 9 contenant Z ;
- 10 sous-groupes d'ordre 2, à savoir les 9 de $\mathcal{Q}_1$ et le centre ;
- 1 sous-groupe d'ordre 1.

Ainsi, P possède $1+15+35+15 = 66$ classes de conjugaisons de sous-groupes non cycliques, dont 51 contiennent Z. On en déduit la conséquence suivante.

Théorème 4.2.15. *Le rang de $D(P)$ vaut 66, celui de $D(P/Z)$ vaut 51 et celui de $E(P)$ vaut 15.*

Nous allons maintenant montrer le troisième point de notre plan, à savoir, déterminer l'unique relation non triviale (à multiple entier près) liant les éléments de $\mathcal{E}'$, afin de pouvoir extraire de l'ensemble $\mathcal{E}'$ une $\mathbb{Z}$-base de $E(P)$. On pourra alors aussi exhiber une $\mathbb{Z}$-base de $D(P)$, et clore ainsi le cas $n = 2$. En effet, on sait déjà que l'ensemble

$$\left\{\Omega_{P/Q} \mid Z \leq Q < P \quad \text{et} \quad |P : Q| \geq 4\right\}$$

est une $\mathbb{Z}$-base de $D(P/Z)$ (cf. théorème 2.0.13).

Remarquons que la somme des lignes de la matrice B_2 qui apparaît dans la preuve de la proposition 4.2.13 vaut 0. Autrement dit,

$$\sum_{R \in \mathcal{Q}_2} \Omega_{P/R} \in \mathrm{Ker}(\beta) = T(P) \quad \text{et donc} \quad \exists\, a \in \mathbb{Z} \quad \text{avec} \sum_{R \in \mathcal{Q}_2} \Omega_{P/R} = a \cdot \Omega_P \ .$$

Proposition 4.2.16. *On a* $\sum_{R\in\mathcal{Q}_2}\Omega_{P/R}=2\cdot\Omega_P$.

Preuve. Comme $T(P)=<\Omega_P>\cong\mathbb{Z}$, l'assertion 2 du théorème 1.5.5 implique que la restriction $\mathrm{Res}^P_S : T(P)\longrightarrow T(S)$, où S est un sous-groupe abélien élémentaire de P de rang 2, est un isomorphisme. Supposons $S\in\mathcal{Q}_2$ et calculons $\mathrm{Res}^P_S\,\Omega_{P/R}$, pour un $R\in\mathcal{Q}_2$, à l'aide du lemme 1.5.9 et de la formule de Mackey :

$$\mathrm{Res}^P_S\,\Omega_{P/R}=\Omega_X,\ \text{avec } X=\mathrm{Res}^P_S(P/R)=\{*\}\uparrow^P_R\downarrow^P_S\cong$$

$$\cong\coprod_{g\in[S\backslash P/R]}\{*\}\downarrow^{{}^gR}_{{}^gR\cap S}\uparrow^S_{{}^gR\cap S}=\coprod_{g\in[S\backslash P/R]}S/{}^gR\cap S\ .$$

Distinguons les différents cas possibles pour les six sous-groupes de $\mathcal{Q}_2$.

1. Si $S=R$, alors on a $X=\{*\}\coprod Y$, car on peut choisir $[R\backslash P/R]$ avec $1\in[R\backslash P/R]$. Par conséquent, $\Omega_X=0$, par la proposition 1.2.9.
2. Si $|S\cap{}^gR|=1,\ \forall\, g\in P$, alors $X\cong\coprod_{|[S\backslash P/R]|}S$ et donc, $\Omega_X=\Omega_S$, par le lemme 1.5.7.
3. Sinon, il existe un unique $1<Q<S$, à conjugaison près, tel que Q est contenu dans un conjugué de R. En effet, si $Q'\neq_P Q$ satisfait les mêmes conditions, alors on a nécessairement $S=QQ'$. De plus, par le corollaire 4.1.5 et la description des sous-groupes de P, on a

   $$R<\big(C_P(Q)\cap C_P(Q')\big)=S\times Z\ .$$

   En effet, on a $C_P(Q)\cap C_P(Q')=C_P(QQ')=C_P(S)=S\times Z$. Mais alors, $R<(S\times Z)$ avec $R,\ S\in\mathcal{Q}_2$ et donc $R=S$, ce qui contredit notre hypothèse.

   Ainsi, $X=(\underbrace{\coprod\coprod S}_{A})\coprod(\underbrace{\coprod\coprod S/Q}_{B})$ et donc, par le lemme 1.5.8,

   $$\Omega_X=\Omega_A+\Omega_B-\Omega_{A\times B}=\Omega_S+\Omega_{S/Q}-\Omega_{S\times S/Q}=0.$$

   En effet, S/Q est d'ordre 2 et donc $\Omega_{S/Q}=0$. De la formule de Mackey et de la réciprocité de Frobenius (cf. proposition 2.2.1 de [Bo2]), on tire

   $$S\times S/Q\cong\big(\{*\}\uparrow^S_1\times\{*\}\uparrow^S_Q\big)\cong\big(\{*\}\times\{*\}\uparrow^S_Q\downarrow^S_1\big)\uparrow^S_1\cong\coprod_{|S:Q|}S.$$

   Par suite, $\Omega_{S\times S/Q}=\Omega_{S\coprod S}=\Omega_S$, par le lemme 1.5.7.

Résumons-nous. Pour un $S\in\mathcal{Q}_2$ fixé, on veut calculer $\mathrm{Res}^P_S(\sum_{R\in\mathcal{Q}_2}\Omega_{P/R})$. Vu les trois cas ci-dessus, on obtient :

$$\mathrm{Res}^P_S\Big(\sum_{R\in\mathcal{Q}_2}\Omega_{P/R}\Big)=\sum_{R\in\mathcal{Q}_2}\mathrm{Res}^P_S(\Omega_{P/R})=\sum_{\substack{R\in\mathcal{Q}_2\\ |S\cap{}^gR|=1,\,\forall\, g\in P}}\Omega_S\ =\ 2\cdot\Omega_S\ .$$

En effet, on a $|\mathcal{Q}_2| = 6$ et chaque $S \in \mathcal{Q}_2$ contient trois sous-groupes d'ordre 2. Autrement dit, il existe trois sous-groupes R dans $\mathcal{Q}_2$ pour lesquels il existe un g dans P tel que $|S \cap {}^gR| = 2$. Ainsi, il reste deux sous-groupes T de $\mathcal{Q}_2$ pour lesquels $|S \cap {}^gT| = 1$, $\forall\, g \in P$.

On en déduit que $\mathrm{Res}^P_S(\sum_{R\in\mathcal{Q}_2} \Omega_{P/R}) = 2 \cdot \Omega_S = \mathrm{Res}^P_S(2 \cdot \Omega_P)$ et donc, par injectivité de Res^P_S, on a $\sum_{R\in\mathcal{Q}_2} \Omega_{P/R} = 2 \cdot \Omega_P$.

□

Remarquons que si dans cette preuve on avait considéré S avec $Z < S$, alors on aurait obtenu le même résultat (bien entendu), mais les calculs auraient été différents. En effet, si $Z < S$, alors $S \triangleleft P$ et donc on a, pour $R \in \mathcal{Q}_2$,

- Soit ${}^gR \cap S = 1$, $\forall\, g \in P$. D'où $\mathrm{Res}^P_S(\Omega_{P/R}) = \Omega_S$.
- Soit $|{}^gR \cap S| = 2$, $\forall\, g \in P$ et il existe un unique $Q \in \mathcal{Q}_1$ satisfaisant les conditions $S = <Q, Z>$ et $Q \leq_P R$. On obtient alors $\mathrm{Res}^P_S(\Omega_{P/R}) = -\Omega_S$, en utilisant les mêmes arguments que dans la preuve.
  Or, pour un $Q \in \mathcal{Q}_1$ fixé parmi les neuf de $\mathcal{Q}_1$ (i.e. pour un S fixé), il y a exactement deux des six sous-groupes $R \in \mathcal{Q}_2$ avec $Q \leq_P R$. En effet, un tel R contient trois sous-groupes d'ordre 2 et donc on conclut par un banal argument de comptage, que l'on peut schématiser comme suit.

$$\begin{array}{c} 6 \cdot R \\ 3 \downarrow \uparrow 2 \\ Q \cdot 9 \end{array} \iff 3 \cdot 6 = 2 \cdot 9 \ .$$

Ainsi, on obtient $\mathrm{Res}^P_S(\sum_{R\in\mathcal{Q}_2} \Omega_{P/R}) = (4-2)\cdot\Omega_S = 2\cdot\Omega_S$, comme souhaité.

Introduisons quelques notations.

Définition 4.2.17. *Soient $n \geq 2$ et $E \in \mathcal{Q}_2(P_n)$.*

1. *On pose $\mathcal{Q}'(P_n) = \mathcal{Q}(P_n) \cup \mathcal{Q}_0$, où $\mathcal{Q}_0 = \{1\}$ et 1 désigne le groupe trivial.*
2. *On pose $I_{E,i}(P_n) = \{R \in \mathcal{Q}_{n-i}(P_n) \mid {}^gR \cap E = 1 \ , \ \forall\, g \in P_n\}$.*
3. *On pose $c_0 = 1$, $c_1 = 0$ et on définit récursivement*

$$c_n = -\sum_{i=0}^{n-1} c_i \cdot |I_{E,i}(P_n)| \ .$$

4. *On pose*

$$\omega_n = \sum_{i=0}^{n} c_i \cdot \Big(\sum_{R\in\mathcal{Q}_{n-i}(P_n)} \Omega_{P_n/R} \Big) \ .$$

Remarquons que la valeur des c_n est indépendante du choix de $E \in \mathcal{Q}_2(P_n)$. De plus, de la preuve de la proposition 4.2.16, on tire $c_2 = -2$. En effet, pour un $E \in \mathcal{Q}_2(P_2)$ fixé, on a vu qu'il existe exactement deux sous-groupes R dans $\mathcal{Q}_2(P_2)$ avec ${}^gR \cap E = \{1\}$, $\forall\, g \in P_2$, et donc $c_2 = -\, c_0 \cdot |I_{E,0}(P_2)| = -2$.

Utilisons ces notations pour montrer la proposition suivante.

Proposition 4.2.18. *Soit $n \geq 2$ et posons $P = P_n$. Alors, on a $\omega_n = 0$.*

De plus, si $\sum_{R \in \mathcal{Q}'(P)} a_R \cdot \Omega_{P/R} = 0$ pour des entiers a_R non tous nuls, alors il existe un entier non nul b tel que $a_R = b \cdot c_i$, $\forall\, R \in \mathcal{Q}_{n-i}(P)$ et $\forall\, 0 \leq i \leq n$.

Preuve. Prouvons la proposition par récurrence sur n. Si $n = 2$, alors, par la proposition 4.2.13, on sait que $E^{\Omega}(P)$ est un $\mathbb{Z}$-module libre de rang 14, engendré par l'ensemble $\mathcal{E}$, de cardinal 15. C'est-à-dire qu'il y a exactement une combinaison $\mathbb{Z}$-linéaire nulle non triviale liant les éléments de $\mathcal{E}'$ (à multiple entier près). Par ailleurs, la proposition 4.2.16 nous donne cette relation :

$$\sum_{R \in \mathcal{Q}_2(P)} \Omega_{P/R} = 2 \cdot \Omega_P \text{ , i.e., par définition des } c_i \text{ , } \omega_2 \stackrel{\text{déf}}{=} \sum_{R \in \mathcal{Q}_2(P)} \Omega_{P/R} - 2 \cdot \Omega_P = 0 \,.$$

Supposons $n > 2$ et les deux assertions de la proposition vérifiées pour tout groupe P_m avec $2 \leq m < n$. Soit $Q \in \mathcal{Q}_1(P)$ et posons $P_{n-1} = N_P(Q)/Q$. Considérons la bijection entre les sous-groupes R de $\mathcal{Q}_j(P)$ contenant un conjugué de Q et les sous-groupes $\bar{R}$ de $\mathcal{Q}_{j-1}(P_{n-1})$, $\forall\, 1 \leq j \leq n$, donnée comme suit. Si $R \in \mathcal{Q}_j(P)$ contient un conjugué de Q, alors, par le corollaire 4.1.5 et par la remarque 4.1.6, l'ensemble $\{u \in P \mid Q \leq {}^{u}R\}$ coïncide avec exactement une classe $uN_P(Q) \in P/N_P(Q)$. Par suite, on a une bijection entre les classes de conjugaison dans P des sous-groupes de P contenant un conjugué de Q et les classes de conjugaison dans $N_P(Q)$ des sous-groupes contenant Q. De plus, comme on peut choisir $[P/N_P(Q)]$ arbitrairement, on prend $[P/N_P(Q)]$ tel que l'unique élément $u_{Q,R} \in [P/N_P(Q)]$ vérifiant l'inclusion $Q \leq {}^{u_{Q,R}}R$ satisfasse $({}^{u_{Q,R}}R)/Q \in \mathcal{Q}_{j-1}(P_{n-1})$. On considère alors la bijection $R \mapsto {}^{u_{Q,R}}R \mapsto \bar{R}$, où on a posé $\bar{R} = ({}^{u_{Q,R}}R)/Q$, pour alléger les notations.

Comme $dr'_Q(\Omega_P) = \mathrm{Defres}^P_{P_{n-1}}(\Omega_P) = 0$, on a

$$dr'_Q(\omega_n) = \sum_{i=0}^{n-1} c_i \cdot \Big(\sum_{R \in \mathcal{Q}_{n-i}(P)} dr'_Q\,(\Omega_{P/R}) \Big) =$$

$$= \sum_{i=0}^{n-1} c_i \cdot \Big(\sum_{\bar{R} \in \mathcal{Q}_{n-1-i}(P_{n-1})} \Omega_{P_{n-1}/\bar{R}} \Big) \stackrel{\text{déf}}{=} \omega_{n-1} \;=\; 0 \;,$$

par le lemme 4.1.8 et par hypothèse de récurrence.

Par conséquent, on a $\omega_n \in \mathrm{Ker}(\beta) = T(P) = <\Omega_P>$. Comme dans le cas où $n = 2$, on utilise l'isomorphisme $\mathrm{Res}^P_S : T(P) \longrightarrow T(S)$, où S est un sous-groupe abélien élémentaire de P de rang 2, pour montrer que $\omega_n = 0$. Choisissons $S \in \mathcal{Q}_2$, et calculons

$$\mathrm{Res}^P_S(\omega_n) \;= \sum_{i=0}^{n} c_i \cdot \Big(\sum_{R \in \mathcal{Q}_{n-i}(P)} \mathrm{Res}^P_S\, \Omega_{P/R} \Big) \,.$$

Par le lemme 1.5.7 et la formule de Mackey, on a $\mathrm{Res}^P_S\, \Omega_{P/R} = \Omega_X$, où

$$X = \; \{*\} \uparrow^P_R \downarrow^P_S = \coprod_{g \in [S \backslash P / R]} S \big/ ({}^{g}R \cap S) \,.$$

On a trois possibilités : soit $S \leq_P R$, soit $|{}^gR \cap S| \leq 2,\ \forall\, g \in P$, avec égalité pour certains $g \in P$, soit ${}^gR \cap S = 1,\ \forall\, g \in P$. Donc, les arguments de la preuve de la proposition 4.2.16, nous donnent :

$$\mathrm{Res}_S^P\, \Omega_{P/R} = \begin{cases} \Omega_S & , \quad \text{si } R = P, \text{ ou si } {}^gR \cap S = 1,\ \forall\, g \in P \\ 0 & , \quad \text{sinon .} \end{cases}$$

Finalement,

$$\mathrm{Res}_S^P(\omega_n) = \sum_{i=0}^{n} c_i \cdot \big(\sum_{R \in \mathcal{Q}_{n-i}(P)} \mathrm{Res}_S^P\, \Omega_{P/R} \big) = c_n \Omega_S + \sum_{i=0}^{n-1} \big(c_i \cdot |I_{S,i}(P)| \big) \Omega_S = 0\ ,$$

par définition des c_i. Ainsi, par injectivité de Res_S^P , on a $\omega_n = 0\ ,\ \forall\, n \geq 2$.

Montrons la seconde assertion de la proposition dans le cas où $n > 2$. Supposons qu'il existe des entiers a_R, non tous nuls, tels que $\sum_{R \in \mathcal{Q}'(P)} a_R \cdot \Omega_{P/R} = 0$. Alors, il existe $Q \in \mathcal{Q}_1(P)$, tel que $\{a_R \mid Q \leq_P R\} \neq \{0\}$ et on a, a fortiori,

$$0 = dr'_Q\big(\sum_{R \in \mathcal{Q}'(P)} a_R \cdot \Omega_{P/R} \big) = \sum_{\bar{R} \in \mathcal{Q}'(P_{n-1})} a_R \cdot \Omega_{P_{n-1}/\bar{R}}\ ,$$

selon les mêmes notations que ci-dessus, et avec $\mathcal{Q}'(P_{n-1}) = \mathcal{Q}(P_{n-1}) \cup \mathcal{Q}_0$. Ainsi, par hypothèse de récurrence, il existe un entier non nul b_Q tel que

$$a_R = b_Q \cdot c_i\ ,\ \forall\, R \in \mathcal{Q}_{n-i}(P) \ \text{ tel que } Q \leq_P R \ \text{ et } \forall\, 0 \leq i \leq n-1\ .$$

Or, b_Q ne dépend pas de Q. En effet, soit $Q' \in \mathcal{Q}_1(P)$ avec $Q' \neq Q$ et $Q' \leq_P R$. Alors $a_R = b_Q c_i = b_{Q'} c_i$ et donc on peut poser $b = b_Q$. Ainsi, on peut écrire :

$$0 = \sum_{R \in \mathcal{Q}'(P)} a_R \cdot \Omega_{P/R} = a_1 \cdot \Omega_P + b \cdot \Big(\sum_{i=0}^{n-1} c_i \cdot \big(\sum_{R \in \mathcal{Q}_{n-i}(P)} \Omega_{P/R} \big) \Big)\ .$$

$$\text{Or,} \quad \sum_{i=0}^{n-1} c_i \cdot \big(\sum_{R \in \mathcal{Q}_{n-i}(P)} \Omega_{P/R} \big) \ = \ \omega_n - (c_n \cdot \Omega_P) \ = \ -c_n \cdot \Omega_P\ ,$$

par définition de ω_n et car $\omega_n = 0$. Par conséquent,

$$0 = \sum_{R \in \mathcal{Q}'(P)} a_R \cdot \Omega_{P/R} = a_1 \cdot \Omega_P + b \cdot \big(-c_n \cdot \Omega_P \big) = (a_1 - b \cdot c_n) \cdot \Omega_P\ .$$

En particulier, cette égalité est vérifiée dans $T(P)$ et $T(P) = <\Omega_P> \cong \mathbb{Z}$. Par suite, $a_1 = b \cdot c_n$, ce qui termine la démonstration. □

Remarque 4.2.19. *S. Bouc a démontré que pour tout sous-groupe Q d'un p-groupe fini P, on a l'égalité*

$$\sum_{\substack{U,V \in [s_P] \\ U \leq_P V}} \mu_P(U,V) |V \backslash P / Q|\ \Omega_{P/U} = 0 \quad \textit{(cf. [Bo1] 6.1.1 et lemme 1.5.10).}$$

Ecrivant cette relation successivement pour $Q = 1$ et pour $Q = Z$, et faisant la différence, les termes correspondant à $V \supseteq Z$ s'annulent, et il vient

$$\sum_{\substack{U,V \in \mathcal{Q} \\ U \leq_P V}} \mu_P(U,V) \frac{1}{2}|P/V| \ \Omega_{P/U} = 0 \ .$$

Comme $D(P)$ est sans torsion (cf. corollaire 4.2.4), on peut diviser cette expression par $\frac{1}{2}|P : Q|$, où Q est un élément maximal de $\mathcal{Q}$. On obtient alors la même relation ω_n que dans la proposition ci-dessus. En effet, dans les deux expressions, $\Omega_{P/R}$ a comme coefficient 1, pour tout sous-groupe R maximal dans $\mathcal{Q}$ et donc, par unicité de la relation ω_n (à multiple entier près), ces deux expressions coïncident.

De plus, pour tous $U, V \in \mathcal{Q}$, on a $\mu_P(U,V) = \mu(U,V)$ et donc on peut "facilement" expliciter les coefficients apparaissant dans la relation.

Nous avons ainsi prouvé le quatrième point de notre plan. Remarquons la conséquence suivante de la proposition 4.2.18.

Corollaire 4.2.20. *$E^\Omega(P)$ est un $\mathbb{Z}$-sous-module libre de rang q de $E(P)$. A fortiori, le $\mathbb{Z}$-sous-module libre $\mathrm{Im}(\beta')$ du $\mathbb{Z}$-module libre $\mathrm{Im}(\beta)$ est de rang égal à $(q-1)$.*

Preuve. Par la proposition 4.2.18, l'ensemble $\mathcal{E}'$, de cardinal $(q+1)$, engendre un $\mathbb{Z}$-module libre de rang q. Or, $\mathcal{E}'$ engendre $E^\Omega(P)$, par définition de $E^\Omega(P)$. Ainsi, $E^\Omega(P)$ est un $\mathbb{Z}$-sous-module libre de rang q de $E(P)$. De plus, comme $\mathrm{Ker}(\beta) = \mathrm{Ker}(\beta') = T(P)$ est un $\mathbb{Z}$-module libre de rang 1 (cf. proposition 4.2.9), on a des isomorphismes de $\mathbb{Z}$-modules libres de rang q fini :

$$E^\Omega(P) \cong T(P) \oplus \mathrm{Im}(\beta') \quad \text{et} \quad E(P) \cong T(P) \oplus \mathrm{Im}(\beta) \ .$$

Par suite, $\mathrm{Im}(\beta') \overset{\text{déf}}{=} \beta(E^\Omega(P))$ est un $\mathbb{Z}$-sous-module libre de $\mathrm{Im}(\beta)$ de même rang $(q-1)$. D'où le corollaire.

□

Maintenant, comme annoncé, on va montrer le cinquième et dernier point de notre plan, à savoir que $\mathrm{Im}(\beta)$ est un facteur direct de $\prod_{Q \in \mathcal{Q}_1} E(N_P(Q)/Q)$ de rang $(q-1)$. Ceci impliquera $D^\Omega(P) = D(P)$.

Comme dans le cas où $n = 2$, on va prolonger l'ordre $\leq_P$ ($<_P$ pour l'inclusion stricte) en un ordre total $\preceq$ (resp. $\prec$) sur l'ensemble $\mathcal{Q}(P)$.

Soyons méthodique et définissons cet ordre pas à pas, comme suit. Pour simplifier les notations, posons $t = q_{n,1}$ et $\mathcal{Q} = \mathcal{Q}(P)$, jusqu'à la fin du chapitre.

1. Choisissons un ordre arbitraire $R_1 \prec R_2 \prec \ldots \prec R_t$ sur $\mathcal{Q}_1$.
2. $\forall\, 1 \leq i \leq t$ et $\forall\, 1 \leq j \leq n$, on définit les ensembles

$$A_{R_i} = \{R \in \mathcal{Q} \mid R_i \leq_P R\} \quad \text{et} \quad A_{i,j} = A_{R_i} \cap \mathcal{Q}_j \ .$$

3. Soit $j = 2$ et choisissons un ordre $R_{t+1} \prec \ldots \prec R_{t+q_{n,2}}$ sur les sous-groupes de $\mathcal{Q}_2$ satisfaisant la condition suivante :
   Soient $R_i, R_j \in \mathcal{Q}_2$ et d, e les plus petits entiers entre 1 et t tels que $R_d <_P R_i$ et $R_e <_P R_j$. Si $R_d \prec R_e$, alors $R_i \prec R_j$.
   En d'autres termes, les plus petits sous-groupes abéliens élémentaires de rang 2 de $\mathcal{Q}$ sont tous les sous-groupes de $\mathcal{Q}_2$ qui contiennent R_1, ordonnés arbitrairement. Ensuite, on considère les sous-groupes de $\mathcal{Q}_2$ qui contiennent R_2, mais pas R_1, et ainsi de suite : on complète pas à pas la liste ordonnée des sous-groupes de $\mathcal{Q}$ en rajoutant les sous-groupes de $\mathcal{Q}_2$ qui contiennent R_i, mais aucun des R_j , $\forall\, 2 \leq j < i \leq t$.
4. On continue ainsi. Soit $3 \leq j \leq n$ et notons $a_j = \sum_{l=1}^{j-1} q_{n,l}$. On choisit un ordre $R_{a_j+1} \prec \ldots \prec R_{a_j+q_{n,j}}$ sur les sous-groupes de $\mathcal{Q}_j$ satisfaisant la condition suivante :
   Soient $R_i, R_j \in \mathcal{Q}_j$ et d, e les plus petits entiers entre 1 et t tels que $R_d <_P R_i$ et $R_e <_P R_j$. Si $R_d \prec R_e$, alors $R_i \prec R_j$.
   Autrement dit, on procède exactement comme dans le cas où $j = 2$, en complétant la liste ordonnée des sous-groupes de $\mathcal{Q}$, en rajoutant pas à pas les sous-groupes abéliens élémentaires de rang j de $\mathcal{Q}_j$ qui contiennent R_1, puis ceux qui contiennent R_i, mais aucun des R_l , $\forall\, 1 \leq l < i \leq t$.

Finalement, on a un ordre total $R_1 \prec \cdots \prec R_q$ sur $\mathcal{Q}$ qui prolonge l'ordre partiel $\leq_P$ induit par l'inclusion des sous-groupes à conjugaison près.

De plus, en posant

$$\Omega_{P/R_i} < \Omega_{P/R_j} \quad \text{si} \quad R_i \prec R_j \ ,$$

l'ensemble $\mathcal{E}$ est totalement ordonné.

On peut à présent démontrer le résultat principal de ce chapitre.

Théorème 4.2.21. *Soient $n \geq 2$ et $R \in \mathcal{Q}_n$. Alors*

$$E(P) = E^{\Omega}(P) \quad \textit{et l'ensemble } \mathcal{E}_n = \mathcal{E}' \setminus \{\Omega_{P/R}\} \textit{ est une } \mathbb{Z}\textit{-base de } E(P) \ .$$

A fortiori, on a $D(P) = D^{\Omega}(P)$ et l'ensemble

$$\mathcal{E}_n \cup \{\Omega_{P/S} \mid Z \leq S \leq P \ : \ |P : S| \geq 4\} \quad \textit{est une } \mathbb{Z}\textit{-base de } D(P) \ .$$

Preuve. Prouvons le résultat par récurrence sur n. Si $n = 2$, alors l'égalité $E(P) = E^{\Omega}(P)$ est vérifiée par la proposition 4.2.13. Soit $x \in \mathcal{Q}_2$ et considérons les mêmes notations que dans la proposition 4.2.18. On a

$$\Omega_{P/x} = 2 \cdot \Omega_P - \sum_{\substack{i=10 \\ x_i \neq x}}^{15} \Omega_{P/x_i}$$

et donc l'ensemble $\mathcal{E}_n = \mathcal{E}' \setminus \{\Omega_{P/x}\}$ (de cardinal 15) est une $\mathbb{Z}$-base de $E(P)$. Remarquons, de plus, que l'ordre $x_1 \prec \cdots \prec x_{15}$ satisfait la définition de $\prec$ donnée ci-dessus.

Soit $n > 2$ et supposons que les affirmations du théorème soient vraies pour les groupes P_m , $\forall\, 2 \leq m < n$. Pour exprimer l'image de β', considérons la base ordonnée $\mathcal{E}$ de $E^{\Omega}(P)$ et choisissons judicieusement une base $\mathcal{F}$ de $\prod_{i=1}^{t} E(N_i)$, où N_i désigne le quotient $N_P(R_i)/R_i$, $\forall\, 1 \leq i \leq t$. On sait que N_i est isomorphe au groupe P_{n-1} et on peut considérer la bijection $R \mapsto \overline{R}$ entre les sous-groupes de $A_{i,j}$ et ceux de $\mathcal{Q}_{j-1}(N_i)$, $\forall\, 1 \leq j \leq n$ et $\forall\, 1 \leq i \leq t$, comme dans la preuve de la proposition 4.2.18. Par suite, $\forall\, 1 \leq j \leq n$ et $\forall\, 1 \leq i \leq t$, on a

$$|A_{R_i}| = |\mathcal{Q}(N_i)| = q_{n-1} \quad \text{et} \quad |A_{i,j}| = |\mathcal{Q}_{j-1}(N_i)| = q_{n-1,j-1} \ .$$

Notons $\prec$ l'ordre total sur A_{R_i} induit par l'ordre total $\prec$ défini sur $\mathcal{Q}$ et appelons $R_{i,l}$ les sous-groupes de A_{R_i}, où l'indice l parcourt les entiers entre 1 et q_{n-1}, et tel que l'on ait $R_{i,l} \prec R_{i,l'}$ si $l < l'$.

