Projectivité relative et structure locale d'un groupe fini

Erwan Biland

11 février 2011

Résumé

La théorie de Brauer a pour objet d'étudier les groupes finis à travers leurs représentations. Plus précisément, pour un groupe G et un nombre premier p fixés, la structure de la catégorie des représentations de G sur un corps k de caractéristique p est étroitement liée à la nature des p-sous-groupes de G, et en particulier à l'action de G par conjugaison sur ces sous-groupes.

Dans les notes précédentes, [Bil-2010], nous avons décrit la structure «globale» de la catégorie des kG-modules. Nous nous attachons maintenant à explorer sa structure «locale», dans son articulation avec la structure «p-locale» du groupe G. Nous insistons particulièrement sur l'outil central qu'est la projectivité relative, à partir des résultats fondateurs obtenus par Higman et Green à la fin des années 1950.

Table des matières

1 Introduction

Soit G un groupe fini, et R un anneau commutatif (le plus souvent un corps). Une représentation R-linéaire de G est un R-module E muni d'une action linéaire de G, autrement dit un morphisme de groupes $\lambda_E : G \to \mathrm{Aut}_R(E)$.

En notant $RG = \left\{ \sum_{g \in G} a_g\, g\,,\ a_g \in R \right\}$ l'algèbre du groupe G sur l'anneau R, on étend naturellement λ_E en un morphisme d'algèbres $\lambda_E : RG \to \mathrm{End}_R(E)$, qui fait de E un RG-module. Etudier les représentations k-linéaires de G, c'est donc étudier la catégorie ${}_{RG}\mathscr{M}od$ des RG-modules.

Convenons que l'action de G sur E sera toujours, dans ce papier, une action à gauche. En contrepartie, l'anneau $\mathrm{End}_{RG}(E)$ agira à droite sur E, ce qui fera de E un RG-module-$\mathrm{End}_{RG}(E)$. En ce qui concerne $\mathrm{End}_R(E)$, on le fera lui aussi agir à droite, avec le léger inconvénient que la fonction $\lambda_E : RG \to \mathrm{End}_R(E)$ en devient anti-multiplicative.

Signalons au surplus que tous nos modules seront de type fini, sauf mention explicite du contraire. Par abus de notation, ${}_{RG}\mathscr{M}od$ désignera la catégorie des RG-modules de type fini. L'anneau R sera noethérien (et même bien plus), ce qui garantira le caractère abélien de la catégorie ${}_{RG}\mathscr{M}od$.

Enfin on fixe, pour tout ce papier, un nombre premier p. Convenons dès à présent de noter $\mathbb{K}$ un corps de caractéristique nulle, et k un corps de caractéristique p ; cette convention sera précisée par la suite.

La deuxième partie de ce papier rappelle, et complète, les résultats établis dans [Bil-2010] sur la catégorie de modules d'une algèbre de groupe. Ces résultats sont, pour l'essentiel, valables dans un cadre plus général comme celui des algèbres symétriques ou même des algèbres de Frobenius (voir [CuRe-1962], chapitre IX). C'est d'ailleurs ce point de vue qui avait été adopté dans le papier précédent. Nous l'abandonnons ici car nous souhaitons insister sur les théories des caractères développées par Frobenius puis Brauer ; or cette dernière ne semble pas généralisable aux algèbres symétriques.

Nous parlerons assez peu de la position privilégiée du caractère et du bloc principaux ; le bon cadre pour cela est celui des algèbres augmentées (référence ?).

La troisième partie vise à établir précisément quelques résultats d'usage courant sur les idempotents (théorèmes de relèvement, lemmes de Fitting, de Rosenberg).

La quatrième partie introduit la projectivité relative qui permet de faire le lien entre la catégorie des RG-modules et la structure locale du groupe G. Nous rappelons et démontrons des résultats de Higman et Green.

Enfin, la cinquième partie conduit au second *main theorem* de Brauer, clef de voûte de sa théorie des caractères, qui précise la décomposition en blocs des matrices de décomposition généralisées associées au groupe G pour un nombre premier p.

2 Deux théories des caractères

2.1 Les catégories ${}_{\mathbb{K}G}\mathscr{M}od$ et ${}_{kG}\mathscr{M}od$

Voir [Bil-2010] pour un traitement plus détaillé.

Rappelons que $\mathbb{K}$ est de caractéristique nulle. La catégorie ${}_{\mathbb{K}G}\mathscr{M}od$ est semi-simple. Ses composantes sont associées aux classes d'isomorphisme de $\mathbb{K}G$-modules simples $R_1, \ldots, R_m$, auquelles ont peut associer des idempotents primitifs $\varepsilon_1, \ldots, \varepsilon_m$ du centre de l'algèbre $\mathbb{K}G$. On obtient en particulier :

$$Z\mathbb{K}G = \mathbb{K}\varepsilon_1 \oplus \ldots \oplus \mathbb{K}\varepsilon_m.$$

Comme par ailleurs $Z\mathbb{K}G = \bigoplus \mathbb{K}\mathscr{S}C$, où C parcourt l'ensemble des classes de conjugaison de G et $\mathscr{S}C$ représente la somme des éléments de C, ceci prouve que le nombre k de classes d'isomorphisme de $\mathbb{K}G$-modules simples est aussi le nombre de classes de conjugaison dans G.

Conséquence. La dimension de l'algèbre $ZF(G, \mathbb{K})$ des fonctions centrales de G dans $\mathbb{K}$ est égale au nombre de $\mathbb{K}G$-modules irréductibles.

Le corps k est de caractéristique p strictement positive. Si le nombre p divise l'ordre de G, la catégorie ${}_{kG}\mathscr{M}od$ n'est pas semi-simple. Elle se décompose en blocs, associés aux idempotents primitifs $e_1, \ldots, e_n$ du centre de l'algèbre kG. Chacun de ces idempotents est associé à un ensemble de kG-modules irréductibles. On ne dispose pas d'une description simple de kG ou de son centre.

2.2 Les caractères ordinaires de Frobenius

A la fin du 19e siècle, Frobenius a développé une théorie des caractères, qui est extrêmement efficace pour décrire les représentations linaires du groupe fini G sur un corps $\mathbb{K}$ de caractéristique nulle (*représentations ordinaires*). À un $\mathbb{K}G$-module E, on associe la fonction $\chi_E : G \to \mathbb{K},\ g \mapsto \mathrm{tr}_{E/\mathbb{K}}(\rho_E(g))$. Cette fonction est centrale, c'est-à-dire constante sur les classes de conjugaison de G.

La fonction χ_E, appelée le caractère du $\mathbb{K}G$-module E, renferme beaucoup d'information : par exemple, $\chi_E(1) = \dim_{\mathbb{K}}(E)$. En fait, le résultat fondamental de la théorie de Frobenius est même que le caractère χ_E suffit à caractériser le $\mathbb{K}G$-module E à isomorphisme près. L'outil essentiel pour arriver à ce résultat est un outil de moyennisation.

Le morphisme trace. Soit M un $\mathbb{K}G$-module-$\mathbb{K}G$: M est muni de deux actions linéaires de G, l'une à gauche et l'autre à droite, qui commutent. On note $M^G = \{m \in M \mid \forall g \in G,\ gm = mg\}$. On dispose d'une application :

$$\mathrm{Tr}_1^G : M \to M^G,\ m \mapsto \sum_{g\in G} gmg^{-1}.$$

Exemple fondamental. Soient E et F deux $\mathbb{K}G$-modules. Alors $\mathrm{Hom}_{\mathbb{K}}(E,F)$, agissant à droite, possède une structure naturelle de $\mathbb{K}G$-module-$\mathbb{K}G$. On la définit en posant, pour m dans $\mathrm{Hom}_{\mathbb{K}}(E,F)$, g et h dans G, et x dans E :

$$x[g.m.h] = g.[(h.x)m] \quad \text{c'est-à-dire} \quad g.m.h = \lambda_E(h)m\lambda_F(g).$$

Pour tout sous-groupe H de G, on a alors $[\mathrm{Hom}_{\mathbb{K}}(E,F)]^H = \mathrm{Hom}_{\mathbb{K}H}(E,F)$. On dispose ainsi du morphisme trace $\mathrm{Tr}_1^G : \mathrm{Hom}_{\mathbb{K}}(E,F) \to \mathrm{Hom}_{\mathbb{K}G}(E,F)$.

Ici, comme l'ordre de G est inversible dans $\mathbb{K}$, l'application $\frac{1}{|G|}\mathrm{Tr}_1^G$ est une projection d'image exactement M^G. En appliquant cette remarque à l'exemple précédent, on obtient déduit deux résultats importants.

Théorème de Maschke. Soit E un $\mathbb{K}G$-module, et F un sous-module de E. Il existe un sous-module F' de E tel que $E = F \oplus F'$.

Autrement dit, la catégorie ${}_{\mathbb{K}G}\mathscr{M}od$ est semi-simple : tout $\mathbb{K}G$-module E peut s'écrire (de façon non unique) sous la forme $E = R_1^{\alpha_1} \oplus \ldots \oplus R_m^{\alpha_m}$, où les R_i sont des représentants des classes d'isomorphismes de $\mathbb{K}G$ modules irréductibles.

Remarquons que ce résultat reste vrai en remplaçant $\mathbb{K}$ par un corps dont la caractéristique ne divise pas l'ordre de G.

Produit scalaire. L'espace $ZF(G,\mathbb{K})$ des fonctions centrales sur G peut être muni d'un produit scalaire $\langle\cdot,\cdot\rangle_G$ tel que, pour tous $\mathbb{K}G$-modules E et F,

$$\langle\chi_E,\chi_F\rangle_G = \dim_{\mathbb{K}} \mathrm{Hom}_{\mathbb{K}G}(E,F).$$

Explicitement, on a $\langle\chi_E,\chi_F\rangle_G = \left[\mathrm{Tr}_1^G(\chi_{\mathrm{Hom}_{\mathbb{K}}(E,F)})\right](1,1) = \dfrac{1}{|G|}\displaystyle\sum_{g\in G}\chi_E(g^{-1})\chi_F(g),$

Ainsi, si R_i est un $\mathbb{K}G$-module simple, le nombre $\left\langle\chi_{R_i},\chi_E\right\rangle_G$ est tout simplement la multiplicité α_i de R_i comme facteurs directs de E.

Conséquence. Les caractères irréductibles χ_{R_i} sont linéairement indépendant. Par l'argument de dimension énoncé plus haut, on en déduit que les caractères ordinaires irréductibles forment une base de l'algèbre $ZF(G,\mathbb{K})$.

2.3 Les caractères modulaires de Brauer

L'objectif de Brauer est double. Il s'agit d'une part de généraliser la théorie de Frobenius pour décrire les représentations du groupe G sur un corps k dont la caractéristique divise l'ordre de G (ce qu'on appelle les *représentations modulaires*). D'autre part, il s'agit de relier les représentations ordinaires et les représentations modulaires d'un même groupe G.

Soit donc k un corps de caractéristique $p > 0$, et E un kG-module.

Il semble naturel de définir le caractère de E comme précédemment, en posant $\chi_E(g) = \mathrm{tr}_{E/k}(\rho_E(g))$. Mais on s'aperçoit très vite que cette idée est mauvaise. Considérons par exemple un k-espace vectoriel E de dimension p, sur lequel G agit trivialement : $\forall g \in G,\ \forall x \in E,\ gx = x$. Le caractère χ_E serait alors la fonction nulle...

Disgression. On peut remarquer que le même problème s'est posé en géométrie algébrique, lorsqu'on a voulu utiliser des méthodes homologiques pour obtenir des propriétés de fonctions zeta associées à des variétés sur des corps finis : la cohomologie des faisceaux algébriques cohérents donnant des résultats en caractéristique positive, elle n'était pas assez précise pour démontrer les conjectures de Weil. Là aussi, la solution est venu des nombres p-adiques, ou plutôt l-adiques en l'occurence...

C'est paradoxalement en visant le second objectif (relier les représentations ordinaires et modulaires) qu'on atteindra le premier, grâce à un outil arithmétique : les anneaux de valuation discrète.

