ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Les sous-groupes génétiques

Baumann Mélanie - melanie.baumann@epfl.ch
Section de Mathématiques - Epfl

Travail de Master

Sous la direction de :
M. le professeur Jacques Thévenaz

5 mai 2008

Table des matières

Introduction

Ce document est le résultat de mon travail de Master, dont les buts sont :

i) d'étudier les $\mathbb{Q}P$-modules irréductibles, où P est un p-groupe, et en particulier les conséquences du théorème de Roquette (théorème 5.2) et les notions de sous-groupe génétique et base génétique. Pour ce faire, je me base sur le polycopié *Biset functors for finite groups* de Serge Bouc, [Bou], pages 169-189 ;

ii) de modifier ou récrire les preuves des principaux théorèmes pour supprimer l'utilisation de la notion de sous-groupe basique ([Bou], définition 9.2.4, page 168) ;

iii) d'appliquer les résultats obtenus à des p-groupes particuliers comme les p-groupes abéliens finis ou les p-groupes finis extra-spéciaux.

Les premiers chapitres de ce travail introduisent les notions nécessaires pour comprendre et prouver les résultats des chapitres 4 et 5. Le but du chapitre 1 est d'introduire la formule d'inversion de Möbius, qui sera utilisée dans les chapitres 3 et 5. Le chapitre 2 permet de démontrer un théorème dû à Artin (théorème 2.9) dont un corollaire permet, si G est un groupe fini, de déterminer le nombre de $\mathbb{Q}G$-modules irréductibles distincts à isomorphismes près. Les notions développées permettent notamment de déterminer les tables de caractères rationnels de quelques groupes finis. Le chapitre 3 introduit la notion de (H, G)-bi-ensemble et ses propriétés. En particulier, cela va permettre de prouver certains résultats pour les opérations sur les KG-modules (où K est un corps de caractéristique 0 et G un groupe fini) comme l'inflation, la déflation, la restriction ou l'induction.

Les chapitres suivants représentent la partie clé de ce travail. Le chapitre 4 donne quelques résultats sur les p-groupes de p-rang normal 1, en particulier qu'un tel groupe P possède (à isomorphisme près) un unique $\mathbb{Q}P$-module irréductible et fidèle. Le chapitre 5 introduit le théorème de Roquette et ses conséquences, ce qui permet de définir la notion de sous-groupes génétiques. Les résultats obtenus par la suite permettent de donner une description des sous-groupes génétiques qui s'affranchit de la notion de KG-module. Le chapitre finit par un théorème qui dit quand deux sous-groupes génétiques correspondent au même module irréductible. Cela permet d'introduire la notion de base génétique. Dans ce chapitre, la plupart

des résultats se base sur le polycopié de Serge Bouc, [Bou]. Afin de permettre de comparer les preuves et voir les modifications apportées pour supprimer les sous-groupes basiques, les références au polycopié sont données.

Le dernier chapitre présente des applications de cette théorie à quelques p-groupes finis particuliers, comme les p-groupes abéliens finis ou les p-groupes finis extra-spéciaux.

A la fin du travail se trouvent trois annexes contenant des rappels. L'annexe A contient quelques résultats sur les groupes, l'annexe B des définitions et des résultats sur les KG-modules et l'annexe C quelques rappels sur les formes bilinéaires.

Au sujet de la bibliographie, j'aimerais rajouter que la plupart des livres sont utilisés pour donner des références sur des résultats de bases sur les groupes ou les modules. D'autres part, je souhaiterais encore citer un excellent document publié sur internet, à savoir *Tout ce que vous avez toujours voulu savoir sur LaTeX sans jamais avoir osé le demander* de Vincent Lazano, [Laz07], qui m'a permis de résoudre de nombreux problèmes liés à la rédaction d'un document mathématique.

Je tiens à remercier M. le professeur Jacques Thévenaz, pour son encadrement, ses conseils et sa relecture.

Notations

Voici quelques notations utilisées dans ce projet :

- $\mathbb{N}$ est l'ensemble des entiers naturels $\{0, 1, 2, \ldots\}$;
- $\mathbb{N}^*$ est l'ensemble des entiers naturels non-nuls $\{1, 2, 3, \ldots\}$;
- $\mathbb{R}^*$ est l'ensemble des nombres réels non-nuls $\mathbb{R}\backslash\{0\}$;
- $\mathbb{R}_+^*$ est l'ensemble des nombres réels strictement positifs $\{x \in \mathbb{R} \,\big|\, x > 0\}$.
- Soit G est un groupe. On note $H \leq G$ si H est un sous-groupe de G et $H < G$ si H est un sous-groupe propre de G. Similairement, on note $H \trianglelefteq G$ si H est un sous-groupe normal de G et $H \lhd G$ si H est un sous-groupe normal propre de G.
- On note $\mathbf{1}$ le groupe trivial. Si G est un groupe, on note 1_G (ou parfois 1 si le groupe G est clair par le contexte) l'élément neutre de G.
- Soit G est un groupe et H un sous-groupe de G. On note $N_G(H)$ le normalisateur de H dans G, c'est-à-dire

$$N_G(H) = \big\{g \in G \,\big|\, gHg^{-1} = H\big\}.$$

- Soit G un groupe. On note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G, c'est-à-dire l'ensemble des isomorphismes de G dans G.
- Soit G un groupe. Si $x, y \in G$, on note $[x, y]$ l'élément $xyx^{-1}y^{-1}$ de G. On note $[G, G]$ le groupe dérivé de G, c'est-à-dire le groupe engendré par l'ensemble

$$\big\{[x, y] \,\big|\, x, y \in G\big\}.$$

- Soit G un groupe. On note $Z(G)$, le centre de G, c'est-à-dire

$$Z(G) = \{x \in G \,\big|\, xa = ax,\ \forall\ a \in G\}.$$

- Soit p un nombre premier et n un entier strictement positif. On note $\mathbb{F}_{p^n}$ l'unique corps (à isomorphisme près) à p^n éléments.
- Soit K un corps et $n \in \mathbb{N}^*$. On note $GL_n(K)$ l'ensemble des matrices $n \times n$ inversibles à coefficients dans K.

- Soit K un corps, V un espace vectoriel sur K et $v_1, \ldots, v_n$ des éléments de V. On note $\mathrm{Vect}\{v_1, \ldots, v_n\}$ l'espace vectoriel sur K engendré par $v_1, \ldots, v_n$.
- Soit E un ensemble, on note $|E|$ la cardinalité de cette ensemble.
- Soit R un anneau (ou un corps). On note 0_R et 1_R les éléments neutres pour l'addition et la multiplication respectivement.
- Soit K un corps et G un groupe fini. On note $C_K(G)$ l'ensemble des fonctions centrales de G dans K, c'est-à-dire l'ensemble

$$\big\{ f : G \to K \,\big|\, f(x) = f(gxg^{-1}),\ \forall\ x, g \in G \big\}.$$

  On note $R_K(G)$ le groupe de Grothendieck de l'ensemble des classes d'isomorphismes des KG-modules. C'est le groupe abélien libre de base l'ensemble des classes d'isomorphismes de KG-modules irréductibles.
- Soit K un corps et G un groupe fini. Alors on note $\mathbf{1}_G$ le caractère trivial de G sur K et χ_{reg} le caractère régulier.

Chapitre 1

La formule d'inversion de Möbius

Dans ce chapitre, on introduit quelques propriétés sur les ensembles partiellement ordonnés pour définir la fonction de Möbius et prouver la formule d'inversion de Möbius. Ce chapitre se base essentiellement sur le livre *Enumerative Combinatorics* de Richard P. Stanley, [Sta86], pages 96-100 et 113-117. On va traiter le cas d'un anneau quelconque, alors que le livre de Richard P. Stanley ne traite que le cas d'un corps. Certains résultats obtenus pour les corps ne sont plus valables pour un anneau mais la formule d'inversion de Möbius reste valable.

Définition 1.1 *Un ensemble P muni d'une relation d'ordre $\leq$ est appelé un* ***ensemble partiellement ordonné*** *.*

Notation 1.2 *Si P est un ensemble partiellement ordonné, on note $x < y$ si $x \leq y$ et $x \neq y$.*

Définition 1.3 *Soit P et Q deux ensembles partiellement ordonnés. Alors P et Q sont* ***isomorphes (comme ensembles partiellement ordonnés)*** *s'il existe une application bijective $f : P \to Q$ telle que*

$$x \leq y \text{ dans } P \text{ si et seulement si } f(x) \leq f(y) \text{ dans } Q.$$

Définition 1.4 *Soit P un ensemble partiellement ordonné. Un* ***sous-ensemble partiellement ordonné*** *de P est un sous-ensemble Q de P muni de la relation d'ordre $x \leq y$ dans Q si et seulement si $x \leq y$ dans P, pour tout $x, y \in Q$.*

On va étudier un exemple particulier de sous-ensemble partiellement ordonné :

Définition 1.5 *Soit P un ensemble partiellement ordonné. Soit $x, y \in P$ tels que $x \leq y$. On définit* ***l'intervalle*** *$[x, y]$ par*

$$[x, y] = \{z \in P \,\big|\, x \leq z \leq y\}.$$

Si tous les intervalles de P sont finis, on dit que P est un ensemble partiellement ordonné ***localement fini*** *.*

On peut remarquer que l'ensemble vide n'est pas un intervalle.