Par hypothèse de récurrence, on peut choisir arbitrairement un sous-groupe $\overline{R}_{i,m} \in \mathcal{Q}_{n-1}(N_i)$, tel que l'ensemble $\mathcal{F}_i = \{\Omega_{N_i/\overline{R}_{i,l}} \mid l \neq m\}$ soit une base de $E(N_i)$, $\forall\, 1 \leq i \leq t$. Autrement dit, on choisit un sous-groupe $R_{i,m}$ dans $A_{i,n}$, $\forall\, 1 \leq i \leq t$. Prenons $m = q_{n-1} - q_{n-1,n-1} + 1$, afin que $R_{i,m}$ soit l'élément minimal $\min(A_{i,n})$ de l'ensemble $A_{i,n}$, $\forall\, 1 \leq i \leq t$. Ainsi,

$$\mathcal{F} = \coprod_{i=1}^{t} \mathcal{F}_i \quad \text{est une } \mathbb{Z}\text{-base de } \prod_{i=1}^{t} E(N_i) \ , \quad \text{par hypothèse de récurrence.}$$

Posons $r = (q - q_{n,n} + 1)$. On a $R_r = \min(\mathcal{Q}_n)$ et, par définition de l'ordre sur $\mathcal{Q}_n$, cela force $R_r \in A_{1,n}$ (i.e. $R_r \in A_{R_1}$) car, $\forall\, 1 \leq i \leq t$, l'ensemble $A_{i,n}$ n'est pas vide. De plus, comme l'ordre sur les ensembles A_{R_i} est induit par l'ordre sur $\mathcal{Q}$, on a nécessairement $R_r = R_{i,m}$, pour tout $1 \leq i \leq t$ avec $R_r \in A_{R_i}$. Montrons que R_r est le seul sous-groupe de $\mathcal{Q}$ avec cette propriété.

Soit $1 \leq s \leq q$ tel que $R_s = R_{i,m}$, $\forall\, 1 \leq i \leq t$ tel que $R_s \in A_{R_i}$. Par choix des sous-groupes $R_{i,m}$, on a $R_s \in \mathcal{Q}_n$, ce qui implique $r \leq s \leq q$ car $R_r = \min(\mathcal{Q}_n)$. Supposons, par l'absurde, $r < s$. Soit e le plus petit entier tel que $1 \leq e \leq t$ et tel que $R_e <_P R_s$. Autrement dit, e est tel que $\forall\, 1 \leq d < e$ et $\forall\, R \in \mathcal{Q}_n$ avec $R_d <_P R$, alors $R \prec R_s$, par définition de l'ordre $\prec$. On a $1 < e$, sinon $R_s \in A_{R_1}$ et donc $R_s = R_{1,m} = R_r$, ce qui est impossible car $R_s \neq R_r$, par hypothèse. Considérons le sous-groupe $C_P(R_1) \cap R_s$ de P. Par le même résultat de [Su] que l'on a utilisé dans la preuve du corollaire 4.1.5, on a $C_P(R_1) = R_1 \times P_{n-1}$. En particulier, on en tire que $|C_P(R_1)| = 2^{2n}$ et donc $|C_P(R_1) \cap R_s| = 2^{n-1} > 1$ (car $R_1 \not<_P R_s$ implique $R_s \not< C_P(R_1)$). Par suite, il existe un entier $1 \leq d \leq t$ tel que $R_d <_P R_s$ et tel que $R_d < C_P(R_1)$. Ainsi, on a $R_s \in A_{R_d}$ et $R_d R_1$ est un sous-groupe abélien élémentaire de rang 2 de P et donc il est conjugué à un élément de $\mathcal{Q}_2$, car $R_d R_1$ ne contient pas Z. Par un argument de récurrence sur n, l'égalité $C_P(R_1) = R_1 \times P_{n-1}$ implique que chaque sous-groupe de $\mathcal{Q}$ est contenu dans un conjugué d'un sous-groupe de $\mathcal{Q}_n$ et donc il existe $R \in \mathcal{Q}_n$ tel que $R_d R_1 <_P R$. En particulier, on en tire que $R \prec R_s$, car $1 < e$ et $R_1 <_P R$. D'autre part, $R_d <_P R$ implique que $R_s \preceq R$, car comme $R_s \in A_{R_d}$, on a $R_s = R_{d,m}$, par hypothèse sur R_s. On aboutit ainsi à une contradiction, ce qui prouve qu'un tel sous-groupe $R_s \in \mathcal{Q}$

avec $r < s$ ne peut exister. En résumé, on a montré l'affirmation souhaitée :

$$R = R_{i,m} \text{ pour tout } 1 \leq i \leq t \text{ tel que } R \in A_{R_i} \iff R = R_r. \tag{4.2}$$

Autrement dit, $R = \min(A_{i,n})$, $\forall\, 1 \leq i \leq t$ tel que $R \in A_{R_i} \iff R = \min(\mathcal{Q}_n)$.

Concentrons-nous à présent sur la matrice $B = (B_{e,f})$ de l'application β' exprimée selon les bases $\mathcal{E}$ et $\mathcal{F}$. On définit $B_{e,f}$ comme suit. Soient $1 \leq e \leq q$ et $\Omega_{N_i/\overline{R}_{i,l}}$ le f-ième élément de $\mathcal{F}$. Alors $B_{e,f}$ est la composante de $dr'_i(\Omega_{P/R_e})$ selon $\Omega_{N_i/\overline{R}_{i,l}}$, où, rappelons-le,

$$dr'_i = \mathrm{Defres}^P_{N_i} \ : E^\Omega(P) \longrightarrow \ E(N_i) \ , \ \forall\, 1 \leq i \leq t \ .$$

En d'autres termes, les images des éléments de $\mathcal{E}$ par β' sont exprimées dans $\mathcal{F}$ et rangées dans les lignes de B, qui est ainsi de taille $q \times |\mathcal{F}|$. Par ailleurs, on peut identifier les indices des lignes de B avec les sous-groupes de $\mathcal{Q}$ dans le sens suivant. La e-ième ligne de B est l'image de Ω_{P/R_e} et donc la e-ième ligne de B correspond au sous-groupe $R_e \in \mathcal{Q}$. De même, les indices des colonnes de B correspondent aux éléments $\Omega_{N_i/\overline{R}_{i,l}} \in \mathcal{F}$, que l'on identifie aux paires $(R_i, R_{i,l})$ avec $R_{i,l} \in A_{R_i}$ et $1 \leq i \leq t$. Par la suite, moyennant ces correspondances, on utilisera des sous-groupes, respectivement des paires de sous-groupes, comme indices des lignes, respectivement des colonnes de B, lorsque cela conviendra mieux pour nos propos. Introduisons les notations suivantes, pour toute matrice M ayant la même taille que B :

- Si $R \in \mathcal{Q}$, disons $R = R_s$, pour un $1 \leq s \leq q$, on note $M[R]$ la s-ième ligne de M.
- Si $1 \leq f \leq |\mathcal{F}|$, on note $M(f)$ la f-ième colonne de M.

Le choix de la bijection $R \mapsto \overline{R}$ que nous avons fait (cf. proposition 4.2.18) implique que si $R \in A_{R_i}$, alors on a $\overline{R} \in \mathcal{Q}(N_i)$, $\forall\, 1 \leq i \leq t$. Ainsi, par le lemme 4.1.8, on a, $\forall\, 1 \leq i \leq t$ et $\forall\, 1 \leq e \leq q$,

$$dr'_i(\Omega_{P/R_e}) = \begin{cases} \Omega_{N_i/\overline{R}_e} \ , & \text{si } R_e \in A_{R_i} \\ 0 \ , & \text{sinon .} \end{cases}$$

Pour déterminer les coefficients $B_{e,f}$ correspondant à cette image, on doit écrire $dr'_i(\Omega_{P/R_e})$ dans la base $\mathcal{F}$, i.e. dans $\mathcal{F}_i$. Pour ce faire, on utilise la relation liant les éléments de $\mathcal{E}'(N_i)$ (cf. définition 4.2.17 et proposition 4.2.18) :

$$0 \ = \ \sum_{j=0}^{n-1} c_j \cdot \Bigg(\sum_{\overline{R} \in \mathcal{Q}_{n-1-j}(N_i)} \Omega_{N_i/\overline{R}} \Bigg) \ , \quad \text{où les } c_j \text{ sont des entiers.}$$

En particulier, $c_0 = 1$ et $\overline{R} \in \mathcal{Q}_{n-1-j}(N_i) \iff R \in A_{i,n-j}$. Donc pour $R_{i,m}$ on peut écrire

$$\Omega_{N_i/\overline{R}_{i,m}} = -\sum_{j=0}^{n-1} c_j \cdot \Bigg(\sum_{\substack{R \in A_{i,n-j} \\ R \neq R_{i,m}}} \Omega_{N_i/\overline{R}} \Bigg) \ ,$$

comme combinaison $\mathbb{Z}$-linéaire des éléments de $\mathcal{F}$. Par conséquent, les coefficients $B_{e,f}$ de B sont donnés par les égalités suivantes :

$$dr'_i(\Omega_{P/R_e}) = \begin{cases} \Omega_{N_i/\overline{R}_e}\ , & \text{si } R_e \in A_{R_i} \text{ et } R_e \neq R_{i,m} \\ -\sum_{j=0}^{n-1} c_j \cdot \left(\sum_{\substack{R \in A_{i,n-j} \\ R \neq R_{i,m}}} \Omega_{N_i/\overline{R}} \right)\ , & \text{si } R_e = R_{i,m} \\ 0 \quad , & \text{sinon .} \end{cases}$$

Il en résulte que B est une matrice ayant au plus deux termes non nuls par colonne. En effet, considèrons la colonne $B(f)$ correspondant à la paire $(R_i, R_{i,l})$, où $1 \leq f \leq |\mathcal{F}|$, $1 \leq i \leq t$ et $R_{i,l} \in A_{R_i}$. On distingue trois cas, d'après les égalités ci-dessus :

(a) Le coefficient $B_{e,f}$ vaut 1 si $R_e = R_{i,l}$;
(b) Le coefficient $B_{e,f}$ vaut $(-c_j)$ si $R_e = R_{i,m}$;
(c) Le coefficient $B_{e,f}$ est nul sinon.

Ainsi, la colonne $B(f)$ possède :

- un unique terme non nul, valant 1, et apparaissant dans la ligne $B[R_{i,l}]$, si $R_{i,l} \in \mathcal{Q}_{n-j}$, et si $c_j = 0$ (par exemple, si $j = 1$) ;
- exactement deux termes non nuls si $c_j \neq 0$, à savoir :
  - un 1, situé dans la ligne $B[R_{i,l}]$,
  - un $(-c_j)$, situé dans une des $q_{n,n}$ dernières lignes de B, car $R_{i,m} \in A_{i,n}$. De plus, comme $R_{i,m} = \min(A_{i,n})$, le choix de l'ordre sur $\mathcal{E}$ implique que la ligne où apparaît le coefficient $(-c_j)$ est nécessairement

    en-dessous de la ligne $B[R_{i,l}]$, si $j < n$, ou bien
    en-dessus de la ligne $B[R_{i,l}]$, si $j = n$.

Par le corollaire 4.2.20, on sait que B est une matrice de rang $(q-1)$. Autrement dit, B possède exactement un diviseur élémentaire nul. On va montrer que les $(q-1)$ diviseurs élémentaires non nuls de B valent 1. Comme toute matrice obtenue en effectuant des opérations élémentaires sur les lignes ou sur les colonnes de B possède les mêmes diviseurs élémentaires que B, on va "simplifier" B par des opérations élémentaires sur les lignes et sur les colonnes, afin de faciliter nos calculs.

Soit $r = (q - q_{n,n} + 1)$ comme dans la preuve de l'assertion 4.2 ci-dessus et considérons la ligne $B[R_r]$, c'est-à-dire l'expression de $\beta'(\Omega_{P/R_r})$ dans $\mathcal{F}$, où $R_r = \min(\mathcal{Q}_n)$. L'assertion 4.2 implique les deux faits suivants :

- $\forall\, 1 \leq f \leq |\mathcal{F}|$ tel que $B_{r,f} \neq 0$, où la colonne $B(f)$ correspond à la paire $(R_i, R_{i,l})$ avec $1 \leq i \leq t$, $R_{i,l} \in A_{i,j}$ et $1 \leq j \leq n$, alors $B_{r,f} = -c_j$.
- $B[R_r]$ est l'unique ligne de B ayant cette propriété. En effet, $\forall\, 1 \leq s \leq q$ avec $s \neq r$, il existe $1 \leq f \leq |\mathcal{F}|$ et $1 \leq i \leq t$ tel que $B(f)$ correspond à la paire (R_i, R_s), i.e. $R_s \in A_{R_i}$ et $R_s \neq R_{i,m}$. Dans ce cas, on a $B_{s,f} = 1$.

Comme $R \in \mathcal{Q}_n$ et $c_0 = 1$, la matrice résultant de l'opération élémentaire suivante a les mêmes diviseurs élémentaires que B, car le coefficient de $B[R_r]$ vaut 1. On remplace $B[R_r]$ par la combinaison linéaire de lignes :

$$\sum_{j=0}^{n-1} c_j \cdot \left(\sum_{R \in \mathcal{Q}_{n-j}} B[R] \right) .$$

On produit ainsi une ligne nulle. En effet, β' est un homomorphisme et donc cela revient à remplacer $\beta'(\Omega_{P/R_r}) \in \mathcal{E}$ par

$$\sum_{j=0}^{n-1} c_j \cdot \Big(\sum_{R \in \mathcal{Q}_{n-j}} \beta'(\Omega_{P/R}) \Big) = \beta' \left(\sum_{j=0}^{n-1} c_j \cdot \Big(\sum_{R \in \mathcal{Q}_{n-j}} \Omega_{P/R} \Big) \right) =$$

$$= \beta'(\omega_n - c_n \cdot \Omega_P) = -c_n \cdot \beta'(\Omega_P) = 0 \ ,$$

par définition de ω_n et car $\omega_n = 0$ et $\Omega_P \in \mathrm{Ker}(\beta')$.

Appelons $B^{(1)}$ la matrice, équivalente par lignes à B, résultant de cette opération. Ainsi, $B^{(1)}$ est une matrice de taille $q \times |\mathcal{F}|$ qui a les caractéristiques suivantes :

1. La ligne $B^{(1)}[R_r]$ est nulle ;
2. Pour tout $1 \leq s \leq q$ avec $s \neq r$, on a $B^{(1)}[R_s] = B[R_s]$ et donc $B^{(1)}[R_s]$ possède (au moins) un terme qui vaut 1.
3. Pour tout $1 \leq f \leq |\mathcal{F}|$, la colonne $B^{(1)}(f)$ possède au plus deux termes non nuls, puisque l'opération élémentaire effectuée sur B n'a fait qu'annuler tous les coefficients non nuls de la ligne $B[R_r]$ et puisque $B(f)$ possède au plus deux termes non nuls.
4. Soient $1 \leq s \leq q$, $1 \leq i \leq t$, $1 \leq j \leq n$ et $1 \leq f \leq |\mathcal{F}|$ des entiers tels que $R_s \in A_{i,j}$, $R_s \neq R_{i,m}$ et tels que $B^{(1)}(f)$ correspond à la paire (R_i, R_s). Du calcul des coefficients de B, il résulte que :
   (i) $B^{(1)}_{s,f} = 1$.
   (ii) Si $j < n$, alors $B^{(1)}_{e,f} = 0$, $\forall\, e < s$ et $\forall\, e$ tel que $R_e \notin (\mathcal{Q}_n \cup \mathcal{Q}_j)$.
   (iii) Si $j = n$, alors $B^{(1)}_{e,f} = 0$, $\forall\, e > s$ et $\forall\, e$ tel que $R_e \notin \mathcal{Q}_n$.
   Les égalités (ii) et (iii) sont dues au choix de l'ordre sur $\mathcal{E}$ et au choix de $R_{i,m} = \min(A_{i,n})$.

Par récurrence sur $(r+1)$, ... , q , on va faire des opérations élémentaires sur les colonnes de $B^{(1)}$, afin d'obtenir une matrice $B^{(q_{n,n})}$ dont les $(q_{n,n} - 1)$ dernières lignes contiennent exactement un terme non nul et tel que celui-ci vaille 1. Considérons la ligne $B^{(1)}[R_{r+1}]$ et la colonne $B^{(1)}(f_1)$ correspondant à une paire $(R_{i_1}, R_{r+1}) \in \mathcal{F}$, pour un $1 \leq i_1 \leq t$ (f_1 existe par le point 2). On a ainsi $B^{(1)}_{r+1,f_1} = 1$. Par le point 4, tous les coefficients de $B^{(1)}(f_1)$ en-dessous de $B^{(1)}_{r+1,f_1}$ et tous ceux au-dessus de $B^{(1)}_{r,f_1}$ sont nuls. De plus, $B^{(1)}_{r,f_1} = 0$ car $B^{(1)}[R_r]$ est une ligne nulle. Utilisons alors $B^{(1)}(f_1)$ pour des opérations élémentaires sur les colonnes afin d'annuler les coefficients $B^{(1)}_{r+1,g}$ non nuls, pour tout $1 \leq g \leq |\mathcal{F}|$ avec $g \neq f_1$, sans modifier aucun coefficient d'aucune autre ligne de $B^{(1)}$. La matrice $B^{(2)}$ obtenue est équivalente par colonnes à $B^{(1)}$ et possède les mêmes lignes que B, sauf $B^{(2)}[R_r]$, qui est nulle, et $B^{(2)}[R_{r+1}]$, qui a un unique terme $B^{(2)}_{r+1,f_1}$ non nul. De plus, $B^{(2)}_{r+1,f_1} = 1$ et c'est l'unique terme non nul de $B^{(2)}(f_1)$, où f_1 correspond à une paire (R_{i_1}, R_{r+1}) , avec $1 \leq i_1 \leq t$.

Soit $2 \leq s < q$ et $B^{(s)}$ une matrice équivalente par colonnes à $B^{(1)}$ telle que

- La ligne $B^{(s)}[R_r]$ est nulle ;
- $\forall\, 1 \leq e \leq (r-1)$ et $\forall\, (r+s) \leq e \leq q$, on a $B^{(s)}[R_e] = B[R_e]$.
- $\forall\, (r+1) \leq e \leq (r+s-1)$, la ligne $B^{(s)}[R_e]$ a un unique terme $B^{(s)}_{e,f_{e-r}}$ non nul. De plus, $B^{(s)}_{e,f_{e-r}} = 1$ et c'est l'unique terme non nul de la colonne $B^{(s)}(f_{e-r})$ correspondant à la paire $(R_{i_{e-r}}, R_e)$, où $1 \leq i_{e-r} \leq t$.

Considérons la ligne $B^{(s)}[R_{r+s}]$ et soit $1 \leq f_s \leq |\mathcal{F}|$ tel que $B^{(s)}(f_s)$ correspond à la paire (R_{i_s}, R_{r+s}), pour un $1 \leq i_s \leq t$ (f_s existe et $B^{(s)}_{r+s,f_s} = 1$, par les points 2 et 4). Par le point 4 et par hypothèse de récurrence, tous les termes en-dessous de $B^{(s)}_{r+s,f_s}$ et tous ceux au-dessus de $B^{(s)}_{r+s,f_s}$ sont nuls (puisque $B^{(s)}_{r+s,f_{e-r}} = 0$, $\forall\, (r+1) \leq e \leq (r+s-1)$). Utilisons $B^{(s)}(f_s)$ pour annuler les coefficients $B^{(s)}_{r+s,g}$ non nuls, $\forall\, 1 \leq g \leq |\mathcal{F}|$ avec $g \neq f_s$, sans modifier aucun coefficient d'aucune autre ligne de $B^{(s)}$. La matrice $B^{(s+1)}$ obtenue est équivalente par colonnes à $B^{(1)}$ et $B^{(s+1)}$ a les mêmes lignes que $B^{(s)}$, sauf $B^{(s)}[R_{r+s}]$, qui a un unique terme $B^{(s)}_{r+s,f_s}$ non nul. De plus, $B^{(s)}_{r+s,f_s} = 1$ et c'est l'unique terme non nul de $B^{(s)}(f_s)$. Au terme de notre récurrence, la matrice $B^{(q_{n,n})}$ vérifie

- La ligne $B^{(q_{n,n})}[R_r]$ est nulle.
- $\forall\, 1 \leq e \leq (r-1)$, on a $B^{(q_{n,n})}[R_e] = B[R_e]$ (et $R_e \notin \mathcal{Q}_n$).
- $\forall\, (r+1) \leq e \leq q_{n,n}$, on a $R_e \in \mathcal{Q}_n$ et $B^{(q_{n,n})}[R_e]$ a un unique terme $B^{(q_{n,n})}_{e,f_{e-r}}$ non nul. De plus, $B^{(q_{n,n})}_{e,f_{e-r}} = 1$ et c'est l'unique terme non nul de la colonne $B^{(q_{n,n})}(f_{e-r})$ correspondant à la paire $(R_{i_{e-r}}, R_e)$, où $1 \leq i_{e-r} \leq t$.

Considérons maintenant les $(r-1)$ premières lignes de $B^{(q_{n,n})}$, qui sont les mêmes que dans B. Comme pour les $q_{n,n}$ dernières lignes, on va effectuer des opérations élémentaires sur les colonnes de $B^{(q_{n,n})}$, afin d'obtenir une matrice qui n'a plus qu'un seul terme non nul par ligne (sauf la r-ième, qui est nulle) et au plus un terme non nul par colonne, celui-ci valant 1. On procède cette fois par récurrence descendante sur les entiers $(r-1)$, ... , 1 pour échelonner pas à pas la matrice $B^{(q_{n,n})}$. En effet, le point 2 implique que $B^{(q_{n,n})}[r-1]$ possède un coefficient $B^{(q_{n,n})}_{r-1,f}$ égal à 1, où f correspond à une paire (R_i, R_{r-1}). Or, $R_{r-1} \notin \mathcal{Q}_n$ et l'éventuel autre terme non nul de $B^{(q_{n,n})}(f)$ se trouve dans les $q_{n,n}$ dernières lignes, mais les colonnes (R_j, R) où ceux-ci apparaissent vérifient $R \in \mathcal{Q}_n$. Donc $B^{(q_{n,n})}_{r-1,f}$ est l'unique terme non nul de $B^{(q_{n,n})}(f)$. On peut ainsi utiliser $B^{(q_{n,n})}(f)$ afin d'annuler, par des opérations élémentaires sur les colonnes de $B^{(q_{n,n})}$, tous les coefficients $B^{(q_{n,n})}_{r-1,g}$, $\forall\, 1 \leq g \leq |\mathcal{F}|$ avec $g \neq f$, sans modifier aucun coefficient d'aucune autre ligne de $B^{(q_{n,n})}$. Les arguments utilisés pour continuer à échelonner $B^{(q_{n,n})}$ étant exactement pareils que ceux utilisés pour obtenir $B^{(q_{n,n})}$ de $B^{(1)}$ par des opérations élémentaires sur les colonnes, nous ne les répétons pas. Nous nous contenterons de retenir le résultat final de l'échelonnement, à savoir, une matrice C de taille $q \times |\mathcal{F}|$ ayant un unique terme non nul par ligne sauf la r-ième, qui est nulle, et au plus un terme non nul par colonne, celui-ci valant 1. En particulier, les $(q-1)$ diviseurs élémentaires non nuls de C valent 1. Comme C a été obtenue à partir de B par des opérations

élémentaires sur les lignes et sur les colonnes, les diviseurs élémentaires de B sont égaux à ceux de C.

Ainsi, on a atteint notre but, car on a montré que les $(q-1)$ diviseurs élémentaires non nuls de l'application β' valent 1. Par conséquent, $\mathrm{Im}(\beta')$ est un facteur direct de $\prod_{i=1}^{t} E(N_i)$ de rang $(q-1)$. En effet, par le même raisonnement que pour la preuve de la proposition 4.2.13, cela implique que l'on peut trouver des bases

$$\{e_1, \ldots, e_q\} \text{ de } E^{\Omega}(P) \text{ et } \{f_1, \ldots, f_s\} \text{ de } \prod_{i=1}^{t} E(N_i) \ ,$$

avec $s = t \cdot q_{n-1}$, $\beta'(e_i) = f_i$, $\forall\, 1 \leq i \leq (q-1)$ et $\beta'(e_q) = 0$.

Ainsi, comme β est aussi de rang $(q-1)$ et comme $\mathrm{Im}(\beta') \subseteq \mathrm{Im}(\beta)$, on a nécessairement l'égalité $\mathrm{Im}(\beta') = \mathrm{Im}(\beta)$. Le même raisonnement que dans le corollaire 4.2.14 (c'est-à-dire dans le cas où $n = 2$) nous permet alors de conclure $E^{\Omega}(P) = E(P)$ et $D^{\Omega}(P) = D(P)$.

De plus, la relation donnée par la proposition 4.2.18 nous permet d'écrire

$$\Omega_{P/R} = -\sum_{j=0}^{n-1} c_j \cdot \Big(\sum_{S \in \mathcal{Q}_{n-j} \ , \ S \neq R} \Omega_{P/S} \Big) \ , \quad \text{pour un } R \in \mathcal{Q}_n \ ,$$

par exemple $R = \min(\mathcal{Q}_n)$. Par conséquent, l'ensemble $\mathcal{E} = \mathcal{E}' \setminus \{\Omega_{P/R}\}$ est une $\mathbb{Z}$-base de $E(P)$ et donc, a fortiori, l'ensemble

$$\mathcal{E} \cup \{\Omega_{P/S} \mid Z \leq S \leq P \ : \ |P:S| \geq 4\} \quad \text{ est une } \mathbb{Z}\text{-base de } D(P) \ .$$

□

Le fait que $D(P)$ est engendré par les syzygies relatifs implique immédiatement le corollaire suivant.

Corollaire 4.2.22. *L'homomorphisme $q : D_{\mathcal{O}}(P) \longrightarrow D_k(P)$ induit par le passage au quotient modulo l'idéal maximal $\wp$ de $\mathcal{O}$ (cf. section 1.4) est surjectif. Autrement dit, tout kP-module d'endo-permutation couvert se relève en un $\mathcal{O}P$-module d'endo-permutation couvert et donc la réduction modulo l'idéal $\wp$ induit un isomorphisme $D'_{\mathcal{O}}(P) \cong D'_k(P)$.*

De plus, si $R \in \mathcal{Q}_n$, alors l'ensemble suivant est une $\mathbb{Z}$-base de $D^{\Omega}_{\mathcal{O}}(P)$.

$$\{[\Omega^1_{P/S}(\mathcal{O})] \mid S \in \mathcal{Q}' \setminus \{R\}\} \cup \{[\Omega^1_{P/S}(\mathcal{O})] \mid Z \leq S < P \ : \ |P:S| \geq 4\} \ .$$

□

Nous avons ainsi atteint le but que nous nous étions fixés, à savoir, déterminer le groupe de Dade d'un 2-groupe extraspécial du type D_8^{*n} , $n \geq 2$. Comme nous l'avons déjà mentionné, ce pas ne constitue qu'un minuscule "saut de puce" sur la route menant à la classification des modules d'endo-permutation.

Remarquons tout de même qu'il nous a permis d'exhiber certains outils qui se sont révélés fort utiles pour l'analyse de la structure du groupe de Dade, et que ces outils peuvent, probablement, se généraliser à d'autres familles de p-groupes finis.

De plus, comme dans le cas d'un p-groupe métacyclique, on constate qu'aucun module d'endo-permutation "exotique" n'est apparu, et que tous les kP-modules d'endo-permutation couverts sont équivalents à un syzygy relatif.

Sur cette remarque nous mettons un terme à la première partie de ce travail de thèse, que nous avons consacrée à l'étude de la structure du groupe de Dade. Dans la seconde partie, nous allons nous intéresser à certaines occurrences de ces modules dans la théorie de la représentation des groupes finis et justifier ainsi l'intérêt qu'on leur porte.

Deuxième partie

Mode d'emploi des modules d'endo-permutation

Chapitre 5

Sources de modules simples

Le premier thème que nous avons choisi d'aborder pour commencer cette deuxième partie concerne les modules d'endo-permutation comme source de modules simples. Plus précisément, nous allons considérer le contexte suivant. On se donne un nombre premier p, un groupe fini p-résoluble G, un corps k algébriquement clos de caractéristique p et un kG-module simple L de vortex P, où P est un p-sous-groupe de Sylow de G. Alors la source de L, c'est-à-dire l'unique kP-module indécomposable S de vortex P et isomorphe à un facteur direct de $\mathrm{Res}_P^G L$ tel que L est un facteur direct de $\mathrm{Ind}_P^G S$, est un kP-module d'endo-permutation couvert.