Système p-modulaire. Soit $\mathbb{K}$ une extension finie de $\mathbb{Q}_p$. Soit $\mathcal{O}$ l'anneau (local) des entiers de $\mathbb{K}$, $\mathfrak{m}$ son idéal maximal, et k son corps résiduel (fini, de caractéristique p). Nous appelerons le triplet $(\mathbb{K}, \mathcal{O}, k)$ un système p-modulaire, suivant [Ben-1984]. Notons $\mathbb{U}_{\mathbb{K}}^{(p')}$ le groupe des racines de l'unité d'ordre premier à p dans $\mathbb{K}$, et $\mathbb{U}_k$ le groupe des racines de l'unité dans k. On sait alors que $\mathbb{U}_{\mathbb{K}}^{(p')}$ est contenu dans $\mathcal{O}$, et que la projection de $\mathcal{O}$ sur k induit un isomorphisme de $\mathbb{U}_{\mathbb{K}}^{(p')}$ sur $\mathbb{U}_k$ (lemme d'Hensel). Si ζ est une racine de l'unité dans k, nous noterons $\tilde{\zeta}$ son unique antécédent par cet isomorphisme.

De manière générale, dans tout ce papier, nous noterons $x \mapsto \bar{x}$ la projection de $\mathcal{O}$ sur k (qui a toujours un sens, au besoin par produit tensoriel), et $y \mapsto \tilde{y}$ le relèvement de k dans $\mathcal{O}$ (auquel on donnera un sens précis pour certains objets, comme on vient de le faire pour les racines de l'unité).

$$\begin{tikzcd}
\mathbb{K} \arrow[d, bend left, "\text{les racines de l'unité de } \mathbb{K} \text{ sont en fait dans } \mathcal{O}"] \\
\mathcal{O} \arrow[u, hook] \arrow[d] \\
k \arrow[u, bend right, "\text{relèvement des racines de l'unité}"']
\end{tikzcd}$$

Caractère modulaire. Soit E un kG-module. Pour $g \in G$, notons $\zeta_1, \ldots, \zeta_n$ les valeurs propres de $\lambda_E(g)$ (avec multiplicité), et posons :

$$\varphi_E(g) = \tilde{\zeta}_1 + \ldots + \tilde{\zeta}_n \in \mathbb{K}.$$

La fonction φ_E ainsi définie sera appelée le caractère modulaire de E.

Problème de rationalité. On n'a volontairement pas supposé le corps $\mathbb{K}$ «assez gros». Il peut donc arriver que le corps résiduel k ne contienne pas toutes les valeurs propres de $\lambda_E(g)$. Dans ce cas, les $\tilde{\zeta}_i$ se trouvent dans une extension algébrique de $\mathbb{K}$, mais la valeur $\varphi_E(g)$ obtenue sera tout de même dans $\mathbb{K}$, et même dans $\mathcal{O}$.

Retour sur les définitions précédentes. Par définition de φ_E, pour tout $g \in G$, on a $\overline{\varphi_E(g)} = \mathrm{tr}_{E/k}(\lambda_E(g))$. Mais le caractère modulaire φ_E contient plus d'information que le caractère «naïf» $\bar{\varphi}_E$. Par exemple, $\varphi_E(1) = \dim_k E$. Mais on peut aussi retrouver grâce à φ_E le noyau de λ_E, le centre de $\lambda_E(G)$...

Il ne faut pas pour autant surestimer l'information apportée par φ_E. Pour $g \in G$, il existe une unique décomposition $g = rs = sr$, avec r un p'-élément, ou élément p-régulier, de G (son ordre est premier à p) et s un p-élément, ou élément p-singulier (son ordre est une puissance de p). Comme r et s commutent, on peut co-trigonaliser les matrices $\lambda_E(r)$ et $\lambda_E(s)$, si nécessaire sur une extension algébrique de k. Or $s-1$ est nilpotent, donc la matrice de s est unipotente ; on en déduit que $\lambda_E(g)$ et

$\lambda_E(r)$ ont les mêmes valeurs propres, donc que $\varphi_E(g) = \varphi_E(r)$. Il est donc raisonnable de considérer le caractère modulaire φ_E comme une fonction centrale sur $G_{p'}$, l'ensemble des éléments p-réguliers de G, et non sur G tout entier.

Il y a à cela une autre raison. Soit E un $\mathscr{O}G$-module, libre comme $\mathscr{O}$-module. On dispose alors d'une fonction trace $\mathrm{tr}_{E/\mathscr{O}}$. On peut définir ainsi un caractère de E, que nous noterons χ_E car il coïncide en fait avec le caractère ordinaire du $\mathbb{K}G$-module $\mathbb{K} \otimes_{\mathscr{O}} E$. On peut aussi associer à E le kG-module $\bar{E}$, et donc le caractère modulaire $\varphi_{\bar{E}}$. Pour $g \in G$, notons $\zeta_1, \ldots, \zeta_n$ les valeurs propres de $\lambda_E(g)$. Alors les valeurs propres de $\lambda_{\bar{E}}(g) = \overline{\lambda_E(g)}$ sont clairement $\bar{\zeta}_1, \ldots, \bar{\zeta}_n$. Ainsi $\chi_E(g) = \zeta_1 + \ldots + \zeta_n$ et $\varphi_E(g) = \tilde{\bar{\zeta}}_1 + \ldots + \tilde{\bar{\zeta}}_n$, donc $\bar{\chi}_E(g) = \bar{\varphi}_E(g)$. Mais, si l'un des ζ_i est une racine de l'unité d'ordre non premier à p, on a $\zeta_i \neq \tilde{\bar{\zeta}}_i$, et donc *a priori* $\chi_E(g) \neq \varphi_E(g)$. Par contre ceci ne peut pas se produire si g est un élément p-régulier : dans ce cas $\chi_E(g) = \varphi_E(g)$.

En conclusion, nous décidons définitivement de considérer les caractères modulaires comme des fonctions centrales sur $G_{p'}$. Avec cette convention, nous venons de prouver que $\varphi_{\bar{E}}$ est la restriction à $G_{p'}$ de χ_E. Signalons tout de même, dès à présent, que cette restriction ne sera pas nécessaire pour les caractères modulaires des kG-modules *projectifs*, comme on le verra au prochain paragraphe.

Indépendance linéaire des caractères modulaires. Si $S_1, \ldots, S_n$ sont des kG-modules irréductibles deux à deux non isomorphes, alors les caractères modulaire $\varphi_{S_1}, \ldots, \varphi_{S_n}$ sont linéairement indépendants. On en déduit que le caractère modulaire φ_E d'un kG-module E détermine entièrement les classes d'isomorphisme des facteurs de composition de E (c'est-à-dire l'image de E dans le groupe de Grothendieck de la catégorie ${}_{kG}\mathscr{M}od$). Dans le cas particulier où E est semi-simple, le caractère modulaire φ_E détermine la classe d'isomorphisme de E.

> **Démonstration.** L'application naturelle de kG sur $\prod_{i=1}^n \lambda_{S_i}(kG)$ est surjective. Chaque $\lambda_{S_i}(kG)$ est une k-algèbre simple, donc isomorphe à $\mathscr{M}_{r_i}(D_i)$, où D_i est une algèbre à division de dimension finie sur k. Mais k est fini, donc D est en fait une extension (commutative) finie de k. Via cette identification, on a $\bar{\varphi}_{S_i} = \mathrm{tr}_{D/k} \circ \mathrm{tr}_{\mathscr{M}_{r_i}(D_i)/D_i} \circ \lambda_{M_i}$. Comme $\mathrm{tr}_{D/k}$ et $\mathrm{tr}_{\mathscr{M}_{r_i}(D_i)/D_i}$ sont surjectives, il existe $x_i \in kG$ tel que $\bar{\varphi}_{S_j}(x_i) = \delta_{i,j}$ pour tout j. On en déduit que les fonctions $\bar{\varphi}_{S_1}, \ldots, \bar{\varphi}_{S_n}$ sont linéairement indépendants sur k, puis que les caractères modulaires $\varphi_{S_1}, \ldots, \varphi_{S_n}$ sont linéairement indépendants sur $\mathscr{O}$, donc sur $\mathbb{K}$. ☐

Conséquence. Si $S_1, \ldots, S_n$ sont des représentants des classes d'isomorphismes de kG-modules irréductibles, alors la famille $(\varphi_{S_1}, \ldots, \varphi_{S_n})$ de leurs caractères modulaires est une base de l'algèbre $ZF(G_{p'}, \mathbb{K})$. En particulier, le nombre n est égal au nombre de classes de conjugaison de p'-éléments dans G.

> **Démonstration.** Nous savons déjà que les φ_{S_i} sont linéairement indépendants. Reste à prouver qu'ils sont générateurs.
>
> Soit $\psi : G_{p'} \to \mathbb{K}$ une fonction centrale, et $\tilde{\psi}$ un prolongement (quelconque) de ψ en une fonction centrale sur G. Comme les caractères ordinaires irréductibles engendre $ZF(G, \mathbb{K})$, il existe des scalaires λ_i tels que $\tilde{\psi} = \lambda_1 \chi_{R_1} + \ldots + \lambda_m \chi_{R_m}$. Nous avons déjà vu comment associer à R_i un kG-module $\bar{R}_i$ dont le caractère modulaire $\varphi_{\bar{R}_i}$ est la restriction à $G_{p'}$ du caractère ordinaire χ_{R_i}. Ainsi $\psi = \lambda_1 \varphi_{\bar{R}_1} + \ldots + \lambda_m \varphi_{\bar{R}_m}$ est combinaison linéaire de caractères modulaires, donc de caractères modulaires irréductibles. ☐

Nous préciserons ce résultat au paragraphe 4.4, grâce à l'introduction des kG-modules projectifs.

3 Quelques résultats d'usage courant

3.1 Théorèmes de relèvement

Relèvement des idempotents (1). Soit A un anneau, et I un idéal bilatère de A tel que l'application naturelle $A \mapsto \varprojlim_{n \geqslant 1} A/I^n$ soit un isomorphisme ($\bigcap_{n \geqslant 1} I^n = 0$ et A est complet pour la topologie I-adique).

Alors tout idempotent $e \in A/I$ se relève en un idempotent $\tilde{e} \in A$. Plus précisément, toute famille d'idempotents orthogonaux $e_1, \dots, e_\ell$ dans A/I se relève en une famille d'idempotents orthogonaux $\tilde{e}_1, \dots, \tilde{e}_\ell$ dans A.

Démonstration. Commençons par un calcul. Soit J un idéal de A et $a \in A$ tel que $a - a^2 \in J$. Posons $b = 1 - (1 - a^2)^2$. Alors $a - b = (1 - a - a^2)(a - a^2) \in J$, et $b - b^2 = (1 - a^2)^2 - (1 - a^2)^4 = (2 - a^2)(a - a^2)^2 \in J^2$. On notera dans la suite $f : A \to A, a \mapsto 1 - (1 - a^2)^2$.

Soit maintenant e un idempotent de A/I, et $a \in A$ un antécédent quelconque de e. En particulier $e - e^2 = 0$ donc $a - a^2 \in I$. Considérons la suite (a_n) définie par $a_0 = a$ et, pour tout $n \in \mathbb{N}$, $a_{n+1} = f(a_n)$. Alors, d'après le calcul précédent, on montre par récurrence $a_{n+1} - a_n \in I^{2^n}$ (donc la suite converge dans A, pour la topologie I-adique, vers un élément que nous noterons $\tilde{e}$; de plus $\tilde{e} - a_0 \in I$), et $a_n - {a_n}^2 \in I^{2^n}$ (donc $\tilde{e} - \tilde{e}^2 = \lim_{n\to\infty} a_n - {a_n}^2 = 0$). Ainsi $\tilde{e}$ est un idempotent de A relevant e.