Exemple 1.6 L'exemple que l'on va utiliser plus tard (Chapitres 3 et 5) est l'ensemble des sous-groupes normaux d'un groupe fini. Soit G un groupe fini. On pose $P = \{N \subset G \,\big|\, N \trianglelefteq G\}$ muni de la relation d'ordre $N \leq M$ si et seulement si N est un sous-groupe de M. Comme G est un groupe fini, P est fini et donc aussi localement fini.

Définition 1.7 *Soit P un ensemble partiellement ordonné. Un sous-ensemble I de P est un* ***idéal ordonné*** *de P si pour tout $x \in I$, si $y \in P$ est tel que $y \leq x$, alors $y \in I$. Un sous-ensemble J de P est un* ***idéal ordonné dual*** *de P si pour tout $x \in J$, si $y \in P$ est tel que $x \leq y$, alors $y \in J$. Un idéal ordonné I de P est* ***principal*** *s'il existe $x \in P$ tel que $I = \{y \in P \,\big|\, y \leq x\}$. Similairement, un idéal ordonné dual J de P est* ***principal*** *s'il existe $x \in P$ tel que $J = \{y \in P \,\big|\, x \leq y\}$.*

Soit P un ensemble partiellement ordonné localement fini. On note $\mathrm{int}(P)$ l'ensemble des intervalles de P. Soit R un anneau. Si $f : \mathrm{int}(P) \to R$ est une application de $\mathrm{int}(P)$ dans R, on note $f(x, y)$ au lieu de $f([x, y])$, pour tout $x, y \in P$ avec $x \leq y$.

Définition 1.8 *L'****algèbre d'incidence*** *$I(P, R)$ de P sur R est la R-algèbre de toutes les fonctions $f : \mathrm{int}(P) \to R$.*

On peut facilement vérifier que l'ensemble $I(P, R)$ est bien une R-algèbre pour les lois suivantes :

i) Pour tout $f, g \in I(P, R)$, on définit $f + g$ par

$$(f + g)(x, y) = f(x, y) + g(x, y),$$

pour tout $x, y \in P$ tels que $x \leq y$.

ii) Pour tout $\lambda \in R$ et pour tout $f \in I(P, R)$, on définit λf par

$$(\lambda f)(x, y) = \lambda f(x, y),$$

pour tout $x, y \in P$ tels que $x \leq y$.

iii) Pour tout $f, g \in I(P, R)$, on définit $f \cdot g$ par

$$(f \cdot g)(x, y) = \sum_{x \leq z \leq y} f(x, z)g(z, y),$$

pour tout $x, y \in P$ tels que $x \leq y$.

La plupart des propriétés découlent du fait que R est un anneau. L'élément neutre pour l'addition est l'élément $\mathbf{0}$ défini par

$$\mathbf{0}(x,y) = 0_R, \qquad \text{pour tout } x,y \in P \text{ tels que } x \leq y.$$

L'élément neutre pour la multiplication est l'élément δ défini par

$$\delta(x,y) = \begin{cases} 1_R & \text{si } x = y \\ 0 & \textit{sinon}, \end{cases}$$

pour tout $x,y \in P$ tels que $x \leq y$.

Proposition 1.9 *Soit P un ensemble partiellement ordonné localement fini et R un anneau. Soit $f \in I(P,R)$. Alors les conditions suivantes sont équivalentes :*

i) L'application f est inversible,

ii) Pour tout $x \in P$, $f(x,x)$ est inversible.

Preuve:

$\Rightarrow$: Il existe $g \in I(P,R)$ tel que $g \cdot f = \delta = f \cdot g$.
Soit $x \in P$, on a $g(x,x)f(x,x) = (g \cdot f)(x,x) = \delta(x,x) = 1_R$ et $f(x,x)g(x,x) = (f \cdot g)(x,x) = \delta(x,x) = 1_R$, c'est-à-dire que $f(x,x)$ est inversible.

$\Leftarrow$: On définit récursivement $g, h : \mathrm{int}(P) \to R$ par :

$$g(x,y) = \begin{cases} f(x,x)^{-1} & \text{si } x = y \\ -\displaystyle\sum_{x \leq z < y} g(x,z)f(z,y)f(y,y)^{-1} & \text{si } x \neq y \end{cases}$$

et par

$$h(x,y) = \begin{cases} f(x,x)^{-1} & \text{si } x = y \\ -f(x,x)^{-1} \displaystyle\sum_{x < z \leq y} f(x,z)h(z,y) & \text{si } x \neq y \end{cases}$$

pour tout $x,y \in P$ tels que $x \leq y$.
On va montrer que $g \cdot f = \delta$: Soit $x,y \in P$ tel que $x \leq y$. Si $x = y$, alors $g(x,x) = f(x,x)^{-1}$, donc $(g \cdot f)(x,x) = g(x,x)f(x,x) = 1_R = \delta(x,x)$. Si $x \neq y$, alors

$$g(x,y) = -\sum_{x \leq z < y} g(x,z)f(z,y)f(y,y)^{-1}$$

donc on a

$$\delta(x,y) = 0 = \sum_{x \leq z \leq y} g(x,z)f(z,y) = (g \cdot f)(x,y).$$

Ainsi f est inversible à gauche. De manière analogue, on montre que $f \cdot h = \delta$, c'est-à-dire que f est inversible à droite.

□

On définit la fonction ζ dans $I(P, \mathbb{Z})$ par

$$\zeta(x, y) = 1, \qquad \text{pour tout } x, y \in P \text{ tels que } x \leq y.$$

Par la proposition 1.9, la fonction ζ est une fonction inversible. On note μ ou μ_P son inverse. C'est la **fonction de Möbius de** P .

Soit $\eta : \mathbb{Z} \to R$ l'unique homomorphisme d'anneau de $\mathbb{Z}$ dans R. Alors les applications $\eta \circ \zeta$ et $\eta \circ \mu$ sont des éléments de $I(P, R)$. De plus, $\eta \circ \mu$ est l'inverse de $\eta \circ \zeta$ pour la multiplication dans $I(P, R)$. Par la suite, on écrira ζ et μ pour $\eta \circ \zeta$ et $\eta \circ \mu$ respectivement. De plus, si $x, y \in P$ sont tels que $x \leq y$, alors $\mu(x, y)$ peut être vu comme un élément de $\mathbb{Z}$ (ou de R).

Théorème 1.10: Formule d'inversion de Möbius
Soit R un anneau et P un ensemble partiellement ordonné tel que tout idéal ordonné principal est fini. Soit des applications $f, g : P \to R$ de P vers R. Alors

$$g(x) = \sum_{y \leq x} f(y), \qquad \forall\ x \in P$$

si et seulement si

$$f(x) = \sum_{y \leq x} g(y)\mu(y, x), \qquad \forall\ x \in P.$$

Preuve: On commence par remarquer que comme tout idéal ordonné principal est fini, P est un ensemble partiellement ordonné localement fini (Si $x, y \in P$ sont tels que $x \leq y$ alors l'intervalle $[x, y]$ est inclus dans l'idéal ordonné engendré par y qui est fini). Ainsi on peut considérer l'algèbre d'incidence $I(P, R)$. On note R^P l'ensemble des applications de P dans R. C'est un groupe abélien avec comme loi de composition $(f, g) \mapsto f + g$, où $\big(f + g\big)(x) = f(x) + g(x)$, pour tout $x \in P$. On va montrer que R^P est un $I(P, R)$-module à droite pour l'action suivante : Soit $f \in R^P$ et $k \in I(P, R)$, alors $f \star k$ est défini, pour tout $x \in P$, par

$$\big(f \star k\big)(x) = \sum_{y \leq x} f(y)k(y, x).$$

- Pour tout $f \in R^P$, pour tout $k, h \in I(P, R)$, $f \star (k + h) = f \star k + f \star h$:

Soit $f \in R^P$ et $k, h \in I(P,R)$. Alors, pour tout $x \in P$,

$$\begin{aligned}
\big(f \star (k+h)\big)(x) &= \sum_{y \leq x} f(y)\big(k+h\big)(y,x) \\
&= \sum_{y \leq x} f(y)\big(k(y,x) + h(y,x)\big) \\
&= \sum_{y \leq x} \big(f(y)k(y,x) + f(y)h(y,x)\big) \\
&= \sum_{y \leq x} f(y)k(y,x) + \sum_{y \leq x} f(y)h(y,x) \\
&= \big(f \star k\big)(x) + \big(f \star h\big)(x) \\
&= \big(f \star k + f \star h\big)(x)
\end{aligned}$$

Ainsi, on a obtenu que $f \star (k+h) = f \star k + f \star h$.

- Pour tout $f, g \in R^P$, pour tout $k \in I(P,R)$, $(f+g) \star k = f \star k + g \star k$:
  Soit $f, g \in R^P$ et $k \in I(P,R)$. Alors, pour tout $x \in P$,

$$\begin{aligned}
\big((f+g) \star k\big)(x) &= \sum_{y \leq x} \big(f+g\big)(y)k(y,x) \\
&= \sum_{y \leq x} \big(f(y) + g(y)\big)k(y,x) \\
&= \sum_{y \leq x} \big(f(y)k(y,x) + g(y)k(y,x)\big) \\
&= \sum_{y \leq x} f(y)k(y,x) + \sum_{y \leq x} g(y)k(y,x) \\
&= \big(f \star k\big)(x) + \big(g \star k\big)(x) \\
&= \big(f \star k + g \star k\big)(x)
\end{aligned}$$

  Ainsi, on a obtenu que $(f+g) \star k = f \star k + g \star k$.