Cette propriété des modules d'endo-permutation est l'objet du paragraphe 30 de [Th1] et le résultat ci-dessus correspond au théorème 30.5. En fait, comme nous l'avons mentionné dans le chapitre 2, L. Puig avait déjà considéré ce fait, et avait même prouvé un résultat plus précis qui n'a jamais été publié (cf. théorème 8.39 et remarque 8.41 de [Pu1]). Il a montré que la source S de L est isomorphe au chapeau d'un module de la forme

$$\bigotimes_{Q/R\in\mathcal{T}} \mathrm{Ten}_Q^P \,\mathrm{Inf}_{Q/R}^Q(M_{Q/R}), \tag{5.1}$$

où $M_{Q/R}$ est endo-trivial tel que $[M_{Q/R}] \in T^t(Q/R)$, et les quotients Q/R sont des sections de P appartenant à la famille $\mathcal{T}$ des groupes finis cycliques, diédraux, semidiédraux ou quaternioniens.

En particulier, cela implique que $[S]$ est un élément de torsion dans $D(P)$.

Dans ce chapitre, nous allons explicitement réaliser les chapeaux de *tous* les modules d'endo-permutation de la forme 5.1 comme sources de modules simples. Par conséquent, compte tenu des derniers résultats obtenus par J. Carlson sur la structure du sous-groupe de torsion du groupe des endo-triviaux, cela implique que les chapeaux de *tous* les éléments de torsion du groupe de Dade, pour p impair, sont des sources de modules simples.

Pour clore ce paragraphe introductif, précisons que les méthodes que nous allons employer sont fortement inspirées de celles utilisées par Dade dans [Da2].

Autrement dit, nous allons nous donner un nombre premier p, un système p-modulaire $(K, \mathcal{O}, k)$ et un groupe $P \in \mathcal{T}$. Ensuite, nous allons construire un groupe fini p-nilpotent G (et donc p-résoluble) qui admet P comme p-sous-groupe de Sylow et dont le plus grand sous-groupe normal d'ordre premier à p est un q-groupe extraspécial, pour un certain nombre premier q, judicieusement choisi. Puis, nous allons considérer un kG-module simple L, lui aussi bien choisi, et calculer sa source S. Il résultera à la fin de cet exercice que toutes les sources S possibles sont obtenues à l'aide de ce procédé.

Commençons par des préliminaires sur les automorphismes des q-groupes extraspéciaux. Cela va nous être utile pour construire des groupes p-nilpotents.

5.1 Encore des q-groupes extraspéciaux

Nous avons déjà défini ces groupes au chapitre 4. Dans cette section, nous allons donc nous contenter d'apporter quelques compléments concernant leur groupe d'automorphismes.

Soient q un nombre premier impair et Q un q-groupe extraspécial, d'ordre q^3 et d'exposant q. Rappelons que son centre est cyclique d'ordre q et coïncide avec le sous-groupe Q' des commutateurs. En d'autres termes, Q est engendré par deux éléments x et y d'ordre q, satisfaisant la relation ${}^{y}x = x[y,x]$, tels que le commutateur $z = [y,x] = yxy^{-1}x^{-1}$ est d'ordre q et engendre Q'.

Le groupe quotient Q/Q' est un $\mathbb{F}_q$-espace symplectique de dimension 2, pour la forme symplectique notée $[\ ,\ ]$ et induite par les commutateurs. Autrement dit, la matrice de $[\ ,\ ]$ dans la base $\{\bar{x}, \bar{y}\}$ de Q/Q' (si $g \in Q$, on note $\bar{g}$ sa classe dans Q/Q') est $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Ainsi, le groupe des automorphismes de l'espace symplectique Q/Q' est le groupe symplectique $\mathrm{Sp}_2(\mathbb{F}_q)$, qui est égal à $\mathrm{SL}_2(\mathbb{F}_q)$ (cf. Hilfsatz 9.12 [Hu1]).

Notons $\mathrm{Aut}_{Q'}(Q)$ le sous-groupe de $\mathrm{Aut}(Q)$ formé des automorphismes de Q dont la restriction à Q' est l'identité. On a un homomorphisme de groupes

$$\begin{array}{rcl} \pi : \mathrm{Aut}_{Q'}(Q) & \longrightarrow & \mathrm{SL}_2(\mathbb{F}_q) \\ \varphi & \longmapsto & \pi(\varphi)\ , \\ \text{où } \pi(\varphi)(\bar{g}) & = & \overline{\varphi(g)},\ \forall\, g \in \bar{g},\ \forall\, \bar{g} \in Q/Q' \text{ et } \forall\, \varphi \in \mathrm{Aut}_{Q'}(Q). \end{array}$$

Cette application π est bien définie, car, si $\hat{g} \in \bar{g}$, alors il existe $h' \in Q'$, tel que $\hat{g} = gh'$, et on a

$$\varphi(\hat{g}) = \varphi(g)\varphi(h') = \varphi(g)h' \in \overline{\varphi(g)}.$$

C'est clairement un homomorphisme de groupes, puisque φ l'est. De plus, π est surjectif. En effet, considérons

$$\begin{array}{rcl} \varphi : Q & \longrightarrow & Q \\ x & \longmapsto & xy \\ y & \longmapsto & yz \end{array} \qquad \text{et} \qquad \begin{array}{rcl} \psi : Q & \longrightarrow & Q \\ x & \longmapsto & x \\ y & \longmapsto & xy\ . \end{array}$$

Les égalités suivantes prouvent que φ et ψ, définis sur les générateurs de Q, préservent les relations de Q.

$$\begin{array}{lll} \varphi(x)^q = \varphi(y)^q = 1 & \text{et} & \psi(x)^q = \psi(y)^q = 1; \\ [\varphi(y), \varphi(x)] = z & \text{et} & [\psi(y), \psi(x)] = z; \\ {}^{\varphi(y)}\varphi(x) = \varphi(x)z & \text{et} & {}^{\psi(y)}\psi(x) = \psi(x)z\ . \end{array}$$

Par suite, φ et ψ sont deux endomorphismes de groupes qui sont l'identité sur Q'. De plus, φ et ψ sont surjectifs (et donc des automorphismes), puisque

$$x = \varphi(x)\varphi(y)^{-1}z = \psi(x) \quad \text{et} \quad y = \varphi(y)z^{-1} = \psi(x)^{-1}\psi(y).$$

Donc φ, $\psi \in \mathrm{Aut}_{Q'}(Q)$.

Par le théorème 2.8.4 de [Go], on sait que $\mathrm{SL}_2(\mathbb{F}_q)$ est engendré par

$$e = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad \text{et} \quad f = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

La surjectivité de π est alors évidente, puisque dans la base $\{\bar{x}, \bar{y}\}$ de Q/Q', on a matriciellement $\pi(\varphi) = e$ et $\pi(\psi) = f$.

D'autre part, le noyau $\mathrm{Ker}(\pi)$ de π s'identifie à Q/Q'. Pour montrer cette assertion, considérons les deux applications suivantes :

$$\begin{array}{rcl} \mathrm{conj} : Q/Q' \longrightarrow \mathrm{Ker}(\pi) & \text{et} & \tau : \ \mathrm{Ker}(\pi) \longrightarrow \mathrm{Hom}_{\mathbb{F}_q}(Q/Q', Q') \\ \bar{g} \longmapsto \mathrm{conj}(\bar{g}) & & \varphi \longmapsto \tau(\varphi), \end{array}$$

où on définit $\mathrm{conj}(\bar{g})(h) = {}^{g}h$, $\forall h \in Q$ et $\tau(\varphi)(\bar{g}) = g^{-1}\varphi(g)$, pour un représentant g de $\bar{g}$, $\forall\, \bar{g} \in Q/Q'$ et $\forall\, \varphi \in \mathrm{Ker}(\pi)$. Montrons que les applications conj et τ sont bien définies. On a ${}^{g}h = {}^{\hat{g}}h$, $\forall\, h \in Q$ si et seulement si $g^{-1}\hat{g} \in Q'$, i.e. l'application $\mathrm{conj}(\bar{g})$ ne dépend pas du choix de g dans $\bar{g}$. On a aussi $\pi(\mathrm{conj}(\bar{g}))(\bar{h}) = \overline{\mathrm{conj}(\bar{g})(h)} = \overline{{}^{g}h} = \bar{h}$, $\forall\, \bar{h} \in Q/Q'$, i.e. $\mathrm{conj}(\bar{g}) \in \mathrm{Ker}(\pi)$, $\forall\, \bar{g} \in Q/Q'$. Donc conj est bien défini. C'est un homomorphisme de groupes, car $g \mapsto \mathrm{conj}(g)$, $\forall\, g \in Q$ en est un. De plus, $\mathrm{conj}(\bar{g}) \in \mathrm{Aut}_{Q'}(Q)$, car $\mathrm{conj}(\bar{g}) \circ \mathrm{conj}(\overline{g^{-1}}) = \mathrm{Id}$ et on a $\mathrm{conj}(\bar{g})(z) = {}^{g}z = z$, $\forall\, g \in Q$.

D'autre part, τ est bien défini. En effet, on a $\tau(\varphi)(\bar{g}) \in Q'$, car $\varphi \in \mathrm{Ker}(\pi)$, i.e. $\varphi(g) \in \bar{g}$, $\forall\, g \in Q$ et donc $g^{-1}\varphi(g) \in Q'$, $\forall\, g \in Q$. De plus,

$$\tau(\varphi)(gh) = (gh)^{-1}\varphi(gh) = h^{-1}g^{-1}\varphi(g)\varphi(h) = g^{-1}\varphi(g)h^{-1}\varphi(h),$$

car $g^{-1}\varphi(g) \in Q'$. Par suite, on a $\tau(\varphi)(gh) = \tau(\varphi)(g)\tau(\varphi)(h)$, $\forall\, g, h \in Q$ et donc $\tau(\varphi)$ est un homomorphisme de groupes, pour tout $\varphi \in \mathrm{Ker}(\pi)$.

On a aussi $\tau(\varphi\psi) = \tau(\varphi)\tau(\psi)$, $\forall\, \varphi, \psi \in \mathrm{Ker}(\pi)$. En effet, si $\bar{g} \in Q/Q'$, on a, par définition des produits dans $\mathrm{Ker}(\pi) \leq \mathrm{Aut}_{Q'}(Q)$ et dans $\mathrm{Hom}_{\mathbb{F}_q}(Q/Q', Q')$,

$$\tau(\varphi \circ \psi)(\bar{g}) = g^{-1}\varphi\big(\psi(g)\big) = g^{-1}\psi(g)\psi(g)^{-1}\varphi\big(\psi(g)\big) = \tau(\psi)(\bar{g}) \cdot \tau(\varphi)\big(\overline{\psi(g)}\big).$$

Or, $\psi \in \mathrm{Ker}(\pi)$ implique $\overline{\psi(g)} = \bar{g}$. Il s'ensuit que $\tau(\varphi \circ \psi) = \tau(\psi) \cdot \tau(\varphi)$ et donc τ est un homomorphisme de groupes. De plus, si $\varphi \in \mathrm{Ker}(\tau)$, alors

$g = \varphi(g),\ \forall g \in Q$, i.e. $\varphi = \mathrm{Id}_Q$. Donc τ est un homomorphisme de groupes injectif.

Par ailleurs, Q' est isomorphe à $\mathbb{F}_q$ comme $\mathbb{F}_q$-espace vectoriel. Ainsi, on a un isomorphisme de $\mathbb{F}_q$-espaces vectoriels entre $\mathrm{Hom}_{\mathbb{F}_q}(Q/Q', Q')$ et le dual de Q/Q', et donc entre $\mathrm{Hom}_{\mathbb{F}_q}(Q/Q', Q')$ et Q/Q'.

En particulier, on en tire que $|\operatorname{Ker}(\pi)| \leq |Q/Q'|$ et par conséquent, les injections conj et τ sont des isomorphismes. Par suite, on a une suite exacte courte

$$0 \longrightarrow Q/Q' \longrightarrow \mathrm{Aut}_{Q'}(Q) \longrightarrow \mathrm{SL}_2(\mathbb{F}_q) \longrightarrow 0.$$

Si p est un nombre premier distinct de q et P est un p-sous-groupe de $\mathrm{SL}_2(\mathbb{F}_q)$, on a une suite exacte courte, obtenue par restriction,

$$0 \longrightarrow Q/Q' \longrightarrow \pi^{-1}(P) \longrightarrow P \longrightarrow 0. \tag{5.2}$$

Il découle alors du théorème de Schur-Zassenhaus (cf. corollaire 8.40 de [CR]) que celle-ci est scindée puisque Q/Q' et P sont d'ordres premiers entre eux et Q/Q' est abélien. Autrement dit, il existe un homomorphisme de groupes injectif $\sigma : P \longrightarrow \mathrm{Aut}_{Q'}(Q)$, tel que $\pi\sigma = \mathrm{Id}_P$.

Rappelons encore que l'ordre de $\mathrm{SL}_2(\mathbb{F}_q)$ est $q(q^2-1)$ et que $\mathrm{SL}_2(\mathbb{F}_q)$ possède des 2-sous-groupes de Sylow quaternioniens généralisés ainsi que des sous-groupes cycliques d'ordre $q-1$ et $q+1$ (cf. théorème 2.8.3 de [Go]). On en déduit immédiatement le lemme suivant :

Lemme 5.1.1. *Soient p et q deux nombres premiers distincts, P un p-groupe fini cyclique ou, si $p = 2$, éventuellement quaternionien, tel que P s'identifie à un sous-groupe de $SL_2(\mathbb{F}_q)$ et soit Q un q-groupe extraspécial d'ordre q^3 et d'exposant q. Alors il existe un homomorphisme de groupes injectif $\sigma : P \longrightarrow \mathrm{Aut}(Q)$. De plus, on peut choisir σ de telle sorte que sa restriction au centre Q' est l'identité.*

□

5.2 Construction de groupes finis p-nilpotents

Soient p un nombre premier, n un entier strictement positif, et P un p-groupe cyclique d'ordre p^n, ou éventuellement quaternionien d'ordre 2^n, si $p = 2$. Choisissons un nombre premier impair $q \equiv p^n - 1 \pmod{p^{n+1}}$ et considérons un q-groupe extraspécial Q d'ordre q^3 et d'exposant q.

Par choix de q, on a $p^n \mid q+1$ et donc, par le lemme 5.1.1, P s'identifie à un sous-groupe des automorphismes de Q qui fixe le centre Q'. En d'autres termes, on a un groupe fini p-nilpotent $G = Q \rtimes P$, avec P comme p-sous-groupe de Sylow et tel que Q' centralise P, puisque P agit trivialement sur Q' par construction.

Considérons aussi la construction suivante. Si $p = 2$ et P est un groupe quaternionien d'ordre $2^n \geq 8$ et $q \equiv 2^{n-1} + 1 \pmod{2^n}$, on obtient encore un

groupe 2-nilpotent $Q \rtimes P$, car P s'identifie à un 2-sous-groupe (de Sylow) de $\mathrm{SL}_2(\mathbb{F}_q)$. En effet, on a $q+1 \equiv 2 \pmod{2^{n-1}}$ et $q-1 \equiv 2^{n-1} \pmod{2^n}$ et donc $q^2-1 \equiv 2^n \pmod{2^{n+1}}$, i.e. 2^n divise l'ordre de $\mathrm{SL}_2(\mathbb{F}_q)$ (et c'est même la plus grande puissance de 2 avec cette propriété).

Continuons maintenant avec quelques propriétés immédiates des groupes p-nilpotents ainsi construits.

Lemme 5.2.1. *Aussi bien dans le cas cyclique que quaternionien, P possède un unique sous-groupe cyclique d'ordre p. Soit w un générateur de celui-ci. Alors, on peut choisir une section $\sigma : P \longrightarrow \pi^{-1}(P)$ de la suite exacte courte 5.2 telle que w se relève en un automorphisme de Q d'ordre p qui n'a pas de point fixe sur $Q \setminus Q'$. En d'autres termes, si $g \in Q$, alors w et g commutent si et seulement si $g \in Q'$.*

Preuve. Supposons P cyclique et notons $P = <u \mid u^{p^n} = 1>$. Comme σ est injectif, $\sigma(u) \in \mathrm{Aut}_{Q'}(Q)$ est d'ordre $|P|$. Ainsi, $\sigma(w) = \sigma(u)^{p^{n-1}}$ est d'ordre p.

Si $\sigma(w)$ possède un point fixe sur $Q \setminus Q'$, alors $\pi(\sigma(w)) \in \mathrm{SL}_2(\mathbb{F}_q)$ possède un vecteur propre pour la valeur propre 1. Donc $\pi(\sigma(w))$ est semblable à une matrice A, d'ordre p, de la forme $A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$, pour un $a \in \mathbb{F}_q$, puisque le déterminant vaut 1 et 1 est une valeur propre.

Mais alors, on a $p \cdot a = 0$ (car $A^p = \mathrm{Id}$) et donc $a = 0$, car $p \in \mathbb{F}_q^*$. D'où $A = \mathrm{Id}$. Ceci contredit le fait que A est d'ordre p. On en déduit que $\pi(\sigma(w))$ n'a pas de vecteur propre dans Q/Q' pour la valeur propre 1, i.e. $\sigma(w)$ n'a pas de point fixe sur $Q \setminus Q'$.

Supposons $p = 2$ et P quaternionien. Alors, on a $\pi(\sigma(w)) = -\mathrm{Id}$ (i.e. l'unique élément d'ordre 2 de $\mathrm{SL}_2(\mathbb{F}_q)$, pour q impair) et donc 1 n'est pas une valeur propre de $\pi(\sigma(w))$. Par conséquent, $\sigma(w)$ n'a pas de point fixe sur $Q \setminus Q'$. □

Lemme 5.2.2. *Le normalisateur $N = N_G(P)$ de P dans G est $Q' \times P$.*

Preuve. Comme G est p-nilpotent, on a $N = C_Q(P) \times P$. Or $C_Q(P) = Q'$. En effet, on a $Q' \leq C_Q(P)$, puisque Q' centralise P.

Réciproquement, si $g \in C_Q(P)$, alors, en particulier, g et w commutent. Par le lemme précédent, on en déduit que $g \in Q'$ et donc $Q' = C_Q(P)$.

□

Lemme 5.2.3. *Le p-sous-groupe de Sylow P du groupe G construit est d'intersection triviale. En d'autres termes, $\forall\, g \in G \setminus N,\ {}^gP \cap P = \{1\}$.*

Preuve. Soit $g \in G \setminus N$. Il existe d'uniques éléments $h \in Q$ et $u \in P$ tels que $g = hu$. Or, on a ${}^gP = {}^{hu}P = {}^hP$. Donc il suffit de prouver l'assertion dans le cas où $g \in Q$. Soient alors $g \in Q$ et $s \in {}^gP \cap P$. Il existe $s' \in P$ tel que $s = {}^gs'$. On a alors $[g, s'] = 1$. En effet, $[g, s'] = ({}^gs')s'^{-1} = s(s')^{-1} \in P$ et $[g, s'] = g({}^{s'}g)^{-1} \in Q$, car Q est normal dans G. Donc $[g, s'] \in P \cap Q = \{1\}$. Donc $g \in C_Q(<s'>)$.

Supposons $s' \neq 1$ et donc ${}^gP \cap P \neq \{1\}$. Alors on a $w \in <s'>$ et par conséquent $g \in C_Q(<s'>) \leq C_Q(<w>) = Q' \leq N$. □

Construisons à présent un groupe fini 2-nilpotent, ayant un 2-sous-groupe de Sylow semidiédral $P = <u, v \mid u^{2^{n-1}} = v^2 = 1, {}^vu = u^{2^{n-2}-1}>$ d'ordre 2^n, avec $n \geq 4$. Considérons un nombre premier q avec $q \equiv 2^{n-1} - 1 \pmod{2^n}$ et Q est un q-groupe extraspécial d'ordre q^5, d'exposant q. Autrement dit, on peut définir Q par générateurs et relations comme suit. $Q = <x_1,\ x_2,\ y_1,\ y_2>$, où $x_1,\ x_2,\ y_1$ et y_2 satisfont les relations :

$$x_1^q = x_2^q = y_1^q = y_2^q = 1,$$
$${}^{y_i}x_i = x_i[y_i, x_i],\ \forall\, 1 \leq i \leq 2,$$
$$[x_1, x_2] = [y_1, y_2] = [x_i, y_j] = 1,\ \forall\, 1 \leq i \neq j \leq 2.$$

Notons $Q' = <z>$ le centre de Q. On a $z = [y_1, x_1] = [y_2, x_2]$.

On peut aussi considérer Q comme le produit central de deux q-groupes extraspéciaux Q_1 et Q_2 d'ordre q^3, d'exposant q et de centre Q', où Q_i est le sous-groupe de Q engendré par x_i et y_i, pour $i = 1$ et 2.

D'autre part, P possède un sous-groupe quaternionien R, engendré par u^2 et uv, d'ordre 2^{n-1}. Par le paragraphe 5.1, R s'identifie à un sous-groupe de $\mathrm{Aut}_{Q_1'}(Q_1)$, via une section σ de la suite exacte 5.2. Utilisons cette section pour identifier R à un sous-groupe de $\mathrm{Aut}_{Q_2'}(Q_2)$ comme suit. Soit θ l'isomorphisme de Q_1 vers Q_2, envoyant x_1 sur x_2 et y_1 sur y_2 (et donc $\theta(z) = z$), et soit λ l'automorphisme de R, envoyant u^2 sur $(u^2)^{-1}$ et (uv) sur $(u^2)^{2^{n-3}-1}(uv)$. L'application λ est un homomorphisme car

$$\lambda(uv)\lambda(u^2)\lambda(uv)^{-1} = \big((u^2)^{2^{n-3}-1}(uv)\big)(u^2)^{-1}\big((uv)^{-1}(u^2)^{2^{n-3}+1}\big) =$$

$$= (u^2)^{2^{n-3}-1}\big({}^{(uv)}(u^2)\big)^{-1}(u^2)^{2^{n-3}+1} = (u^2),$$

et λ est bijectif car $\lambda^2 = \mathrm{Id}$. Ainsi, si

$$\begin{array}{rcl} \sigma : R & \longrightarrow & \mathrm{Aut}_{Q_1'}(Q_1) \\ u^2 & \longmapsto & \sigma(u^2) \\ uv & \longmapsto & \sigma(uv) \end{array}$$

est une section de la suite exacte courte 5.2 du paragraphe 5.1, alors on obtient un homomorphisme injectif

$$\begin{array}{rcl} \tilde{\sigma} : R & \longrightarrow & \mathrm{Aut}_{Q_2'}(Q_2) \\ u^2 & \longmapsto & \theta\sigma\big(\lambda(u^2)\big)\theta^{-1} = \theta\sigma(u^2)^{-1}\theta^{-1} \\ uv & \longmapsto & \theta\sigma\big(\lambda(uv)\big)\theta^{-1} = \theta\sigma(u^2)^{2^{n-3}-1}\sigma(uv)\theta^{-1}. \end{array}$$

Posons alors

$$\begin{array}{c} \sigma_{\cdot} : P \longrightarrow \mathrm{Aut}_{Q'}(Q), \\ u \longmapsto \sigma_u \\ v \longmapsto \sigma_v, \end{array}$$

où $\sigma_u|_{Q_1} = \tilde{\sigma}(uv)\theta$, $\sigma_v|_{Q_1} = \theta$, $\sigma_u|_{Q_2} = \sigma(uv)\theta^{-1}$ et $\sigma_v|_{Q_2} = \theta^{-1}$,

et où $\sigma_g|_{Q_i}$ désigne la restriction de σ_g à Q_i, pour $g \in \{u, v\}$ et $i = 1$ et 2. Cette application est bien définie et elle étend σ et $\tilde{\sigma}$. En effet, on a

$$\big(\sigma_u^2\big)\big|_{Q_1} = \big(\sigma_u\big)\big|_{Q_2}\big(\sigma_u\big)\big|_{Q_1} = \big(\sigma(uv)\theta^{-1}\big)\big(\tilde{\sigma}(uv)\theta\big) =$$

$$= \sigma(uv)\sigma(u^2)^{2^{n-3}-1}\sigma(uv) = \sigma(u^2)^{2^{n-3}+1}\sigma(uv)^2 = \sigma(u^2)^{2^{n-3}+1}\sigma(u^2)^{2^{n-3}} = \sigma(u^2)$$

et

$$\big(\sigma_u^2\big)\big|_{Q_2} = \big(\sigma_u\big)\big|_{Q_1}\big(\sigma_u\big)\big|_{Q_2} = \big(\theta\sigma(u^2)^{2^{n-3}-1}\sigma(uv)\big)\big(\sigma(uv)\theta^{-1}\big) =$$

$$= \theta\sigma(u^2)^{2^{n-3}-1}\sigma(uv)^2\theta^{-1} = \theta\sigma(u^2)^{-1}\theta^{-1} = \tilde{\sigma}(u^2).$$

On a aussi $\sigma_v^2 = \mathrm{Id}$ et ${}^{\sigma_v}\sigma_u = \sigma_u^{2^{n-2}-1}$, car $\big(\sigma_u\sigma_v\big)\big|_{Q_1} = \sigma(uv)$ et $\big(\sigma_u\sigma_v\big)\big|_{Q_2} = \tilde{\sigma}(uv)$. L'application $\sigma_\cdot$ est donc un homomorphisme de groupe injectif et le sous-groupe de $\mathrm{Aut}_{Q'}(Q)$ engendré par σ_u et σ_v est semi-diédral d'ordre 2^n. On peut ainsi construire un groupe fini 2-nilpotent G, produit semi-direct de P par Q.

De plus, on a $C_Q(P) \leq C_Q(<w>) = Q'$, car ${}^g w = w$ si et seulement si ${}^w g = g$ si et seulement si $g \in Q'$ (cf. lemme 5.2.1). Comme P agit trivialement sur Q', on en tire que $C_Q(P) = Q'$ et donc le normalisateur $N_G(P)$ de P dans G est égal à $Q' \times P$. Le lemme suivant exhibe deux différences que l'on constate par rapport aux constructions précédentes.

Lemme 5.2.4. *P possède deux classes de conjugaison de sous-groupes cycliques d'ordre 2 et P n'est pas un sous-groupe de G d'intersection triviale.*

Preuve. L'unique sous-groupe cyclique $<w>$ d'ordre 2 de R est normal dans P, puisqu'il s'agit du centre de P. Il constitue donc une classe de conjugaison de taille 1. Observons que tous les éléments de P d'ordre 2 non centraux peuvent s'écrire comme un produit $u^{2a}v$, pour un entier a avec $0 \leq a < 2^{n-3}$. Or, pour tout entier b, on a

$${}^{u^b}v = u^b({}^v u)^{-b}v = u^{2b(1-2^{n-3})}v.$$

Donc tous les éléments de P d'ordre 2 non centraux sont conjugués par une puissance de u, et donc P possède 2 classes de conjugaison de sous-groupes cycliques d'ordre 2 : une contenant le centre de P et l'autre contenant tous les autres sous-groupes d'ordre 2.

Considérons maintenant la conjugaison par v dans G, restreinte à Q, i.e. l'automorphisme σ_v de Q d'ordre 2 défini ci-dessus, et observons que σ_v fixe des éléments de $Q \setminus Q'$. En effet, on a ${}^v(x_1x_2) = x_1x_2$, car x_1 et x_2 commutent. Donc $v \in {}^{x_1x_2}P \cap P$, mais $x_1x_2 \notin N_G(P) = Q' \times P$.

□

Lemme 5.2.5. *Si $g \notin N_G(P)$ vérifie ${}^gP \cap P \neq \{1\}$, alors ${}^gP \cap P$ est conjugué à $<v>$.*

98 CHAPITRE 5. SOURCES DE MODULES SIMPLES

Preuve. On a $<w> \leq {}^gP \cap P$ si et seulement si $g \in N_G(P)$. En effet, si $g \in N_G(P)$, alors ${}^gP \cap P = P \geq <w>$.