Pour le résultat plus précis, on raisonne par récurrence. Pour $k \in [\![1, n]\!]$, notons $e'_k = e_k + \dots + e_n$, et supposons avoir relevé la famille d'idempotents orthogonaux $e_1, \dots, e_{k-1}, e'_k$ de A/I en une famille d'idempotents orthogonaux $\tilde{e}_1, \dots, \tilde{e}_{k-1}, \tilde{e}'_k$ de A/I. Notons $A_k = \tilde{e}'_k A \tilde{e}'_k$, et $I_k = \tilde{e}'_k I \tilde{e}'_k$. Alors I_k est un idéal bilatère de l'anneau A_k, et e_k est un idempotent de l'anneau $A_k/I_k \simeq e'_k(A/I)e'_k$. Il existe donc un idempotent $\tilde{e}_k$ relevant e_k dans l'anneau A_k ; de plus $\tilde{e}'_{k+1} = \tilde{e}'_k - \tilde{e}_k$ est un idempotent de A_k relevant e'_{k+1}, et orthogonal à $\tilde{e}_k$. Enfin, $\tilde{e}_k$ et $\tilde{e}_{k+1}$ sont des éléments de A contenus dans A_k, donc orthogonaux à $\tilde{e}_1, \dots, \tilde{e}_{k-1}$. Ainsi $\tilde{e}_1, \dots, \tilde{e}_k, \tilde{e}'_{k+1}$ sont des idempotents orthogonaux de A, et l'hérédité est prouvée. $\square$

Ce résultat s'applique en particulier pour A une $\mathscr{O}$-algèbre, et $I = \mathfrak{m}A$ ou $I = J(A)$; il s'applique aussi pour A une k-algèbre, et $I = J(A)$.

On en déduit aisément qu'un idempotent primitif de A s'envoie sur un idempotent primitif de A/I et, réciproquement, qu'un idempotent primitif de A/I peut se relèver en un idempotent primitif de A.

Remarquons par contre que le relèvement n'est pas unique. Par exemple, si on prend $A = \mathscr{M}_2(\mathbb{Z}_p)$, $I = pA$ et $e = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in A/I = \mathscr{M}_2(\mathbb{F}_p)$, on peut choisir, dans A, $\tilde{e} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ ou $\tilde{e} = \begin{pmatrix} 1 & p \\ 0 & 0 \end{pmatrix}$.

Relèvement des idempotents (2). Avec les mêmes hypothèses, si de plus A est un anneau commutatif, alors le relèvement est unique.

Démonstration. Supposons qu'il existe dans A deux idempotents a et b tels que $a - b \in I$. Posons $c = a(1 - b)$. Alors $c = a(a - b)$ est dans l'idéal I. Mais par ailleurs c est un idempotent, car a et b commutent. Donc $c \in I^n$ pour tout $n \in \mathbb{N}^*$, ce qui entraîne $c = 0$. Ainsi $a = ab$; de même $b = ab$, donc $a = b$. $\square$

Relèvement des idempotents (3). Soit $\pi : A \to B$ un morphisme surjectif de k-algèbres commutatives de dimensions finies. Alors tout idempotent $e \in B$ se relève en un idempotent $\tilde{e} \in A$. Plus précisément, toute famille d'idempotents orthogonaux $e_1, \dots, e_\ell$ dans B se relève en une famille d'idempotents orthogonaux $\tilde{e}_1, \dots, \tilde{e}_\ell$ dans A.

Démonstration. On note $\bar{A} = A/J(A)$ et $\bar{B} = B/J(B)$. Alors π induit un morphisme surjectif $\bar{\pi} : \bar{A} \to \bar{B}$. De plus les algèbres $\bar{A}$ et $\bar{B}$ sont semi-simples, donc $\bar{B}$ peut être vu comme un facteur direct de $\bar{A}$, ce qui permet de relever les idempotents de $\bar{B}$ dans $\bar{A}$. L'énoncé (1), ci-dessus, permet de se ramener dans A. Enfin, l'unicité énoncée en (2) montre que les idempotents obtenus dans A relèvent bien les idempotents dont on était parti dans B. $\square$

On a maintenant, outre le produit tensoriel, deux outils pour «naviguer» entre les différentes catégories de G-modules qui nous intéressent.

$$\begin{tikzcd}
{}_{\mathbb{K}G}\mathscr{M}od \arrow[d, bend left, "\text{choix d'un réseau } G\text{-stable}"] \\
{}_{\mathscr{O}G}\mathscr{M}od \cap {}_{\mathscr{O}}\mathscr{P}roj \arrow[u] \arrow[d] \\
{}_{kG}\mathscr{M}od \arrow[u, bend right, "\text{relèvement des idempotents de } (kG)^H"']
\end{tikzcd}$$

Si E est un $\mathbb{K}G$-module, on peut choisir un réseau de E, c'est-à-dire un sous-$\mathscr{O}$-module E' de type fini et de rang maximal (égal à $\dim_{\mathbb{K}} E$). En posant $E'' = \sum_{g\in G} gE'$, on obtient un réseau de E, qui plus est stable par l'action de G. Ainsi E'' est un $\mathcal{O}G$-module de type fini, libre comme $\mathcal{O}$-module, tel que $\mathbb{K} \otimes_{\mathcal{O}} E'' \simeq E$.

En ce qui concerne le relèvement des idempotents, il ne faut surtout pas oublier l'hypothèse de surjectivité. Typiquement, si H est un sous-groupe de G, l'application évidente $(\mathcal{O}G)^H \to (kG)^H$ est surjective, car on peut expliciter des bases des algèbres de départ et d'arrivée. On peut donc, dans ce cadre, relever les idempotents. Par contre, si M est un $\mathcal{O}G$-module, et $\bar{M} = k \otimes_{\mathcal{O}} M$ le kG-module associé, l'application évidente $\mathrm{End}_{\mathcal{O}H}(M) \to \mathrm{End}_{kH}(\bar{M})$ ne semble généralement pas surjective (**exemple ?**). Il est donc faux, par exemple, qu'un facteur direct du kH-module $\bar{M}$ se relève en un facteur direct du $\mathcal{O}H$-module M (et c'est l'expérience qui parle...).

3.2 Lemmes de Fitting et Rosenberg

Définition. On dit qu'un anneau A est local si le quotient $A/J(A)$ est une algèbre à division, $J(A)$ étant le radical de Jacobson de A.

Lemme (Fitting). Soit G un groupe, et L un $\mathcal{O}G$-module. Le module L est indécomposable si, et seulement si, la $\mathcal{O}$-algèbre $\mathrm{End}_{\mathcal{O}G}(L)$ est locale.

Démonstration. Notons $A = \mathrm{End}_{\mathcal{O}G}(L)$. Dire que L est indécomposable est équivalent à dire qu'il n'existe pas d'idempotent non trivial dans l'algèbre A.

Si A est une $\mathcal{O}$-algèbre qui ne possède pas d'idempotent autre que 1 et 0, par le théorème de relèvement des idempotents, il en est de même de $A/J(A)$. Mais $A/J(A)$ est une k-algèbre semi-simple, donc $A/J(A)$ est simple, c'est-à-dire qu'il existe une k-algèbre à division D et un entier n tel que $A/J(A) \simeq \mathcal{M}_n(D)$. Pour que $\mathcal{M}_n(D)$ ne possède pas d'idempotent non trivial, il faut de plus $n = 1$, d'où $A/J(A) \simeq D$. Ceci prouve que A est une $\mathcal{O}$-algèbre locale.

Réciproquement, supposons que la $\mathcal{O}$-algèbre A est locale, et soit e un idempotent de A. Notons par une barre la réduction modulo $J(A)$. Comme $A/J(A)$ est un corps, $\bar{e} = 1$ ou $\bar{e} = 0$. Quitte à remplacer e par $1 - e$, plaçons-nous dans le deuxième cas. Alors $e \in J(A)$. Or $\bigcap_{n \in \mathbb{N}} J(A)^n = 0$, donc $e = 0$. Ceci prouve qu'il n'y a pas d'idempotent non trivial dans A. □

Remarque. Dans le cas où le $\mathcal{O}G$-module L possède une suite de composition (en particulier si L est en fait un k-module), ceci est une conséquence de la forme classique du lemme de Fitting ($L = \ker u^\infty \oplus \mathrm{im}\, u^\infty$). Mais cette formulation a l'inconvénient de mal se généraliser à un $\mathcal{O}$-module quelconque.

Lemme (Rosenberg). Soit A une $\mathcal{O}$-algèbre, et e un idempotent primitif de A. Si e appartient à une somme d'idéaux bilatères $\sum_\alpha I_\alpha$, alors e appartient à l'un des I_α.

Démonstration. Comme e est un idempotent primitif de A, l'algèbre eAe, d'unité e, ne possède aucun idempotent non trivial. D'après la démonstration précédente, c'est donc une algèbre locale, et tout idéal bilatère propre de eAe est contenu dans $J(eAe)$. Mais $e \in \sum_\alpha (eAe \cap I_\alpha)$, donc il existe un α tel que $eAe \cap I_\alpha$ ne soit pas contenu dans $J(eAe)$. Mais alors $e \in eAe \cap I_\alpha$, ce qui achève la preuve. □

4 Projectivité relative

La catégorie des kG-module n'est pas semi-simple, c'est-à-dire qu'il existe dans cette catégorie des extensions non scindées. Ceci est équivalent à dire qu'il existe des objets non projectifs dans cette catégorie. Pour ne pas s'arrêter à ce constat de non-projectivité de certains objets, nous allons développer dans cette partie une théorie de la projectivité relative, due à Higman et Green, qui cherche à mesurer le *défaut de projectivité* des objets. Concrètement, ce défaut sera mesuré, pour chaque kG-module indécomposable E, par un p-sous-groupe de G, ou plutôt une classe de conjugaison de p-sous-groupes, appelés *vortex* de E.

Nous obtiendrons ainsi une classification des indécomposables de ${}_{kG}\mathcal{M}od$, en associant à chaque E un couple (P, J), où P est un vortex de E et J un kP-module indécomposable, appelé *source* de

E et défini à G-conjugaison près. Cette classification est très fine au sens où chaque couple (P, J) correspond à un nombre fini d'indécomposables de ${}_{kG}\mathscr{M}od$. Elle est par contre impossible à expliciter en pratique car, dès que le groupe P n'est pas cyclique, la catégorie des kP-modules est *sauvage* (beaucoup, beaucoup d'indécomposables).

Quoiqu'il est soit, nous voyons que la projectivité relative met en évidence un lien étroit entre la catégorie des modules sur kG et les relations d'incidence *à conjugaison près* entre p-sous-groupes de G. C'est ce qui en fait une théorie *locale* sur G.

4.1 Critère de Higman

Définition. Soit $j : A \to B$ un morphisme d'anneaux, et E un B-module. On dit que E est un module relativement (B, A)-projectif si, pour toute épimorphisme $f : X \to Y$ dans la catégorie ${}_{B}\mathscr{M}od$, *scindé dans la catégorie* ${}_{A}\mathscr{M}od$, tout morphisme de B-modules $u : E \to Y$ se relève en un morphisme de B-modules $\tilde{u} : E \to X$ qui rend commutatif le diagramme :

$$\begin{tikzcd} & E \arrow[dl, dotted, "\tilde{u}"'] \arrow[d, "u"] & \\ X \arrow[r, shift left, "f"] & Y \arrow[l, shift left, squiggly] \arrow[r] & 0 \end{tikzcd}$$

(la flèche ondulée représente le morphisme de A-module qui scinde f).

Caractérisation. Soit E un B-module de type fini. On a équivalence entre les propriétés :

(i) E est relativement (B, A)-projectif ;

(ii) E est un facteur direct du B-module $\mathrm{Ind}_A^B L = B \otimes_A L$, pour un A-module L ;

(iii) E est un facteur direct du B-module $\mathrm{Ind}_A^B \mathrm{Res}_A^B E = B \otimes_A E$.

Démonstration.

$\boxed{(i)\Rightarrow(iii)}$ Le morphisme d'adjonction $f : B \otimes_A E \to E$, $(b \otimes e) \mapsto be$, est scindé par le morphisme de A-modules $g : E \to B \otimes_A E$, $e \mapsto (1 \otimes e)$. Si E est relativement projectif, on peut donc relever le morphisme Id_E en un morphisme de B-modules $\tilde{u} : E \to B \otimes_A E$, qui fait de E un facteur direct du module induit $B \otimes_A E$.

$\boxed{(iii)\Rightarrow(ii)}$ C'est immédiat.