- Pour tout $f \in R^P$, pour tout $k, h \in I(P,R)$, $f \star (k \cdot h) = (f \star k) \star h$:

Soit $f \in R^P$ et $k, h \in I(P,R)$. Alors, pour tout $x \in P$,

$$\begin{aligned}
\big(f \star (k \cdot h)\big)(x) &= \sum_{y \le x} f(y)\big(k \cdot h\big)(y,x) \\
&= \sum_{y \le x} f(y) \sum_{y \le z \le x} k(y,z)h(z,x) \\
&= \sum_{y \le x} \sum_{y \le z \le x} f(y)k(y,z)h(z,x) \\
&= \sum_{z \le x} \sum_{y \le z} f(y)k(y,z)h(z,x) \\
&= \sum_{z \le x} \Big(\sum_{y \le z} f(y)k(y,z) \Big) h(z,x) \\
&= \sum_{z \le x} \big(f \star k\big)(z)h(z,x) \\
&= \big((f \star k) \star h\big)(x)
\end{aligned}$$

Ainsi on a obtenu que $f \star (k \cdot h) = (f \star k) \star h$.

- Pour tout $f \in R^P$, $f \star \delta = f$:
  Soit $f \in R^P$. Alors, pour tout $x \in P$,

$$\big(f \star \delta\big)(x) = \sum_{y \le x} f(y)\delta(y,x) = f(x).$$

  On a obtenu que $f \star \delta = f$.

Ainsi on a montré que R^P est un $I(P,R)$-module à droite. En particulier, on a que $f \star \zeta = g$ si et seulement si $f = g \star \mu$ car μ est l'inverse de ζ. Ainsi on a montré que

$$g(x) = \sum_{y \le x} f(y), \qquad \forall\ x \in P$$

si et seulement si

$$f(x) = \sum_{y \le x} g(y)\mu(y,x), \qquad \forall\ x \in P.$$

□

Il existe aussi une version duale de ce théorème :

Théorème 1.11 *Soit R un anneau et P un ensemble partiellement ordonné tel que tout idéal ordonné dual principal est fini. Soit des applications $f, g : P \to R$ de P vers R. Alors*

$$g(x) = \sum_{x \le y} f(y), \qquad \forall\ x \in P$$

si et seulement si

$$f(x) = \sum_{x \le y} \mu(x,y)g(y), \qquad \forall\ x \in P.$$

Preuve: La preuve est analogue à la preuve du théorème 1.10 excepté que cette fois, R^P est un $I(P,R)$-module à gauche pour l'action définie par

$$(k \star h)(x) = \sum_{x \leq y} k(x,y)h(y), \qquad \text{pour tout } x \in P,$$

où $k \in I(P,R)$ et $h \in R^P$. □

Chapitre 2

Les $\mathbb{Q}G$-modules

Dans ce chapitre, on va commencer à étudier les $\mathbb{Q}G$-modules. On va prouver un théorème dû à Artin sur les caractères induits qui permettra de connaître le nombre de $\mathbb{Q}G$-modules irréductibles non-isomorphes. Ce chapitre se base essentiellement sur le livre *Representation Theory of Finite Groups and Associative Algebras* de Charles W. Curtis et Irving Reiner, [CR66], pages 272 et 279-282.

Définition 2.1 *Soit G un groupe fini. Un* ***caractère rationnel de*** *G est un caractère de G sur $\mathbb{Q}$ (associé à un $\mathbb{Q}G$-module de dimension finie).*

Remarque 2.2 Soit χ un caractère rationnel d'un groupe fini G. Alors, si $g \in G$, on a $\chi(g) \in \mathbb{Q}$ et $\chi(g)$ est un entier algébrique, donc $\chi(g) \in \mathbb{Z}$.

Remarque 2.3 Soit K un corps de caractéristique 0 et G un groupe fini. Alors le groupe $R_K(G)$ est le groupe de Grothendieck de l'ensemble des classes d'isomorphisme de KG-modules (de dimension finie).

Soit V et W des KG-modules (de dimension finie) et χ, η leurs caractères respectifs. Alors V et W sont isomorphes comme KG-modules si et seulement si $\chi = \eta$ (Une preuve de ce résultat se trouve dans le livre *Representation theory of finite groups and associative algebras* de Charles W. Curtis et Irving Reiner, [CR66], corollaire 30.14, page 214). Ainsi $R_K(G)$ peut être identifié au groupe de Grothendieck de l'ensemble des caractères de G sur K. En particulier, on peut voir $R_K(G)$ comme un sous-ensemble de $C_K(G)$.

Notation 2.4 *Soit K un corps de caractéristique 0, G un groupe fini et soit C_G l'ensemble des sous-groupes cycliques de G. Comme G est fini, C_G l'est aussi. On définit*

$$T_K(G) = \Big\{ \sum_{H \in C_G} a_H \operatorname{Ind}_H^G \mathbf{1}_H \,\Big|\, a_H \in \mathbb{Z},\ \forall\ H \in C_G \Big\}.$$

L'ensemble $T_K(G)$ est l'ensemble des combinaisons linéaires à coefficients dans $\mathbb{Z}$ de caractères de G sur K qui sont induits par les caractères triviaux des groupes appartenant à C_G. C'est un sous-ensemble de $R_K(G)$.

Lemme 2.5 *Soit K un corps de caractéristique 0 et H un groupe cyclique fini. On définit la fonction centrale $f_H : H \to K$ par :*

$$f_H(x) = \begin{cases} |H| & \text{si } x \text{ engendre } H \\ 0 & \text{sinon,} \end{cases}$$

pour tout $x \in H$. Alors la fonction f_H appartient $T_K(H)$.

Preuve: On va montrer le résultat par récurrence sur $|H|$.
Si $|H| = 1$, alors $H = \mathbf{1}$ et $f_H = \mathbf{1}_H \in T_K(H)$ car H est cyclique.
On suppose maintenant le résultat vrai pour tout groupe de cardinalité $< |H|$. Ainsi, en particulier, le résultat est vrai pour tous les sous-groupes propres de H. On note S l'ensemble des sous-groupes propres de H. On va étudier

$$\sum_{E \in S \cup \{H\}} \mathrm{Ind}_E^H f_E.$$

On définit, pour tout $E \in S \cup \{H\}$, $\dot{f}_E : H \to K$ par

$$\dot{f}_E(x) = \begin{cases} f_E(x) & \text{si } x \in E \\ 0 & \text{sinon.} \end{cases}$$

Alors, par le fait que H est abélien et par la définition B.28 on a que

$$\mathrm{Ind}_E^H f_E(x) = \frac{|H|}{|E|} \dot{f}_E(x), \qquad \forall\, x \in H.$$

Soit $x \in H$. Alors

$$\sum_{E \in S \cup \{H\}} \mathrm{Ind}_E^H f_E(x) = \sum_{E \in S \cup \{H\}} \frac{|H|}{|E|} \dot{f}_E(x).$$

Or $\dot{f}_E(x)$ est égal à 0 sauf si x engendre E, c'est-à-dire sauf si $E = \langle x \rangle$. Et $\dot{f}_{\langle x \rangle}(x) = |\langle x \rangle|$. Ainsi on obtient que

$$\sum_{E \in S \cup \{H\}} \mathrm{Ind}_E^H f_E(x) = \frac{|H|}{|\langle x \rangle|} |\langle x \rangle| = |H| = |H| \mathbf{1}_H(x).$$

On remarque alors que

$$f_H = \sum_{E \in S \cup \{H\}} \mathrm{Ind}_E^H f_E - \sum_{E \in S} \mathrm{Ind}_E^H f_E = |H| \mathbf{1}_H - \sum_{E \in S} \mathrm{Ind}_E^H f_E.$$

Or $|H|\mathbf{1}_H$ appartient à $T_K(H)$ (car H est cyclique). De plus, par hypothèse de récurrence, $f_E \in T_K(E)$ pour tout $E \in S$. Mais alors, par transitivité de l'induction (proposition B.26), on a $\mathrm{Ind}_E^H f_E \in T_K(H)$. Ainsi, on a obtenu que f_H est une combinaison $\mathbb{Z}$-linéaire d'éléments de $T_K(H)$ et donc $f_H \in T_K(H)$. □

Lemme 2.6 *Soit K un corps de caractéristique 0, G un groupe fini et H un sous-groupe cyclique de G. Alors*

$$\mathrm{Ind}_H^G f_H(x) = \begin{cases} |N_G(H)| & \textit{si } x \textit{ est conjugué à un générateur de } H \\ 0 & \textit{sinon}, \end{cases}$$

où $N_G(H)$ est le normalisateur de H dans G.