Réciproquement, supposons qu'il existe $g \in Q$ satisfaisant $w \in {}^gP \cap P$. Alors, il existe $s \in P$ tel que ${}^gs = w$. Considérons le commutateur $[g, s]$. On a

$$[g,s] = g\ {}^sg^{-1} \in Q\ ,\ \text{car } Q \lhd G \quad \text{et aussi} \quad [g,s] = {}^gs\ s^{-1} = ws \in P.$$

Il s'ensuit que $[g, s] \in Q \cap P = \{1\}$ et donc g et s commutent. Autrement dit, on a $w = {}^gs = s$, i.e. $g \in C_G(<w>)$. Or, ${}^gw = w \iff {}^wg = g$, et la conjugaison par w dans G, restreinte à Q, correspond à $\sigma(w) \in \mathrm{Aut}_{Q'}(Q)$, qui correspond à $-\mathrm{Id} \in \mathrm{SL}_2(\mathbb{F}_q)$. En d'autres termes, on a ${}^wg = g$ si et seulement si $g \in Q'$. Ainsi, on a $g \in N_G(P)$.

Par conséquent, si $g \notin N_G(P)$ et ${}^gP \cap P \neq \{1\}$, alors ${}^gP \cap P$ ne contient pas w et donc ${}^gP \cap P$ est d'ordre 2. Par le lemme 5.2.4, ${}^gP \cap P$ est conjugué à $<v>$. □

Résumons la situation. Soit p un nombre premier, et P un p-groupe fini. Nous avons construit des groupes finis p-nilpotents de la forme $G = Q \rtimes P$, où Q est un q-groupe extraspécial d'ordre q^3 ou q^5 et d'exposant q, pour un nombre premier q vérifiant les conditions suivantes.

- Si P est cyclique, on a considéré $q \equiv |P| - 1\ (\mathrm{mod}\ p|P|)$ et Q d'ordre q^3.
- Si P est quaternionien, on a construit deux groupes finis 2-nilpotents en choisissant deux nombres premiers q : une fois $q \equiv |P| - 1\ (\mathrm{mod}\ 2|P|)$ et l'autre fois $q \equiv \frac{|P|}{2} + 1\ (\mathrm{mod}\ |P|)$. A chaque fois, Q est d'ordre q^3.
- Si P est semidiédral, on a considéré $q \equiv \frac{|P|}{2} - 1\ (\mathrm{mod}\ |P|)$ et Q d'ordre q^5.

Le choix des congruences des nombres premiers q et des ordres des q-groupes extraspéciaux se justifie dans la section suivante, où nous allons construire des modules simples pour ces groupes finis p-nilpotents.

5.3 Construction de modules simples

Avant de construire des kG-modules simples, apportons quelques compléments aux notions de base sur les représentations.

Définition et proposition 5.3.1. *Soient p un nombre premier, $R \in \{K, \mathcal{O}, k\}$, où $(K, \mathcal{O}, k)$ est un système p-modulaire, G un groupe fini, $H \leq G$, M et M' des RG-modules, N un RH-module et $\rho : H \longrightarrow \mathrm{Aut}_k(N)$ la représentation associée à N.*

1. *On dit que N, respectivement ρ,* **s'étend à** *G s'il existe un RG-module L tel que $L{\downarrow}_H^G \cong N$, respectivement une représentation $\tilde{\rho} : G \longrightarrow \mathrm{Aut}_k(N)$ de G telle que $\tilde{\rho}{\downarrow}_H^G = \rho$.*
2. *Soit $g \in H$. La* **trace** $\mathrm{Tr}(g, N)$ **de** *g* **sur** *N est la trace de l'application k-linéaire $\rho(g) \in \mathrm{Aut}_k(N)$.*

3. *Supposons $R = K$. On définit le* **produit scalaire** $< M, M' >$ **de** M **et** M' *par*
$$< M, M' >= \sum_{g \in G} \mathrm{Tr}(g, M)\, \mathrm{Tr}(g^{-1}, M') \ .$$

4. **Relations d'orthogonalité.** *Supposons $R = K$. Alors on a*
   (a) *M est un KG-module simple si et seulement si $< M, M >= 1$.*
   (b) *Supposons de plus M et M' simples. Alors $M \cong M'$ si et seulement si $< M, M' >= 1$. Sinon on a $< M, M' >= 0$.*

5. *Le* **groupe de Grothendieck** $G_0(RG)$ **des** RG**-modules** *est le groupe abélien défini par générateurs et relations comme suit. Les générateurs sont les classes d'isomorphisme $[M]$ des RG-modules M. On associe à toute suite exacte de RG-modules*
$$0 \to L \to M \to N \to 0 \quad \textit{la relation} \quad [M] = [L] + [N].$$
On note (abusivement) $[M]$ la classe du RG-module M dans $G_0(RG)$.

6. *Supposons $R = K$. Comme $\mathcal{O}$ est un sous-anneau de K, on peut voir M comme un $\mathcal{O}G$-module. Il existe alors un $\mathcal{O}G$-module $\mathcal{O}$-libre L qui vérifie $M \cong K \otimes_{\mathcal{O}} L$. La réduction $\bar{L} = L/\wp L$ de L modulo $\wp$ est un kG-module. On définit ainsi l'***homomorphisme de décomposition** *par*
$$\begin{array}{rcl} d : G_0(KG) & \longrightarrow & G_0(kG) \\ [M] & \longmapsto & [\bar{L}]. \end{array}$$
On retiendra, en particulier, qu'un tel L existe toujours, mais L n'est pas unique. Par contre $[\bar{L}]$ est unique et donc cette application est bien définie (cf. paragraphe 16 de [CR]).

Afin de construire des modules simples dans la situation qui nous intéresse, nous allons utiliser des kQ-modules simples, où Q est un q-groupe extraspécial d'ordre q^{1+2m} et d'exposant q, pour un nombre premier q distinct de la caractéristique p de k et m un entier strictement positif. Commençons alors par décrire les kQ-modules simples. Notons $x_1, \ldots, x_m, y_1, \ldots, y_m$ les générateurs de Q satisfaisant les relations suivantes :
$$x_i^q = y_i^q = 1 \ , \quad {}^{y_i}x_i = x_i[y_i, x_i] \ , \quad [y_i, x_i] = [y_j, x_j] \quad \text{et}$$
$$[x_i, x_j] = [x_i, y_j] = [y_i, y_j] = 1, \quad \forall\, 1 \leq i \neq j \leq m.$$
Notons $z = [y_1, x_1]$ le générateur du centre de Q (qui coïncide avec le sous-groupe Q' des commutateurs, cyclique d'ordre q), et A le sous-groupe abélien élémentaire engendré par $x_1, \ldots, x_m$ et z. On a $|A| = q^{m+1}$ et $A \triangleleft Q$.

Comme k est algébriquement clos, le nombre de kQ-modules simples est égal au nombre de classes de conjugaison des éléments de Q (cf. théorème 3.37 de [CR]). Comptons-les. Si $g \in Q \setminus Q'$, alors g possède $|Q/N_Q(<g>)| = q$ conjugués distincts. En effet, $N_Q(<g>)$ est un produit direct $<g> \times H$, où H

est un q-groupe extraspécial d'ordre $q^{1+2(m-1)}$ et d'exposant q (cf. chapitre 4). Ainsi, les $(q^{1+2m}-q)$ éléments non centraux dans Q sont répartis en classes de conjugaison de taille q. Donc on a $\frac{q^{1+2m}-q}{q}$ classes de conjugaison d'éléments non centraux, auxquelles s'ajoutent les q classes de conjugaison (de taille 1) des éléments de Q'. Ainsi, on a en tout $q^{2m}-1+q$ classes de conjugaison, i.e. $q^{2m}-1+q$ modules simples. Montrons, en les exhibant, que l'on a $(q-1)$ kQ-modules simples de dimension q^m, et q^{2m} de dimension 1. On aura ainsi établi la liste complète des kQ-modules simples.

Soit $\omega \in k$ une racine q-ième de l'unité avec $\omega \neq 1$. Considérons la représentation ψ de degré 1 suivante et notons k_ψ son kA-module associé (de dimension 1) :

$$\begin{array}{rcll} \psi : A & \longrightarrow & k^* & | \\ x_i & \longmapsto & 1,\ 1 \leq i \leq m & | \quad k_\psi \quad \text{est donc défini par :} \\ z & \longmapsto & \omega & | \quad a \cdot \lambda = \psi(a)\lambda,\ \forall\, a \in A,\ \forall\, \lambda \in k\ . \end{array}$$

On a ${}^g\psi \neq \psi$, $\forall g \notin A$. En effet, $\forall\ 1 \leq j \leq m$, on a

$$\begin{array}{rcl} {}^{y_j}\psi : A & \longrightarrow & k^* \\ x_i & \longmapsto & {}^{y_j}x_i \cdot 1 = x_i z^{\delta_{ij}} \cdot 1 = \omega^{\delta_{ij}},\ 1 \leq i \leq m \\ z & \longmapsto & {}^{y_j}z \cdot 1 = z \cdot 1 = \omega\ , \end{array}$$

où δ désigne le symbole de Kronecker. Donc $k_\psi \ncong {}^g k_\psi$, $\forall g \notin A$. Par le théorème 11.11 de [CR], il s'ensuit que le kQ-module induit $L = k_\psi \uparrow_A^Q$ est simple, de dimension q^m. Explicitement, l'ensemble

$$\{(\prod_{j=1}^{m} y_j^{i_j}) \otimes 1 \mid 0 \leq i_j < q\ ,\ \forall\, 1 \leq j \leq m\} \quad \text{est une } k\text{-base de } L$$

et l'action de Q sur L est définie sur les générateurs x_l et y_l de Q par

$$x_l \cdot\ (\prod_{j=1}^{m} y_j^{i_j}) \otimes 1 = (\prod_{j=1}^{m} y_j^{i_j})\underbrace{({}^{(y_l^{-i_l})}x_l)}_{=x_l z^{-i_l} \in A} \otimes 1 = (\prod_{j=1}^{m} y_j^{i_j}) \otimes (x_l z^{-i_l} \cdot 1) =$$

$$= (\prod_{j=1}^{m} y_j^{i_j}) \otimes \omega^{-i_l} = \omega^{-i_l}((\prod_{j=1}^{m} y_j^{i_j}) \otimes 1) \quad ;$$

$$y_l \cdot\ (\prod_{j=1}^{m} y_j^{i_j}) \otimes 1 = (\prod_{j=1}^{m} y_j^{i_j+\delta_{jl}}) \otimes 1 \text{ (avec } y_j^q = 1, \text{ si } i_j = q-1)\ .$$

En particulier, on a $z \cdot l = \omega l$, $\forall\, l \in L$.

Comme k est algébriquement clos, on a $(q-1)$ racines q-ièmes de l'unité non triviales. Or, deux racines distinctes définissent deux modules non isomorphes et donc on obtient $(q-1)$ modules simples non isomorphes de dimension q^m, comme souhaité.

D'autre part, pour tout choix de $2m$ racines q-ièmes de l'unité ω_i et θ_i, pour $1 \leq i \leq m$, on obtient une représentation de degré 1 de Q en posant

$$x_i \longmapsto \omega_i \quad \text{et} \quad y_i \longmapsto \theta_i \ , \ \forall\, 1 \leq i \leq m \ .$$

Deux choix distincts donnent deux représentations distinctes et donc les deux modules associés ne sont pas isomorphes. Ainsi, on obtient autant de kQ-modules non isomorphes de dimension 1 que de choix possibles, à savoir q^{2m} (car k est algébriquement clos). D'où le résultat annoncé :

on a $(q-1)$ kQ-modules simples de dimension q^m et
on a q^{2m} kQ-modules simples de dimension 1.

En caractéristique 0, i.e. sur K, les relations d'orthogonalité permettent de déterminer quand deux KQ-modules simples sont isomorphes. Dans notre cas, même si k n'est pas de caractéristique nulle, kQ est semi-simple et l'homomorphisme d de décomposition induit un isomorphisme entre les kQ-modules simples et les KQ-modules simples (cf. [Se]). Autrement dit, on peut relever tout kQ-module simple L en un unique KQ-module simple L_K (à isomorphisme près). On en déduit alors que, pour tous kQ-modules simples L et M, se relevant en L_K et M_K respectivement, on a

$$L \cong M \iff L_K \cong M_K \iff < L_K, M_K >= 1 \ .$$

Si M et L ne sont pas isomorphes, on a $< L_K, M_K >= 0$.

De la description des kQ-modules simples, on constate que si M est un kQ-module de dimension 1, alors $M\downarrow^Q_{Q'} \cong k$, où k désigne le kQ'-module trivial. Par conséquent, comme kQ est semi-simple, si M est un kQ-module de dimension q^m, alors

– soit M est simple, et on a $M\downarrow^Q_{Q'} \cong (k_\omega)^{q^m}$ pour une racine q-ième de l'unité ω non triviale et où k_ω est le kQ'-module de dimension 1 défini par $z \cdot \lambda = \omega\lambda, \forall\, \lambda \in k$;
– soit M est somme directe de q^m modules de dimension 1 et $M\downarrow^Q_{Q'} \cong k^{q^m}$.

D'où le lemme suivant.

Lemme 5.3.2. *Soient L et M deux kQ-modules de dimension q^m, et L_K, respectivement M_K, les KQ-modules correspondants. Supposons L simple. Alors, L et M sont isomorphes si et seulement si $< L_K\downarrow^Q_{Q'}, M_K\downarrow^Q_{Q'} >= q^{2m}$.*

Preuve. Par hypothèse, L est simple et donc il existe une racine q-ième non triviale de l'unité θ telle que $L_K\downarrow^Q_{Q'} \cong (k_\theta)^{q^m}$.

Si M n'est pas simple, alors $M\downarrow^Q_{Q'} \cong k^{q^m}$ et donc

$$< L_K\downarrow^Q_{Q'}, M_K\downarrow^Q_{Q'} >=< (k_\theta)^{q^m}, k^{q^m} >= \ q^{2m} < k_\theta \ , \ k >= \ 0 \ .$$

Si M est simple, il existe une racine q-ième non triviale de l'unité ω telle que $M\downarrow^Q_{Q'} \cong (k_\omega)^{q^m}$. Ainsi, on a

$$< L_K\downarrow^Q_{Q'}, M_K\downarrow^Q_{Q'} >= \ q^{2m} < k_\theta, k_\omega >= \ q^{2m}\delta_{\theta,\omega} \ .$$

Donc, $< L_K{\downarrow}^Q_{Q'}, M_K{\downarrow}^Q_{Q'} > = q^{2m}$ si et seulement si M et L sont isomorphes. □

En théorie des représentations ordinaires, i.e. sur $\mathbb{C}$, ou plus généralement sur un corps K "assez gros" et de caractéristique nulle, on dispose d'un critère fort utile pour savoir sous quelles conditions on peut étendre un module d'un sous-groupe à un sous-groupe plus grand. Mais, en général, s'il existe une extension, alors celle-ci n'est pas unique (à moins de fixer la valeur du déterminant de la représentation associée), car on peut toujours considérer le produit tensoriel avec un module de dimension 1 (cf. chapitre 1). Qu'en est-il des kG-modules, dans notre situation ?

Définition 5.3.3. *Soient $H \lhd G$ et M un kH-module. On dit que M est* **invariant par** *G si les kH-modules ${}^gM$ et M sont isomorphes, $\forall\, g \in G$. Rappelons que ${}^gM$ désigne le module conjugué à M par g et l'action de H sur ${}^gM$ est donnée par $h \cdot {}^gm = {}^g\big(({}^{g^{-1}}h) \cdot m\big)$, $\forall\, m \in M$, $\forall\, h \in H$ et $\forall\, g \in G$.*

Lemme 5.3.4. *Soit $G = Q \rtimes P$ un groupe fini p-nilpotent, où Q est d'ordre premier à p et P est un p-sous-groupe de Sylow de G. Soit L un kQ-module simple, invariant par G et notons $\rho : Q \longrightarrow \mathrm{Aut}_k(L)$ la représentation irréductible associée. Alors il existe une unique extension $\tilde{\rho} : G \longrightarrow \mathrm{Aut}_k(L)$ de ρ, i.e. il existe une unique extension de l'action de Q sur L à G. A fortiori, à isomorphisme près, il existe un unique kG-module $\tilde{L}$ tel que $\tilde{L}{\downarrow}^G_Q \cong L$.*

Remarque 5.3.5. *Dans les hypothèses du lemme, le théorème III.3.16 de [Fe] démontre l'unicité, à isomorphisme près, du module $\tilde{L}$. Comme nous allons avoir besoin de l'unicité de l'extension de l'action $\tilde{\rho}$ définissant la structure de kG-module sur $\tilde{L}$, ce résultat n'est pas suffisant. Mentionnons aussi que pour la démonstration de l'unicité, nous utilisons les arguments de [Th2].*

Preuve. Prouvons l'existence de l'extension $\tilde{\rho}$ de ρ en commençant par montrer l'existence de l'extension $\tilde{L}$ de L. Si H est un groupe fini, on note $S_K(H)$, respectivement $S_k(H)$, l'ensemble des classes d'isomorphisme des KH-, respectivement kH-modules simples et $d_H : G_0(KH) \longrightarrow G_0(kH)$ l'homomorphisme de décomposition.

Comme p ne divise pas l'ordre de Q, kQ est semi-simple et on a une bijection $d : S_K(Q) \longrightarrow S_k(Q)$, induite par d_Q. Soit $L_K \in d^{-1}([L])$ l'unique KQ-module, à isomorphisme près, qui "relève" L en caractéristique 0. Alors L_K est invariant par G, car, comme ${}^gL \cong L$, on a ${}^gL_K \in d^{-1}([{}^gL]) = d^{-1}([L]) = [L_K]$. Par suite, on a ${}^gL_K \cong L_K$, $\forall\, g \in G$.

Puisque $|G/Q|$ et $|Q|$ sont premiers entre eux, L_K s'étend à G en un KG-module $\tilde{L}_K$ a fortiori simple (cf. théorème 22.3 de [Hu1]) et il existe un $\mathcal{O}G$-module $\mathcal{O}$-libre $L_\mathcal{O}$ tel que $\tilde{L}_K \cong K \otimes_\mathcal{O} L_\mathcal{O}$. Ainsi, $\tilde{L} = L_\mathcal{O}/\wp L_\mathcal{O}$ est un kG-module simple qui étend L, car on a

$$\tilde{L}{\downarrow}^G_Q \cong \big(L_\mathcal{O}{\downarrow}^G_Q\big)/\wp(L_\mathcal{O}{\downarrow}^G_Q) \quad \text{et} \quad K \otimes_\mathcal{O} (L_\mathcal{O}{\downarrow}^G_Q) \cong \tilde{L}_K{\downarrow}^G_Q \cong L_K.$$

D'où $\tilde{L}{\downarrow}^G_Q \in [L]$, i.e. $\tilde{L}$ étend L. Par conséquent, la représentation $\tilde{\rho}$ associée à $\tilde{L}$ vérifie $\tilde{\rho}{\downarrow}^G_Q = \rho$, ce qui prouve l'existence d'une extension de ρ à G.

Prouvons l'unicité de cette extension et, pour éviter toute confusion, notons V le k-espace vectoriel sous-jacent aux modules L et $\tilde{L}$ (car L et $\tilde{L}$, vus comme k-espaces vectoriels, sont identiques). Ainsi,

$$\rho : Q \longrightarrow \mathrm{Aut}_k(V) \quad \text{et} \quad \tilde{\rho} : G \longrightarrow \mathrm{Aut}_k(V)$$

sont les deux représentations irréductibles associées à L et $\tilde{L}$, respectivement, et on a, par hypothèse, $\tilde{\rho}{\downarrow}_Q^G = \rho$.

Soit $\hat{\rho} : G \longrightarrow \mathrm{Aut}_k(V)$ une représentation irréductible de G satisfaisant $\hat{\rho}{\downarrow}_Q^G = \rho$ et considérons l'application

$$\begin{aligned} s : G &\longrightarrow \mathrm{Aut}_{kQ}(V) \\ g &\longmapsto \hat{\rho}(g)\tilde{\rho}(g)^{-1}, \ \forall\, g \in G. \end{aligned}$$

On a $s(g) \in \mathrm{Aut}_k(V)$, $\forall\, g \in G$, car $\hat{\rho}(g)$, $\tilde{\rho}(g) \in \mathrm{Aut}_k(V)$, $\forall\, g \in G$ et donc s est bien définie. De plus, $s(g)$ est kQ-linéaire, car si $h \in Q$ et $v \in V$, alors on a pour tout $g \in G$:

$$s(g)(h \cdot v) = \hat{\rho}(g)\tilde{\rho}(g)^{-1}\big(\rho(h)(v)\big) = \hat{\rho}(g)\tilde{\rho}(g^{-1}hg)\tilde{\rho}(g)^{-1}(v) =$$

$$= \hat{\rho}(g)\hat{\rho}(g^{-1}hg)\tilde{\rho}(g)^{-1}(v) = \rho(h)\hat{\rho}(g)\tilde{\rho}(g)^{-1}(v) = h \cdot s(g)(v).$$

Par le lemme de Schur, comme ρ est irréductible et k est algébriquement clos, $\mathrm{Aut}_{kQ}(V)$ est isomorphe au groupe multiplicatif abélien k^*.

On a, $\forall\, g, h \in G$,

$$s(gh) = \hat{\rho}(g)\hat{\rho}(h)\tilde{\rho}(h)^{-1}\tilde{\rho}(g)^{-1} = \hat{\rho}(g)s(h)\tilde{\rho}(g)^{-1} =$$

$$= \hat{\rho}(g)\tilde{\rho}(g)^{-1}s(h) = s(g)s(h).$$

Ainsi, s est un homomorphisme de groupes. De plus, pour tout $g \in Q$, on a $s(g) = \hat{\rho}(g)\tilde{\rho}(g)^{-1} = \rho(g)\rho(g)^{-1} = 1$ et donc $Q \leq \mathrm{Ker}(s)$. En identifiant $\mathrm{Aut}_{kQ}(V)$ à k^*, s induit l'homomorphisme de groupes suivant.

$$\begin{aligned} \bar{s} : G/Q &\longrightarrow k^* \\ \bar{g} &\longmapsto s(g), \end{aligned}$$

Or G/Q est un p-groupe, puisqu'isomorphe à P, et k^* ne contient pas de racine p-ième non triviale de l'unité (car $X^p - 1 = (X-1)^p$ dans $k[X]$). Par suite, $\bar{s}$ ne peut être que l'homomorphisme trivial, c'est-à-dire

$$1 = \bar{s}(\bar{g}) = s(g) = \hat{\rho}(g)\tilde{\rho}(g)^{-1}, \ \forall\, g \in \bar{g} \in G/Q.$$

Par conséquent, on a $\hat{\rho} = \tilde{\rho}$ et donc l'extension $\tilde{\rho}$ de ρ est unique.

En termes de kG-modules, l'unicité de $\tilde{\rho}$ implique l'unicité à isomorphisme près de l'extension $\tilde{L}$ de L. D'où la dernière affirmation du lemme.

□

Appliquons ces résultats aux modules simples considérés dans le cas des groupes p-nilpotents $G = Q \rtimes P$ construits dans la section 5.2, avec P cyclique, quaternionien ou semidiédral. Soit m l'entier tel que $|Q| = q^{1+2m}$ et choisissons arbitrairement un kQ-module simple L de dimension q^m. Autrement dit,

$\dim L = q$, si $|Q| = q^3$ et P est cyclique ou quaternionien, et
$\dim L = q^2$, si $|Q| = q^5$ et P est semidiédral.

Notons ω la racine q-ième non triviale de l'unité satisfaisant $z \cdot l = \omega l,\ \forall\, l \in L$.

Lemme 5.3.6. *Dans ces hypothèses, il existe une unique extension à G de l'action de Q sur L. Par suite, L s'étend en un unique kG-module simple $\tilde{L}$, à isomorphisme près.*

Preuve. Par le lemme 5.3.4, il suffit de montrer que $L \cong {}^uL,\ \forall\, u \in P$. Or, $\forall\, u \in P$, les kQ-modules L et ${}^uL$ sont des modules simples de dimension q^m avec $m = 1$ ou 2. D'où ${}^uL \cong L$ si et seulement si $< {}^uL_K{\downarrow}^Q_{Q'}, L_K{\downarrow}^Q_{Q'} >= q^{2m}$, par le lemme 5.3.2. Comme $z \cdot l = \omega\, l\ ,\ \forall\, l \in L$, on a $\mathrm{Tr}(z^i, L_K) = q^m\omega^i,\ \forall\, 0 \leq i < q$. De plus, z est central et donc

$$z \cdot {}^ul = {}^u\big(({}^{u^{-1}}z) \cdot l\big) = {}^u(z \cdot l) = \omega({}^ul),\ \forall\ {}^ul \in {}^uL.$$

Par suite, $\mathrm{Tr}(z^i,\, {}^uL_K) = \mathrm{Tr}(z^i, L_K) = q^m\omega^i,\ \forall\, 0 \leq i < q$. D'où

$$< {}^uL_K{\downarrow}^Q_{Q'}, L_K{\downarrow}^Q_{Q'} >= \ q^{-1}\sum_{i=0}^{q-1} \mathrm{Tr}(z^i,\, {}^uL_K)\,\mathrm{Tr}(z^{-i}, L_K) =$$

$$= q^{-1}\sum_{i=0}^{q-1}(q^m\omega^i)(q^m\omega^{-i}) = q^{2m}.$$

Donc L est invariant par G, ce qui prouve le lemme.

□

Ainsi, pour tout groupe p-nilpotent G que nous avons construit, on considère un kG-module simple $\tilde{L}$ de dimension q^m, avec $m = 1$ ou 2 et l'action de G sur $\tilde{L}$ est déterminée de manière unique. De plus, comme $p \not| \dim \tilde{L}$, le kG-module $\tilde{L}$ est de vortex P (cf. proposition 1.2.5). Rappelons que l'on veut déterminer la source de $\tilde{L}$. Pour cela, on va considérer le kP-module $\tilde{L}{\downarrow}^G_P$ et utiliser le théorème IX.4.1 de [Fe], rappelé ci-dessous. Nous avons légèrement modifié l'énoncé originel, en remplaçant l'hypothèse "F est un corps de rupture pour G" par celle plus contraignante "F est algébriquement clos", car nous n'avons pas défini la première notion et car la situation que nous considérons satisfait les hypothèses de cette version du théorème.

Théorème 5.3.7. *Soient p un nombre premier, F un corps algébriquement clos de caractéristique p et G un groupe fini p-nilpotent, de la forme $H \rtimes P$, avec $p \not| |H|$ et P un p-sous-groupe de Sylow de G. Soit V un FH-module simple invariant par G. Alors V s'étend en un FG-module W de manière unique et $W{\downarrow}^G_P$ est un FP-module d'endo-permutation.*

Par suite, $\tilde{L}{\downarrow}^G_P$ est un kP-module d'endo-permutation couvert. A fortiori, la source S de $\tilde{L}$ est aussi un kP-module d'endo-permutation couvert. En effet, par définition, S est un facteur direct de $\tilde{L}{\downarrow}^G_P$. Donc $\mathrm{End}_k\, S$ est un kP-module

de permutation, car c'est un facteur direct d'un module de permutation (cf. lemme 1.2.2). De plus, $\tilde{L}\downarrow_P^G$ est couvert, car $\tilde{L}$ est de vortex P, et donc S est couvert. Relevons aussi que l'on avait déjà montré la première partie du théorème.

Remarque 5.3.8. *Le fait que la source de $\tilde{L}$ soit un kP-module d'endo-permutation est connu, comme nous l'avons mentionné en début de chapitre. En effet, dans le cadre plus général des groupes finis p-résolubles (qui inclut la famille des groupes finis p-nilpotents), le théorème 30.5 de [Th1] montre que la source d'un kG-module simple de vortex P est un kP-module d'endo-permutation, pour un p-sous-groupe P d'un groupe fini p-résoluble G. De plus, le théorème 8.39 et la remarque 8.41 de [Pu1] décrivent plus précisément ces sources, à savoir, ce sont les chapeaux de kP-modules de la forme $\bigotimes_{(Q/R)\in\mathcal{T}} \mathrm{Ten}_Q^P \mathrm{Inf}_{Q/R}^Q(M_{Q/R})$, où $M_{Q/R}$ est un $k[Q/R]$-module endo-trivial de torsion et où $\mathcal{T}$ est une famille de sections de P qui sont des groupes cycliques, quaternioniens ou semidiédraux.*

Ainsi, pour déterminer la source de $\tilde{L}$, on doit trouver un kP-module d'endo-permutation couvert indécomposable S tel que $\tilde{L}$ soit isomorphe à un facteur direct de $S\uparrow_P^G$ et tel que S soit isomorphe au chapeau du kP-module d'endo-permutation couvert $\tilde{L}\downarrow_P^G$.

Notation. On pose $X \mid Y$, si X et Y sont deux modules tels que X est isomorphe à un facteur direct de Y.