$\boxed{(ii)\Rightarrow(i)}$ Supposons E facteur direct du B-module $B \otimes_A L$, et notons ι, π l'injection de E dans $B \otimes_A L$ et une projection de $B \otimes_A L$ sur E. Considérons un diagramme comme ci-dessus, avec $g \in \mathrm{Hom}_A(Y, X)$ tel que $fg = \mathrm{Id}_Y$. Notons $v : L \to X, \ell \mapsto g \circ u \circ \pi(1 \otimes \ell)$. C'est un morphisme de A-modules. Par la propriété universelle de l'induction, v se prolonge en un unique morphisme de B-modules $\tilde{v} : B \otimes_A L \to X$, $(b \otimes \ell) \mapsto bv(\ell)$. On vérifie immédiatement que $f \circ \tilde{v} = u \circ \pi$, puisque :

$$f \circ \tilde{v}(b \otimes \ell) = f(bv(\ell)) = bf \circ v(\ell)) = bf \circ g \circ u \circ \pi(1 \otimes \ell) = bu \circ \pi(1 \otimes \ell) = u \circ \pi(b \otimes \ell).$$

Finalement, en posant $\tilde{u} = \tilde{v} \circ \iota$, on obtient $f \circ \tilde{u} = f \circ \tilde{v} \circ \iota = u \circ \pi \circ \iota = u$.

Ainsi E est bien relativement projectif. $\square$

Définition. En vue du critère de Higman, il sera utile de parler de projectivité relative pour des morphismes, et non des modules. On dira qu'un morphisme $u \in \mathrm{Hom}_B(E, F)$ est relativement (B, A)-projectif s'il se factorise via un module relativement projectif (ou, ce qui revient au même, par un module induit $\mathrm{Ind}_A^B L$). On remarque que cette définition généralise, en quelque sorte, la précédente, puisqu'un module E est relativement projectif si, et seulement si, le morphisme Id_E est relativement projectif.

Dorénavant, on notera R, indifféremment, l'anneau $\mathscr{O}$ ou k (si rien n'est précisé, les définitions et résultats valent pour ces deux cas de figure). On fixe un sous-groupe H du groupe fini G, et on étudie les définitions précédentes pour $A = RH$ et $B = RG$, j étant l'injection canonique.

Les résultats énoncés ci-dessous sont valables dans un contexte plus large (algèbre symétriques, voire algèbres de Frobenius), mais on ne le développera pas ici.

Trace relative. Soit M un RG-module-RG. Pour $K \leqslant G$, notons $M^K = \{m \in M \mid \forall k \in K,\ kmk^{-1} = m\}$. Considérons alors l'application $\mathrm{Tr}_H^G : M^H \to M^G$ définie par :

$$\mathrm{Tr}_H^G(m) = \sum_{g \in G/H} g.m.g^{-1}.$$

Nous ne rappelons pas ici les identités classiques vérifiées par la fonction trace, que le lecteur pourra vérifier quand elle seront utilisées. Elles sont exposées dans [AlBr-1979].

Exemple fondamental. Soient E et F deux RG-modules. Alors, comme nous l'avons vu au paragraphe 2.2, $\mathrm{Hom}_R(E,F)$ est naturellement un RG-bimodule. De plus, pour $K \leqslant G$, nous avons $[\mathrm{Hom}_R(E,F)]^K = \mathrm{Hom}_{RK}(E,F)$. Il faut noter que l'image du morphisme trace relative Tr_H^G : $\mathrm{Hom}_{RH}(E,F) \to \mathrm{Hom}_{RG}(E,F)$ est un *idéal bilatère* en un sens très fort : pour tous $u \in \mathrm{Hom}_{RG}(E',E)$, $v \in \mathrm{Hom}_{RH}(E,F)$, $w \in \mathrm{Hom}_{RG}(F,F')$, on a $\mathrm{Tr}_H^G(w \circ v \circ u) = w \circ \mathrm{Tr}_H^G(v) \circ u$.

Critère de Higman. Soient E et F deux RG-modules. Alors $\mathrm{Hom}_R(E,F)$ est un RG-bimodule. L'image du morphisme Tr_H^G : $\mathrm{Hom}_{RH}(E,F) \to \mathrm{Hom}_{RG}(E,F)$ est l'ensemble $\mathrm{Hom}_{RH}^{RG}(E,F)$ des homomorphismes de RG-modules relativement (RG,RH)-projectifs de E dans F.

Démonstration.
On note $i_H : RH \to RG$ l'injection canonique, et $t_H : RG \to RH$ définie par $t_H\left(\sum_{g\in G} \alpha_g g\right) = \sum_{h \in H} \alpha_h h$.
Ce sont des morphismes de RH-modules. De plus $t_H \circ i_H = \mathrm{Id}_{RH}$ et $\mathrm{Tr}_H^G(i_H \circ t_H) = \mathrm{Id}_G$.

$\boxed{\Rightarrow}$ Soit $u \in \mathrm{Hom}_{RH}^{RG}(E,F)$. Il existe un RH-module L et des morphismes $w : E \to \mathrm{Ind}_{RH}^{RG} L$ et $v : \mathrm{Ind}_{RH}^{RG} L \to F$ tels que $u = v \circ w$.
On écrit $u = v \circ [\mathrm{Id}_{RG} \otimes \mathrm{Id}_L] \circ w$. Or il existe $f \in \mathrm{End}_{RH}(RG)$ tel que $\mathrm{Id}_{RG} = \mathrm{Tr}_H^G(f)$. Alors :

$$u = v \circ [\mathrm{Tr}_H^G(f) \otimes \mathrm{Id}_L] \circ w = v \circ \mathrm{Tr}_H^G[f \otimes \mathrm{Id}_L] \circ w = \mathrm{Tr}_H^G\Big(v \circ [f \otimes \mathrm{Id}_L] \circ w\Big).$$

Ainsi u appartient à l'image de la fonction trace relative de H à G.

$\boxed{\Leftarrow}$ Soit $u = \mathrm{Tr}_H^G(v)$, avec $v \in \mathrm{Hom}_{RH}(E,F)$. En identifiant le RH-module E à $RH \otimes_{RH} E$, il existe un unique morphisme de RG-modules $\tilde{v} : \mathrm{Ind}_{RH}^{RG} E \to F$ tel que $v = \tilde{v} \circ [i_H \otimes \mathrm{Id}_E]$. Alors :

$$u = \mathrm{Tr}_H^G(v) = \mathrm{Tr}_H^G\left(\tilde{v} \circ [i_H \otimes \mathrm{Id}_E]\right) = \tilde{v} \circ \mathrm{Tr}_H^G[i_H \otimes \mathrm{Id}_E].$$

Ainsi v se factorise via un module induit de RH à RG : v est relativement (RG,RH) projectif. ☐

Remarque. Soit P un p-sous-groupe de Sylow de H. Alors $\mathrm{Tr}_P^G = \mathrm{Tr}_H^G \circ \mathrm{Tr}_P^H$. Or l'entier $[H:P]$ est inversible dans R, donc $\frac{1}{[H:P]}\mathrm{Tr}_P^H : M^P \to M^H$ est un projecteur d'image M^H. Ainsi $\mathrm{im}\,\mathrm{Tr}_H^G = \mathrm{im}\,\mathrm{Tr}_P^G$. En particulier, il est équivalent pour un module d'être relativement (RG,RH)-projectif ou relativement (RG,RP)-projectif. L'étude de la projectivité relative concerne donc en réalité uniquement les p-sous-groupes de G, c'est en cela qu'elle apporte des informations sur la structure *p-locale* du groupe G.

4.2 Vortex et source d'un indécomposable

Vortex d'un RG-module indécomposable [Gre-1959]. Soit E un RG-module indécomposable. Notons $\mathscr{V}_E$ l'ensemble des sous-groupes H de G tels que E soit relativement (RG,RH)-projectif. Cet ensemble, muni du préordre partiel $\leqslant_G$, admet un élément minimum V_E, qui est un p-sous-groupe unique à conjugaison près. Le sous-groupe V_E est appelé vortex du RG-module indécomposable E.

Démonstration. L'ensemble $\mathscr{V}_E$ est manifestement fini, donc l'existence d'un élément minimal est immédiate. Montrons qu'il est minimum, ce qui entraînera l'unicité à conjugaison près. Pour cela, nous allons prouver que $(\mathscr{V}_E, \leqslant_G)$ est un treillis, à savoir que tout couple d'éléments admet un minorant commun.

Soient H et K deux éléments de $\mathscr{V}_E$.

Alors $\mathrm{Id}_E \in \mathrm{im}\,\mathrm{Tr}_H^G \cap \mathrm{im}\,\mathrm{Tr}_K^G$. Il existe donc $u \in \mathrm{End}_{RH}(E)$ et $v \in \mathrm{End}_{RK}(E)$ tels que $\mathrm{Id}_E = \mathrm{Tr}_H^G(u) = \mathrm{Tr}_K^G(v)$. Mais alors :

$$\mathrm{Id}_E = \mathrm{Tr}_H^G(u)\mathrm{Tr}_K^G(v) = \sum_{g \in K\backslash G/H} \mathrm{Tr}_{H\cap K^g}^G(u.v^g) \quad \in \quad \sum_{g\in G} \mathrm{im}\,\mathrm{Tr}_{H\cap K^g}^G.$$

Or E est indécomposable donc, par le lemme de Fitting, $\mathrm{End}_{RG}(E)$ est une algèbre locale. Par ailleurs, comme on l'a vu plus haut, les $\mathrm{im}\,\mathrm{Tr}_{H\cap K^g}^G$ sont des idéaux bilatères, dont la somme contient Id_E, c'est-à-dire est égale à $\mathrm{End}_{RG}(E)$. Donc il existe au moins un $g \in G$ tel que $\mathrm{im}\,\mathrm{Tr}_{H\cap K^g}^G = \mathrm{End}_{RG}(E)$, et donc $\mathrm{Id}_E \in \mathrm{Tr}_{H\cap K^g}^G$.

Ainsi $H \cap K^g$ appartient à $\mathscr{V}_E$, et minore à la fois H et K pour le préordre $\leqslant_G$, ce qui prouve le résultat annoncé.

Enfin, V_E est un p-groupe d'après la remarque faite au paragraphe précédent sur les p-groupes et la projectivité relative. □

Vortex et restriction. Soit E un RG-module indécomposable, P un vortex de E et H un sous-groupe de G. Si F est une composante du kH-module $\mathrm{Res}_H^G E$, et Q un vortex de F, alors il existe $g \in G$ tel que $Q \leqslant_H P^g \cap H$. Si, de plus, E est relativement (RG, RH)-projectif, on peut supposer $P \leqslant H$; alors il existe au moins une composante F de $\mathrm{Res}_H^G E$ admettant P pour vortex.

Démonstration. Par le critère de Higman, il existe $u \in \mathrm{End}_{kP}(E)$ tel que :

$$\mathrm{Id}_E = \mathrm{Tr}_P^G(u) = \sum_{g\in H\backslash G/P} \mathrm{Tr}_{P^g\cap H}^H(u^g)$$

Ainsi Id_F, qui se factorise par Id_E, appartient à la somme des idéaux bilatères $\mathrm{im}\,\mathrm{Tr}_{P^g\cap H}^H$. Par le lemme de Rosenberg, il existe $g \in G$ tel que $\mathrm{Id}_F \in \mathrm{im}\,\mathrm{Tr}_{P^g\cap H}^H$. Ainsi F est relativement $(RH, R[P^g \cap H])$-projectif, d'où le premier résultat.

Si maintenant $P \leqslant H$, on sait que E est un facteur direct de $\mathrm{Ind}_H^G \mathrm{Res}_H^G E$, donc de $\mathrm{Ind}_h^G F$ pour au moins une composante F de $\mathrm{Res}_H^G E$. Si ce F a un vortex Q strictement plus petit que P, alors E est relativement (RH, RQ)-projectif, ce qui contredit la minimalité de P. On obtient ainsi le second résultat. □

Source d'un indécomposable. Soit E un RG-module indécomposable, et P un vortex de E. On appelle source de E un RP-module indécomposable J tel que E soit un facteur direct de $\mathrm{Ind}_P^G J$. Un tel RP-module est unique à isomorphisme près, modulo l'action par conjugaison de $N_G(P)$ sur P.