Preuve: Soit $x \in G$. Par la définition B.28, on a

$$\mathrm{Ind}_H^G f_H(x) = \frac{1}{|H|} \sum_{g \in G} \dot{f}_H(gxg^{-1}),$$

où $\dot{f}_H : G \to K$ est défini par

$$\dot{f}_H(y) = \begin{cases} f_H(y) & \text{si } y \in H \\ 0 & \text{sinon,} \end{cases}$$

pour tout $y \in G$. Ainsi, si x n'est pas conjugué à un générateur de H dans G, alors

$$\mathrm{Ind}_H^G f_H(x) = 0.$$

On suppose maintenant que x est conjugué dans G à un générateur de H, que l'on note y. Alors le nombre de conjugués de x dans G qui génèrent H est égal au nombre de conjugués de y dans G qui génèrent H. Or, si $t \in G$, alors y et tyt^{-1} sont de même ordre. Donc tyt^{-1} engendre H si et seulement si tyt^{-1} appartient à H, c'est-à-dire si et seulement si $t \in N_G(H)$ (car y engendre H). Ainsi le nombre de conjugués de x qui engendrent H est égal à $|N_G(H)|$. Par conséquent

$$\mathrm{Ind}_H^G f_H(x) = \frac{|N_G(H)|}{|H|}|H| = |N_G(H)|.$$

□

Lemme 2.7 *Soit G un groupe fini, χ un caractère rationnel de G et $x, y \in G$ tels que $\langle x \rangle = \langle y \rangle$. Alors $\chi(x) = \chi(y)$.*

Preuve: On pose $H = \langle x \rangle = \langle y \rangle$ et $\psi = \mathrm{Res}_H^G \chi$. Alors ψ est un caractère rationnel de H. Donc il existe une représentation linéaire (matricielle) $\rho : H \to GL_n(\mathbb{Q})$ dont le caractère est ψ. Alors $\rho(x) \in GL_n(\mathbb{Q}) \subset GL_n(\mathbb{C})$ et $\rho(x)$ est conjuguée dans $GL_n(\mathbb{C})$ à une matrice diagonale A. Or $\rho(x)$ est d'ordre fini divisant $|H|$, donc A aussi et donc

$$A = \begin{pmatrix} \varepsilon_1 & & 0 \\ & \ddots & \\ 0 & & \varepsilon_n \end{pmatrix},$$

où $\varepsilon_1, \ldots, \varepsilon_n$ sont des racines $|H|^{\text{ième}}$ de l'unité. Or y est aussi un générateur du groupe cyclique $H = \langle x \rangle$, donc il existe $m \in \mathbb{N}^*$ tel que $\text{pgcd}(m, |H|) = 1$ et $y = x^m$. Alors $\rho(y) = \rho(x^m) = \rho(x)^m$ est conjugué dans $GL_n(\mathbb{C})$ avec la matrice

$$A^m = \begin{pmatrix} \varepsilon_1^m & & 0 \\ & \ddots & \\ 0 & & \varepsilon_n^m \end{pmatrix}.$$

Ainsi on a que $\psi(x) = \text{Tr}(\rho(x)) = \text{Tr}(A) = \varepsilon_1 + \ldots + \varepsilon_n$ et $\psi(y) = \text{Tr}(\rho(y)) = \text{Tr}(A^m) = \varepsilon_1^m + \ldots + \varepsilon_n^m$.

Soit ξ une racine $|H|^{\text{ième}}$ primitive de l'unité dans $\mathbb{C}$. Comme le pgcd de m et $|H|$ est égal à 1, on peut considérer le $\mathbb{Q}$-automorphisme $\varphi : \mathbb{Q}(\xi) \to \mathbb{Q}(\xi)$ qui envoie ξ sur ξ^m. On a

$$\varphi(\psi(x)) = \varphi(\varepsilon_1 + \ldots + \varepsilon_n) = \varphi(\varepsilon_1) + \ldots + \varphi(\varepsilon_n) = \varepsilon_1^m + \ldots + \varepsilon_n^m = \psi(y).$$

Or $\psi(x) \in \mathbb{Q}$, donc on a aussi $\varphi(\psi(x)) = \psi(x)$. Ainsi $\chi(x) = \psi(x) = \varphi(\psi(x)) = \psi(y) = \chi(y)$, c'est-à-dire que $\chi(x) = \chi(y)$. □

Remarque 2.8 Une conséquence du lemme 2.7 est qu'un caractère rationnel est uniquement déterminé par ses valeurs sur un ensemble complet de générateurs des sous-groupes cycliques de G à conjugaison près. Si $x, y \in G$ sont tels que $\langle x \rangle$ et $\langle y \rangle$ sont conjugués dans G, alors $\chi(x) = \chi(y)$, pour tout caractère rationnel χ de G.

Théorème 2.9: dû à Artin sur les caractères induits
Soit G un groupe fini et χ un caractère rationnel quelconque de G. Alors $|G|\chi \in T_{\mathbb{Q}}(G)$. En d'autres termes, il existe $n \in \mathbb{N}^*$, des entiers $\{a_i\}_{i=1}^n$ et des sous-groupes cycliques $\{H_i\}_{i=1}^n$ de G tels que :

$$\chi = \sum_{i=1}^{n} \frac{a_i}{|G|} \text{Ind}_{H_i}^G \mathbf{1}_{H_i}.$$

Preuve: Par le lemme 2.5, on sait que pour tout sous-groupe cyclique H de G, $f_H \in T_{\mathbb{Q}}(H)$. Alors, par transitivité de l'induction (proposition B.26), on a $\text{Ind}_H^G f_H \in T_{\mathbb{Q}}(G)$. Il suffit donc de montrer que $|G|\chi$ est une combinaison linéaire (à coefficients dans $\mathbb{Z}$) des $\text{Ind}_{H_i}^G f_{H_i}$ pour certains sous-groupes cycliques H_i de G.

Soit $H_1, \ldots, H_m$ un ensemble complet de représentants des sous-groupes cycliques de G à conjugaison près. Pour tout $i = 1, \ldots, m$, soit $x_i \in G$ un générateur de H_i. On pose

$$\tau = \sum_{i=1}^{m} |G : N_G(H_i)| \chi(x_i) \text{Ind}_{H_i}^G f_{H_i}.$$

C'est une fonction centrale. On va montrer que $|G|\chi = \tau$.

Soit $x \in G$. Alors $\langle x \rangle$ est conjugué à exactement un des sous-groupes cycliques $H_1, \ldots, H_m$. On va dire que $\langle x \rangle$ et H_j sont conjugués. Alors $\mathrm{Ind}_{H_j}^G f_{H_j}(x) = |N_G(H_j)|$ et pour tout $i \in \{1, \ldots, m\}$ avec $i \neq j$, on a $\mathrm{Ind}_{H_i}^G f_{H_i}(x) = 0$ (lemme 2.6). Par conséquent,

$$\tau(x) = |G : N_G(H_j)|\chi(x_j)|N_G(H_j)| = |G|\chi(x_j).$$

Mais comme $\langle x \rangle$ et H_j sont conjugués, x est conjugué à un générateur y de H_j. Ainsi $\langle y \rangle = H_j = \langle x_j \rangle$ et donc par le lemme 2.7, $\chi(y) = \chi(x_j)$. Or x et y sont conjugués donc $\chi(x) = \chi(y) = \chi(x_j)$. Ainsi

$$\tau(x) = |G|\chi(x_j) = |G|\chi(x).$$

On a montré que $\tau = |G|\chi$. Or $|G : N_G(H_i)|\chi(x_i)$ appartient à $\mathbb{Z}$ pour tout $i \in \{1, \ldots, m\}$, donc τ est une combinaison $\mathbb{Z}$-linéaire des éléments $\mathrm{Ind}_{H_1}^G f_{H_1}, \ldots, \mathrm{Ind}_{H_m}^G f_{H_m}$ qui appartiennent à $T_{\mathbb{Q}}(G)$. Ceci implique que $\tau \in T_{\mathbb{Q}}(G)$, c'est-à-dire que $|G|\chi \in T_{\mathbb{Q}}(G)$. □

Corollaire 2.10 *Le nombre de $\mathbb{Q}G$-modules (de dimension finie) irréductibles non-isomorphes coïncide avec le nombre de sous-groupes cycliques de G à conjugaison près.*

Preuve: Soit $\chi_1, \ldots, \chi_r$ un ensemble complet de caractères rationnels irréductibles distincts de G. Soit $H_1, \ldots, H_s$ un ensemble complet de sous-groupes cycliques de G à conjugaison près. Soit $x_i \in G$ un générateur de H_i, pour tout $i \in \{1, \ldots, s\}$. On doit montrer que $r = s$. De fait, on va montrer que $\{\chi_1, \ldots, \chi_r\}$ et $\{\mathrm{Ind}_{H_1}^G f_{H_1}, \ldots, \mathrm{Ind}_{H_s}^G f_{H_s}\}$ sont des ensembles linéairement indépendants qui engendrent le même $\mathbb{Q}$-sous-espace vectoriel de $C_{\mathbb{Q}}(G)$. On pose

$$V = \mathrm{Vect}\{\chi_1, \ldots, \chi_r\} \quad \text{et} \quad W = \mathrm{Vect}\{\mathrm{Ind}_{H_1}^G f_{H_1}, \ldots, \mathrm{Ind}_{H_s}^G f_{H_s}\}.$$

On va commencer par monter que $V = W$.

$\subset$: Par le lemme 2.5 et par la transitivité de l'induction (proposition B.26), pour tout $i \in \{1, \ldots, s\}$,

$$\mathrm{Ind}_{H_i}^G f_{H_i} \in T_{\mathbb{Q}}(G) \subset R_{\mathbb{Q}}(G) \subset V.$$

Ainsi $W \subset V$.

$\supset$: Par la preuve du théorème 2.9, on sait aussi que, pour tout $1 \leq j \leq m$, χ_j est une combinaison $\mathbb{Q}$-linéaire de $\mathrm{Ind}_{H_1}^G f_{H_1}, \ldots, \mathrm{Ind}_{H_s}^G f_{H_s}$, c'est-à-dire que $\chi_j \in W$. Ainsi $V \subset W$.