Par transitivité de la restriction, on a $\tilde{L}\downarrow_P^G = (\tilde{L}\downarrow_N^G)\downarrow_P^N$, où $N = N_G(P)$. Par la correspondance de Green (cf. paragraphe 20A de [CR]), on sait que $\tilde{L}\downarrow_N^G$ possède un unique facteur direct indécomposable M de vortex P, et donc $S \mid M\downarrow_P^N$, car S est de vortex P.

Comme $M \mid \tilde{L}\downarrow_N^G$, on a $\dim M \leq \dim \tilde{L} = q^m$, avec $m = 1$, si P est cyclique ou quaternionien, et $m = 2$, si P est semidiédral. D'autre part, on a aussi

$$\tilde{L}\downarrow_N^G \mid M\uparrow_N^G\downarrow_N^G \cong M \oplus \Bigg(\bigoplus_{g\in[N\backslash G/N],\, g\neq 1} \underbrace{{}^gM\downarrow_{g_{N\cap N}}^{g_N}\uparrow_{g_{N\cap N}}^N}_{(I)} \Bigg). \tag{5.3}$$

Par construction de G, les facteurs directs de (I) sont de vortex trivial (et donc des kN-modules projectifs) ou éventuellement de vortex cyclique d'ordre 2 et non normal dans P, si P est semidiédral (cf. section 5.2).

Rappelons que $N = Q' \times P$. Le lemme suivant montre que $M\downarrow_P^N$ est un kP-module indécomposable et donc isomorphe à S.

Lemme 5.3.9. *Soit $N = A \times P$ un groupe fini, où A est un groupe abélien d'ordre premier à p et P un p-groupe, et soit V un kN-module indécomposable. Alors, $V\downarrow_P^N$ est un kP-module indécomposable.*

Preuve. Comme A est un groupe d'ordre premier à p, l'algèbre de groupe kA est semi-simple et possède $|A|$ modules simples S_i, de dimension 1, puisque A est abélien.

On a donc un isomorphisme $V\downarrow_A^N \cong \bigoplus_{i=1}^{|A|} S_i^{n_i}$, pour des entiers positifs n_i et où $S_i^{n_i}$ est appelée la composante isotypique de $V\downarrow_A^N$ correspondant au kA-module simple S_i, pour tout i. Comme $\dim S_i = 1$, la représentation λ_i associée à S_i est de degré 1, i.e. les éléments a de A agissent par multiplication par un scalaire $\lambda_i(a)$ sur S_i.

Par ailleurs, le groupe N agit par permutation sur l'ensemble $\mathcal{S}$ des composantes isotypiques de $V\downarrow_A^N$. De plus, cette action est transitive, car V est indécomposable. Comme A agit trivialement sur $\mathcal{S}$, l'action de P sur $\mathcal{S}$ est transitive. Mais, comme P centralise A, l'action de P sur $\mathcal{S}$ est triviale. En effet, on a

$$a \cdot (u \cdot s) = (au) \cdot s = (ua) \cdot s = u \cdot (a \cdot s) = u \cdot (\lambda_i(a)s) = \lambda_i(a)(u \cdot s),\ \forall\, a \in A,$$

et donc $u \cdot s \in S_i,\ \forall\, u \in P$ et $\forall\, s \in S_i$. Par suite, $V\downarrow_A^N \cong S^n$ pour un kA-module simple S et un entier $n \in \mathbb{N}$.

Considérons les kN-modules indécomposables $V_A = k_\chi$ et $V_P = k_{\chi^{-1}} \otimes V$, sur lesquels N agit comme suit. Soit $g \in N$, disons $g = au$ pour un $a \in A$ et un $u \in P$. On a $g \cdot r = \chi(a)r,\ \forall\, r \in V_A$, et

$$g \cdot (r \otimes v) = (g \cdot r) \otimes (g \cdot v) = \chi^{-1}(a)r \otimes \chi(a)(u \cdot v) = r \otimes (u \cdot v),\ \forall\, r \otimes v \in V_P.$$

On remarque que P agit trivialement sur V_A, car $u \cdot r = r,\ \forall\, u \in P,\ \forall\, r \in k$. De même, A agit trivialement sur V_P, car $a \cdot (r \otimes v) = r \otimes v,\ \forall\, a \in A,\ \forall\, r \otimes v \in V_P$. De plus, $V \cong V_A \otimes V_P$ comme kN-modules, car $k \cong (k_\chi \otimes k_{\chi^{-1}})$ est un isomorphisme de kN-modules. Ainsi, $V\downarrow_P^N \cong V_A\downarrow_P^N \otimes V_P\downarrow_P^N \cong k \otimes V_P\downarrow_P^N \cong V_P\downarrow_P^N$. Or V_P est un kN-module indécomposable, car V l'est par hypothèse, et comme A agit trivialement sur V_P, la restriction $V_P\downarrow_P^N$ est indécomposable. Par conséquent, $V\downarrow_P^N$ est indécomposable.

□

Distinguons les cas suivant les différents p-groupes considérés.

5.3.1 Cas d'un groupe cyclique

Supposons P cyclique. Par le lemme 5.2.3, P est un sous-groupe de G d'intersection triviale et donc les facteurs directs apparaissant dans (I) sont projectifs et de dimension divisible par $|P|$. La relation 5.3 implique alors la congruence $\dim L \equiv \dim M \ (\mod |P|)$. Ainsi, comme $q \equiv -1 \ (\mod |P|)$, le lemme 5.3.9 implique la congruence $\dim S \equiv -1 \ (\mod |P|)$.

Or, $\Omega_P^1(k)$ est l'unique kP-module indécomposable de dimension congrue à -1 modulo $|P|$. On a donc $\dim S = |P| - 1$ et S est isomorphe à $\Omega_P^1(k)$.

5.3.2 Cas d'un groupe quaternionien

Supposons que P est un 2-groupe quaternionien. Par le lemme 5.2.3, P est un sous-groupe de G d'intersection triviale, pour les deux groupes 2-nilpotents construits et donc les facteurs directs de (I) sont projectifs et de dimension

divisible par l'ordre de P, comme dans le cas cyclique. De plus, la relation 5.3 donne la congruence $\dim L \equiv \dim M$ (mod $|P|$). On a ainsi

Si $q \equiv |P| - 1$ (mod $2|P|$), alors $\dim S \equiv -1$ (mod $|P|$).
Si $q \equiv \frac{|P|}{2} + 1$ (mod $|P|$), alors $\dim S \equiv \frac{|P|}{2} + 1$ (mod $|P|$).

Prouvons que S est endo-trivial dans les deux cas. Soit $n \geq 3$ et posons

$$P = <u, v \mid u^{2^{n-1}} = 1, u^{2^{n-2}} = v^2, {}^v u = u^{-1}> \quad \text{(et donc } |P| = 2^n)$$

et $w = u^{2^{n-2}}$ le générateur du centre Z de P (et unique élément d'ordre 2 de P). Notons

$$Q = <x, y \mid x^q = y^q = 1, \ {}^y x = x[y, x]> \text{ , et } z = [y, x] \text{ (générateur de } Q').$$

Par le lemme 1.2.11, il suffit de montrer que $S{\downarrow}_Z^P$ est endo-trivial. Pour ce faire, nous allons procéder comme suit, afin de déterminer l'action de Z sur $\tilde{L}$.

1. On définit une action $*$ de w sur $\tilde{L}$.
2. On vérifie que $*$ est compatible avec l'action $\cdot$ de Q sur $\tilde{L}$, c'est-à-dire

$$w * (g \cdot \xi) = {}^w g \cdot (w * \xi) \ , \ \forall \xi \in \tilde{L} \quad \text{et} \quad \forall g \in Q \ .$$

Ainsi, en définissant $(gw) * \xi = g \cdot (w * \xi)$, $\forall \xi \in \tilde{L}$ et $\forall g \in Q$, on obtient une action (notée $*$) du groupe $Q \rtimes Z$ sur $\tilde{L}$. Par unicité de l'extension de l'action définissant la structure de $k[Q \rtimes Z]$-module sur $\tilde{L}$ (cf. lemme 5.3.4), l'action que nous avons notée $*$ est cette unique action (notée $\cdot$) de $Q \rtimes Z$ sur $\tilde{L}$.

Commençons les calculs. Comme ceux-ci sont identiques pour les deux congruences de q, nous n'avons pas besoin de distinguer les deux cas.

Par construction de G (cf. paragraphe 5.2), il existe deux entiers positifs a et b, avec $0 \leq a, b < q$ et tels que ${}^w x = x^{-1} z^a$ et ${}^w y = y^{-1} z^b$. De plus, par construction de $\tilde{L}$, on sait que $\{y^i \otimes 1 \mid 0 \leq i < q\}$ est une k-base de $\tilde{L}$.

Pour le point 1, posons

$$w * y^i \otimes 1 = \omega^{(i-l)b} \big(y^{-i-a} \otimes 1\big), \ \forall 0 \leq i < q,$$

où l est l'unique entier entre 0 et $q-1$ tel que $2l \equiv -a$ (mod q). On a :

$$w^2 * y^i \otimes 1 = w * \big(\omega^{(i-l)b} (y^{-i-a} \otimes 1)\big) = \omega^{(i-l)b + (-i-a-l)b} y^i \otimes 1 = \omega^{(-a-2l)b} y^i \otimes 1,$$

et donc $w^2 * y^i \otimes 1 = y^i \otimes 1$, $\forall 0 \leq i < q$, par choix de l. Vérifions le point 2.

$$ {}^w x \cdot (w * y^i \otimes 1) = x^{-1} z^a (w * y^i \otimes 1) = \omega^{(i-l)b+a} x^{-1} \cdot y^{-i-a} \otimes 1 =$$

$$= \omega^{(i-l)b+a} y^{-i-a} \otimes (x^{-1} z^{i+a} \cdot 1) = \omega^{(i-l)b-i} y^{-i-a} \otimes 1.$$

D'autre part,

$$w * (x \cdot y^i \otimes 1) = w * y^i \otimes (x z^{-i} \cdot 1) = \omega^{-i} w * y^i \otimes 1 = \omega^{(i-l)b-i} y^{-i-a} \otimes 1.$$

Ainsi, ${}^w x \cdot (w * y^i \otimes 1) = w * (x \cdot y^i \otimes 1)$. De même, on a :

$$ {}^w y \cdot (w * y^i \otimes 1) = y^{-1} z^b \cdot (\omega^{(i-l)b} y^{-i-a} \otimes 1) = \omega^{(i-l)b+b} y^{-i-a-1} \otimes 1,$$

et d'autre part, $w * (y \cdot y^i \otimes 1) = w * y^{i+1} \otimes 1 = \omega^{(i+1-l)b} y^{-i-1-a} \otimes 1$. D'où l'égalité ${}^w y \cdot (w * y^i \otimes 1) = w * (y \cdot y^i \otimes 1)$ et donc le point 2 est satisfait. Comme rappelé ci-dessus, il existe une unique extension à $Q \rtimes Z$ de l'action de Q sur L et donc $*$ et $\cdot$ désignent la même action (que nous allons dorénavant noter $\cdot$).

Maintenant, on peut aisément expliciter $S{\downarrow}_Z^P$. Remarquons que

$$ w \cdot y^i \otimes 1 \neq y^i \otimes 1, \ \forall\, 0 \leq i < q \ , \text{ si } i \neq l, \quad \text{et} \quad w \cdot y^l \otimes 1 = y^l \otimes 1 \ .$$

Autrement dit, il y a un vecteur de la k-base $\{y^i \otimes 1 \mid 0 \leq i < q\}$ de $\tilde{L}$ fixe par Z (c'est-à-dire un vecteur propre pour la valeur propre 1).

Pour tous les indices i compris strictement entre l et $\frac{q-1+2l}{2}$, considérons les $\frac{q-1}{2}$ k-sous-espaces $W_i = k<y^i \otimes 1, y^{-i-a} \otimes 1>$. Ceux-ci sont invariants par Z et Z agit librement sur chacun, par définition de l'action de w sur $\tilde{L}$. Ce sont donc des kZ-sous-modules libres de rang 1. Par suite, leur somme W est directe et forme un kZ-sous-module libre facteur direct de $\tilde{L}$ de codimension 1. De plus, $k<y^l \otimes 1>$ est un supplémentaire de W. On en déduit que $\tilde{L}{\downarrow}_Z^G$ se décompose comme somme directe $k \oplus (kZ)^{\frac{q-1}{2}}$.

Par conséquent, comme S est de vortex P et $S \,|\, \tilde{L}{\downarrow}_P^G$, on a, par le théorème de Krull-Schmidt, $S{\downarrow}_Z^P \cong k \oplus S'$, pour un kZ-module libre S', de rang $\leq \frac{q-1}{2}$. Par suite, S est endo-trivial.

Par la section 6 de [CaTh1], on sait qu'on a huit kP-modules endo-triviaux indécomposables de vortex P, à isomorphisme près. Les dimensions de ceux-ci permettent, en particulier, de connaître l'ordre de leur classe d'équivalence dans $D(P)$ et nous permettent de déterminer un ensemble de modules dont les classes engendrent tout $T(P)$. En effet, à isomorphisme près, on a :

- les deux modules endo-triviaux indécomposables $\Omega_P^1(k)$ et son dual $\Omega_P^3(k)$, de dimension $|P|-1$ et d'ordre 4 ;
- le module $\Omega_P^2(k)$ (auto-dual), de dimension $|P|+1$ et d'ordre 2 ;
- deux modules de dimension $\frac{|P|}{2}+1$ et d'ordre 2 : un kP-module endo-trivial indécomposable "exceptionnel" V et son dual ;
- les deux modules $\Omega_P^1(V)$ et son dual, de dimension $\frac{|P|}{2}-1$ et d'ordre 4 ;
- et, bien entendu, le module trivial, de dimension 1.

En comparant S aux modules de cette liste, on tire les conclusions suivantes.

- Pour $q \equiv |P|-1 \ (\mod\ 2|P|)$, on a $\dim S = |P|-1$. Donc S est isomorphe soit à $\Omega_P^1(k)$, soit à $\Omega_P^3(k)$, et $[S]$ est d'ordre 4 dans $D(P)$.
- Pour $q \equiv \frac{|P|}{2}+1 \ (\mod\ |P|)$, on a $\dim S = \frac{|P|}{2}+1$. Donc S est isomorphe soit à V, soit à son dual, et $[S]$ est d'ordre 2 dans $D(P)$.

Remarque 5.3.10. *On retiendra, en particulier, que les classes des deux modules réalisés engendrent tout $T(P)$ (cf. section 6 de [CaTh1]).*

5.3.3 Cas d'un groupe semidiédral

Soit $P = <u, v \mid u^{2^{n-1}} = v^2 = 1, {}^v u = u^{2^{n-2}-1}>$ un groupe semidiédral d'ordre 2^n et notons $w = u^{2^{n-2}}$ le générateur du centre Z de P, $R = <u^2, uv>$ le sous-groupe quaternionien d'indice 2 dans P et $E = <v, w>$ l'unique sous-groupe abélien élémentaire de rang 2 de P, à conjugaison près. On a, selon les notations de la section 5.2, un groupe fini 2-nilpotent $G = Q \rtimes P$, où Q est un q-groupe extraspécial d'ordre q^5 et d'exposant q, pour un nombre premier q tel que $q \equiv \frac{|P|}{2} - 1 \ (\mod |P|)$.

Par le lemme 5.2.4, P n'est pas un sous-groupe de G d'intersection triviale, car ${}^g P \cap P$ peut être cyclique d'ordre 2, conjugué à $<v>$. Il s'ensuit que les facteurs directs de (I) sont de vortex trivial ou cyclique d'ordre 2 et donc de dimension divisible par $\frac{|P|}{2}$. D'où, $\dim \tilde{L} \equiv \dim M \ (\mod \frac{|P|}{2})$, par la relation 5.3. Comme $q^2 \equiv 1 - |P| \ (\mod 2|P|)$, on a $\dim S \equiv 1 \ (\mod \frac{|P|}{2})$.

On va montrer que S est isomorphe au kP-module $V = \Omega^1_P\big(\Omega^1_{P/<v>}(k)\big)$. Par le paragraphe 7 de [CaTh1], on sait que :

$$V \text{ est endo-trivial, de dimension } \frac{|P|}{2} + 1 \ , \quad \text{et que}$$
$$\Omega^2_R(k) \,|\, V{\downarrow}^P_R \quad \text{et} \quad k \,|\, V{\downarrow}^P_E \ .$$

Ainsi, par l'assertion 2 du théorème 1.5.5, il nous suffit de vérifier que $\Omega^2_R(k) \,|\, S{\downarrow}^P_R$ et que $S{\downarrow}^P_E$ est un kE-module endo-trivial avec $k \,|\, S{\downarrow}^P_E$. Commençons par rappeler l'action de Q sur L (cf. section 5.3), où Q est le produit central $Q_1 * Q_2$ et où Q_i est engendré par x_i et par y_i satisfaisant $z = [y_i, x_i]$, pour $i = 1$ et 2 (z étant le générateur du centre Q' de Q). L'ensemble

$$\mathcal{L} = \{T_{i,j} \mid \ 0 \leq i, j < q\} \text{ est une } k\text{-base de } L, \text{ où } T_{i,j} = y_1^i y_2^j \otimes 1 \ , \ 0 \leq i, j < q.$$

L'action de Q sur L est alors donnée, $\forall\, 0 \leq i, \ j < q$, par

$$x_1 \cdot T_{i,j} = \omega^{-i} T_{i,j} \ , \ x_2 \cdot T_{i,j} = \omega^{-j} T_{i,j} \ , \ y_1 \cdot T_{i,j} = T_{i+1,j} \text{ et } y_2 \cdot T_{i,j} = T_{i,j+1} \ .$$

Considérons les kQ_i-modules simples L_i de dimension q, construits selon la méthode employée pour le cas d'un 2-groupe quaternionien d'ordre $\frac{|P|}{2}$, avec $q \equiv \frac{|P|}{2} - 1 \ (\mod |P|)$ et à partir de la même racine q-ième de l'unité ω que pour L, pour $i = 1$ et 2. Formons le produit tensoriel $X = L_1 \otimes L_2$ (sur k) et munissons ce k-espace vectoriel de dimension q^2 d'une structure de kQ-module comme suit. Tout élément de Q peut s'écrire $g_1 g_2$, avec $g_i \in Q_i$, et, par définition du produit central, $g_1 g_2 = h_1 h_2$ si et seulement s'il existe un élément central $z' \in Q'$ tel que $g_1 = h_1 z'$ et $g_2 = h_2 z'^{-1}$. Posons alors

$$g_1 g_2 \cdot l_1 \otimes l_2 = g_1 \cdot l_1 \otimes g_2 \cdot l_2, \ \forall\, g_i \in Q_i \quad \text{et} \quad \forall\, l_i \in L_i \ , \ i = 1, 2.$$

Cette définition ne dépend pas de l'écriture $g_1 g_2$. En effet, $g_1 g_2 = h_1 h_2$ si et seulement s'il existe un entier a tel que $g_1 = h_1 z^a$ et $g_2 = h_2 z^{-a}$. On a alors

$$g_1 g_2 \cdot l_1 \otimes l_2 = h_1 z^a \cdot l_1 \otimes h_2 z^{-a} \cdot l_2 = \omega^a \omega^{-a} (h_1 \cdot l_1 \otimes h_2 \cdot l_2) = h_1 h_2 \cdot l_1 \otimes l_2.$$

L'égalité suivante montre que X est un kQ-module de dimension q^2.

$$(g_1g_2\ h_1h_2)\cdot l_1\otimes l_2 = g_1g_2\cdot(h_1h_2\cdot l_1\otimes l_2),\ \forall\, g_i,h_i\in Q_i,\ \forall\, l_i\in L_i,\ i=1,2.$$

L'ensemble $\mathcal{X}=\{Y_{i,j}\mid 0\leq i,\ j<q\}$ de X, où $Y_{i,j}=(y_1^i\otimes 1)\otimes(y_2^j\otimes 1)$, pour tous $0\leq i,\ j<q$, est une k-base de X. Posons $\phi : X\longrightarrow L$ l'isomorphisme de k-espaces vectoriels défini sur les bases $\mathcal{X}$ et $\mathcal{L}$ de X et de L respectivement par $\phi(Y_{i,j})=T_{i,j}$, $\forall\, 0\leq i,\ j<q$. En fait, ϕ est un isomorphisme de kQ-modules, car

$$\phi(g\cdot Y_{i,j}) = g\cdot T_{i,j} = g\cdot\phi(Y_{i,j})\ ,\ \forall\, g\in Q\ ,\ \forall\, 0\leq i,\ j<q\ .$$

En effet, on a $\phi(x_1\cdot Y_{i,j})=\omega^{-i}T_{i,j}=x_1\cdot\phi(Y_{i,j})$, $\forall\, 0\leq i,\ j<q$ et on vérifie de même $\phi(g\cdot Y_{i,j})=g\cdot\phi(Y_{i,j})$, $\forall\, g\in\{x_2,\ y_1,\ y_2\}$ et $\forall\, 0\leq i,\ j<q$. Par suite, X est un kQ-module simple (car L est simple) et X s'étend en un kG-module simple $\tilde{X}$ (avec k-base $\mathcal{X}$) isomorphe à $\tilde{L}$, et sur lequel l'action de G est définie de manière unique. Plus précisément, on peut décrire cette action à l'aide de l'action $\cdot$ de G sur $\tilde{L}$ comme suit :

$$g\cdot Y_{i,j}=\phi^{-1}\big(g\cdot\phi(Y_{i,j})\big)\ ,\ \forall\, Y_{i,j}\in\mathcal{X}\text{ et }\forall\, g\in G\ .$$

Ainsi, dorénavant, on identifiera $\tilde{X}$ avec $\tilde{L}$, en utilisant ϕ (que l'on n'écrira pas, pour ne pas surcharger les notations). Nous allons immédiatement justifier l'introduction de $\tilde{X}$ dans les calculs suivants, où nous allons déterminer explicitement l'action du sous-groupe E sur $\tilde{X}$. L'avantage d'utiliser $\tilde{X}$ au lieu de $\tilde{L}$ réside dans le fait que l'on peut se ramener au cas d'un groupe quaternionien, précédemment traité.

Rappelons que l'on veut montrer (moyennant l'identification entre $\tilde{X}$ et $\tilde{L}$) que $\tilde{X}\downarrow_E^G$ est un kE-module endo-trivial avec $k\,|\,\tilde{X}\downarrow_E^G$, où $E=<w,v>$ est l'unique sous-groupe abélien élémentaire de P de rang 2, à conjugaison près. Pour ce faire, nous allons procéder exactement comme dans le cas quaternionien, afin de trouver l'action de E sur $\tilde{X}$. Autrement dit :

1. On définit une action $*$ de E sur $\tilde{X}$.
2. On vérifie que $*$ est compatible avec l'action $\cdot$ de Q sur $\tilde{X}$, c'est-à-dire

$$s*(g\cdot\xi)={}^sg\cdot(s*\xi)\ ,\ \forall\,\xi\in\tilde{X}\ ,\ \forall\, s\in E\quad\text{et}\quad\forall\, g\in Q\ .$$

On obtient alors une action $*$ de $Q\rtimes E$ sur $\tilde{X}$, donnée par

$$(gs)*\xi=g\cdot(s*\xi)\ ,\ \forall\,\xi\in\tilde{X}\ ,\ \forall\, s\in E\quad\text{et}\quad\forall\, g\in Q\ .$$

Par le lemme 5.3.4, l'extension de l'action définissant la structure de $k[Q\rtimes E]$-module de $\tilde{X}$ est unique et donc $*$ et $\cdot$ désignent la même action, d'où le résultat cherché, à savoir la description de l'action $\cdot$ de E sur $\tilde{X}$ (et donc sur $\tilde{L}$).

Posons

$$v*Y_{i,j}=Y_{j,i}\quad\text{et}\quad w*Y_{i,j}=\omega^{(i+j+a)b}Y_{-i-a,-j-a},\ \forall\, 0\leq i,j<q,$$

où $a,\ b$ et l sont les entiers satisfaisant

$$0 \leq a,\ b,\ l < q\ ,\ {}^{w}x_i = x_i^{-1}z^a\ ,\ {}^{w}y_i = y_i^{-1}z^b,\ i = 1,2 \quad \text{et} \quad 2l \equiv -a\ (\ \mathrm{mod}\ q)$$

et les indices sont considérés modulo q (cf. section 5.3.2). Rappelons encore que la définition de la conjugaison par v dans G sur les générateurs de Q est donnée par ${}^{v}x_1 = x_2,\ {}^{v}x_2 = x_1,\ {}^{v}y_1 = y_2$ et ${}^{v}y_2 = y_1$. Vérifions à présent le point 1.

$$v^2 * Y_{i,j} = v * Y_{ji} = Y_{i,j} = \omega^{(i+j+a)b} w * Y_{-i-a,-j-a} = w^2 * Y_{i,j} \quad \text{et}$$
$$v * w * Y_{i,j} = \omega^{(i+j+a)b} Y_{-j-a,-i-a} = w * v * Y_{i,j},\ \forall\, Y_{i,j} \in \mathcal{X}\ .$$

Vérifions le point 2. On a, $\forall\, Y_{i,j} \in \mathcal{X}$,

$${}^{v}x_1 \cdot (v * Y_{i,j}) = x_2 \cdot Y_{j,i} = \omega^{-i} Y_{j,i} = v * (x_1 \cdot Y_{i,j}) \quad \text{et}$$

$$\begin{aligned} &{}^{w}x_1 \cdot (w * Y_{i,j}) = x_1^{-1}z^a \cdot (\omega^{(i+j+a)b} Y_{-i-a,-j-a}) = \\ &= \omega^{a+(i+j+a)b} x_1^{-1} \cdot Y_{-i-a,-j-a} = \omega^{-i+(i+j+a)b} Y_{-i-a,-j-a} = \\ &= \omega^{-i} w * Y_{i,j} = w * (x_1 \cdot Y_{i,j})\ . \end{aligned}$$

De même on vérifie ces égalités en remplaçant x_1 par x_2, par y_1 et par y_2. Donc le point 2 et satisfait et on en déduit que l'action $*$ de $Q \rtimes E$ sur $\tilde{X}$ coïncide avec l'action $\cdot$ cherchée. Avant d'étudier $S{\downarrow}_E^P$, on va utiliser les deux lemmes suivants pour montrer que S est un kP-module endo-trivial.

Lemme 5.3.11. *$\tilde{X}{\downarrow}_E^G$ est égal au KE-module*

$$k \oplus \big(k[E/{<}v{>}]\big)^{\frac{q-1}{2}} \oplus \big(k[E/{<}vw{>}]\big)^{\frac{q-1}{2}} \oplus (kE)^{(\frac{q-1}{2})^2}.$$

Preuve. Considérons les k-sous-espaces vectoriels de $\tilde{X}$ suivants (où la notation $[\alpha]$ désigne la partie entière d'un nombre réel α) :

$$k{<}Y_{l,l}{>};\quad W_i = k{<}Y_{i,i}, \omega^{(2i+a)b} Y_{l-i,l-i}{>},\ \forall\ \left[\frac{l+1}{2}\right] \leq i \neq l \leq \left[\frac{q+l}{2}\right];$$

$$W_i' = k{<}Y_{l+i,l-i}, Y_{l-i,l+i}{>},\ \forall\, 0 < i \leq \frac{q-1}{2};$$

$$W_{ij} = k{<}Y_{i,j}, Y_{j,i}, \omega^{(i+j+a)b} Y_{-i-a,-j-a}, \omega^{(i+j+a)b} Y_{-j-a,-i-a}{>},$$

$\forall\, 0 \leq i,j < q$, avec $i \neq j$ et $i + j \neq -a$. On dénombre ainsi $\frac{q-1}{2}$ sous-espaces W_i et W_i' distincts et $(\frac{q-1}{2})^2$ sous-espaces W_{ij} distincts. Ce sont des kE-sous-modules de permutation de $\tilde{X}$. En effet :

- $k{<}Y_{l,l}{>}$ est isomorphe au kE-module trivial.
- W_i est isomorphe à $k{<}Y_{i,i}{>}{\uparrow}_{<v>}^E \cong k[E/{<}v{>}]$ comme kE-module, car v agit trivialement sur W_i et w permute $Y_{i,i}$ et $\omega^{(2i+a)b} Y_{l-i,l-i}$, pour tout entier i tel que $\left[\frac{l+1}{2}\right] \leq i \neq l \leq \left[\frac{q+l}{2}\right]$.
- De même, W_i' est isomorphe comme kE-module à $k[E/{<}vw{>}]$, pour tout $0 < i \leq \frac{q-1}{2}$.