Vocabulaire. On dira qu'un RG-module indécomposable E est *cuspidal* si son vortex est un p-Sylow de G. L'autre cas extrême est celui où le vortex est 1 : ce cas est celui qui se rapproche le plus de la projectivité absolue, qui sera étudiée au paragraphe 4.4.

4.3 Induction dans un p-groupe

Théorème [Gre-1959]. Soit G un p-groupe, H un sous-groupe de G, et L un $\mathscr{O}H$-module indécomposable. Alors le $\mathscr{O}G$-module $\mathrm{Ind}_H^G L$ est indécomposable.

Démonstration. Quitte à raisonner par récurrence, on va supposer que H est un sous-groupe maximal de G, c'est-à-dire d'indice p. Alors H est automatiquement distingué dans G, et on peut choisir un élément $g \in G$ tel que $G/H = \langle \bar{g} \rangle$.

Notons $M = \mathrm{Ind}_H^G L = \mathscr{O}G \otimes_{\mathscr{O}H} L = L_0 \oplus \ldots \oplus L_{p-1}$, où $L_i = g^i \otimes L$.

Le groupe H agit sur L_i via $h.(g^i \otimes x) = g^i \otimes (h^{g^i} x)$.

Commençons par le cas où il existe un isomorphisme de $\mathscr{O}H$-modules $\psi : L_0 \to L_1,\ 1 \otimes x \mapsto g \otimes \varphi(x)$. Alors ψ s'étend, par la propriété universelle de l'induction, en un automorphisme de $\mathscr{O}G$-modules $\tilde{\psi} : M \to M,\ g^i \otimes x \mapsto g^{i+1} \otimes \varphi(x)$ (où $i+1$ doit se comprendre modulo p). Pour tous i et j, $\tilde{\psi}^j$ induit un isomorphismes de $\mathscr{O}H$-modules de L_i sur L_{i+j}.

Soit $f \in \mathrm{End}_{\mathscr{O}G}(M)$. Pour $x \in L_0$, notons $f(x) = f_0(x) + \ldots + f_{p-1}(x)$ avec $f_i(x) \in L_i$, et posons $f_i'(x) = [\tilde{\psi}]^{-i}(f_i(x)) \in L_0$. En notant toujours par un tilde l'endomorphisme induit de H à G, on obtient $f = \tilde{f}_0' + \tilde{\psi}\tilde{f}_1' + \ldots + \tilde{\psi}^{p-1}f_{p-1}'$.

Finalement, en notant $B = \mathrm{End}_{\mathscr{O}G}(M)$ et $A = \mathrm{End}_{\mathscr{O}H}(L)$ (identifié à une sous-algèbre de B), on obtient $B = A + \tilde{\psi}A + \ldots + \tilde{\psi}^{p-1}A$, avec $\tilde{\psi}^p$ un élément inversible de A.

Remarquons que A s'identifie à l'ensemble des éléments de B qui préservent les sous-modules $L_0, \ldots, L_p$. La conjugaison par $\tilde{\psi}$ induit donc un automorphisme de A ; ceci implique aussi qu'elle préserve le radical de Jacobson $J(A)$. Retenons que $J(A)\tilde{\psi} = \tilde{\psi}J(A)$.

On va maintenant travailler sur les radicaux de Jacobson de A et B, qui contiennent $\mathfrak{m}A$ et $\mathfrak{m}B$ respectivement. Notons donc par une barre la réduction modulo $\mathfrak{m}$ (au passage, on supprime les tildes). On a alors $\bar{B} = \bar{A} + \bar{\psi}\bar{A} + \ldots + \bar{\psi}^{p-1}\bar{A}$. Notons $I = J(\bar{A}) + \bar{\psi}J(\bar{A}) + \ldots + \bar{\psi}^{p-1}J(\bar{A})$. D'après la remarque précédente, comme $J(\bar{A})$ est nilpotent, I est un idéal bilatère et nilpotent de $\bar{B}$; il est donc contenu dans $J(\bar{B})$.

Notons $D = A/J(A)$, et rappelons que c'est une k-algèbre à division. On obtient $B/I = D + \bar{\psi}D + \ldots + \bar{\psi}^{p-1}D$, avec $\bar{\psi}^p$ un élément non nul de D.

Si le corps k est algébriquement clos, alors $D = k$ et il existe $\lambda \in k$ tel que $\lambda^k = \bar{\psi}^k$, d'où $\bar{\psi} - \lambda \in J(\bar{B})$. Dans ce cas on obtient $B/J(B) = \bar{B}/J(\bar{B}) \simeq k$, donc le théorème est prouvé (après s'être débarassé du cas resté pendant, qui se traite par Krull-Schmidt).

Si le corps k est supposé fini, on reste bloqué. Une façon de finir serait de prouver qu'il existe une extension de $\mathbb{K}$ «assez grosse» pour que, pour toute extension $\mathbb{L}$, dès qu'un $\mathscr{O}_{\mathbb{K}}H$-module L est indécomposable, le $\mathscr{O}_{\mathbb{L}}H$-module $\mathscr{O}_{\mathbb{L}} \otimes_{\mathscr{O}_{\mathbb{K}}} L$ soit encore indécomposable. **A éclaircir... Lire [Bro-1976].** □

Le théorème de Green est très important pour comprendre la notion de vortex et de source. Soit en effet E un $\mathscr{O}G$-module indécomposable, P son vortex et J sa source. Notons de plus S un p-Sylow de G contenant P. Alors le $\mathscr{O}S$-module $\mathrm{Ind}_P^S J$ est indécomposable. C'est en induisant de S à G qu'apparaît la décomposabilité, qui fait que E n'est pas un induit, mais seulement un facteur direct d'un induit.

Conséquence. Pour G un p-groupe et $H \leqslant G$, tout kG-module relativement (kG, kH)-projectif est un induit de H à G (et plus seulement un facteur direct d'un induit).

Application. Soit G un groupe fini, H un sous-groupe de G, et E un kG-module relativement (kG, kH)-projectif. Alors le degré $\dim_k E$ est un multiple de $[G : H]_p$.

Démonstration. Soit P un p-Sylow de G, et F une composante du kP-module $\mathrm{Res}_P^G E$. Comme vu au paragraphe 4.1, il existe $g \in G$ tel que F soit relativement $(kP, k[P \cap H^g])$-projectif. Mais alors, d'après le théorème de Green, il existe un $k[P \cap H^g]$-module L tel que $F = \mathrm{Ind}_{P \cap H^g}^P L$, donc le degré $\dim_k F = [P : P \cap H^g] \dim_k L$ est un multiple de $[P : P \cap H^g]$, donc de $[G : H]_p$ (car P est un p-Sylow de G).

Le résultat vient en sommant les degré des composantes de $\mathrm{Res}_P^G E$. □

Généralisation du théorème de Green. Soit G un groupe fini. Supposons qu'il existe un p'-groupe K et un p-groupe P tel que $G = K \times P$ (produit direct). Si H est un sous-groupe de G d'indice une puissance de p, et L un $\mathscr{O}H$-module indécomposable, alors le $\mathscr{O}G$-module $\mathrm{Ind}_H^G L$ est indécomposable. En particulier, tout kG-module relativement (kG, kH)-projectif est un induit de H à G.

Démonstration. Comme $[G : H]$ est une puissance de p, le sous-groupe H contient K. Soit $Q = P \cap H$ le p-Sylow de H ; alors $H = K \times Q$.

Il nous faut maintenant élucider un peu la structure du $\mathscr{O}H$-module L. Nous pouvons voir L comme un $\mathscr{O}K$-module-$\mathscr{O}Q$, en envoyant l'action de Q à droite. De même, $\mathrm{Ind}_H^G L$ sera vu comme un $\mathscr{O}K$-module-$\mathscr{O}P$, dont il faut prouver qu'il est indécomposable.

Comme L est indécomposable, il existe un unique idempotent primitif ε de $Z\mathscr{O}K$ tel que $\varepsilon M = M$.

Soit S un facteur direct indécomposable du $\mathscr{O}K$-module $\mathscr{O}K\varepsilon$. Alors $\mathbb{K}S = \mathbb{K} \otimes_{\mathscr{O}} S$ est un $\mathbb{K}K$-module irréductible, car K est un p'-groupe (donc on dispose d'un théorème de Maschke sur $\mathscr{O}$), et $\bar{S} = k \otimes_{\mathscr{O}} S$ est irréductible (car c'est un projectif indécomposable et on dispose du théorème de Maschke sur k).

De plus, $\bar{S}$ est un objet générateur dans la catégorie des $kK\bar{\varepsilon}$-modules, donc le morphisme naturel $\bar{\mu} : \bar{S} \otimes_{\mathrm{End}_{kK}(\bar{S})} \bar{S}^\vee \to kK\bar{\varepsilon}$ est surjectif. Par le lemme de Nakayama, le morphisme $\mu : S \otimes_{\mathrm{End}_{\mathscr{O}K}(S)} S^\vee \to \mathscr{O}K\varepsilon$

est donc surjectif, donc S est un objet générateur dans la catégorie des $\mathscr{O}K\varepsilon$-modules. Par conséquent, μ est même un isomorphisme de $\mathscr{O}K$-modules-$\mathscr{O}K$.

Par ailleurs $\mathbb{K}S$ est irréductible, donc (**si on s'autorise à supposer $\mathbb{K}$ assez gros**) $\mathrm{End}_{\mathbb{K}K}(S) = \mathbb{K}\mathrm{Id}_S$. Or $\mathrm{End}_{\mathscr{O}K}(S)$ s'injecte dans $\mathrm{End}_{\mathbb{K}K}(S)$, d'où $\mathrm{End}_{\mathscr{O}K}(S) = \mathscr{O}\mathrm{Id}_S \simeq \mathscr{O}$.

Notons $M = S^\vee \otimes_{\mathscr{O}K} L$, vu comme un module-$\mathscr{O}P$. Alors, d'après ce qui précède, $L \simeq S \otimes_{\mathscr{O}} M$ comme $\mathscr{O}K$-module-$\mathscr{O}P$, et M est indécomposable.

Dès lors le module $\mathrm{Ind}_H^G L$, comme $\mathscr{O}K$-module-$\mathscr{O}P$, est isomorphe à $S \otimes_{\mathscr{O}} \mathrm{Ind}_Q^P M$. Or $\mathrm{Ind}_Q^P M$ est un module-$\mathscr{O}P$ indécomposable par le théorème de Green, et $\mathrm{Ind}_Q^P M \simeq S^\vee \otimes_{\mathscr{O}K\varepsilon} \mathrm{Ind}_H^G L$, donc $\mathrm{Ind}_H^G L$ est indécomposable. □

4.4 Caractères modulaires projectifs

Nous allons maintenant nous intéresser aux RG-modules projectifs, selon la définition classique. Un module est projectif si et seulement si il est facteur direct d'un module libre.

Pour $R = k$, tout k-module est libre, donc tout induit de 1 à G est libre sur kG. Par conséquent, un kG-module E est projectif si, et seulement si, il est relativement (kG, k)-projectif. La projectivité absolue est ainsi un cas particulier de la projectivité relative, et comme telle se caractérise par le critère de Higman.

Pour $R = \mathscr{O}$, un $\mathscr{O}G$-module E est projectif si, et seulement si, il est à la fois projectif sur $\mathscr{O}$ (c'est-à-dire libre puisque $\mathscr{O}$ est local) et relativement $(\mathscr{O}G, \mathscr{O})$-projectif.

La projectivité absolue a sur la projectivité relative l'énorme avantage de pouvoir se relever de k à $\mathscr{O}$.

Proposition. Soit E un kG-module projectif. Alors il existe un $\mathscr{O}G$-module projectif L (**unique à isomorphisme près ?**) tel que $E \simeq k \otimes_{\mathscr{O}} L$.