Il reste à voir que les ensembles $\{\chi_1, \ldots, \chi_r\}$ et $\{\mathrm{Ind}_{H_1}^G f_{H_1}, \ldots, \mathrm{Ind}_{H_s}^G f_{H_s}\}$ sont linéairement indépendants. Or on sait déjà que l'ensemble $\{\chi_1, \ldots, \chi_r\}$ est linéairement indépendant dans V (théorème B.20).
Soit $\lambda_1, \ldots, \lambda_s \in \mathbb{Q}$ tels que

$$\sum_{i=1}^{s} \lambda_i \mathrm{Ind}_{H_i}^G f_{H_i} = 0.$$

Alors, si $j \in \{1, \ldots, s\}$,

$$0 = \sum_{i=1}^{s} \lambda_i \operatorname{Ind}_{H_i}^G f_{H_i}(x_j) = \lambda_j |N_G(H_j)|$$

(par le lemme 2.6 et le fait que $\langle x_j \rangle$ est conjugué à H_j et n'est pas conjugué à H_i si $i \neq j$). Ainsi, pour tout $j \in \{1, \ldots, s\}$, $\lambda_j = 0$, c'est-à-dire que l'ensemble $\{\operatorname{Ind}_{H_1}^G f_{H_1}, \ldots, \operatorname{Ind}_{H_s}^G f_{H_s}\}$ est linéairement indépendant. Ainsi on a obtenu que $\{\chi_1, \ldots, \chi_r\}$ et $\{\operatorname{Ind}_{H_1}^G f_{H_1}, \ldots, \operatorname{Ind}_{H_s}^G f_{H_s}\}$ sont des bases de V et donc $r = s$. □

On va maintenant utiliser ce résultat pour trouver les tables de caractères rationnels de quelques groupes.

Exemple 2.11: Le groupe cyclique C_p
Soit p un nombre premier et $G = C_p = \langle x \,|\, x^p = 1 \rangle$. Alors il y a deux sous-groupes cycliques (à conjugaison près) : $\mathbf{1}$ et G. Donc il y a deux caractères rationnels irréductibles distincts : Le caractère trivial $\mathbf{1}_G$ et un autre caractère χ_2. Or on sait que $\mathbf{1}_G + d\chi_2 = \chi_{\text{reg}}$, où d est un entier entre 1 et $\chi_2(1_G)$ et χ_{reg} est le caractère régulier de G (théorème B.11 et proposition B.12). Ainsi on a

$$\begin{aligned} \mathbf{1}_G(x) + d\chi_2(x) &= \chi_{\text{reg}}(x) \\ \Rightarrow 1 + d\chi_2(x) &= 0 \\ \Rightarrow \chi_2(x) &= -\frac{1}{d} \in \mathbb{Z} \end{aligned}$$

Mais alors, la seule possibilité pour d est 1, d'où $\chi_2 = \chi_{\text{reg}} - \mathbf{1}_G$. Voici la table de caractères rationnels de G est :

	1	x
$\mathbf{1}_G$	1	1
χ_2	$p-1$	-1

Exemple 2.12: Le groupe cyclique C_{p^2}
Soit p un nombre premier et $G = C_{p^2} = \langle x \,|\, x^{p^2} = 1 \rangle$. Alors il y a trois sous-groupes cycliques (à conjugaison près) : $\mathbf{1}$, $\langle x^p \rangle$ et G. Donc il y a trois caractères rationnels irréductibles distincts : Le caractère trivial et deux autres caractères χ_2 et χ_3. Or $G/\langle x^p \rangle$ est isomorphe à C_p et ainsi par inflation des caractères rationnels irréductibles de C_p, on obtient deux caractères rationnels irréductibles de G. Le premier est le caractère trivial. On note le second χ_2. Il ne reste plus qu'à trouver ce que vaut χ_3. Soit ν l'induction à C_{p^2} du caractère rationnel non trivial de $C_p = \langle x^p \rangle$. Alors la formule B.27 permet d'obtenir les valeurs de ν :

$$\nu(x^i) = \begin{cases} p(p-1) & \text{si } i = 0 \\ -p & \text{si } i \neq 0 \text{ et } p|i \\ 0 & \text{sinon.} \end{cases}$$

Mais alors on a $\langle \nu, \chi_1 \rangle_G = \langle \nu, \chi_2 \rangle_G = 0$ donc il existe $z \in \mathbb{Z}^*$ tel que $\nu = z\chi_3$. En particulier, $\chi_3(x) = \frac{1}{z}\nu(x) = 0$. Il existe des entiers $1 \leq d \leq \chi_2(1_G)$ et $1 \leq e \leq \chi_3(1_G)$ tels que

$$\mathbf{1}_G + d\chi_2 + e\chi_3 = \chi_{\text{reg}}$$

(c'est une conséquence du théorème B.11 et de la proposition B.12). Donc, si on évalue en x, on a

$$1 - d + 0 = 0 \Longrightarrow d = 1$$

et ainsi $\mathbf{1}_G + \chi_2 + e\chi_3 = \chi_{\text{reg}}$ et donc

$$\chi_3 = \frac{1}{e}(\chi_{\text{reg}} - \mathbf{1}_G - \chi_2).$$

Alors, si on évalue en x^p, on a

$$\chi_3(x^p) = \frac{1}{e}(0 - 1 - (p-1)) = -\frac{p}{e} \in \mathbb{Z},$$

donc e est égal à 1 ou p. Or si e est égal à p, alors $\chi_3(1_G) = p - 1 < e$, ce qui est impossible. Donc e est égal à 1 et

$$\chi_3 = \chi_{\text{reg}} - \mathbf{1}_G - \chi_2.$$

Voici la table de caractères rationnels de G est :

	1	x	x^p
$\mathbf{1}_G$	1	1	1
χ_2	$p-1$	-1	$p-1$
χ_3	$p(p-1)$	0	$-p$

Exemple 2.13: Le groupe $C_2 \times C_2$
Soit $G = C_2 \times C_2$, où $C_2 = \langle x \,|\, x^2 = 1 \rangle$. Le groupe G possède 4 sous-groupes cycliques (à conjugaison près). Donc on doit trouver 4 caractères rationnels irréductibles. Or tous les caractères irréductibles de G sur $\mathbb{C}$ sont aussi des caractères de G sur $\mathbb{Q}$ (on peut prendre les même modules), d'où on a tous les caractères rationnels de G. Voici la table de caractères rationnels de G.

	1	$(x,1)$	$(1,x)$	(x,x)
$\mathbf{1}_G$	1	1	1	1
χ_2	1	1	-1	-1
χ_3	1	-1	-1	1
χ_4	1	-1	1	-1

Exemple 2.14: Le groupe $C_p \times C_p$
Soit $G = C_p \times C_p$, où $C_p = \langle x \,|\, x^p = 1 \rangle$. Le groupe G possède $p + 2$ sous-groupes cycliques (à conjugaison près). Donc, par le corollaire 2.10, G possède $p + 2$ caractères rationnels irréductibles. Le premier caractère

est le caractère trivial. Pour tout $1 \leq j \leq p$, le groupe $G/\langle(x, x^j)\rangle$ est isomorphes au groupe C_p, dont on connaît les caractères rationnels irréductibles (exemple 2.11). On note χ_j le caractère inflaté du caractère non-trivial de $G/\langle(x, x^j)\rangle \cong C_p$. Cela donne p caractères rationnels de G qui sont irréductibles et distincts. Il en reste un à trouver. Or $G/\langle(1, x)\rangle$ est aussi isomorphe à C_p. On inflate le caractère non-trivial que l'on note χ_{p+1}. C'est aussi un caractère rationnel irréductible de G différent de ceux qu'on avait déjà trouvés. Ainsi on a trouvé tous les caractères rationnels de $C_p \times C_p$, dont voici la table de caractères rationnels :

	$(1,1)$	$(1,x)$	(x,x^i) $0 \leq i \leq p-1$
$\mathbf{1}_G$	1	1	1
χ_j	$p-1$	-1	$p\delta_{ij}-1$
χ_{p+1}	$p-1$	$p-1$	-1

où $1 \leq j \leq p$ et

$$\delta_{ij} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{sinon.} \end{cases}$$

Exemple 2.15: Le groupe symétrique S_3
Soit $G = S_3$. On va étudier les caractères rationnels irréductibles de G. Il y a trois sous-groupes cycliques à conjugaison près : $\mathbf{1}$, $\langle(1\ 2)\rangle$ et $\langle(1\ 2\ 3)\rangle$. Donc il y a trois caractères rationnels irréductibles distincts sur S_3. Les deux caractères linéaires de G sur $\mathbb{C}$ sont aussi des caractères sur $\mathbb{Q}$: le caractère trivial $\mathbf{1}_G$ et le caractère signe χ_2. Il reste un seul caractère rationnel irréductible à trouver : χ_3. Soit $V = \mathbb{Q}^3$ un $\mathbb{Q}$-espace vectoriel, et $\{e_1, e_2, e_3\}$ sa base canonique. Alors V est un $\mathbb{Q}G$-module si on définit l'action de S_3 sur V par :

$$\sigma e_i = e_{\sigma(i)}, \quad \forall\ \sigma \in S_3, \quad \forall\ i \in \{1, 2, 3\}.$$

On définit $v_1 = e_1 + e_2 + e_3$, $v_2 = e_1 - e_2$ et $v_3 = e_1 - e_3$. Alors $\{v_1, v_2, v_3\}$ est une base de V. On pose $W_1 = \text{Vect}\{v_1\}$ et $W_2 = \text{Vect}\{v_2, v_3\}$. Alors $V = W_1 \oplus W_2$ et on peut facilement vérifier que W_1 et W_2 sont des $\mathbb{Q}G$-sous-modules de V et que W_1 est le $\mathbb{Q}G$-module trivial. Notons ψ le caractère de W_2. Alors si on calcule $\langle\psi, \psi\rangle_G$, on obtient 1, donc ψ est forcément irréductible et c'est le dernier caractère que l'on cherchait : $\chi_3 = \psi$. Ainsi la table de caractères rationnels de S_3 sur $\mathbb{Q}$ est :

	1	$(1\ 2)$	$(1\ 2\ 3)$
$\mathbf{1}_G$	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

On peut remarquer que les tables de caractères sur $\mathbb{Q}$ et $\mathbb{C}$ sont les mêmes (exemple B.52).