– W_{ij} est un kE-module isomorphe à $k{<}Y_{i,j}{>}\uparrow_1^E$ et donc libre de rang 1, $\forall\, 0 \leq i,j < q$, avec $i \neq j$ et $i+j \neq -a$.

Le kE-sous-module de $\tilde{X}$ engendré par les sous-modules $k{<}Y_{l,l}{>}$, W_i, W_i' et W_{ij} est une somme directe. En effet, il possède une k-base obtenue en partitionnant, selon les sous-modules sus-cités, une k-base de $\tilde{X}$, construite en modifiant les éléments de la base $\mathcal{X}$ par des scalaires. De plus, la dimension de cette somme directe vaut

$$1 + (\frac{q-1}{2}) \cdot 2 + (\frac{q-1}{2}) \cdot 2 + (\frac{q-1}{2})^2 \cdot 4 = q^2 = \dim \tilde{X} \ .$$

D'où une égalité de kE-modules entre $X{\downarrow}_E^G$ et

$$k \oplus \big(k[E/{<}v{>}]\big)^{\frac{q-1}{2}} \oplus \big(k[E/{<}vw{>}]\big)^{\frac{q-1}{2}} \oplus (kE)^{(\frac{q-1}{2})^2}.$$

□

En particulier, on en déduit un isomorphisme $\tilde{X}{\downarrow}_Z^G \cong k \oplus \big(kZ\big)^{(\frac{q^2-1}{2})}$ de kZ-modules et donc on a $S{\downarrow}_Z^G \cong k \oplus F$, où $Z = {<}w{>}$ est le centre de P et F un kZ-module libre.

Lemme 5.3.12. *Soit P un 2-groupe semidiédral de centre Z et M un kP-module d'endo-permutation indécomposable de vortex P. Supposons que la restriction $M{\downarrow}_Z^P$ est un kZ-module endo-trivial. Alors M est un kP-module endo-trivial.*

Preuve. Comme M est indécomposable et couvert, M est endo-trivial si et seulement si $\mathrm{Def}_{N_P(Q)/Q}^{N_P(Q)} \mathrm{Res}_{N_P(Q)}^P([M]) = [k]$, pour tout sous-groupe non trivial Q de P, par le théorème 1.5.5.

Soit Q un sous-groupe non trivial de P, alors soit Q contient Z, soit Q appartient à l'unique classe de conjugaison de sous-groupes cycliques d'ordre 2 non centraux de P. Dans ce cas, le normalisateur $N_P(Q)$ de Q est abélien élémentaire d'ordre 4. En effet, on a $N_P(Q) = C_P(Q)$, car Q est cyclique d'ordre 2 et il découle immédiatement des relations de P que $C_P(Q) = QZ$. Par conséquent, $N_P(Q)/Q$ est cyclique d'ordre 2 et $D(N_P(Q)/Q) = \{[k]\}$. Il s'ensuit que $\mathrm{Def}_{N_P(Q)/Q}^{N_P(Q)} \mathrm{Res}_{N_P(Q)}^P([M]) = [k]$.

Supposons que Q contient Z. Alors

$$\mathrm{Def}_{N_P(Q)/Q}^{N_P(Q)} \mathrm{Res}_{N_P(Q)}^P = \mathrm{Def}_{N_P(Q)/Q}^{N_P(Q)/Z} \mathrm{Res}_{N_P(Q)/Z}^{P/Z} \mathrm{Def}_{P/Z}^P \, .$$

Par hypothèse, $M{\downarrow}_Z^P$ est isomorphe à $k \oplus F$, pour un kZ-module libre F. Donc, si $A = \mathrm{End}_k M$, alors A est isomorphe à $k \oplus F'$ comme kZ-module, pour un kZ-module libre F'. Par suite, $\mathrm{Def}_{P/Z}^P([A]) = [A^Z/A_1^Z] = [k] = [\mathrm{End}_k k]$ et donc $\mathrm{Def}_{P/Z}^P([M]) = [k]$, par définition (cf. chapitre 1). A fortiori, on a $\mathrm{Def}_{N_P(Q)/Q}^{N_P(Q)/Z} \mathrm{Res}_{N_P(Q)/Z}^{P/Z} \mathrm{Def}_{P/Z}^P([M]) = [k]$. Donc M est endo-trivial.

□

Considérons $S{\downarrow}_R^P$. Par transitivité de la restriction, on a

$$\tilde{X}{\downarrow}_R^G \cong (\tilde{L}_1 \otimes \tilde{L}_2){\downarrow}_R^H \cong (\tilde{L}_1{\downarrow}_R^{H_1}) \otimes (\tilde{L}_2{\downarrow}_R^{H_2}) \ .$$

Par le cas quaternionien précédemment traité, on sait que $\tilde{L}_i\downarrow_R^{H_i}$ est un kR-module d'endo-permutation couvert, dont le chapeau S_i est isomorphe à $\Omega_R^1(k)$ ou à $\Omega_R^3(k)$, pour $i=1$ et 2. Montrons que $S_1\cong S_2$.

Dans la section 5.2, on avait considéré deux isomorphismes de groupes dont il convient à présent de rappeler la définition. On avait appelé θ l'isomorphisme de Q_1 vers Q_2, envoyant x_1 sur x_2 et y_1 sur y_2 (et donc $\theta(z)=z$), et λ l'automorphisme de R, envoyant u^2 sur $(u^2)^{-1}$ et (uv) sur $(u^2)^{2^{n-3}-1}(uv)$. Soit alors φ l'isomorphisme de groupes de H_1 vers H_2, envoyant hs sur $\theta(h)\lambda(s)$, pour tout $h\in Q_1$ et pour tout $s\in R$, et notons $\mathrm{Res}_\varphi(\tilde{L}_2)$ le kH_1-module obtenu par restriction de $\tilde{L}_2$ par φ, c'est-à-dire où $g\cdot l$ est défini comme l'élément $\varphi(g)\cdot l$, pour l'action d'origine de H_2 sur $\tilde{L}_2$, pour tout $g\in H_1$ et pour tout $l\in\mathrm{Res}_\varphi(\tilde{L}_2)$.

On a

$$\mathrm{Tr}(z^i,\mathrm{Res}_\varphi(\tilde{L}_2)\downarrow_{Q'}^{H_1})=\mathrm{Tr}(\varphi(z^i),\tilde{L}_2\downarrow_{Q'}^{H_2})=\mathrm{Tr}(z^i,\tilde{L}_2\downarrow_{Q'}^{H_2})=q\omega^i=\mathrm{Tr}(z^i,\tilde{L}_1\downarrow_{Q'}^{H_1}),$$

pour tout $0\leq i\leq q-1$. D'où, $<\mathrm{Res}_\varphi(\tilde{L}_2)\downarrow_{Q'}^{H_1},\tilde{L}_1\downarrow_{Q'}^{H_1}>=q^2$ et donc les kH_1-modules $\mathrm{Res}_\varphi(\tilde{L}_2)$ et $\tilde{L}_1$ sont isomorphes, par le lemme 5.3.2.

Par suite, on a $\tilde{L}_1\downarrow_R^{H_1}\cong\big(\mathrm{Res}_\varphi(\tilde{L}_2)\big)\downarrow_R^{H_1}\cong\mathrm{Res}_\lambda(\tilde{L}_2\downarrow_R^{H_2})$, car la restriction de φ à R est λ. Considérons alors le diagramme commutatif de kR-modules (où les lignes sont exactes)

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \Omega_R^1(k) & \longrightarrow & kR & \longrightarrow & k & \longrightarrow & 0\\
 & & \lambda\downarrow & & \lambda\downarrow & & \mathrm{Id}\downarrow & & \\
0 & \longrightarrow & \Omega_R^1(k) & \longrightarrow & kR & \longrightarrow & k & \longrightarrow & 0
\end{array}$$

On en déduit que $\mathrm{Res}_\lambda(\Omega_R^1(k))$ est isomorphe à $\Omega_R^1(k)$ et plus généralement que $\mathrm{Res}_\lambda(\Omega_R^n(k))$ est isomorphe à $\Omega_R^n(k)$, pour tout entier n (et pour tout automorphisme λ de R). Par conséquent, on a $\mathrm{Res}_\lambda(\tilde{L}_2\downarrow_R^{H_2})\cong\tilde{L}_2\downarrow_R^{H_2}$. Il s'ensuit que $\tilde{L}_1\downarrow_R^{H_1}\cong\tilde{L}_2\downarrow_R^{H_2}$ et donc $S_1\cong S_2$. En particulier, on en déduit que $\Omega_R^2(k)$ est isomorphe à un facteur direct de $S_1\otimes S_2$ et donc on a $\Omega_R^2(k)\,|\,\tilde{X}\downarrow_R^G$. Ainsi, $\tilde{X}\downarrow_R^G\in[\Omega_R^2(k)]$, car $\tilde{X}\downarrow_R^G$ est un kR-module d'endo-permutation couvert. En effet, $\tilde{X}\downarrow_P^G$ est un kP-module d'endo-permutation, par le théorème 5.3.7 et il est couvert, car $\tilde{X}$ est de vortex P. De plus, la restriction de P à R induit un homomorphisme entre $D(P)$ et $D(R)$ (cf. section 1.5).

Résumons la situation. Comme S est un kP-module d'endo-permutation couvert indécomposable et comme $S\downarrow_Z^P\cong k\oplus F$, le lemme 5.3.12 implique que S est endo-trivial. De plus, comme $S\downarrow_E^P\,|\,\tilde{X}\downarrow_E^G$, le lemme 5.3.11 implique que $S\downarrow_E^P$ a un facteur direct trivial. Ainsi, S est un kP-module endo-trivial dont les restrictions aux sous-groupes R et E de P sont dans les classes de $\Omega_R^2(k)$ et k respectivement. Par injectivité de la restriction $T(P)\longrightarrow T(R)\oplus T(E)$ (cf. théorème 1.5.5), on conclut, comme souhaité, que S est isomorphe au kP-module endo-trivial $\Omega_P^1\big(\Omega_{P/<v>}^1(k)\big)$ de dimension $\frac{|P|}{2}+1$.

Nous avons ainsi réalisé explicitement quelques exemples de modules d'endo-permutation comme sources de modules simples pour des groupes finis p-nilpotents. A présent, au lieu de continuer au cas par cas, nous allons nous constituer

une sorte de "boîte-à-outils", qui nous permettra de réaliser beaucoup d'autres modules comme sources, à partir de situations connues. Commençons par décrire l'outil induit par l'opération d'inflation.

5.4 Inflation

Soient p un nombre premier, P un p-groupe fini et P' un sous-groupe normal de P. Notons $\bar{P}$ le quotient P/P'. Soit M un $k\bar{P}$-module d'endo-permutation indécomposable couvert tel que l'on sait construire un groupe fini p-nilpotent G avec $\bar{P}$ comme p-sous-groupe de Sylow et un kG-module simple L dont la source est isomorphe à M. Nous allons montrer qu'on peut alors réaliser explicitement le kP-module d'endo-permutation indécomposable $\mathrm{Inf}_{\bar{P}}^{P} M$ comme source d'un kG'-module simple L', pour un groupe fini p-nilpotent G'.

Par hypothèse, G est de la forme $Q \rtimes \bar{P}$ pour un groupe fini Q d'ordre premier à p et on a un homomorphisme de groupes $\sigma : \bar{P} \longrightarrow \mathrm{Aut}(Q)$. Considérons l'application $\sigma' : P \longrightarrow \mathrm{Aut}(Q),\ u \mapsto \sigma(\bar{u})$, où $\bar{u}$ désigne la classe de u dans $\bar{P}$, pour tout $u \in P$. On a en particulier $\sigma'(u) = \mathrm{Id}_Q,\ \forall\, u \in P'$. De plus, comme σ est un homomorphisme de groupes, σ' l'est aussi et donc, par définition du produit semi-direct, on obtient un groupe p-nilpotent $G' = Q \rtimes P$ avec P comme p-sous-groupe de Sylow.

Le sous-groupe $\{1\} \times P'$ est normal dans G' et le quotient $G'\big/\big(\{1\} \times P'\big)$ est isomorphe à G. Soit alors $L' = \mathrm{Inf}_{G}^{G'} L$ le kG'-module obtenu par inflation de G à G' (cf. section 1.5). Le kG'-module L' est simple. En effet, si N' est un sous-module non nul de L' et si on identifie G au quotient $G'\big/\big(\{1\} \times P'\big)$, alors on obtient un sous-module N non nul de L. Par simplicité de L, on a $N = L$ et donc $N' = L'$ est un kG'-module simple, de même dimension que L. Or, L est de vortex $\bar{P}$, car sa dimension est première à p (cf. proposition 1.2.5), et donc L' est de vortex P.

Par hypothèse, on a $M \,|\, L\downarrow_{\bar{P}}^{G}$ et donc $\mathrm{Inf}_{\bar{P}}^{P} M \,|\, \mathrm{Inf}_{\bar{P}}^{P}(L\downarrow_{\bar{P}}^{G}) \cong L'\downarrow_{P}^{G'}$. En d'autres termes, comme $\mathrm{Inf}_{\bar{P}}^{P} M$ est un kP-module d'endo-permutation indécomposable (cf. proposition 3.17 de [Da1]), $\mathrm{Inf}_{\bar{P}}^{P} M$ est isomorphe à la source du kG'-module simple L'.

5.5 Induction tensorielle

Soient p un nombre premier, P un p-groupe fini, C un sous-groupe de P et M un kC-module d'endo-permutation indécomposable de vortex C, tel que l'on sait explicitement construire un kG-module simple L de source M, pour un groupe fini p-nilpotent G de la forme $Q \rtimes C$, avec C comme p-sous-groupe de Sylow et Q d'ordre premier à p. Supposons également que la restriction $L\downarrow_{Q}^{G}$ est un kQ-module simple. Dans ce paragraphe, nous allons réaliser l'unique facteur direct indécomposable de vortex P de $\mathrm{Ten}_{C}^{P} M$ comme source d'un module simple pour un groupe fini p-nilpotent, ayant P comme p-sous-groupe de Sylow.

Soit $[P/C] = \{v_0, \ldots, v_r\}$ un système de représentants des classes à gauche de P/C, avec $r = |P : C| - 1$. Sans limiter la généralité, on peut supposer $v_0 = 1$.

Pour tout $0 \leq i \leq r$, on définit formellement un groupe ${}^{v_i}Q = \{ {}^{v_i}g \mid g \in Q\}$, où la loi de composition est donnée par ${}^{v_i}g\, {}^{v_i}h = {}^{v_i}(gh),\ \forall\, g, h \in Q$.

Posons $H = \prod_{i=0}^{r} {}^{v_i}Q$. On peut faire agir P sur H de la manière suivante. Soient $({}^{v_i}h_i)_{i=0}^{r} \in H$ et $u \in P$. Comme la multiplication à gauche par u agit par permutation sur $[P/C]$, il existe une unique permutation $\sigma_u \in S_{r+1}$ (où S_{r+1} agit sur l'ensemble $\{0, \ldots, r\}$) et il existe des éléments uniques $c(u, i) \in C$, $0 \leq i \leq r$, tels que $uv_i = v_{\sigma_u(i)} c(u, i)$. On pose alors

$$ {}^{u}({}^{v_i}h_i)_{i=0}^{r} = \big({}^{v_i}\big({}^{c(u,\sigma_u^{-1}(i))}h_{\sigma_u^{-1}(i)}\big)\big)_{i=0}^{r}. $$

On a ${}^{1}h = h,\ \forall h \in H$, car $1v_i = v_i,\ \forall\, 0 \leq i \leq r$. De même, on a l'égalité ${}^{(uu')}h = {}^{u}({}^{u'}h),\ \forall\, h \in H,\ \forall\, u, u' \in P$. En effet, par associativité dans P, on a $(uu')v_i = u(u'v_i),\ \forall\, 0 \leq i \leq r$, et donc

$$ \sigma_{uu'} = \sigma_u \sigma_{u'} \quad \text{et} \quad c(uu', i) = c(u, \sigma_{u'}(i))c(u', i),\ \forall\, 0 \leq i \leq r. $$

D'où

$$ {}^{u}\big({}^{u'}({}^{v_i}h_i)_{i=0}^{r}\big) = {}^{u}\left({}^{v_i}\big({}^{c(u',\sigma_{u'}^{-1}(i))}h_{\sigma_{u'}^{-1}(i)}\big)\right)_{i=0}^{r} = $$

$$ = \left({}^{v_i}\big({}^{\left(c(u,\sigma_u^{-1}(i))\cdot c(u',\sigma_{u'}^{-1}(\sigma_u^{-1}(i)))\right)}h_{\sigma_{u'}^{-1}(\sigma_u^{-1}(i))}\big)\right)_{i=0}^{r} = $$

$$ = \left({}^{v_i}\big({}^{c(uu',\sigma_{uu'}^{-1}(i))}h_{\sigma_{uu'}^{-1}(i)}\big)\right)_{i=0}^{r} = {}^{(uu')}({}^{v_i}h_i)_{i=0}^{r}. $$

A l'aide de cette action, on construit un groupe fini p-nilpotent $G' = H \rtimes P$, dans lequel les groupes ${}^{v_i}Q,\ \forall\, 0 \leq i \leq r$ sont des sous-groupes conjugués.

Par hypothèse, pour tout $0 \leq i \leq r$, le $k[{}^{v_i}Q]$-module ${}^{v_i}(L{\downarrow}_Q^G)$ est simple. Considérons le produit tensoriel externe $\tilde{L} = \bigotimes_{i=0}^{r} {}^{v_i}(L{\downarrow}_Q^G)$ de ces modules. Par le théorème 10.33 de [CR], $\tilde{L}$ est un kH-module simple, car k est algébriquement clos. Posons, $\forall\, u \in P$ et $\forall\, x = \otimes_{i=0}^{r} {}^{v_i}x_i$, où $x_i \in L,\ \forall\, 0 \leq i \leq r$,

$$ u * x = \bigotimes_{i=0}^{r} {}^{v_i}\big(c(u, \sigma_u^{-1}(i)) \cdot x_{\sigma_u^{-1}(i)}\big), $$

pour l'action d'origine, notée "$\cdot$", de Q sur $L{\downarrow}_Q^G$, et où on écrit

$uv_i = v_{\sigma_u(i)} c(u, i),\ \forall\, 0 \leq i \leq r$, comme auparavant.

Cette action de P, étendue par k-linéarité à $\tilde{L}$, munit $\tilde{L}$ d'une structure de kP-module. En effet, pour tous $, u, u' \in P$ et pour tout $x = \otimes_{i=0}^{r} x_i \in \tilde{L}$, on a $1 * x = x$ et

$$ u * (u' * x) = u * \left(\bigotimes_{i=0}^{r} {}^{v_i}\big(c(u', \sigma_{u'}^{-1}(i)) \cdot x_{\sigma_{u'}^{-1}(i)}\big) \right) = $$

$$= \bigotimes_{i=0}^{r} {}^{v_i}\Big(c(u, \sigma_u^{-1}(i)) \cdot \Big(c(u', \sigma_{u'}^{-1}(\sigma_u^{-1}(i))) \cdot x_{\sigma_{u'}^{-1}(\sigma_u^{-1}(i))} \Big) \Big) =$$

$$= \bigotimes_{i=0}^{r} {}^{v_i}\Big(\Big(c(u, \sigma_u^{-1}(i)) c(u', \sigma_{u'}^{-1}(\sigma_u^{-1}(i))) \Big) \cdot x_{\sigma_{u'}^{-1}(\sigma_u^{-1}(i))} \Big) =$$

$$= \bigotimes_{i=0}^{r} {}^{v_i}\big(c(uu', \sigma_{uu'}^{-1}(i)) \cdot x_{\sigma_{uu'}^{-1}(i)} \big) = (uu') * x.$$

Pour tous $h = ({}^{v_i}h_i)_{i=0}^{r} \in H$, $x = \otimes_{i=0}^{r} {}^{v_i}x_i \in \tilde{L}$ et $u \in P$, on définit $(hu) * x = h \cdot (u * x)$. Ainsi, on munit $\tilde{L}$ d'une structure de kG'-module. En effet, le calcul suivant montre que les actions de P et de H sont compatibles :

$$(uh) * x = {}^{u}h \cdot (u * x) = {}^{v_i}\big({}^{c(u,\sigma_u^{-1}(i))}h_{\sigma_u^{-1}(i)} \big) \cdot (u * x) =$$

$$= \bigotimes_{i=0}^{r} {}^{v_i}\Big({}^{c(u,\sigma_u^{-1}(i))}h_{\sigma_u^{-1}(i)} \cdot \big(c(u, \sigma_u^{-1}(i)) \cdot x_{\sigma_u^{-1}(i)} \big) \Big) =$$

$$= \bigotimes_{i=0}^{r} {}^{v_i}\Big(c(u, \sigma_u^{-1}(i)) h_{\sigma_u^{-1}(i)} \cdot x_{\sigma_u^{-1}(i)} \Big) = u * (h \cdot x).$$

Par ailleurs, $\tilde{L}{\downarrow_P^{G'}}$ et $\mathrm{Ten}_C^P(L{\downarrow_C^G})$ sont isomorphes comme kP-modules. En effet, par construction, ce sont deux k-espaces vectoriels isomorphes, de dimension égale à $(\dim L)^{r+1}$. De plus, par définition de l'action de P sur $\tilde{L}$ d'une part, et par définition du module $\mathrm{Ten}_C^P(L{\downarrow_C^G})$ induit tensoriellement d'autre part, l'action de P coïncide sur ces deux kP-modules.

Or, $\mathrm{Ten}_C^P M$ est un facteur direct de $\mathrm{Ten}_C^P(L{\downarrow_C^G})$. En effet, pour tout indice $0 \leq i \leq r$, le $k[\,{}^{v_i}C]$-module ${}^{v_i}M$ est un facteur direct de ${}^{v_i}(L{\downarrow_C^G})$. Par conséquent, on peut écrire $\mathrm{Ten}_C^P M \,|\, \tilde{L}{\downarrow_P^{G'}}$. De plus, $\tilde{L}$ est de vortex P, car $p \not| \dim \tilde{L}$ (cf. proposition 1.2.5) et $\mathrm{Ten}_C^P M$ est un kP-module d'endo-permutation couvert. On en déduit alors que la source de $\tilde{L}$ est isomorphe au chapeau de $\mathrm{Ten}_C^P M$.

Remarque 5.5.1. *Si l'on considère l'induction tensorielle selon le point de vue fonctoriel introduit par S. Bouc dans [Bo3], alors on évite le choix d'un système de représentants des classes à gauche de P/C. En effet, le groupe H que nous avons défini ci-dessus est isomorphe au groupe*

$$\mathrm{Hom}_C(P, Q) = \{\varphi : P \longrightarrow Q \mid \varphi(c \cdot u) = c \cdot \varphi(u),\ \forall\, c \in C,\ \forall\, u \in P\}$$

des applications C-équivariantes de P vers Q, où on considère P et Q comme des C-ensembles pour la multiplication à gauche par C dans P et, respectivement, pour l'action de C sur Q (par conjugaison) dans G.

De même, le kH-module $\tilde{L}$ est isomorphe à un quotient de $k\,\mathrm{Hom}_C(P, \{L\})$, où $\{L\}$ désigne L vu comme C-ensemble. Plus précisément, dans les notations de la section 9.4 de [Bo3], on a $\tilde{L} \cong t_P(L)$. Ainsi, si on applique le lemme 9.9 et la remarque 9.10 de [Bo3], on obtient le même résultat que nous avons prouvé

dans cette section, c'est-à-dire que $\tilde{L}$ est un kG'-module simple de source isomorphe au chapeau de $\mathrm{Ten}_C^P L$.

Remarquons que cette preuve ne nécessite aucun choix de représentants des classes et qu'elle est bien plus "élégante" que celle que nous avons donnée. Toutefois, comme elle utilise un formalisme que nous n'avons pas défini précédemment, nous avons préféré donner une preuve directe du résultat.

5.6 Produit tensoriel

Soit $\mathcal{C}$ une famille finie d'indices. Supposons qu'à tout indice $C \in \mathcal{C}$ on associe un kP-module d'endo-permutation indécomposable M_C de vortex P, tel qu'on sait construire explicitement un groupe fini p-nilpotent $G_C = Q_C \rtimes P$, avec Q_C d'ordre premier à p, et un kG_C-module simple L_C de source M_C. On va démontrer le résultat suivant.

Théorème 5.6.1. *Si $L_C\downarrow_{Q_C}^{G_C}$ est un kQ_C-module simple, pour tout $C \in \mathcal{C}$, alors on peut expliciter un groupe fini p-nilpotent G et un kG-module simple $\tilde{L}$ de vortex P et de source isomorphe au chapeau de $\otimes_{C\in\mathcal{C}} M_C$.*

Preuve. Posons $G = \left(\prod_{C\in\mathcal{C}} Q_C\right) \rtimes P$ pour l'action diagonale de P sur $\prod_{C\in\mathcal{C}} Q_C$, i.e.

$$^u(h_C)_{C\in\mathcal{C}} = (\,^u h_C)_{C\in\mathcal{C}},\ \forall u \in P,\ \forall (h_C)_{C\in\mathcal{C}} \in \prod_{C\in\mathcal{C}} Q_C.$$

Cette action est bien définie. En effet, on a

$$^{(uu')}(h_C)_{C\in\mathcal{C}} = (\,^{(uu')}h_C)_{C\in\mathcal{C}} = (\,^u(\,^{u'}h_C))_{C\in\mathcal{C}} = \,^u(\,^{u'}(h_C)_{C\in\mathcal{C}}),$$

pour tous $u, u' \in P$ et pour tout $(h_C)_{C\in\mathcal{C}} \in \prod_{C\in\mathcal{C}} Q_C$. Considérons le k-espace vectoriel $L = \bigotimes_{C\in\mathcal{C}}(L_C\downarrow_{Q_C}^{G_C})$ (produit tensoriel sur k). C'est un $k[\prod_{C\in\mathcal{C}} Q_C]$-module pour l'action suivante.

$$(h_C)_{C\in\mathcal{C}} \cdot \otimes_{C\in\mathcal{C}}\, x_C = \otimes_{C\in\mathcal{C}}(h_C \cdot x_C),\ \forall\, x_C \in L_C\downarrow_{Q_C}^{G_C},\ \forall\, h_C \in Q_C \text{ et } \forall\, C \in \mathcal{C}.$$

Comme k est algébriquement clos, L est un $k[\prod_{C\in\mathcal{C}} Q_C]$-module simple (cf. théorème 10.33 de [CR]).

On peut étendre L en un kG-module $\tilde{L}$, a fortiori simple, en faisant agir P diagonalement. En effet, posons $u \cdot \otimes_{C\in\mathcal{C}}\, x_C = \otimes_{C\in\mathcal{C}}\, u \cdot x_C\ , \forall u \in P$ et définissons

$$\big((h_C)_{C\in\mathcal{C}}\, u\big)\cdot\otimes_{C\in\mathcal{C}}\, x_C = (h_C)_{C\in\mathcal{C}}\cdot\big(u\cdot\otimes_{C\in\mathcal{C}}\, x_C\big),\ \forall u \in P,\ \forall\,(h_C)_{C\in\mathcal{C}} \in \prod_{C\in\mathcal{C}} Q_C$$

et $\forall\, \otimes_{C\in\mathcal{C}}\, x_C \in \tilde{L}$. Le calcul suivant montre que les actions de P et de $\prod_{C\in\mathcal{C}}\, Q_C$ sont compatibles :

$$\big(u((h_C)_{C\in\mathcal{C}}\big) \cdot \otimes_{C\in\mathcal{C}}\, x_C = (\,^u h_C) \cdot u \cdot \otimes_{C\in\mathcal{C}}\, x_C = \otimes_{C\in\mathcal{C}}\, u \cdot h_C \cdot x_C =$$

$$= u \cdot \otimes_{C\in\mathcal{C}}\, h_C \cdot x_C = u \cdot (h_C)_{C\in\mathcal{C}} \cdot \otimes_{C\in\mathcal{C}}\, x_C.$$

Ainsi nous avons, explicitement, un groupe fini p-nilpotent G, avec P comme p-sous-groupe de Sylow et un kG-module simple $\tilde{L}$ de vortex P. En effet, chaque L_C est de dimension première à p et la dimension de $\tilde{L}$ est le produit des dimensions des L_C.

Par hypothèse, M_C est un facteur direct de $L_C\downarrow_P^{G_C}$, $\forall\, C \in \mathcal{C}$, et donc $\bigotimes_{C\in\mathcal{C}} M_C$ est un facteur direct de $\bigotimes_{C\in\mathcal{C}}(L_C\downarrow_P^{G_C})$.