Démonstration. Il suffit de traiter le cas où E est indécomposable. Alors E est l'enveloppe projective d'un kG-module irrédutible. En particulier, E est un facteur direct de kG. Il existe donc un idempotent primitif $e \in kG$ tel que $E = kGe$. Mais alors e se relève en un idempotent primitif $\tilde{e}$ de $\mathscr{O}G$. Notons $L = \mathscr{O}G\tilde{e}$. Alors $E \simeq k \otimes_{\mathscr{O}} L$. □

Insistons sur la puissance de ce résultat. Si E est un kG-module quelconque, il ne peut en général pas se relever en un $\mathscr{O}G$-module $\mathscr{O}$-projectif L. En admettant qu'il le puisse, ce relèvement n'est pas unique (exemple du module principal pour $G = \mathbb{Z}/p\mathbb{Z}$). Et quand bien même E serait relativement (kG, kH)-projectif, L ne serait pas nécessairement relativement $\mathscr{O}G, \mathscr{O}H)$-projectif (**exemple ?**).

Proposition. Soit E un kG-module projectif, et L un $\mathscr{O}G$-module projectif tel que $E \simeq k \otimes_{\mathscr{O}} L$. Alors le caractère ordinaire χ_L est nul sur $G \setminus G_{p'}$, donc indépendant du choix de L. Appelons-le caractère modulaire projectif de E, et notons-le Φ_E.

Démonstration. Nous savons déjà que la restriction de χ_L à $G_{p'}$ est le caractère modulaire $\varphi_{\overline{L}}$, c'est-à-dire φ_E. Il suffit donc de montrer que χ_L est nul sur $G \setminus G_{p'}$ pour prouver qu'il est indépendant du choix du relèvement L.

Soit $g \in G$, r sa partie p-régulière et s sa partie p-singulière. On suppose $g \notin G_{p'}$, c'est-à-dire $s \neq 1$. Le groupe cyclique $\langle g \rangle$ est isomorphe au produit direct $\langle r \rangle \times \langle s \rangle$.

Notons d'abord que L est un $\mathscr{O}$-module libre, donc $\chi_L(g) = \mathrm{tr}_{L/\mathscr{O}}(\lambda_L(g))$ est défini sans faire référence au corps $\mathbb{K}$. Par ailleurs L est relativement $(\mathscr{O}G, \mathscr{O})$-projectif. Le module restreint $\mathrm{Res}_{\langle g \rangle}^G L$ est donc relativement $(\mathscr{O}\langle g \rangle, \mathscr{O})$-projectif. A fortiori, il est relativement $(\mathscr{O}\langle g \rangle, \mathscr{O}\langle r \rangle)$-projectif. D'après le théorème de Green (généralisé), il existe donc un $\mathscr{O}\langle r \rangle$-module M tel que $\mathrm{Res}_{\langle g \rangle}^G L = \mathrm{Ind}_{\langle r \rangle}^{\langle r \rangle} M$.

De plus M est nécessairement libre sur $\mathscr{O}$, puisque L l'est. On dispose donc de son caractère ordinaire $\chi_M \in ZF(\{1\}, \mathscr{O})$. Par la formule d'induction des caractères, puisque g n'est manifestement conjugué, dans le groupe cyclique $\langle g \rangle$, à aucun élément de $\langle r \rangle$,

$$\chi_L(g) = \chi_{\mathrm{Res}_{\langle g \rangle}^G L}(g) = \sum_{h \in \langle g \rangle / \langle r \rangle \,;\, {}^h g \in \langle r \rangle} \chi_M({}^h g) = 0$$

□

Nous noterons $ZF^{pr}(G, \mathcal{O})$ le sous-$\mathcal{O}$-module de $ZF(G, \mathcal{O})$ engendré par les caractères modulaires projectifs. Définissons alors un accouplement entre $ZF^{pr}(G, \mathcal{O})$ et $ZF(G_{p'}, \mathcal{O})$ en posant, pour deux kG-modules E et F, E étant projectif :

$$\langle \Phi_E, \varphi_F \rangle_{G'_p} = \frac{1}{|G|} \sum_{g \in G_{p'}} \Phi_E(g^{-1}) \varphi_F(g).$$

Théorème. Supposons le corps k assez gros. L'accouplement ainsi défini est à valeur dans $\mathcal{O}$ et définit une dualité parfaite entre $ZF^{pr}(G, \mathcal{O})$ et $ZF(G_{p'}, \mathcal{O})$. En effet, pour un kG-module projectif E et un kG-module quelconque F,

$$\langle \Phi_E, \varphi_F \rangle_{G'_p} = \dim_k \operatorname{Hom}_{kG}(E, F).$$

Démonstration. Rappelons que, si E est une enveloppe projective de F, alors $\dim_k \operatorname{Hom}_{kG}(E, F) = 1$ (car k est assez gros). La première partie de l'énoncé découle donc de la seconde, qu'il s'agit maintenant de prouver.

Notons $H = \operatorname{Hom}_k(E, F)$, sur lequel on fait agir G par conjugaison. Rappelons que, par convention, nos morphismes agissent à droite. Les parenthèses ne seront écrites que si elles sont nécessaire pour expliciter la priorité des opérations.

Comme E est projectif, il existe $u \in \operatorname{End}_k(E)$ tel que $\operatorname{Tr}_1^G(u) = \operatorname{Id}_E$. Posons $v \in \operatorname{End}_k(H)$ défini par $mv = um$ pour tout $m \in H = \operatorname{Hom}_k(E, F)$.

Pour $m \in H$ et $x \in E$, on calcule (revoir la définition des bimodules $\operatorname{End}_k(H)$ et $\operatorname{Hom}_k(E, F)$ en 2.2) :

$$\begin{aligned} m\operatorname{Tr}_1^G(v) &= m.\sum_{g \in G}(gvg^{-1}) = \sum_{g \in G} m\lambda_H(g^{-1})v\lambda_H(g) = \sum_{g \in G}\Big[\lambda_E(g)m\lambda_F(g^{-1})\Big]v\lambda_H(g) \\ &= \sum_{g \in G}\Big[u\lambda_E(g)m\lambda_F(g^{-1})\Big]\lambda_H(g) = \sum_{g \in G}\lambda_E(g^{-1})u\lambda_E(g)m\lambda_F(g^{-1})\lambda_F(g) = \operatorname{Tr}_1^G(u)m = m \end{aligned}$$

Ceci prouve que $\operatorname{Tr}_1^G(v) = \operatorname{Id}_H$, et donc que H est un kG-module projectif. Si quelqu'un a une preuve plus simple, je suis preneur...

Puisque H est projectif, il se relève en un $\mathcal{O}G$-module projectif $\tilde{H}$, tel que $H \simeq k \otimes_{\mathcal{O}} \tilde{H}$. Comme $\tilde{H}$ est un facteur direct d'un $\mathcal{O}G$-module libre, on montre facilement que $H^G \simeq k \otimes_{\mathcal{O}} (\tilde{H}^G)$ et $(\mathbb{K} \otimes \tilde{H})^G = \mathbb{K} \otimes (\tilde{H}^G)$. Ainsi :

$$\dim_k \operatorname{Hom}_{kG}(E, F) = \dim_k H^G = \dim_{\mathbb{K}} (\mathbb{K} \otimes \tilde{H})^G.$$

Or, en notant χ_0 le caractère ordinaire principal (celui de la représentation triviale de degré 1), on sait que

$$\dim_{\mathbb{K}} (\mathbb{K} \otimes \tilde{H})^G = \left\langle \chi_{\tilde{H}}, \chi_0 \right\rangle_G = \langle \Phi_H, \chi_0 \rangle_G = \langle \Phi_H, \varphi_0 \rangle_{G_{p'}}.$$

Enfin, H est isomorphe comme kG-module au produit tensoriel $E^* \otimes_k F$, donc :

$$\langle \Phi_H, \varphi_0 \rangle_{G_{p'}} = \langle \Phi_E, \varphi_F \rangle_{G_{p'}},$$

ce qui achève la démonstration. □

Remarquons par ailleurs que, via la restriction à $G_{p'}$, on peut considérer $ZF^{pr}(G, \mathcal{O})$ comme un sous-module de $ZF(G, \mathcal{O})$. Les facteurs invariants de ce sous-module sont exactement ceux de la matrice de Cartan de l'algèbre kG. Ces facteurs invariants réapparaîtront au paragraphe 5.1, lorsqu'il sera question des groupes de défaut des blocs de kG.

Application. Le $\mathcal{O}$-module $ZF(G_{p'}, \mathcal{O})$ est engendré par les caractères modulaires φ_E des kG-modules irréductibles.

Démonstration. Nous savons déjà que le sous-$\mathcal{O}$-module engendré par les φ_E est libre et de même rang que $ZF(G_{p'}, \mathcal{O})$, à savoir le nombre de classes de conjugaison dans $G_{p'}$. Nous allons montrer que ce sous-module contient les fonctions caractéristiques des classes de conjugaison de $G_{p'}$, ce qui fournira le résultat annoncé.

Soit C une classe de conjugaison de p'-éléments de G, et ψ_C sa fonction caractéristique. Il existe donc des scalaires $a_E \in \mathbb{K}$ tels que $\psi_C = \sum_E a_E \varphi_E$ (où E parcourt un système de représentants des classes d'isomorphisme de kG-modules projectifs indécomposables). En utilisant la dualité définie plus haut, pour tout E, on a

$$a_E = \langle \Phi_E, \psi_C \rangle_{G_{p'}} = \frac{1}{|G|} \sum_{g \in C} \Phi_E(g^{-1}) = \frac{1}{|G|} \Phi_E(x),$$

où $x = \sum_{g \in C} g^{-1}$ appartient à $Z\mathscr{O}G$.

Soit $\tilde{E}$ un $\mathscr{O}G$-module projectif relevant E, et $u = \lambda_{\tilde{E}}(x) \in \mathrm{End}_{\mathscr{O}G}(\tilde{E})$. Alors u est un morphisme projectif, donc il existe $v \in \mathrm{End}_{\mathscr{O}}(\tilde{P})$ tel que $u = \mathrm{Tr}_1^G(v)$. Mais alors :

$$\Phi_E(x) = \mathrm{tr}_{\tilde{E}/\mathscr{O}}(u) = \mathrm{tr}_{\tilde{E}/\mathscr{O}}[\mathrm{Tr}_1^G(v)] = \mathrm{tr}_{\tilde{E}/\mathscr{O}}\Big[\sum_{g \in G} \lambda_E(g^{-1}) v \lambda_E(g)\Big] = |G| \, \mathrm{tr}_{\tilde{E}}(v),$$

car $\mathrm{tr}_{\tilde{E}/\mathscr{O}}$ est une fonction centrale sur $\mathrm{End}_{\mathscr{O}}(\tilde{E})$. En particulier, $a_E = \frac{1}{|G|}\Phi_E(x) = \mathrm{tr}_{\tilde{P}}(v) \in \mathscr{O}$, ce qui achève la preuve. $\square$

5 Application à la théorie des blocs

5.1 Groupe de défaut d'un bloc

Définition. La lettre R représente toujours le corps k ou l'anneau $\mathscr{O}$. L'algèbre RG est naturellement un RG-module-RG. Nous choisirons de la considérer ici comme un $R[G \times G]$-module, en notant $(g, h).x = gxh^{-1}$. Notons $\Delta : G \to G \times G$ le morphisme diagonal : $\Delta(g) = (g, g)$. Remarquons que $RG = \mathrm{Ind}_{\Delta(G)}^{G \times G} R$, où R représente le $R\Delta(G)$-module trivial.

Soit e un bloc G, c'est-à-dire un idempotent primitif de ZRG. L'algèbre RGe est un facteur direct indécomposable du $R[G \times G]$-module RG ; elle est donc relativement $(R[G \times G], R\Delta(G))$-projective. Soit P un vortex de RGe ; alors $P \leqslant_{G \times G} \Delta(G)$. Choisissons P contenu dans $\Delta(G)$, et appelons groupe de défaut du bloc e le groupe $D_e = \Delta^{-1}(P)$

Le groupe de défaut D_e est un p-sous-groupe de G, unique à conjugaison près dans G.