Exemple 2.16: Le groupe des quaternions Q_8
Soit $G = Q_8$ le groupe des quaternions. Les éléments de Q_8 sont 1, -1, i, $-i$, j, $-j$, k et $-k$. On a les règles de calculs suivantes : $ij = k = -ji$ et $i^2 = -1 = j^2$. Ainsi on obtient la table de calculs suivante (le reste des produits se déduit de la table en utilisant le fait que -1 est un élément central) :

$\nearrow$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Quelques calculs permettent d'obtenir que $[Q_8, Q_8] = \{1, -1\}$ (propriétés A.11) et $Q_8/[Q_8, Q_8] \cong C_2 \times C_2$. Or on connaît la table de caractères rationnels de $C_2 \times C_2$ (exemple 2.13) et donc par inflation, on obtient les quatre caractères linéaires rationnels de G que l'on va noter $\chi_1 = \mathbf{1}_G$, χ_2, χ_3 et χ_4. Or G a 5 sous-groupes cycliques (à conjugaison près) : $\mathbf{1}$, $\langle -1 \rangle$, $\langle i \rangle$, $\langle j \rangle$ et $\langle k \rangle$. Ainsi il reste un caractère rationnel irréductible à trouver, que l'on va noter χ_5.
On considère l'anneau des quaternions

$$\mathbb{H} = \left(\frac{-1, -1}{\mathbb{Q}} \right) = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k,$$

où $i^2 = -1 = j^2$, $ij = k = -ji$. On peut le munir de la structure de $\mathbb{Q}Q_8$-module qui découle du fait que Q_8 est inclus dans $\mathbb{H}$. Or, on peut montrer que c'est un corps gauche et de plus que tout $\mathbb{Q}Q_8$-sous-module de $\mathbb{H}$ est un idéal de $\mathbb{H}$ (la multiplication à gauche par un élément de $\mathbb{H}$ correspond à l'action d'un élément de $\mathbb{Q}Q_8$). Ainsi, $\mathbb{H}$ est irréductible et est de dimension supérieure à 1. Cela nous donne le dernier caractère de Q_8 : On le note χ_5. Voici la table de caractères rationnels de Q_8.

	1	-1	i	j	k
$\mathbf{1}_G$	1	1	1	1	1
χ_2	1	1	-1	-1	1
χ_3	1	1	-1	1	-1
χ_4	1	1	1	-1	-1
χ_5	4	-4	0	0	0

Chapitre 3

Le groupe de Burnside

Dans ce chapitre, on va rappeler la notion de G-ensemble, puis définir la notion de (G, H)-bi-ensemble et étudier leurs propriétés. Ensuite, on va définir le groupe de Burnside et voir les liens avec les KG-modules. Pour finir le chapitre, on va introduire quelques notions et propriétés qui seront utiles pour les chapitres suivants. Les parties 3.1, 3.2, 3.3 et 3.4 se basent essentiellement sur *Burnside Rings* de Serge Bouc, [Bou00] et sur le polycopié *Biset functors for finite groups* de Serge Bouc, [Bou].

3.1 Rappels sur les G-ensembles

Définition 3.1 *Soit G un groupe. Un **G-ensemble (à gauche)** est un ensemble X muni d'une application $G \times X \to X$, $(g, x) \mapsto g \cdot x = gx$ qui satisfait aux propriétés suivantes :*

i) Pour tout $g, h \in G$ et pour tout $x \in X$, on a $g \cdot (h \cdot x) = (gh) \cdot x$.

ii) Pour tout $x \in X$, on a $1_G \cdot x = x$, où 1_G est l'élément neutre de G.

Remarque 3.2 De manière analogue, on peut définir un G-ensemble à droite. De fait, un G-ensemble à droite est un G^{op}-ensemble à gauche. Par la suite, on omettra en général le "à gauche" lorsqu'on parle de G-ensemble à gauche. De plus, la plupart des résultats seront énoncés pour des G-ensembles à gauche mais il existe des résultats analogues pour les G-ensembles à droite.

Définition 3.3 *Soit G un groupe et X, Y des G-ensembles. Un **morphisme de G-ensembles** de X vers Y est une application $f : X \to Y$ qui est tel que $f(gx) = gf(x)$, pour tout $g \in G$ et pour tout $x \in X$.*
Un morphisme de G-ensembles $f : X \to Y$ est un isomorphisme de G-ensemble s'il existe un morphisme de G-ensembles $f' : Y \to X$ tel que $f \circ f' = \mathrm{Id}_Y$ et $f' \circ f = \mathrm{Id}_X$.

Remarque 3.4 Un morphisme de G-ensembles $f : X \to Y$ est un isomorphisme si et seulement si f est bijectif.

Définition 3.5 *Soit G un groupe et X un G-ensemble. Si H est un sous-groupe de G et $x \in X$, l'ensemble*

$$\mathrm{Orb}_H(x) = \big\{ y \in X \,\big|\, \exists\ h \in H \text{ tel que } y = hx \big\}$$

*est appelé une H-**orbite de** x . L'ensemble de toutes les H-orbites est noté $H\backslash X$. On note $[H\backslash X]$ un ensemble de représentants des H-orbites (on note X/H l'ensemble des H-orbites et $[X/H]$ un ensemble de représentants des orbites si X est un G-ensemble à droite). Si X possède une seule orbite, alors X est **transitif**. Le **stabilisateur de** x est l'ensemble*

$$G_x = \{ g \in G \,|\, gx = x \}.$$

*C'est un sous-groupe de G. **L'ensemble des points fixes par** H est l'ensemble*

$$X^H = \{ x \in X \,|\, hx = x,\ \forall\ h \in H \}.$$

Lemme 3.6 *Soit G un groupe. Tout G-ensemble transitif X est isomorphe à G/H pour un certain sous-groupe H de G.*

Preuve: Il suffit de voir que l'application $\varphi : G/G_x \to X$ définie par $\varphi(gG_x) = g \cdot x$ est un isomorphisme de G-ensembles (bien défini). □

Si I est un ensemble et $\{X_i\}_{i \in I}$ est une famille de G-ensembles indexée par I, alors l'union disjointe $\bigsqcup_{i \in I} X_i$ est aussi un G-ensemble (l'action de $g \in G$ sur un élément x de l'union est égal à l'action de g sur x dans le G-ensemble X_i, où i est l'unique élément de I tel que $x \in X_i$).

Lemme 3.7 *Soit G un groupe et X un G-ensemble. Si $[G\backslash X]$ est un ensemble de représentants des G-orbites de X, alors l'application*

$$\varphi : \bigsqcup_{x \in [G\backslash X]} G/G_x \to X$$

définie par $\varphi(gG_x) \mapsto g \cdot x$ est un isomorphisme de G-ensembles.

Preuve: Il suffit de vérifier que l'application φ est un isomorphisme de G-ensembles (bien défini). □

3.2 Définitions et propriétés des (H, G)-bi-ensembles

Définition 3.8 *Soit G et H des groupes. Alors un (H, G)-**bi-ensemble** est un $(H \times G^{\mathrm{op}})$-ensemble. De manière équivalente, un (H, G)-**bi-ensemble** U est un H-ensemble à gauche et un G-ensemble à droite tel que*

$$(h \cdot u) \cdot g = h \cdot (u \cdot g), \quad \forall\ h \in H,\ \forall\ u \in U,\ \forall\ g \in G.$$

*Cet élément sera en général simplement écrit $h \cdot u \cdot g$ ou même hug. Un (H, G)-bi-ensemble U est est dit **fini** si U est fini.*

Les notions que l'on a définies précédemment pour les G-ensembles sont aussi valables pour les (H, G)-bi-ensembles :

- Soit G et H des groupes et U, V des (H, G)-bi-ensembles. Un **morphisme de (H, G)-bi-ensembles** de U vers V est une application $f : U \to V$ qui est telle que

$$f(h \cdot u \cdot g) = h \cdot f(u) \cdot g, \quad \forall\ g \in G,\ \forall\ h \in H,\ \forall\ u \in U.$$

  Un morphisme de (H, G)-bi-ensembles $f : U \to V$ est un isomorphisme de (H, G)-bi-ensembles s'il existe un morphisme de (H, G)-bi-ensembles $f' : V \to U$ tel que $f \circ f' = \mathrm{Id}_V$ et $f' \circ f = \mathrm{Id}_U$.

- Soit U un (H, G)-bi-ensemble. La (H, G)**-orbite** de $u \in U$ est l'ensemble

$$\{v \in U \,\big|\, \exists\ (h, g) \in H \times G \text{ tel que } hug = v\}.$$

  L'ensemble des (H, G)-orbites de U est noté $H\backslash U/G$. On note $[H\backslash U/G]$ un ensemble de représentants dans U des (H, G)-orbites. Le bi-ensemble U est **transitif** si la cardinalité de $H\backslash U/G$ est égal à 1, c'est-à-dire si pour tout $u, v \in U$, il existe $h \in H$ et $g \in G$ tels que $v = h \cdot u \cdot g$.
  Soit $u \in U$. Le stabilisateur de u dans U est l'ensemble

$$(H, G)_u = \big\{(h, g) \in H \times G \,\big|\, h \cdot u = u \cdot g\big\}.$$

  C'est un sous-groupe de $H \times G$.