De plus, $\bigotimes_{C\in\mathcal{C}}(L_C\downarrow_P^{G_C})$ et $\tilde{L}\downarrow_P^G$ sont isomorphes comme kP-modules. En effet, ils sont égaux comme k-espaces vectoriels et P agit diagonalement, de la même manière sur chaque composante. Par conséquent, la source du kG-module simple $\tilde{L}$ est isomorphe à l'unique facteur direct indécomposable de vortex P du kP-module d'endo-permutation couvert $\otimes_{C\in\mathcal{C}} M_C$.

□

5.7 Morale

Commençons par souligner une propriété des constructions que nous avons présentées dans ce chapitre, ainsi qu'un moyen de généraliser les constructions des deux sections précédentes.

Remarque 5.7.1. *Soient p un nombre premier, P un p-groupe fini, G un groupe fini p-nilpotent ayant P comme p-sous-groupe de Sylow et appelons Q le plus grand sous-groupe normal de G d'ordre premier à p. Dans toutes les situations réalisées, on a toujours pu construire explicitement un kG-module simple L en étendant un kQ-module simple et donc tel que la restriction $L\downarrow_Q^G$ est un kQ-module simple, satisfaisant ainsi les hypothèses nécessaires aux constructions des deux sections précédentes.*

Relevons le fait qu'en général, si L est un kG-module simple, sa restriction à kQ n'est pas un module simple. Cependant, $L\downarrow_Q^G$ est une somme directe finie $\oplus_{i=0}^r {}^{v_i}T$ de modules simples conjugués (sans limiter la généralité, supposons $v_0 = 1$), ayant des sous-groupes d'inertie I_i (conjugués) et, a fortiori, strictement contenus dans G. Rappelons que si T est un kQ-module simple, son sous-groupe d'inertie est le sous-groupe $I = \{g \in G \mid {}^gT \cong T\}$ de G. Par la théorie de Clifford (cf. paragraphe 11 de [CR]), on sait que T s'étend en un kI-module $\tilde{T}$, a fortiori simple, et le kG-module induit $\mathrm{Ind}_I^G \tilde{T}$ est simple. De plus, $\tilde{T}$ et $\mathrm{Ind}_I^G \tilde{T}$ ont la même source. Par suite, on ne peut pas appliquer directement les constructions des deux sections précédentes (car l'hypothèse $L\downarrow_Q^G$ n'est pas satisfaite), mais on peut les adapter en considérant le kG-module simple $\mathrm{Ind}_I^G \tilde{T}$ au lieu de L.

Résumons-nous. Dans la section 5.3, nous avons explicitement réalisé des modules d'endo-permutation comme sources de modules simples pour des groupes finis p-nilpotents. Puis, dans les trois sections suivantes, on s'est constitué une boîte-à-outils nous permettant de construire bien d'autres modules d'endo-permutation comme sources, à partir de situations connues. Ainsi, en combinant ces résultats, on en déduit la conséquence suivante.

Théorème 5.7.2. *Soient p un nombre premier, P un p-groupe fini et k un corps algébriquement clos de caractéristique p. Tous les kP-modules d'endo-permutation indécomposables de torsion de vortex P qui sont les chapeaux d'un kP-module de la forme $\bigotimes_{(Q/R)\in\mathcal{T}} \mathrm{Ten}_Q^P \mathrm{Inf}_{Q/R}^Q(M_{Q/R})$, où $M_{Q/R}$ est un $k[Q/R]$-module endo-trivial de torsion et où $\mathcal{T}$ est une famille de sections de P qui sont des groupes cycliques, quaternioniens ou semidiédraux, sont explicitement réalisables comme sources de modules simples de vortex P pour des groupes finis p-nilpotents.*

Remarque 5.7.3. *Dans l'énoncé du théorème, l'expression "module de torsion" est un abus de langage pour "module dont la classe dans le groupe de Dade est un élément de torsion".*

Preuve. En utilisant les résultats précédents, il suffit de vérifier que tout kP-module endo-trivial indécomposable de torsion de vortex P est explicitement réalisable comme source d'un module simple de vortex P pour un groupe fini p-nilpotent, pour un p-groupe P cyclique, quaternionien ou semidiédral. Et en fait, par définition de la loi de groupe dans $T(P)$ (et dans $D(P)$), et par le théorème 5.6.1, on n'a besoin que des modules dont les classes engendrent le sous-groupe de torsion de $T(P)$.

Si P est cyclique (d'ordre au moins 3), alors le sous-groupe de torsion de $T(P)$ est fini et engendré par la classe de $\Omega_P^1(k)$, que l'on a réalisé comme source d'un module simple pour un groupe fini p-nilpotent au paragraphe 5.3.1.

Si P est quaternionien, alors le sous-groupe de torsion de $T(P)$ est isomorphe à $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, où $\mathbb{Z}/4\mathbb{Z}$ est engendré par un kP-module endo-trivial de dimension $|P|-1$ (i.e. par $\Omega_P^1(k)$ ou $\Omega_P^3(k)$) et $\mathbb{Z}/2\mathbb{Z}$ est engendré par le kP-module endo-trivial "exceptionnel" ou son dual, de dimension $\frac{|P|}{2}+1$. Les classes des deux modules réalisés comme sources de modules simples pour deux groupes finis 2-nilpotents au paragraphe 5.3.2 engendrent donc tout le sous-groupe de torsion de $T(P)$ (cf. remarque 5.3.10).

Si P est semidiédral, alors on a, à isomorphisme près, un unique kP-module endo-trivial de torsion (auto-dual, d'ordre 2) et c'est celui que l'on a réalisé comme source d'un module simple pour un groupe fini 2-nilpotent au paragraphe 5.3.3. D'où le théorème. □

Le théorème 8.39 et la remarque 8.41 de [Pu1] décrivent explicitement les kP-modules qui peuvent être des sources de modules simples pour des groupes finis p-résolubles. Ces modules sont ceux du théorème, à savoir les kP-modules d'endo-permutation indécomposables de torsion de vortex P qui sont des facteurs directs d'un kP-module de la forme $\bigotimes_{(Q/R)\in\mathcal{T}} \mathrm{Ten}_Q^P \mathrm{Inf}_{Q/R}^Q(M_{Q/R})$, où $M_{Q/R}$ est un $k[Q/R]$-module endo-trivial de torsion et où $\mathcal{T}$ est une famille de sections de P qui sont des groupes cycliques, quaternioniens ou semidiédraux. Il en découle immédiatement la conséquence suivante.

Corollaire 5.7.4. *Soient p un nombre premier, P un p-groupe fini et k un corps algébriquement clos de caractéristique p. Alors tout kP-module d'endo-permutation indécomposable de vortex P qui peut être une source d'un module*

simple de vortex P pour un groupe fini p-résoluble est explicitement réalisable comme source d'un module simple de vortex P pour un groupe fini p-nilpotent.

Pour terminer cette section, considérons ce dernier résultat.

Corollaire 5.7.5. *Soit p un nombre premier impair. Alors tout kP-module d'endo-permutation indécomposable de torsion est la source d'un module simple. De plus, on peut explicitement réaliser ces modules comme sources de modules simples pour des groupes finis p-nilpotents.*

Preuve. Si p est impair, alors tout kP-module d'endo-permutation couvert indécomposable de torsion est le chapeau d'un kP-module d'endo-permutation de la forme $\bigotimes_{(Q/R)\in\mathcal{T}} \mathrm{Ten}_Q^P \mathrm{Inf}_{Q/R}^Q(M_{Q/R})$, où $M_{Q/R}$ est un $k[Q/R]$-module endo-trivial de torsion et où $\mathcal{T}$ est une famille de sections cycliques de P, par le point 7 du théorème 1.5.5. On conclut alors immédiatement, par le théorème 5.7.2.

□

5.8 Exemple

Considérons $p = 2$, $P = <u, v \mid u^4 = 1, u^2 = v^2, {}^v u = u^{-1}>$ un groupe quaternion d'ordre 8 et $k = \mathbb{F}_4$. Nous voulons réaliser le kP-module M de dimension 3 donné dans la section 6 de [CaTh1]. Autrement dit, les actions de u et v sont données respectivement par les matrices

$$U = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \quad \text{et} \quad V = \begin{pmatrix} 1 & 0 & 0 \\ \omega & 1 & 0 \\ 0 & \omega^{-1} & 1 \end{pmatrix},$$

pour une racine cubique ω de l'unité non triviale (i.e. ω est une racine du polynôme $t^2 + t + 1 \in k[t]$). Par choix de k, on sait qu'un tel scalaire existe.

Si nous voulons réaliser un kP-module endo-trivial de dimension 3 comme source d'un module simple, il faut apporter quelques légères modifications à notre méthode, puisque celle-ci ne nous permet de construire directement qu'un module de dimension 5. Avant de commencer les calculs, mentionnons que J. Thévenaz est à l'origine de cet exemple.

Pour construire un groupe fini 2-nilpotent, il nous faut trouver un nombre premier q congru à la dimension de M modulo 8. Prenons $q = 3$ et considérons un 3-groupe extraspécial Q d'ordre 27 et d'exposant 3. Autrement dit, Q peut se présenter par générateurs et relations comme suit.

$$Q = <x, y, z \mid x^3 = y^3 = z^3 = 1, [y, x] = z, [x, z] = [y, z] = 1>.$$

L'action de P sur Q qui va définir le produit semi-direct que nous allons

considérer est induite par l'inclusion

$$\begin{array}{rcl} \sigma : P & \longrightarrow & \mathrm{SL}_2(\mathbb{F}_3) \\ u & \longmapsto & \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ v & \longmapsto & \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} . \end{array}$$

On en déduit ainsi le groupe 2-nilpotent $G = Q \rtimes P$, d'ordre 216 et où on a :

$${}^{u}x = xyz^{-1} \ ; \ {}^{u}y = xy^{-1}z \ ; \ {}^{u}z = z \quad \text{et} \quad {}^{v}x = y \ ; \ {}^{v}y = x^{-1}z \ ; \ {}^{v}z = z \ .$$

Construisons un kG-module simple $\tilde{L}$ de source M. Considérons le sous-groupe abélien élémentaire $A = <x, z>$ de Q de rang 2 et la représentation

$$\begin{array}{rcl} \psi : A & \longrightarrow & k^* \\ x & \longmapsto & 1 \\ z & \longmapsto & \omega \ . \end{array}$$

Notons k_ω le kQ-module de dimension 1 correspondant et posons $L = k_\omega \uparrow_A^Q$.

On sait, par les résultats de ce chapitre que L est un kQ-module simple, de dimension 3 et qui s'étend à G. Explicitement, on peut considérer la k-base

$$\mathcal{B} = \{ \ 1 \otimes 1 \ , \ y \otimes 1 \ , \ y^2 \otimes 1 \ \}$$

de L, dans laquelle $x,\ y$ et z agissent respectivement par les matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega^{-1} & 0 \\ 0 & 0 & \omega \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} \omega & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega \end{pmatrix} .$$

L'extension $\tilde{L}$ de L est définie par les actions de u et v sur $\mathcal{B}$ par les matrices

$$U' = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \quad \text{et} \quad V' = \begin{pmatrix} 1 & \omega & \omega \\ \omega^{-1} & 1 & 0 \\ \omega^{-1} & 0 & 1 \end{pmatrix} ,$$

respectivement.

On doit alors montrer que U et U' sont semblables, de même que V et V'. En effet, on a $\tilde{L}\downarrow_P^G \cong M$ si et seulement si u et v agissent sur $\tilde{L}\downarrow_P^G$ et sur M de la même manière. Autrement dit, les divergences matricielles entre U et U' et entre V et V' proviennent d'un changement de base. Si on considère la matrice inversible

$$S = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix} \ , \quad \text{on obtient} \quad {}^{S}U = U' \quad \text{et} \quad {}^{S}V = V' \ .$$

D'où le résultat.

Terminons cet exemple avec la remarque suivante. Calculons les matrices $W = U^2$ et $W' = U'^2$, correspondant à l'action du centre $Z(P)$ sur M, respectivement $\tilde{L}{\downarrow}_P^G$:

$$W = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \quad \text{et} \quad W' = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

On remarque que dans les deux cas, on a un facteur direct trivial, correspondant à la deuxième colonne de W, respectivement la première de W'. Par conséquent, on a bien que les restrictions $\tilde{L}{\downarrow}_{Z(P)}^G$ et $M{\downarrow}_{Z(P)}^P$ sont isomorphes à $k \oplus k[Z(P)]$ et donc ces deux modules sont endo-triviaux, par le théorème 1.5.5.

5.9 Un autre exemple

Explicitons à présent un nouvel exemple qui illustre le fait que la méthode que nous avons donnée dans ce chapitre n'est pas nécessairement la plus "économique". En effet, considérons un groupe cyclique P d'ordre 3 et cherchons à réaliser $\Omega_P^1(\mathbb{F}_3)$. Selon notre démarche, on devrait trouver un nombre premier impair q, congru à 2 modulo 3. On peut prendre $q = 5$. Mais alors le module simple $\tilde{L}$ que l'on construit est aussi de dimension 5 et donc, pour déterminer sa source, il va falloir détecter un facteur direct libre dans la restriction de $\tilde{L}$ à P. Or, il y a une réalisation de $\Omega_P^1(\mathbb{F}_3)$ comme source bien plus facile à expliciter, et c'est celle-ci que nous allons développer dans cette section.

Posons $P = <u \mid u^3 = 1>$, $k = \mathbb{F}_3(i)$, pour une racine quatrième primitive i de l'unité (avec donc $i \neq \pm 1$) et $Q = <x, y | x^4 = 1, y^2 = x^2, {}^y x = x^{-1}>$ un groupe quaternion d'ordre 8. Soit G le produit semi-direct $Q \rtimes P$, pour l'action de P sur Q donnée par ${}^u x = y$ et ${}^u y = xy$. On a ainsi un groupe fini 3-nilpotent, d'ordre 24.

On sait que Q possède un kQ-module simple L de dimension 2. En effet, les éléments de Q forment cinq classes de conjugaison et donc on a cinq $\mathbb{C}Q$-modules simples, dont la somme des carrés des dimensions vaut $8 = |Q|$. Par choix de k, on a également cinq kQ-modules simples (de mêmes dimensions). En utilisant la table des caractères (par exemple), on peut déterminer le caractère de L. On obtient ainsi les actions de x et de y sur L qui peuvent s'écrire matriciellement (dans une certaine base) comme suit.

$$x \text{ agit par } \quad X = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad \text{et } y \text{ par } \quad Y = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Or, L s'étend à G en $\tilde{L}$. En effet, on peut considérer l'action suivante de u donnée matriciellement (dans la même base que ci-dessus) :

$$U = \begin{pmatrix} 1-i & -1-i \\ 1-i & 1+i \end{pmatrix}.$$

En effet, on a ainsi ${}^U X = Y$, ${}^U Y = XY$ et $U^3 = \mathrm{Id}$.

En particulier, il résulte que $\tilde{L}\downarrow_P^G$ est un kP-module de dimension 2. Or kP est unisériel, et donc, par le théorème de Krull-Schmidt, on a deux alternatives possibles pour un module M de dimension 2 :

1. M est indécomposable et donc isomorphe à $\Omega_P^1(k)$. Dans ce cas, la matrice U est semblable à la matrice $A = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$, où la base de $\Omega_P^1(k)$ considérée est $\{u-1,\ u^2-1\}$.
2. M est isomorphe à la somme directe $k \oplus k$. Autrement dit, u agit trivialement sur M et donc U est la matrice identité, ce qui n'est pas le cas.

Par conséquent, on a $\tilde{L}\downarrow_P^G \cong \Omega_P^1(k)$ et la base dans laquelle est exprimée U est l'ensemble $\left\{(\frac{-1+i}{2})(u^2+u+1),\ -(\frac{1+i}{2})(u-1)\right\}$.

Chapitre 6

Equivalences splendides

6.1 Introduction

Nous allons maintenant considérer les modules d'endo-permutation et leur rôle dans l'analyse locale des équivalences dérivées entre blocs. Plus précisément, la situation qui nous intéresse est la suivante. Si $(K, \mathcal{O}, k)$ est un système p-modulaire pour un nombre premier p, si G est un groupe fini p-nilpotent avec un p-sous-groupe de Sylow P, alors J. Rickard a remarqué que certains RP-modules d'endo-permutation couverts (où $R = \mathcal{O}$ ou $R = k$) possèdent une résolution de permutation endo-scindée C. Par suite, C induit une équivalence dérivée splendide entre un bloc B du groupe p-nilpotent G et RP. Ce type de phénomène revêt une grande importance dans l'analyse de la structure locale des blocs et c'est probablement ce qui a motivé J. Rickard à se demander si tout RP-module d'endo-permutation couvert possède une résolution de permutation endo-scindée, pour tout p-groupe fini P et pour tout nombre premier p. En fait, par la suite, il a lui-même démontré que le RQ_8-module exceptionnel de dimension 3 n'a pas de résolution de permutation endo-scindée, répondant ainsi négativement à la question qu'il se posait.

Nous avons décidé de poursuivre la recherche de modules d'endo-permutation possédant une résolution de permutation endo-scindée, en utilisant, entres autres, les résultats obtenus dans la première partie.

A présent il conviendrait probablement d'ouvrir une parenthèse catégorique et faire une brève incursion dans l'univers des équivalences dérivées et de la conjecture de Broué. Cependant, cela nous demanderait d'introduire une grande quantité de nouvelles notions, des catégories dérivées de Grothendieck aux équivalences dérivées splendides de Rickard, en passant par les isotypies de Broué. Et finalement, tout ceci ne nous concerne qu'indirectement, puisque pour atteindre notre objectif, nous n'avons besoin que de la définition d'une résolution de permutation endo-scindée d'un module. C'est la raison pour laquelle nous allons nous contenter de définir ce type de résolution, en renvoyant le lecteur intéressé aux articles [Br] et [Ri] pour de plus amples informations sur le sujet.

6.2 Résolutions de permutation endo-scindées

Soit G un groupe fini et considérons les mêmes notations et conventions que dans le chapitre 1.

Définition 6.2.1. *Soit M un RG-module.*

1. *M est dit de p-**permutation** si $M\downarrow_P^G$ est un RP-module de permutation, pour un p-sous-groupe de Sylow P de G.*
2. *Soit*
$$(C.,\ \partial.)\ =\ \left(\ldots \xrightarrow{\partial_{n+2}} C_{n+1} \xrightarrow{\partial_{n+1}} C_n \xrightarrow{\partial_n} C_{n-1} \xrightarrow{\partial_{n-1}} \ldots\right)$$
un complexe de RG-modules.
*Le **dual** de $(C.,\ \partial.)$ est le complexe $(C.^*,\ \partial.^*)$, où*
$(C.^*)_n = (C_{-n})^* = \mathrm{Hom}_R(C_{-n}, R)$ *(cf. chapitre 1) et*
$(\partial^*)_n(\varphi) = \varphi \circ \partial_{-n+1} \in (C.^*)_{n-1},\ \forall\, \varphi \in (C.^*)_n$ *et* $\forall\, n \in \mathbb{Z}$.
3. *Soient $(C., \partial.)$ et $(D.,\ \partial'.)$ deux complexes de RG-modules. On définit le produit tensoriel $((C \otimes D)., d.)$ comme le complexe avec*
$$(C \otimes D)_n = \bigoplus_{p+q=n} C_p \otimes D_q \text{ et } d_n : (C \otimes D)_n \longrightarrow (C \otimes D)_{n-1} \text{ tel que}$$
$$d_n(x \otimes y) = \partial_p(x) \otimes y + (-1)^p x \otimes \partial'_q(y),\ \forall\, x \otimes y \in C_p \otimes D_q,$$
pour tous entiers p et q avec $p + q = n$ et ce pour tout entier n.
4. *Soit $(C., \partial.) = \left(\ldots \xrightarrow{\partial_{n+2}} C_{n+1} \xrightarrow{\partial_{n+1}} C_n \xrightarrow{\partial_n} C_{n-1} \xrightarrow{\partial_{n-1}} \ldots\right)$ un complexe borné de RG-modules. On dit que c'est une **résolution de permutation endo-scindée de** M si les conditions suivantes sont vérifiées.*
   (a) *C_n est un RG-module de p-permutation, pour tout entier n.*
   (b) *$H_n(C.) \cong \begin{cases} M\ , & si\ n = 0 \\ 0\ , & sinon\ . \end{cases}$*
   (c) *Le complexe $C^*. \otimes C.$ est scindé.*

Avant de poursuivre, démontrons un résultat bien connu en algèbre homologique.

Lemme 6.2.2. *Soit $(C., \partial.)$ un complexe de RG-modules borné et scindé. Alors on a*
$$C_i \cong H_i(C.) \oplus \mathrm{Im}(\partial_{i+1}) \oplus \mathrm{Im}(\partial_i)\ ,\ \forall\, i \in \mathbb{Z}.$$

Preuve. Soit $s.$ une section de $(C., \partial.)$ et soient n et m les entiers tels que
$$(C., \partial.)\ = \left(0 \longrightarrow C_n \xrightarrow{\partial_n} C_{n-1} \xrightarrow{\partial_{n-1}} \ldots \xrightarrow{\partial_{m+2}} C_{m+1} \xrightarrow{\partial_{m+1}} C_m \longrightarrow 0\right).$$
Pour tout indice i avec $n \geq i \geq m$, on a une suite exacte courte scindée
$$S_i\ = \left(0 \longrightarrow \mathrm{Ker}(\partial_i) \xrightarrow{\sigma_i} C_i \xrightarrow{\partial_i} \mathrm{Im}(\partial_i) \longrightarrow 0\right),$$

où σ_i est l'inclusion. En effet, l'application s_{i-1} restreinte à $\mathrm{Im}(\partial_i)$ est une section de S_i, car par définition, on a $\partial_i s_{i-1}\partial_i = \partial_i$. Par suite, on a

$$C_i \cong \mathrm{Ker}(\partial_i) \oplus \mathrm{Im}(\partial_i)\ . \tag{6.1}$$

D'autre part, on a aussi une suite exacte courte scindée

$$T_i\ = \left(0 \longrightarrow \mathrm{Im}(\partial_{i+1}) \xrightarrow{\sigma'_i} \mathrm{Ker}(\partial_i) \xrightarrow{\pi_i} H_i(C.) \longrightarrow 0\right),$$

où σ'_i est l'inclusion et π_i le passage au quotient.

En effet, l'application $\partial_{i+1}s_i : \mathrm{Ker}(\partial_i) \longrightarrow \mathrm{Im}(\partial_{i+1})$ est une rétraction de T_i. C'est-à-dire que la composition $\partial_{i+1}s_i\sigma'_i$ est l'identité sur $\mathrm{Im}(\partial_{i+1})$ et ceci est vrai, car $\partial_{i+1}s_i\partial_{i+1} = \partial_{i+1}$ par hypothèse. On en déduit l'isomorphisme suivant :

$$\mathrm{Ker}(\partial_i) \cong H_i(C.) \oplus \mathrm{Im}(\partial_{i+1})\ . \tag{6.2}$$

Finalement, les relations 6.1 et 6.2 impliquent

$$C_i \cong H_i(C.) \oplus \mathrm{Im}(\partial_{i+1}) \oplus \mathrm{Im}(\partial_i),\ \forall\, i \in \mathbb{Z}.$$

□

La définition de résolution de permutation endo-scindée est due à J. Rickard. Il constate, en particulier, que si G est un p-groupe et M un RG-module ayant une résolution de permutation endo-scindée $(C., \partial.)$, alors M est un RG-module d'endo-permutation. En effet, on a alors, par le théorème 10.30 de [CR] et le théorème de Künneth (cf. théorème 2.7.1 [Be]) :

$$\mathrm{End}_R\, M \cong M^* \otimes M \cong H_0(C.^*) \otimes H_0(C.) \cong H_0(C^*. \otimes C.).$$

Or, $C^*. \otimes C.$ est borné et scindé. Par le lemme précédent, cela implique que $H_0(C^*. \otimes C.)$ est un facteur direct de $(C^*. \otimes C.)_0$ et donc c'est un module de permutation (cf. corollaire 27.2 de [Th1]).

Cette remarque amène J. Rickard à se demander si tous les RP-modules d'endo-permutation, pour un p-goupe fini P, possèdent une résolution de permutation endo-scindée et c'est sur cette question que nous allons nous pencher à présent. Mentionnons quelques résultats utiles obtenus par J. Rickard (cf. [Ri]).

Propriétés. Soit P un p-groupe fini.

1. Soit M un kP-module d'endo-permutation ayant une résolution de permutation endo-scindée. Alors M se relève en un $\mathcal{O}P$-module ayant une résolution de permutation endo-scindée (proposition 7.1).
2. Si $Q \triangleleft P$ et M est un $R[P/Q]$-module d'endo-permutation ayant une résolution de permutation endo-scindée, alors le RP-module $\mathrm{Inf}_{P/Q}^{P}\, M$ a aussi une résolution de permutation endo-scindée (lemme 7.3).
3. Si M et N sont deux RP-modules d'endo-permutation ayant une résolution de permutation endo-scindée $C.$ et respectivement $D.$, alors $C. \otimes D.$ est une résolution de permutation endo-scindée du RP-module $M \otimes N$ (lemme 7.4).

4. Si M et N sont deux RP-modules d'endo-permutation tels que $M \oplus N$ a une résolution de permutation endo-scindée, alors M et N ont aussi une résolution de permutation endo-scindée (lemme 7.5).
5. Soit M un kP-module d'endo-permutation ayant une résolution de permutation endo-scindée. Alors tout module qui est isomorphe à une somme directe de modules de la forme $\mathrm{Ind}_Q^P \mathrm{Res}_Q^P M$, pour des sous-groupes Q de P, a aussi une résolution de permutation endo-scindée (lemme 7.6).

   De ces quatre dernières assertions, J. Rickard déduit la proposition 7.2 suivante.
6. Si P est abélien, alors tout module d'endo-permutation a une résolution de permutation endo-scindée.
7. Si $C. = \left(\ldots \longrightarrow C_1 \longrightarrow C_0 \longrightarrow k \longrightarrow 0 \right)$ est une résolution projective minimale du kP-module trivial k, alors

$$C.^{(n)} = \left(0 \longrightarrow C_n \longrightarrow C_{n-1} \longrightarrow \ldots \longrightarrow C_0 \longrightarrow k \longrightarrow 0 \right) \qquad (6.3)$$

   est une résolution de permutation endo-scindée de $\Omega_P^n(k)$, pour tout entier n positif.

   En effet, $C.^{(n)}$ est borné et, comme kP est une k-algèbre symétrique et que les C_i sont projectifs, ceux-ci sont aussi libres et donc des kP-modules de permutation.

   Par définition d'une résolution projective, on a $H_i(C.^{(n)}) = 0$, $\forall\, 0 \leq i < n$ et, par "construction", $H_n(C.) \cong \Omega_P^n(k)$ (cf. section 1.2).

   De plus, le complexe $C.^{(n)} \otimes (C.^{(n)})^*$ est scindé car tous les termes, sauf celui en degré 0, sont injectifs (cf. section 2D de [CR]). Ainsi, $C.^{(n)}$ est une résolution de permutation endo-scindée de $\Omega_P^n(k)$.

   Par "symétrie", pour un entier n négatif, on tronque une résolution injective minimale de k pour obtenir une résolution de permutation endo-scindée de $\Omega_P^n(k)$.

   Que peut-on dire de la déflation ?
8. Soient M un kP-module d'endo-permutation ayant une résolution de permutation endo-scindée C et Q un sous-groupe normal de P. On définit le complexe $\bar{C}(Q)$. par $\bar{C}(Q)_n = \bar{C}_n(Q)$, pour tout entier n et selon les notations du chapitre 1 concernant les quotients de Brauer. Alors on a un isomorphisme de complexes $\bar{C}(Q). \otimes \left(\bar{C}(Q).\right)^* \cong \overline{C \otimes C}(Q)$ et donc $\bar{C}(Q).$ est une résolution de permutation endo-scindée d'un $R[P/Q]$-module de la classe de $\mathrm{Def}_{P/Q}^P[M]$.

   Terminons cette liste de propriétés avec une généralisation de la propriété 7, due à J. Alperin (cf. preuve du théorème 1 de [Al3]), et démontrée également par S. Bouc (cf. lemme 2.3.7 de [Bo1]).