Démonstration. Il suffit de vérifier que $\Delta(D)$ et $\Delta(D')$ sont conjugués dans $G \times G$ si, et seulement si, D et D' sont conjugués dans G. $\square$

Caractérisation 1. Soit e un bloc de G et D un groupe de défaut de e. Alors l'idempotent e appartient à l'image de $\mathrm{Tr}_D^G : (RG)^D \to (RG)^G$, et D est, à conjugaison près, le plus petit sous-groupe de G vérifiant cette propriété.

Démonstration. Par hypothèse, le $R[G \times G]$-module RGe est relativement $(R[G \times G], R\Delta(D))$-projectif, et *a fortiori* $(R[G \times G], R[D \times G])$-projectif.

Or on a un isomorphisme canonique de $\mathrm{End}_{R[1 \times G]}(RGe)$ (agissant à gauche) sur RGe, comme RG-modules-RG. Via cet isomorphisme, Id_B est envoyé sur e. Via cet isomorphisme, $\mathrm{Tr}_{D \times G}^{G \times G}$ devient Tr_D^G. Donc e appartient à l'image de $\mathrm{Tr}_D^G : (RGe)^D \to (RGe)^G$.

Réciproquement, soit H un sous-groupe de G tel que e appartienne à l'image de $\mathrm{Tr}_H^G : (RG)^H \to (RG)^G$. Soit $u \in RG$ tel que $e = \mathrm{Tr}_H^G(u)$; alors $e = e^2 = \mathrm{Tr}_H^G(u)e = \mathrm{Tr}_H^G(ue)$, donc on peut supposer $u \in RGe$. Alors, par le raisonnement précédent, Id_{RGe} est dans l'image de $\mathrm{Tr}_{H \times G}^{G \times G}$, donc RGe est relativement $(G \times G, H \times G)$-projectif. Par définition du groupe de défaut, on a donc $\Delta(D) \leqslant_{G \times G} H \times G$, dont on déduit immédiatement $D \leqslant_G H$. $\square$

Corollaire. Soit e un idempotent primitif de $Z\mathscr{O}G$, et $\bar{e}$ son image dans ZkG. Les blocs e et $\bar{e}$ ont les mêmes groupes de défaut.

Démonstration. Soit H un sous-groupe de G. S'il existe $u \in (\mathscr{O}G)^H$ tel que $e = \mathrm{Tr}_H^G(u)$, alors $\bar{u} \in (kG)^H$ et $\bar{e} = \mathrm{Tr}_H^G(\bar{u})$.

Réciproquement, s'il existe $v \in (kG)^H$ tel que $\bar{e} = \mathrm{Tr}_H^G(v)$, alors il existe $u \in (\mathscr{O}G)^H$ tel que $\bar{u} = v$, d'où $e - \mathrm{Tr}_H^G(u) \in \mathfrak{m}.Z\mathscr{O}G$. L'idempotent primitif e est donc dans la somme des idéaux bilatères $\mathfrak{m}.Z\mathscr{O}G$ et $\mathrm{im}\,\mathrm{Tr}_H^G$. Par le lemme de Rosenberg, e est alors dans l'un de ces idéaux. Mais e est idempotent non nul, donc il ne saurait être dans $\mathfrak{m}.Z\mathscr{O}G$, car $\bigcap_{n\in\mathbb{N}}(\mathfrak{m}.Z\mathscr{O}G)^n = 0$.

On a ainsi prouvé que e appartient à l'image de Tr_H^G si, et seulement si, il en est de même pour $\bar{e}$, ce qui entraîne le résultat. □

Ordre du groupe de défaut. Ici $R = \mathscr{O}$. Soit $e \in \mathscr{O}G$ un bloc, et D un groupe de défaut de e. On appelle défaut du bloc e l'entier d tel que $|D| = p^d$.

Notons $[G : D]_p$ la p-composante de l'indice de D dans G. Alors $e \in \mathscr{O}G_{p'}$, et

$$\begin{aligned}[G : D]_p &= \mathrm{pgcd}\Big\{f(e)\ ;\ f \in ZF(G_{p'}, \mathscr{O})\Big\} \\ &= \min\Big\{(\dim_k S)_p\,;\ S \in \mathrm{Irr}(kG\bar{e})\Big\} \\ &= \min\Big\{(\dim_{\mathbb{K}} R)_p\,;\ R \in \mathrm{Irr}(\mathbb{K}Ge)\Big\}.\end{aligned}$$

Démonstration. A l'aide de la matrice de décomposition D de G, sans oublier que $E = {}^tD$, calculons :

$$\begin{aligned} e &= \sum_{R\in\mathrm{Irr}(\mathbb{K}Ge)} \varepsilon_\chi = \frac{1}{|G|}\sum_{g\in G}\Big[\sum_{R\in\mathrm{Irr}(\mathbb{K}Ge)} \chi_R(1)\chi_R(g^{-1})\Big]\,g \\ &= \frac{1}{|G|}\sum_{g\in G}\Big[\sum_{R\in\mathrm{Irr}(\mathbb{K}Ge)}\Big(\sum_{S\in\mathrm{Irr}(kG\bar{e})} d_{SR}\,\varphi_S(1)\Big)\chi_R(g^{-1})\Big]\,g \\ &= \frac{1}{|G|}\sum_{g\in G}\Big[\sum_{S\in\mathrm{Irr}(kG\bar{e})} \varphi_S(1)\Big(\sum_{R\in\mathrm{Irr}(\mathbb{K}Ge)} d_{SR}\,\chi_R(g^{-1})\Big)\Big]\,g \\ &= \frac{1}{|G|}\sum_{g\in G}\Big[\sum_{S\in\mathrm{Irr}(kG\bar{e})} \varphi_S(1)\Phi_{P_S}(g^{-1})\Big]\,g, \end{aligned}$$

d'où $e \in \mathbb{K}G_{p'}$ car $\Phi(g^{-1}) = 0$ pour $g \notin G_{p'}$. Ceci prouve $e \in \mathscr{O}G_{p'}$.

Prouvons maintenant la première égalité annoncée.

Par définition du groupe de défaut, e appartient à l'image de Tr_D^G ; soit $x \in (\mathscr{O}G)^D$ tel que $e = \mathrm{Tr}_D^G(x)$. Alors, pour toute fonction $f \in ZF(G_{p'}, \mathscr{O})$,

$$f(e) = f(\sum_{g\in G/D}(gxg^{-1}) = \sum_{g\in G/D} f(gxg^{-1}) = [G : D]\,f(x),$$

car f est une fonction centrale. Donc $f(e)$ est un multiple de $[G : D]_p$ dans $\mathscr{O}$.

Pour achever la preuve, on va travailler sur les fonctions caractéristiques ψ_C des classes de conjugaison C de p' éléments de G. Notons x_C un élément de C, et $\mathscr{S}C \in Z\mathscr{O}G$ la somme des éléments de C. On appelle groupe de défaut de la classe C un p-Sylow D_C de $C_G(x_C)$.

Notons $e = \sum_C \alpha_C \mathscr{S}C$, d'où $\bar{e} = \sum_C \bar{\alpha}_C\overline{\mathscr{S}C}$ après réduction modulo $\mathfrak{m}$.

On vérifie aisément que l'image de la trace $\mathrm{Tr}_H^G : (kG)^H \to (kG)^G$ est engendrée par les $\overline{\mathscr{S}C}$, pour $D_C \leqslant_G H$. En particulier, $\bar{e} \in \mathrm{im}\,\mathrm{Tr}_H^G$ si, et seulement si, $\bar{\alpha}_C \neq 0 \Rightarrow D_C \leqslant_G H$.

On a donc $\bar{\alpha}_C \neq 0 \Rightarrow D_C \leqslant_G D$; de plus, il existe une classe C telle que $\bar{\alpha}_C \neq 0$ et $D_C = D$. En effet, dans le cas contraire, $\bar{e}$ serait dans la somme des idéaux bilatères $\mathrm{im}\,\mathrm{Tr}_H^G$, pour $H < D$. Le lemme de Rosenberg le ferait alors appartenir à l'un des $\mathrm{im}\,\mathrm{Tr}_H^G$, contredisant la minimalité de D.

Pour la classe C qui vient d'être singularisée, on obtient

$$\psi_C(e) = \alpha_C\,|C| = \alpha_C\,[G : C_G(x_C)] = \alpha_C\,[G : C_G(x_C)]_{p'}\,[G : D]_p,$$

où α_C et $[G : C_G(x_C)]_{p'}$ sont inversibles dans $\mathscr{O}$. Il existe donc une fonction $f = \lambda\psi_C \in ZF(G_{p'}, \mathscr{O})$ telle que $f(e) = [G : D]_p$. Ceci achève de prouver la première égalité.

Comme les φ_S engendrent $ZF(G_{p'}, \mathscr{O})$, on a $\frac{|G|_p}{|D|} = \mathrm{pgcd}\{\varphi_S(e)\ ;\ M \in Irr(kG)\}$ (le pgcd est pris dans l'anneau $\mathscr{O}$). Or $\varphi_S(e) = \varphi_S(1) = \dim_k(S) \in \mathbb{N}^*$, d'où le résultat annoncé.

Enfin, par surjectivité du morphisme de décomposition, les restrictions à $G_{p'}$ des χ_E engendrent également $ZF(G_{p'}, \mathscr{O})$, d'où le dernier résultat. □

Caractérisation 2. Soit e un bloc de G et D un groupe de défaut de e. Alors tous les RGe-modules sont relativement (RG, RD)-projectifs, et D est, à conjugaison près, le plus petit sous-groupe de G vérifiant cette propriété.

Plus précisément, D est un vortex d'au moins un RGe-module S irréductible : D est, à conjugaison près, le plus grand vortex d'un RGe-module indécomposable.

Démonstration. Pour tout RGe-module e, on a par définition $\lambda_E(e) = \mathrm{Id}_E$. Or $e \in \operatorname{im} \mathrm{Tr}_D^G$ donc, par le critère de Higman, E est relativement (RG, RD)-projectifs.

Réciproquement, d'après la proposition précédente, il existe un kGe-module irréductible S tel que $(\dim_k S)_p = [G : D]_p$. Soit P un vortex de S. Comme S est relativement (RG, RP)-projectif, $\dim_k S$ est un multiple de $[G : P]_p$, donc $|D| \geqslant |P|$. Mais par ailleurs D est un groupe de défaut de B donc E est relativement (G, D)-projectif, ce qui impose $P \leqslant_G D$. Ces deux conditions imposent que P et D soient conjugués dans G, c'est-à-dire que D est aussi un vortex de S. ☐

Exemple 1. Le bloc e est de défaut nul si son groupe de défaut est 1. Dans ce cas tous les kG-modules relevant de ce bloc sont projectifs, et en particulier les irréductibles. L'algèbre de bloc RGe est donc semi-simple ; comme elle est de plus indécomposable par définition d'un bloc, on en déduit qu'il n'y a, à isomorphisme près, qu'un seul kGe-module irréductible S dans un tel bloc. A noter que l'irréductible S est aussi projectif, il se relève en un $\mathscr{O}G$-module $\mathscr{O}$-libre, qui donne par produit tensoriel un $\mathbb{K}Ge$-module R dont on peut montrer facilement qu'il est irréductible, et même qu'il est le seul $\mathbb{K}Ge$ irréductible à isomorphisme près (par exemple par dimension de kGe et $\mathbb{K}Ge$).

Réciproquement, on montre que, s'il existe un seul $\mathbb{K}G$-module irréductible à isomorphisme près , alors le bloc e est de défaut nul.

Exemple 2. Notons S_0 le kG-module principal ($S_0 = k$ avec action triviale de G). On appelle bloc principal de kG l'idempotent primitif central e_0 tel que $e_0 S_0 \neq 0$. Le bloc principal est de défaut maximal : ses groupes de défaut sont les p-Sylow de G.