- Si I est un ensemble et $\{U_i\}_{i \in I}$ est une famille de (H, G)-bi-ensembles indexée par I, alors l'union disjointe $\bigsqcup_{i \in I} U_i$ est aussi un (H, G)-bi-ensemble.

Exemple 3.9 Soit $(G, \cdot)$ un groupe. Alors l'ensemble G est un (G, G)-bi-ensemble pour l'action

$$h \star x \star g = h \cdot x \cdot g, \qquad \forall\ h, x, g \in G.$$

On appelle ce bi-ensemble le **bi-ensemble identité** et on le note Id_G .
Plus généralement, si H est un sous-groupe de G, alors l'ensemble G/H est un $(G, N_G(H)/H)$-bi-ensemble pour l'action

$$g \star xH \star kH = (g \cdot x \cdot k)H, \qquad \forall\ g, x \in G,\ \forall\ k \in N_G(H)$$

et l'ensemble $H\backslash G$ est un $(N_G(H)/H, G)$-bi-ensemble pour l'action

$$kH \star Hx \star g = H(k \cdot x \cdot g), \qquad \forall\ k \in N_G(H),\ \forall\ x, g \in G.$$

Si H et K sont des sous-groupes de G, alors l'ensemble G est un (H, K)-bi-ensemble pour l'action

$$h \star g \star k = h \cdot g \cdot k, \qquad \forall\ h \in H,\ \forall\ g \in G,\ \forall\ k \in K.$$

Lemme 3.10 *Soit G et H des groupes.*

i) Si L est un sous-groupe de $H \times G$, alors l'ensemble $(H \times G)/L$ est un (H, G)-bi-ensemble transitif pour l'action définie par

$$h \cdot (b, a)L \cdot g = (hb, g^{-1}a)L, \quad \forall\, h \in H,\ \forall\, (b, a)L \in (H \times G)/L,\ \forall\, g \in G.$$

ii) Si U est un (H, G)-bi-ensemble, soit $[H\backslash U/G]$ un ensemble de représentants des (H, G)-orbites de U. Alors il existe un isomorphisme de (H, G)-bi-ensembles

$$X \cong \bigsqcup_{u \in [H\backslash U/G]} (H \times G)/(H, G)_u.$$

En particulier, tout (H, G)-bi-ensemble transitif est isomorphe à $(H \times G)/L$, pour un certain sous-groupe L de $H \times G$.

Preuve: Pour le point *i)*, il suffit de vérifier les conditions. Le point *ii)* est une reformulation du lemme 3.7 pour les bi-ensembles. □

Exemple 3.11: Les bi-ensembles élémentaires
Soit $(G, \cdot)$ un groupe. Les exemples suivants de bi-ensembles sont fondamentaux pour la suite :

- Si H est un sous-groupe de G, alors l'ensemble G est un (H, G)-bi-ensemble pour l'action

  $$h \star x \star g = h \cdot x \cdot g, \qquad \forall\, h \in H,\ \forall\, x, g \in G.$$

  On note ce bi-ensemble Res^G_H, où Res signifie **restriction** .
- Si H est un sous-groupe de G, alors l'ensemble G est un (G, H)-bi-ensemble pour l'action

  $$g \star x \star h = g \cdot x \cdot h, \qquad \forall\, g, x \in G,\ \forall\, h \in H.$$

  On note ce bi-ensemble Ind^G_H, où Ind signifie **induction** .
- Si $N \trianglelefteq G$ et si $H = G/N$, alors l'ensemble H est un (G, H)-bi-ensemble pour l'action

  $$g \star x \star h = gN \cdot x \cdot h, \qquad \forall\, g \in G, \forall\, x, h \in H.$$

  On note ce bi-ensemble Inf^G_H, où Inf signifie **inflation** .
- Si $N \trianglelefteq G$ et si $H = G/N$, alors l'ensemble H est un (H, G)-bi-ensemble pour l'action

  $$h \star x \star g = h \cdot x \cdot gN, \qquad \forall\, h, x \in H,\ \forall\, g \in G.$$

  On note ce bi-ensemble Def^G_H, où Def signifie **déflation** .

- Si H un groupe et $f : G \to H$ un isomorphisme de groupes, alors l'ensemble H est un (H, G)-bi-ensemble pour l'action

$$h \star x \star g = h \cdot x \cdot f(g), \qquad \forall h, x \in H, \ \forall\ g \in G.$$

  On note ce bi-ensemble $\mathrm{Iso}(f)$ ou Iso_G^H si l'isomorphisme f est clairement défini par le contexte.

Définition 3.12 *Soit G et H des groupes et soit U un (H, G)-bi-ensemble. On définit le (G, H)-**bi-ensemble opposé** U^{op} comme suit : U^{op} est égal à U comme ensemble et il est muni de l'action définie par*

$$g \star u \star h = h^{-1} \cdot u \cdot g^{-1} \text{ dans } U, \qquad \forall\ g \in G, \ \forall\ u \in U^{\mathrm{op}}, \ \forall\ h \in H.$$

Exemple 3.13 Soit G un groupe et H un sous-groupe. Alors il existe un isomorphisme de (H, G)-bi-ensemble

$$\mathrm{Res}_H^G \xrightarrow{\cong} (\mathrm{Ind}_H^G)^{\mathrm{op}}$$

qui est défini par $g \mapsto g^{-1}$ et un isomorphisme de (G, H)-bi-ensemble

$$\mathrm{Ind}_H^G \xrightarrow{\cong} (\mathrm{Res}_H^G)^{\mathrm{op}}$$

qui est défini par $g \mapsto g^{-1}$.
Soit N un sous-groupe normal de G. Alors il existe un isomorphisme de $(G/N, G)$-bi-ensemble

$$\mathrm{Def}_{G/N}^G \xrightarrow{\cong} (\mathrm{Inf}_{G/N}^G)^{\mathrm{op}}$$

qui est défini par $g \mapsto g^{-1}$ et un isomorphisme de $(G, G/N)$-bi-ensemble

$$\mathrm{Inf}_{G/N}^G \xrightarrow{\cong} (\mathrm{Def}_{G/N}^G)^{\mathrm{op}}$$

qui est défini par $g \mapsto g^{-1}$.

3.3 La composition de bi-ensembles

On va maintenant définir la composition de bi-ensembles et étudier ses propriétés :

Définition 3.14 *Soit G, H et K des groupes. Si U est un (H,G)-bi-ensemble et V un (K, H)-bi-ensemble, la composition de V et U est l'ensemble des H-orbites sur le produit cartésien $V \times U$, où l'action à droite de H est définie par*

$$(v, u) \star h = (v \cdot h, h^{-1} \cdot u), \qquad \forall\ (v, u) \in V \times U, \ \forall\ h \in H.$$

On le note $V \times_H U$. La H-orbite de $(v, u) \in V \times U$ est noté par $(v,_H u)$. L'ensemble $V \times_H U$ est un (K, G)-bi-ensemble pour l'action définie par

$$k \star (v,_H u) \star g = (k \cdot v,_H u \cdot g), \qquad \forall\ k \in K, \ \forall\ (v,_H u) \in V \times_H U, \ \forall\ g \in G.$$

Définition 3.15 *Soit G un groupe. Une* ***section*** (T, S) *est la donnée de deux sous-groupes S et T de G tels que $S \trianglelefteq T$.*

Exemple 3.16 Soit G un groupe et (T, S) une section de G. Alors il existe un isomorphisme de $(G, T/S)$-bi-ensemble

$$\mathrm{Ind}_T^G \times_T \mathrm{Inf}_{T/S}^T \xrightarrow{\cong} G/S$$

envoyant $(g,_T tS)$ sur gtS. C'est pourquoi le $(G, T/S)$-bi-ensemble G/S sera noté $\mathrm{Indinf}_{T/S}^G$.
Similairement, il existe un isomorphisme de $(T/S, G)$-bi-ensemble

$$\mathrm{Def}_{T/S}^T \times_T \mathrm{Res}_T^G \xrightarrow{\cong} S\backslash G$$

envoyant $(tS,_T g)$ sur Stg. C'est pourquoi le $(T/S, G)$-bi-ensemble $S\backslash G$ sera noté $\mathrm{Defres}_{T/S}^G$.