9. Soit X un P-ensemble fini. Alors

$$C. = \Big(0 \longrightarrow RX \xrightarrow{\varepsilon} R \longrightarrow 0\Big) \tag{6.4}$$

est une résolution de permutation endo-scindée de $\Omega^1_X(R)$, où

$$C_0 = RX \text{ et } \varepsilon(\sum_{x\in X} \lambda_x x) = \sum_{x\in X} \lambda_x,\ \forall\ \sum_{x\in X} \lambda_x x \in RX.$$

En particulier, par les points 3 et 4 ci-dessus, cela entraîne que tous les syzygies relatifs $\Omega^n_X(R)$ ont une résolution de permutation endo-scindée, pour tout entier n et pour tout P-ensemble fini X. En effet, $\Omega^n_X(R)$ est le chapeau de $\Omega^1_X(R)^{\otimes n}$, si n est positif, sinon, si n est négatif, alors $\Omega^n_X(R)$ est le chapeau de $\big(\Omega^1_X(R)^{\otimes(-n)}\big)^*$.

Preuve. (cf. [Al3]) On a $C.$ borné et ses termes sont des RP-modules de permutation.

De plus, on a $H_i(C.) = 0$, si $i \neq 0$, et $H_0(C.) \cong \mathrm{Ker}(\varepsilon) = \Omega^1_X(R)$.

Par ailleurs, $C.^*$ est isomorphe au complexe $\big(0 \longrightarrow R \xrightarrow{\sigma} RX \longrightarrow 0\big)$, où $C^*_0 = RX$ et $\sigma(1) = \sum_{x\in X} x$. Ainsi, on obtient $H_i(C.^*) = 0$, si $i \neq 0$, et $H_0(C.) = RX/\,\mathrm{Im}(\sigma) = \Omega^1_X(R)^*$. Considérons le complexe

$$C.\otimes C.^* = \Big(0 \longrightarrow RX\otimes R \longrightarrow (RX\otimes RX)\oplus(R\otimes R) \longrightarrow R\otimes RX \longrightarrow 0\Big).$$

$C.\otimes C.^*$ est isomorphe au complexe

$$D. = \Big(0 \longrightarrow RX \xrightarrow{\varphi_1} (RX\otimes RX)\oplus R \xrightarrow{\varphi_0} RX \longrightarrow 0\Big),$$

où $\varphi_1(x) = \begin{pmatrix} x\otimes\sigma(1) \\ -\varepsilon(x)\end{pmatrix}$ et $\varphi_0\begin{pmatrix} x\otimes y \\ 1\end{pmatrix} = \varepsilon(x)y + \sigma(1),\ \forall\, x, y \in X.$

$D.$ est exact sauf en degré 0, où on a

$$H_0(D.) \cong H_0(C.)\otimes H_0(C.^*) \cong \Omega^1_P(X)\otimes\Omega^1_P(X)^* \cong R\oplus L,$$

pour un RP-module libre L, car $\Omega^1_X(R)$ est endo-trivial. Posons alors

$$\begin{array}{rccl} \psi_0 : & D_0 & \longrightarrow & D_1 \\ & \begin{pmatrix} x\otimes y \\ 1\end{pmatrix} & \longmapsto & (1+\delta_{x,y})y + \sigma(1) \qquad \text{et} \end{array}$$

$$\begin{array}{rccl} \psi_{-1} : & D_{-1} & \longrightarrow & D_0 \\ & x & \longmapsto & \begin{pmatrix} -\sum_{\substack{y\in X \\ y\neq x}} x\otimes y \\ \varepsilon(x)\end{pmatrix}. \end{array}$$

Ces deux applications sont des homomorphismes de RP-modules et ils satisfont $\varphi_0\psi_{-1} = \mathrm{Id}_{D_{-1}}$ et $\psi_0\varphi_1 = \mathrm{Id}_{D_1}$. Par suite, $D.$ est scindé et donc $C.$ est une résolution de permutation endo-scindée de $\Omega^1_X(R)$.

□

On constate en particulier que, si un module a une résolution de permutation endo-scindée, alors celle-ci se "comporte bien" par rapport aux opérations d'inflation, de produit tensoriel, de restriction, de déflation et bien entendu d'isomorphisme.

On pourrait croire qu'il en est de même pour l'induction tensorielle, mais ça n'est pas aussi simple. En effet, si Q est un sous-groupe de P et si $C.$ est une résolution de permutation endo-scindée d'un RQ-module d'endo-permutation couvert M, alors le complexe $\mathrm{Ten}_Q^P(C.)$, défini dans la section 4.1 du deuxième volume de [Be], n'est pas scindé en général. En effet, considérons le contre-exemple suivant. Soit $k = \mathbb{F}_2$, soit P un groupe cyclique d'ordre 2 et Q son sous-groupe trivial. Le complexe de kQ-modules et homomorphismes de kQ-modules

$$C. \ = \ 0 \longrightarrow k \xrightarrow{\mathrm{Id}} k \longrightarrow 0$$

est scindé. Or, le complexe $\mathrm{Ten}_Q^P C.$ est le complexe exact

$$\mathrm{Ten}_Q^P C. \ = \ 0 \longrightarrow k \xrightarrow{\sigma} kP \xrightarrow{\varepsilon} k \longrightarrow 0,$$

où, par définition de l'induite tensorielle d'un complexe, on obtient que $\varepsilon : kP \longrightarrow k$ est l'augmentation et $\sigma : k \longrightarrow kP$ est la trace tr_Q^P de Q à P. Par conséquent, $\mathrm{Ten}_Q^P C.$ n'est pas scindé.

Toutefois, S. Bouc démontre que si $M = \Omega_X^1(R)$ pour un Q-ensemble fini X, alors $\mathrm{Ten}_Q^P(0 \to RX \to R \to 0)$ est une résolution de permutation endo-scindée du RP-module $\mathrm{Ten}_Q^P \Omega_X^1(R)$. La preuve de cette assertion n'est pas aussi aisée qu'on pourrait le croire, et nous renvoyons le lecteur sceptique au paragraphe 5.4 de [Bo1] pour s'en convaincre. En fait, S. Bouc démontre ce fait dans la preuve de "sa" formule (cf. lemme 1.5.10). Or, si on utilise celle-ci, c'est pour remplacer les modules induits tensoriellement par des syzygies relatifs (afin de travailler avec des modules de dimension plus petite, par exemple), qui eux possèdent une résolution de permutation endo-scindée, comme on vient de le montrer.

En résumé, si l'on "assemble" les morceaux du puzzle constitués par les divers résultats de J. Rickard et de S. Bouc, on en déduit immédiatement la proposition suivante.

Proposition 6.2.3. *Soit P un p-groupe fini. Si $D(P) = D^\Omega(P)$, alors tout RP-module d'endo-permutation couvert M a une résolution de permutation endo-scindée.*

Considérons à présent les résultats obtenus dans la première partie et montrons le théorème suivant.

Théorème 6.2.4. *Soit P un p-groupe métacyclique si p est impair, ou diédral, quaternionien, semi-diédral ou extraspécial du type D_8^{*n} (avec $n \geq 1$), si $p = 2$. Alors les seuls RP-modules d'endo-permutation couverts qui n'ont pas de résolution de permutation endo-scindée sont les RP-modules "exceptionnels" (de dimension $\frac{|P|}{2} \pm 1$), pour le cas $p = 2$ et P un groupe quaternionien.*

Remarque 6.2.5. *Pour la preuve de ce théorème, nous allons utiliser l'***anneau de Green** $a(P)$ *des RP-modules. On considère le groupe abélien $a(P)$ défini par générateurs et relations comme suit (cf. section 5.1 du premier volume de [Be]).*

> *Les générateurs sont les classes d'isomorphisme $[M]$ des RP-modules M (de type fini).*
>
> *Les relations sont données par les suites exactes courtes scindées. Explicitement, on pose $[M] = [N] + [L]$ s'il existe une suite exacte scindée $0 \to N \to M \to L \to 0$ de RP-modules.*

En particulier, l'élément neutre pour l'addition dans $a(P)$ est le RP-module nul. Remarquons aussi que le groupe de Grothendieck $G_0(RP)$, défini dans la section 5.3, est un quotient de $a(P)$.

Posons $[M] \cdot [N] = [M \otimes N]$, pour tous RP-modules M, N et L. Cette multiplication munit $a(P)$ d'une structure d'anneau commutatif et admet la classe du module trivial R comme élément neutre.

Pour alléger les notations, on écrira simplement M la classe $[M]$ d'un RP-module M.

Preuve du théorème 6.2.4 . Dans tous les groupes considérés, tous les modules d'endo-permutation couverts sont dans la classe d'un élément de $D_R^\Omega(P)$, sauf si P est un groupe quaternionien et M un RP-module de dimension $\frac{|P|}{2} \pm 1$. Par la proposition ci-dessus et par la proposition 7.1 de [Ri], il nous suffit donc de montrer, pour $R = k$, qu'aucun de ces kP-modules exceptionnels ne peut avoir une résolution de permutation endo-scindée.

Le cas $P = Q_8$ a été prouvé par J. Rickard, et il en a fait part à J. Thévenaz, lors d'un entretien privé au congrès d'Oberwolfach en avril 1996. En fait, sa preuve se généralise comme suit à $P = Q_{2^n}$, pour $n \geq 3$.

Soit M un kP-module de dimension $\frac{|P|}{2} \pm 1$ et supposons que M possède une résolution de permutation endo-scindée

$$C. = \left(0 \longrightarrow C_n \xrightarrow{\partial_n} C_{n-1} \xrightarrow{\partial_{n-1}} \dots \xrightarrow{\partial_{-m+2}} C_{-m+1} \xrightarrow{\partial_{-m+1}} C_{-m} \longrightarrow 0\right),$$

où m et n sont deux entiers positifs. Comme les C_i sont des kP-modules de permutation, on a $C_i^* \cong C_i$. Par suite, on peut identifier $C.^*$ au complexe :

$$C.^* = \left(0 \longrightarrow C_{-m} \xrightarrow{\partial^*_{-m+1}} C_{-m+1} \xrightarrow{\partial^*_{-m+2}} \dots \xrightarrow{\partial^*_{n-1}} C_{n-1} \xrightarrow{\partial^*_n} C_n \longrightarrow 0\right),$$

où $(C.^*)_i = C_{-i}$, $\forall\ -m \leq i \leq n$.

Soit $Y. = C.^* \otimes C.$ et notons $d.$ la différentielle de ce complexe. On a

$$Y_l = \bigoplus_{i+j=l} (C_i \otimes C_j^*) = \bigoplus_{i+j=l} (C_i \otimes C_{-j})\ ,\ \forall\ -m-n \leq l \leq m+n.$$

Considérons dans $a(P)$ l'élément

$$x = \sum_{-m-n \leq l \leq m+n} \big((-1)^l \sum_{i+j=l} (C_i \otimes C_{-j})\big) =$$

$$= \sum_{-m\leq i,j\leq n} (-1)^{i+j}(C_i \otimes C_{-j}) = \sum_{-m\leq i,j\leq n} (-1)^{i+j}(C_i \otimes C_j),$$

par commutativité de l'addition dans $a(P)$.

Dans $\mathbb{Z}/2\mathbb{Z}\otimes_{\mathbb{Z}} a(P)$, c'est-à-dire en considérant les coefficients modulo 2 dans l'anneau de Green, on obtient

$$x = \sum_{-m\leq i\leq n} (C_i \otimes C_i) + \sum_{-m\leq i<j\leq n} 2(-1)^{i+j}(C_i \otimes C_j) = \sum_{-m\leq i\leq n} (C_i)^2. \quad (6.5)$$

En effet, on a $C_i \otimes C_j \cong C_j \otimes C_i$ pour tous i et j et donc tous les termes $C_i \otimes C_j$ avec $i \neq j$ "apparaissent" deux fois (avec le même coefficient) dans l'expression de x. Par conséquent, on a $x = Y_0$ dans $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} a(P)$.

D'autre part, par hypothèse, $(Y., d.)$ est scindé et vérifie

$$H_n(Y.) \cong \begin{cases} \mathrm{End}_k M \cong k \oplus L\ , & \text{si } n = 0\ , \\ 0\ , & \text{sinon}\ , \end{cases}$$

pour un kP-module libre L. De l'égalité $\dim M = \frac{|P|}{2} \pm 1$ s'ensuit l'égalité $\dim \mathrm{End}_k M = (\dim M)^2 = 1 + |P|(\frac{|P|}{4} \pm 1)$. Donc L est libre de rang $\frac{|P|}{4} \pm 1$.

Or, par le lemme 6.2.2, on a $Y_i \cong H_i(Y.) \oplus \mathrm{Im}(d_{i+1}) \oplus \mathrm{Im}(d_i)$, $\forall\, i \in \mathbb{Z}$. Il s'ensuit :

$$x = \sum_{-m-n\leq l\leq m+n} (-1)^l Y_l \ = \sum_{-m-n\leq l\leq m+n} (-1)^l H_l(Y.) \ = \ H_0(Y.) \ = \ k \oplus L\ . \quad (6.6)$$

Assertion. Si C est un kP-module de permutation, alors dans la décomposition de $C \otimes C$ en somme directe de kP-modules indécomposables, on a un nombre pair de facteurs libres de rang 1.

(N.B. : par le théorème de Krull-Schmidt, une telle décomposition de $C \otimes C$ est unique à isomorphisme et ordre des facteurs près, ce qui justifie l'expression "la décomposition de $C \otimes C$...".)

Preuve de l'assertion . Par le théorème de Krull-Schmidt, C est isomorphe à une somme directe $\oplus_H k[P/H]$, où H parcourt un ensemble de sous-groupes de P et peut apparaître plusieurs fois dans la somme. Chaque facteur $k[P/H]$ est un kP-module indécomposable et isomorphe au module induit $k\uparrow_H^P$ (cf. paragraphe 27 de [Th1]).

Regardons les différents facteurs qui peuvent apparaître dans $C \otimes C$.

Par la formule de réciprocité de Frobenius et la formule de Mackey (cf. proposition 3.3.3 et théorème 3.3.4 du premier volume de [Be]), on a, pour tous sous-groupes H et K de P,

$$k\uparrow_K^P \otimes\ k\uparrow_H^P \cong \big(k\uparrow_K^P \downarrow_H^P \otimes\ k\big)\uparrow_H^P \cong \sum_{g\in[H\backslash P/K]} \big(k\uparrow_{gK\cap H}^H\big)\uparrow_H^P .$$

D'où, dans $a(P)$:

$$k[P/K] \cdot k[P/H] = \sum_{g\in[H\backslash P/K]} k[P/{}^gK \cap H]. \quad (6.7)$$

Si $|H| = |K| = 1$, alors on a $k[P/K] \cdot k[P/H] = |P|\ kP$, par la relation 6.7. Comme $|P|$ est pair, l'assertion est vérifiée.

Si $|H| > 1$ et $H = K$, alors H contient le centre $Z(P)$ d'ordre 2, car c'est l'unique sous-groupe de P d'ordre 2 (cf. chapitre 5). Par suite, ${}^gH \cap H$ contient toujours $Z(P)$, pour tout $g \in P$ et donc $Z(P)$ agit trivialement sur ce module. Il s'ensuit, par la relation 6.7, que $k[P/H] \cdot k[P/H]$ n'a aucun facteur direct libre de rang 1. Comme 0 est pair, l'assertion est vérifiée.

Finalement, par distributivité dans $a(P)$, on a

$$\big(k[P/H] + k[P/K]\big)^2 = \underbrace{\big(k[P/H]\big)^2}_{(I)} + \underbrace{\big(k[P/K]\big)^2}_{(II)} + \underbrace{2 \sum_{g \in [K\backslash P/H]} k[P/{}^gK \cap H]}_{(III)}.$$

Par les deux cas précédents (I) et (II) ont un nombre pair de facteurs directs libres de rang 1. Et il est clair que (III) a nécessairement un nombre pair de facteurs directs libres de rang 1. D'où l'assertion.

Résumons-nous. D'une part, on a $x = k + (\frac{|P|}{4} \pm 1)kP$ dans $a(P)$, par la relation 6.6. Comme 8 divise $|P|$, le nombre $\frac{|P|}{4} \pm 1$ de facteurs directs libres de rang 1 de x est impair. D'autre part, la relation 6.5 et l'assertion ci-dessus impliquent que x possède un nombre pair de facteurs directs libres de rang 1. D'où une contradiction !

On en conclut que M ne peut pas avoir de résolution de permutation endo-scindée et ceci termine la preuve du théorème.

□

6.3 Exemple

Considérons un groupe semi-diédral P d'ordre 16 et $k = \mathbb{F}_2$. Posons

$$P = <u,\ v \mid u^8 = v^2 = 1,\ {}^vu = u^3> \quad \text{et} \quad V = <v>.$$

Nous allons exhiber des résolutions de permutation endo-scindées de quelques kP-modules endo-triviaux.

On sait, par le théorème 7.1 de [CaTh1] que $T(P)$ est engendré par Ω_P, d'ordre infini, et $[\Omega^1_P(\Omega^1_{P/V}(k))]$, d'ordre 2. Les assertions suivantes résultent immédiatement des relations 6.3 et 6.4.

1. Le complexe $T. = \big(0 \longrightarrow\ k\ \longrightarrow 0\big)$, où $T_0 = k$, est une résolution de permutation endo-scindée du kP-module trivial k.

2. Le complexe $R. = \big(0 \longrightarrow\ k[P/V] \xrightarrow{\partial'_1} k\ \longrightarrow 0\big)$, où $R_1 = k[P/V]$ et où $\partial'_1(x) = 1,\ \forall\, x \in [P/V]$, est une résolution de permutation endo-scindée de $\Omega^1_{[P/V]}(k)$.

   Comme $<[\Omega^1_P(\Omega^1_{P/V}(k))]>$ est cyclique d'ordre 2, on a ainsi une résolution de permutation endo-scindée de chaque kP-module endo-trivial

indécomposable de torsion (toujours à isomorphisme près). Donc, par le lemme 10.2 de [CaTh1], on a exhibé une résolution de permutation endo-scindée de tout kP-module d'endo-permutation indécomposable de torsion.

3. Le complexe $C. = \big(0 \longrightarrow \ kP \xrightarrow{\partial_1} k \ \longrightarrow 0\big)$, où $C_1 = kP$ et où la différentielle est définie par $\partial_1(x) = 1, \ \forall\, x \in P$, est une résolution de permutation endo-scindée de $\Omega^1_P(k)$.

4. Le dual $C.^* = \big(0 \longrightarrow \ k \xrightarrow{\partial_1^*} kP \ \longrightarrow 0\big)$ du complexe $(C.)$ vérifie $C^*_{-1} = kP$ et $\partial_1^*(1) = \sum_{x\in P} x$. C'est une résolution de permutation endo-scindée de $\Omega_P^{-1}(k)$.

5. Considérons le "prolongement"

$$\tilde{C}. = \left(0 \longrightarrow \ kP \ \oplus \ kP \xrightarrow{\partial_2} kP \xrightarrow{\partial_1} k \ \longrightarrow 0\right)$$

du complexe $(C.)$, où l'on définit $\partial_2(x,y) = x(u-1)+y(v-1), \ \forall\, x, \ y \in P$. C'est une résolution de permutation endo-scindée de $\Omega^2_P(k)$.

En effet, soit $D.$ une résolution projective minimale de k. Tous les termes de $(D.)$ étant libres, leur dimension est divisible par 16.

De plus, on a $\dim \Omega^1_P(k) = 15$ et $<\Omega_P> \cong \mathbb{Z}$. Supposons $\dim D_2 = 16$. Cela implique $\dim \Omega^2_P(k) = 1$ et donc $\Omega^2_P(k) \cong k$. Par conséquent, on a $<\Omega_P> \cong \mathbb{Z}/2\mathbb{Z}$. D'où une contradiction. Il s'ensuit qu'on a $\dim D_2 \geq 32$.

Ainsi, il nous suffit de vérifier que $\mathrm{Im}(\partial_2) = \Omega^1_P(k)$. On sait que $\Omega^1_P(k)$ est engendré par $u-1$ et $v-1$. De plus, on a $u-1 = \partial_2(1,0)$ et $v-1 = \partial_2(0,1)$. D'où l'égalité voulue.

6. Le dual $\tilde{C}.^* = \big(0 \longrightarrow \ k \xrightarrow{\partial_1^*} kP \xrightarrow{\partial_2^*} (kP \oplus kP) \ \longrightarrow 0\big)$ du complexe $(\tilde{C}.)$, où on a $\partial_2^*(x) = \sum_{y\in P} \big((x,y)-(y,x)\big), \ \forall\, x \in P$, est une résolution de permutation endo-scindée de $\Omega_P^{-2}(k)$. En effet, par le théorème de Künneth (cf. section 2.7 du premier volume de [Be]), le dual de $\tilde{C}.$ reste exact en kP et on a $\mathrm{Im}(\partial_2^*) \cong \big(\mathrm{Ker}(\partial_2)\big)^*$.

Terminons cet exemple avec la remarque suivante, concernant $\Omega^2_P(k)$. Nous savons qu'il existe un kP-module L projectif (et donc libre) satisfaisant

$$\Omega^2_P(k) \oplus L \cong \Omega^1_P(k) \otimes \Omega^1_P(k),$$

par définition de la loi de composition dans le groupe de Dade. Calculons la dimension de L. On a

$$\dim(\Omega^2_P(k)) = 32 - 15 = 17 \quad \text{et} \quad \dim(\Omega^1_P(k) \otimes \Omega^1_P(k)) = 15^2 = 225.$$

Par suite, $\dim L = 225 - 17 = 208 = 13 \cdot 16$ et donc $L \cong (kP)^{13}$.

Y a-t-il des superstitieux dans l'audience ?

Chapitre 7

Conclusion

Dans ces dernières lignes, nous faisons une synthèse du travail que nous avons accompli durant ces quatre années et que nous avons relaté dans le présent ouvrage. Nous faisons également le point sur les questions encore ouvertes et les principales conjectures actuelles.

Dans la première partie, nous nous sommes intéressés au groupe de Dade de certains p-groupes finis. Nous sommes parvenus à déterminer le groupe de Dade de deux familles de groupes :

- La famille des p-groupes métacycliques pour un nombre premier p impair ;
- La famille des 2-groupes extraspéciaux, de la forme D_8^{*n}, où n est un entier valant au moins 2.

Dans la seconde partie, nous avons focalisé notre attention sur deux situations où les modules d'endo-permutation apparaissent et nous avons obtenu les résultats suivants :

- Nous avons explicitement réalisé tous les modules d'endo-permutation qui peuvent être des sources de modules simples pour des groupes finis p-résolubles.
- Nous avons constaté que parmi tous les modules d'endo-permutation que l'on connaît actuellement, les seuls qui n'ont pas de résolution de permutation endo-scindée sont les modules "exceptionnels" apparaissant pour les groupes quaternioniens.

Cette dernière affirmation soulève la principale question encore ouverte :

> "Existe-t-il des modules d'endo-permutation dont la classe ne peut pas s'exprimer comme combinaison linéaire des syzygies relatifs et des quelques exceptions qui interviennent dans le groupe de Dade des groupes quaternioniens ?"

On conjecture que la réponse est négative, mais on ne peut encore le prouver.

Remarquons, en particulier, que si cette conjecture s'avère exacte, alors il s'ensuivra que tout module d'endo-permutation de torsion indécomposable est source d'un module simple. De plus, nous aurons une réalisation explicite de

chacun de ces modules comme source d'un module simple pour un groupe fini p-nilpotent.

Cela impliquera également qu'à l'exception des modules exceptionnels pour les groupes quaternioniens, tous les modules d'endo-permutation ont une résolution de permutation endo-scindée.

Cependant, même si cette conjecture était démontrée, et de ce fait la classification des modules d'endo-permutation achevée, le travail de recherche autour de ces modules ne serait pas encore terminé. En effet, il resterait en suspens la question de "recollement" que nous avons mentionnée dans le chapitre 2 et que nous aurions pu aborder dans la seconde partie.

Etant donné que ce problème s'étend au-delà de la frontière de la théorie de la représentation des groupes finis et envahit les champs d'intérêts de certains de nos confrères topologues, nul doute que les investigations autour des modules d'endo-permutation ont encore de beaux jours devant elles !

Bibliographie

[Al1] J. L. Alperin, *Invertible modules for groups*, Notices AMS, vol. 24 (1977).

[Al2] J. L. Alperin, *Local representation theory*, Cambridge studies in advanced mathematics 11, Cambridge University Press, 1986.

[Al3] J. L. Alperin, *A construction of endo-permutation modules*, J. Group Theory **4** (2001), 3–10.

[Al4] J. L. Alperin, *Lifting endo-trivial modules*, J. Group Theory **4** (2001), 1–2.

[Be] D. J. Benson, *Representations and cohomology I, II*, Cambridge Studies in advanced Mathematics 30, Cambridge University Press, 1991.

[Bo1] S. Bouc, *Tensor induction of relative syzygies*, J. reine angew. Math. (Crelle), **523** (2000), 113–171.

[Bo2] S. Bouc, *Burnside Rings*, Handbook of Algebra, **2** (2000), 739–804.

[Bo3] S. Bouc, *Non-Additive Exact Functors and Tensor Induction for Mackey Functors*, AMS Memoirs **683**, vol. 144 (2000), 275–349.

[BoTh] S. Bouc and J. Thévenaz, *The group of endo-permutation modules*, Invent. Math. **139** (2000), 275–349.

[Br] M. Broué, *Rickard equivalences and block theory*, Groups '93 Galway/St. Andrews, Vol. 1 (Galway, 1993), 58–79, London Math. Soc. Lecture Note Ser., 211, Cambridge Univ. Press, Cambridge, 1995.

[Ca] J. Carlson, *Endo-trivial modules over (p,p)-groups*, Illinois J. of Math. **2** (1980), 287–295.

[CaRo] J. Carlson, R. Rouquier, *Self-equivalences of stable module categories*, Math. Z. 233, No.1, 165-178 (2000).

[CaTh1] J. Carlson, J. Thévenaz, *Torsion endo-trivial modules*, Algebr. Represent. Theory **3** (2000), 303–335.

[CaTh2] J. Carlson, J. Thévenaz, *The classification of torsion endo-trivial modules*, Preprint (2003).

[CR] C. W. Curtis, I. Reiner, *Methods of representation theory with applications to finite groups and orders I*, Pure and applied mathematics, John Wiley and Sons, 1981.

[Da1] E. C. Dade, *Blocks with cyclic defect groups I*, Ann. Math. **84** (1966), 20-48.

[Da2] E. C. Dade, *Endo-permutation modules over p-groups, I, II*, Ann. Math. **107** (1978), 459–494, **108** (1978), 317–346.

[DH] K. Doerk, T. Hawkes, *Finite soluble groups*, Walter de Gruyter, 1992.

[Di] J. Dietz, *Stable splittings of classifying spaces of metacyclic p-groups, p odd*, J. Pure Appl. Algebra **90** (1993), 115–136.

[Fe] W. Feit, *The Representation Theory of Finite groups*, North Holland Publishing Company, 1982.

[Go] D. Gorenstein, *Finite groups*, Harper and Row, 1968.

[HL] M. E. Harris, M. Linckelmann, *Splendid derived equivalences for blocks of finite p-solvable groups*, J. London Math. Soc. (2) **62** (2000), no. 1, 85–96.

[Hu1] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, 1967.

[Hu2] B. Huppert, *Character theory of finite groups*, Walter de Gruyter, 1998.

[Is] I. M. Isaacs, *Character theory of finite groups*, Acad. Press, 1976.

[Li] M. Linckelmann, *Stable equivalences of Morita type for self-injective algebras and p-groups*, Math. Z. **223** (1996), 87–100.

[Ma1] N. Mazza, *The Dade group of a metacyclic p-group*, J. Algebra, à paraître.

[Ma2] N. Mazza, *Endo-permutation modules as sources of simple modules*, J. Group Theory, à paraître.

[Pu1] L. Puig, *Notes sur les P-algèbres de Dade*, Preprint, 1988.

[Pu2] L. Puig, *Affirmative answer to a question of Feit*, J. Algebra **131** (1990), 513–526.

[Pu3] L. Puig, *Une correspondance de modules pour les blocs à groupes de défaut abéliens*, Geom. Dedic. **37** (1991), 9–43.

[Ri] J. Rickard, *Splendid equivalences : derived categories and permutation modules*, Proc. London math. soc. **3** (1996), 331–358.

[Se] J.-P. Serre, *Représentations linéaires des groupes finis*, Hermann, 1978.

[Su] M. Suzuki, *Group theory II*, Springer, 1986.

[Th1] J. Thévenaz, *G-algebras and modular representation theory*, Oxford, 1995.

[Th2] J. Thévenaz, *Extension of group representations from a normal subgroup*, Comm. Algebra **11** (1983), 391–425.

[Ur] J.-M. Urfer, *Groupe de Dade et modules endo-triviaux*, Travail de Diplôme, Université de Lausanne, 2002.