Démonstration. On a ici $\mathrm{End}_{kG}(S_0) = \mathrm{End}_k(S_0) = k\mathrm{Id}_{S_0}$. Pour $H \leqslant G$, la fonction Tr_H^G est la multiplication par $[G : H]$ dans $\mathrm{End}_k(S_0)$. En particulier, si H ne contient pas un p-Sylow de G, alors $[G : H] = 0$ dans k, et $\mathrm{Id}_{S_0} \notin \operatorname{im} \mathrm{Tr}_H^G$. Ainsi les vortex de S_0 sont les p-Sylow de G, d'où le résultat. ☐

5.2 La correspondance de Brauer

La correspondance de Brauer entre blocs de G et blocs d'un sous-groupe local est ici traitée *a minima*, en vue du théorème de Nagao et du deuxième théorème de Brauer. Il sera nécessaire, à l'avenir, d'approfondir le rôle du foncteur de Brauer et des modules de permutation, qui jouent un rôle central dans la théorie moderne des représentations modulaires des groupes finis.

Le résumé présenté ici est une version abrégée de la présentation de [AlBr-1979].

Morphisme de Brauer. Soit P un p-sous-groupe de G. On appelle morphisme de Brauer l'application $\mathrm{Br}_P : kG \to kC_G(P)$ définie par $\mathrm{Br}_P\Big(\sum_{x\in G} \alpha_x x\Big) = \sum_{x \in C_G(P)} \alpha_x x$.

Propriétés.

L'application Br_P est un morphisme de $kN_G(P)$-modules (pour l'action par conjugaison).

Soit H un sous-groupe de G. Alors $\ker \mathrm{Br}_P \cap (kG)^H = \sum_{P \nleqslant_H Q \leqslant H} \operatorname{im}[\mathrm{Tr}_Q^H : (kG)^Q \to (kG)^H]$.

Si, de plus, H contient P, alors Br_P induit un morphisme d'algèbres de $(kG)^H$ dans $(kC_G(P))^{N_H(P)}$.

Correspondance entre blocs de G et blocs locaux.

En particulier, Br_P induit un morphisme d'algèbres de $ZkG = (kG)^G$ dans $(kC_G(P))^{N_G(P)}$. Remarquons que, pour tout sous-groupe H de G tel que $C_G(P) \leqslant H \leqslant N_G(P)$, on a $(kC_G(P))^{N_G(P)} \subseteq ZkH$.

Par conséquent, si e est un idempotent primitif central de kG (c'est-à-dire un bloc), alors son image $\mathrm{Br}_P(e)$ est un idempotent central de ZkH. Notons bien que $\mathrm{Br}_P(e)$ n'est généralement pas primitif, et peut même être nul ; on peut en tout cas l'écrire comme une somme, éventuellement vide, de blocs de H.

On a ainsi défini une correspondance : à un bloc de G on associe un ensemble de blocs de H.

Notons $e_1, \dots, e_n$ les blocs de G et $e'_1, \dots, e'_{n'}$ ceux de H. On a clairement :

$$\sum_{i=1}^{n} \mathrm{Br}_P(e_i) = \mathrm{Br}_P(\sum_{i=1}^{n} e_i) = \mathrm{Br}_P(1) = 1 = \sum_{j=1}^{n'} e'_j$$

Ainsi tout bloc e'_j de H apparaît dans l'écriture de l'idempotent $\mathrm{Br}_P(e_i)$ pour une, et une seule, valeur de i. On a donc une correspondance réciproque de type fonctionnel : à un bloc de H on associe un unique bloc de G.

Relèvement à $\mathscr{O}$. L'application Br_P pourrait encore être définie en remplaçant k par $\mathscr{O}$, mais elle n'aurait plus de bonnes propriétés. Toutefois, le relèvement des idempotents établit une bijection canonique entre idempotents (resp. blocs) de ZkG ou ZkH et idempotents (resp. blocs) de $Z\mathscr{O}G$ ou $Z\mathscr{O}H$. Si $e \in Z\mathscr{O}G$ est un idempotent, nous conviendrons donc de noter $\mathrm{Br}_P(e)$ l'idempotent de $Z\mathscr{O}H$ qui est en fait issu du relèvement de $\mathrm{Br}_P(\bar{e}) \in ZkH$.

5.3 Restriction à un sous-groupe local

Théorème (Nagao). Soit P un p-sous-groupe de G, et H un sous-groupe de G tel que $P \leqslant H \leqslant N_G(P)$. Soit e un idempotent de $Z\mathscr{O}G$. Notons $e_P = \mathrm{Br}_P(e)$ l'idempotent correspondant de $Z\mathscr{O}H$, et $e'_P = 1 - e_P$. Alors, pour tout kGe-module L, on a

$$\mathrm{Res}_H^G L = L_1 \oplus L_2,$$

où L_1 est un $\mathscr{O}He_P$-module, et L_2 un $\mathscr{O}He'_P$-module dont les vortex des composantes ne contiennent pas P.

Démonstration. On pose $L_1 = e_P L$, et $L_2 = e'_P L$, vus comme des $\mathscr{O}H$-modules. Il reste à étudier les vortex des composantes de L_2.

Les idempotents e et e'_P appartiennent tous deux à $(\mathscr{O}G)^H$ et commutent, donc $e' = e'_P e$ est un idempotent de $(\mathscr{O}G)^H$. On a clairement $L_2 = e'L$. Si on note $u = \lambda_L(e') \in \mathrm{End}_{\mathscr{O}H}(L)$, on obtient $L_2 = Lu$ (rappelons que les anneaux d'endomorphismes opèrent à droite par convention). Si M est une composante de L_2, alors il existe un idempotent primitif $v \in \mathrm{End}_{\mathscr{O}H}(L)$ tel que $M = Lv$ et $uv = v$.

Comme Br_P est un morphisme d'algèbres de ZkG dans ZkH, on a, après réduction modulo $\mathfrak{m}$, $\mathrm{Br}_P(\bar{e}') = \mathrm{Br}_P(\bar{e}) - \mathrm{Br}_P(\bar{e})^2 = 0$. Ainsi $\bar{e}' \in (kG)^H \cap \ker \mathrm{Br}_P = \sum_{P \not\leqslant_H Q \leqslant H} \mathrm{im}[\mathrm{Tr}_Q^H : (kG)^Q \to (kG)^H]$.

On obtient $e' \in \mathfrak{m}(\mathscr{O}G)^H + \sum_{P \not\leqslant_H Q \leqslant H} \mathrm{im}[\mathrm{Tr}_Q^H : (\mathscr{O}G)^Q \to (\mathscr{O}G)^H]$.

Or le morphisme structural λ_L, quoique anti-multiplicatif, est compatible avec les traces relatives, donc $u \in \mathfrak{m}\mathrm{End}_{\mathscr{O}H}(L) + \sum_{P \not\leqslant_H Q \leqslant H} \mathrm{im}[\mathrm{Tr}_Q^H : \mathrm{End}_{\mathscr{O}Q}(L) \to \mathrm{End}_{\mathscr{O}H}(L)]$. De plus $v = uv$, et les images des traces relatives sont des idéaux bilatères, donc $v \in \mathfrak{m}\mathrm{End}_{\mathscr{O}H}(L) + \sum_{P \not\leqslant_H Q \leqslant H} \mathrm{im}[\mathrm{Tr}_Q^H : \mathrm{End}_{\mathscr{O}Q}(L) \to \mathrm{End}_{\mathscr{O}H}(L)]$.

Mais v est un idempotent primitif donc, par le lemme de Rosenberg, il existe un sous-groupe Q de H tel que $P \not\leqslant_H Q$ et $v \in \mathrm{im}\,\mathrm{Tr}_Q^H$ (comme on l'a déjà vu, un idempotent non nul ne saurait appartenir à $\mathfrak{m}\mathrm{End}_{\mathscr{O}H}(L)$). Ainsi $M = Lv$ est un $\mathscr{O}H$-module relativement $(\mathscr{O}H, \mathscr{O}Q)$-projectif. Un vortex de M est dès lors plus petit que Q (à conjugaison près), donc il ne contient pas P. ☐

Théorème (Brauer, main theorem 2). Soit G un groupe fini, P un p-sous-groupe cyclique de G, et H un sous-groupe de G tel que $P \leqslant H \leqslant C_G(P)$. Soit e un idempotent de $Z\mathscr{O}G$, et $e_P = \mathrm{Br}_P(e)$ l'idempotent correspondant de $Z\mathscr{O}H$.

Pour tout $\mathbb{K}Ge$-module L, il existe un $\mathbb{K}He_P$-module L_1 tel que :

$$\forall g \in H, \qquad \langle g_p \rangle = P \quad \Rightarrow \quad \chi_L(g) = \chi_{L_1}(g).$$

Démonstration. Comme précédemment, notons $L_1 = e_P L$ et $L_2 = (1 - e_P)L$. Remarquons que L_1 et L_2 ne dépendent pas du choix de H, car e_P n'en dépend pas. Une fois g fixé, il est donc indifférent de supposer $H = \langle g \rangle$. De toute façon $P \leqslant H \leqslant N_G(P)$, ce qui permet d'appliquer le théorème de Nagao.

A supposer que L_2 soit non nul, soit M un facteur direct indécomposable du $\mathscr{O}H$-module L_2, et $\chi_M \in ZF(K, \mathscr{O})$ son caractère ordinaire. Il s'agit de montrer que $\chi_M(g) = 0$.

Soit Q un vortex du $\mathscr{O}H$-module M. Comme H est cyclique, P est son unique p-Sylow, donc $Q \leqslant P$. De plus, par le théorème de Nagao, $P \nleqslant Q$, donc $Q < P$. Notons $K = \langle g_{p'} \rangle$; ainsi $H = KP$ (produit direct). Remarquons que $KQ < KP = H$, donc g n'appartient pas, même à conjugaison près, au sous-groupe KQ.

Par ailleurs, le module M est relativement $(\mathscr{O}H, \mathscr{O}Q)$-projectif, et *a fortiori* relativement $(\mathscr{O}H, \mathscr{O}KQ)$-projectif. D'après le théorème de Green, tel que généralisé plus haut, il existe un $\mathscr{O}KQ$-module N tel que $M = \mathrm{Ind}_{KQ}^{H} N$.

Mais alors, d'après la formule d'induction des caractères, $\chi_M(g) = [\mathrm{Ind}_{KQ}^{G} \chi_N](g) = 0$, car g n'est pas conjugué à un élément de KQ. Ceci prouve le théorème. $\square$

Références

[AlBr-1979] J. Alperin, M. Broué, *Local methods in block theory*, Ann. of Math. **110** (1979), 143-157.

[Ben-1984] D. Benson, *Modular representation theory : new trends and methods*. Lecture Notes in Mathematics **1081**. Springer-Verlag, Berlin, 1984.

[Bil-2010] E. Biland, *Blocs de Brauer et triangle CDE*, disponible sur `http://erwanbiland.fr/`.

[Bra-1979] R. Brauer, *Theory of group characters* (notes de conférences de 1959), Lectures in mathematics, Kyoto University, 1979.

[Bro-1976] M. Broué, *Sur l'induction des modules indécomposables et la projectivité relative*. Math. Z. **149** (1976), no. 3, 227 ?245.

[Bro-1992] M. Broué, *Equivalence of blocks of group algebras*, Three lectures given at the International Conference on Representations of Algebras, Ottawa, 1992.

[Bro-2007] M. Broué, *Introduction à la théorie des représentations* (notes personnelles), cours de master à l'Université Paris 7, 2007.

[Bro-2009] M. Broué, *Higman's criterion revisited*. Michigan Math. J. **58** (2009), no. 1, 125 ?179.

[CuRe-1962] C. W. Curtis, I. Reiner, *Representation theory of finite groups and associative algebras*. Reprint of the 1962 original. AMS Chelsea Publishing, Providence, RI, 2006.

[Dad-1971] E.C. Dade, *Character theory pertaining to finite simple groups*, in *Finite simple groups* éd. par M. Powell et G. Higman, Academic Press, 1971, p.249-327.

[Gor-1980] D. Gorenstein, *Finite Groups*. Reprint of the 1980 original. AMS Chelsea Publishing, Providence, RI, 2007.

[Gre-1959] J. A. Green, *On the indecomposable representations of a finite group*. Math. Z. **70** (1958/59), 430 ?445.

[Ser-1967] J.-P. Serre, *Représentations linéaires des groupes finis*, Hermann, 1967.

[The-1995] J. Thevenaz, *G-Algebras and Modular Representation Theory*, Oxford Univ. Press, 1995.