Proposition 3.17 *Soit G un groupe et (B, A), (D, C) deux sections de G.*

i) L'ensemble des (A, C)-orbites $A\backslash G/C$ est un $(B/A, D/C)$-bi-ensemble pour l'action

$$bA \star AgC \star dC = A(bgd)C, \qquad \forall\ b \in B,\ \forall\ g \in G,\ \forall\ d \in D.$$

ii) Il existe un isomorphisme de $(B/A, D/C)$-bi-ensemble

$$\mathrm{Defres}_{B/A}^G \times_G \mathrm{Indinf}_{D/C}^G \cong A\backslash G/C.$$

Preuve:

i) L'action est bien définie car A et C sont des sous-groupes normaux de B et D respectivement. De plus, on peut vérifier que l'action vérifie bien les propriétés voulues pour que $A\backslash G/C$ soit un $(B/A, D/C)$-bi-ensemble.

ii) On sait que $\mathrm{Defres}_{B/A}^G$ et $\mathrm{Indinf}_{D/C}^G$ sont isomorphes à $A\backslash G$ et G/C respectivement. Il suffit donc de trouver un isomorphisme entre $A\backslash G \times_G G/C$ et $A\backslash G/C$. On définit $\varphi : A\backslash G \times_G G/C \longrightarrow A\backslash G/C$ par

$$\varphi(Ag,_G hC) = AghC.$$

L'application φ est bien définie :
On doit montrer que si $(Ag,_G hC) = (Ak,_G lC)$, alors $AghC = AklC$. Or si $(Ag,_G hC) = (Ak,_G lC)$, alors il existe $i \in G$ tel que $(Ak, lC) = (Agi, i^{-1}hC)$, donc il existe $a \in A$ et $c \in C$ tel que $k = agi$ et $l = i^{-1}hc$. Ainsi $AklC = Aagii^{-1}hcC = AghC$.

L'application φ est un morphisme de $(B/A, D/C)$-bi-ensembles :
Soit $(Ag,_G\, hC) \in A\backslash G \times_G G/C$, $b \in B$ et $d \in D$. Alors

$$\begin{aligned}\varphi(bA \star (Ag,_G\, hC) \star dC) &= \varphi(Abg,_G\, hdC)\\ &= Abghd C\\ &= bA \star AghC \star dC\\ &= bA \star \varphi(Ag,_G\, hC) \star dC.\end{aligned}$$

L'application φ est injective :
Soit $(Ag,_G\, hC)$ et $(Ak,_G\, lC)$ dans $A\backslash G \times_G G/C$ tels que $\varphi(Ag,_G\, hC) = \varphi(Ak,_G\, lC)$, c'est-à-dire tels que $AghC = AklC$. Il existe $a \in A$ et $c \in C$ tels que $kl = aghc$ et donc $lc^{-1}h^{-1} = k^{-1}ag$. On pose $i = g^{-1}a^{-1}k$. Alors $i^{-1} = k^{-1}ag = lc^{-1}h^{-1}$ et donc $(Agi, i^{-1}hC) = (Ak, lC)$, c'est-à-dire $(Ag,_G\, hC) = (Ak,_G\, lC)$.
L'application φ est surjective :
Soit $AgC \in A\backslash G/C$. Alors $\varphi(Ag,_G\, 1_G C) = AgC$.

□

Proposition 3.18 *Soit G, H, K et L des groupes.*

i) Si U est un (H, G)-bi-ensemble, V un (K, H)-bi-ensemble et W un (L, K)-bi-ensemble, alors il existe un isomorphisme canonique de (L, G)-bi-ensembles

$$W \times_K (V \times_H U) \xrightarrow{\cong} (W \times_K V) \times_H U$$

défini par $(w,_K\, (v,_H\, u)) \mapsto ((w,_K\, v),_H\, u)$, pour tout $w \in W$, $v \in V$ et $u \in U$.

ii) Si U est un (H, G)-bi-ensemble et V un (K, H)-bi-ensemble, alors il existe un isomorphisme canonique de (G, K)-bi-ensembles

$$(V \times_H U)^{\mathrm{op}} \xrightarrow{\cong} U^{\mathrm{op}} \times_H V^{\mathrm{op}}$$

défini par $(v,_H\, u) \mapsto (u,_H\, v)$.

iii) Soit U, U' des (H, G)-bi-ensembles et V, V' des (K, H)-bi-ensembles. Alors il existe des isomorphismes canoniques de (K, G)-bi-ensembles

$$V \times_H (U \sqcup U') \cong (V \times_H U) \sqcup (V \times_H U')$$

$$(V \sqcup V') \times_H U \cong (V \times_H U) \sqcup (V' \times_H U).$$

iv) Si U est un (H, G)-bi-ensemble, alors il existe des isomorphismes canoniques de (H, G)-bi-ensembles

$$\mathrm{Id}_H \times_H U \xrightarrow{\cong} U \xleftarrow{\cong} U \times_G \mathrm{Id}_G$$

définis par $(h,_H\, u) \mapsto h \cdot u$ et $(u,_G\, g) \mapsto u \cdot g$, pour tout $h \in H$, pour tout $u \in U$ et pour tout $g \in G$.

Preuve: On vérifie facilement que les applications données sont des isomorphismes de bi-ensembles (bien définis). Pour le point *iii)*, les isomorphismes sont faciles à trouver (c'est les applications évidentes entre les deux bi-ensembles). □

Remarque 3.19 Une conséquence du point *i)* de la proposition 3.18 est que l'on peut noter $W \times_K V \times_H U$ à la place de $W \times_K (V \times_H U)$ ou $(W \times_K V) \times_H U$. De même, on note $(w,_K v,_H u)$ pour l'élément $((w,_K v),_H u)$ de $(W \times_K V) \times_H U$.

Notation 3.20 *Soit G, H et K des groupes. Si L est un sous-groupe de $H \times G$ et si M est un sous-groupe de $K \times H$, alors on définit*

$$M * L = \{(k,g) \in K \times G \,\big|\, \exists\ h \in H \text{ tel que } (k,h) \in M \text{ et } (h,g) \in L\}.$$

Il est facile de voir que c'est un sous-groupe de $K \times G$.

Notation 3.21 *Soit G et H des groupes et L un sous-groupe de $H \times G$. On définit les ensembles suivants :*

$$\begin{aligned} p_1(L) &= \{h \in H \,\big|\, \exists\ g \in G \text{ tel que } (h,g) \in L\} \\ p_2(L) &= \{g \in G \,\big|\, \exists\ h \in H \text{ tel que } (h,g) \in L\} \\ k_1(L) &= \{h \in H \,\big|\, (h,1_G) \in L\} \\ k_2(L) &= \{g \in G \,\big|\, (1_H,g) \in L\} \\ q(L) &= L/\big(k_1(L) \times k_2(L)\big). \end{aligned}$$

On peut montrer que $p_1(L)$ et $k_1(L)$ sont des sous-groupes de H, $p_2(L)$ et $k_2(L)$ sont des sous-groupes de G. De plus, $k_i(L)$ est un sous-groupe normal de $p_i(L)$ pour $i = 1, 2$ et $(k_1(L) \times k_2(L))$ est un sous-groupe normal de L. Ainsi les ensembles $q(L)$, $p_1(L)/k_1(L)$ et $q_2(L)/k_2(L)$ sont des groupes. Il existe des isomorphismes canoniques de groupes

$$p_1(L)/k_1(L) \cong q(L) \cong p_2(L)/k_2(L).$$

Une preuve de ces résultats se trouve dans *Biset functors for finite groups* de Serge Bouc, [Bou], pages 26 et 27.

Lemme 3.22: ***La formule de Mackey pour les bi-ensembles***
Soit G, H et K des groupes. Si L est un sous-groupe de $H \times G$ et si M est un sous-groupe de $K \times H$, alors il existe un isomorphisme de (K,G)-bi-ensemble

$$\big((K \times H)/M\big) \times_H \big((H \times G)/L\big) \cong \bigsqcup_{h \in [p_2(M) \backslash H / p_1(L)]} (K \times G)/(M * {}^{(h,1_G)}L),$$

où $[p_2(M)\backslash H/p_1(L)]$ est un ensemble de représentants des classes doubles.

Preuve: Une preuve de ce lemme se trouve dans l'article *Foncteurs d'ensembles munis d'une double action* de Serge Bouc, [Bou96], proposition 1. □

Lemme 3.23 *Soit G et H des groupes.*

i) Si (D, C) est une section de H et (B, A) une section de G tels qu'il existe un isomorphisme de groupe $f : B/A \to D/C$, alors

$$L_{(D,C),f,(B,A)} = \left\{(h, g) \in H \times G \,\middle|\, h \in D, g \in B \text{ et } hC = f(gA)\right\}$$

est un sous-groupe de $H \times G$.

ii) Réciproquement, si L est un sous-groupe de $H \times G$ alors il existe une unique section (D, C) de H, une unique section (B, A) de G et un unique isomorphisme de groupes $f : B/A \to D/C$ tels que

$$L = L_{(D,C),f,(B,A)}.$$

Preuve:

i) On remarque d'abord que $(1_H, 1_G)$ est un élément de $L_{(D,C),f,(B,A)}$ car comme f est un isomorphisme, $f(A) = C$.
Soit maintenant $(h, g), (k, l) \in L_{(D,C),f,(B,A)}$. Alors $h, k \in D$, $g, l \in B$ et $hC = f(gA)$, $kC = f(lA)$. On a ainsi $hk \in D$, $gl \in B$ et $hkC = hC \cdot kC = f(gA) \cdot f(lA) = f(glA)$ et donc $(h, g) \cdot (k, l) \in L_{(D,C),f,(B,A)}$.
Pour finir, soit $(h, g) \in L_{(D,C),f,(B,A)}$. Alors $h \in D$, $g \in D$ et $hC = f(gA)$. Donc on a $h^{-1} \in D$, $g^{-1} \in B$ et $h^{-1}C = (hC)^{-1} = f(gA)^{-1} = f(g^{-1}A)$ et donc $(h, g)^{-1} \in L_{(D,C),f,(B,A)}$.

ii) Pour l'existence, il suffit de voir que $L = L_{(p_1(L),k_1(L)),f,(p_2(L),k_2(L))}$, où f est l'isomorphisme canonique entre $p_2(L)/k_2(L)$ et $p_1(L)/k_1(L)$.
Pour l'unicité, soit (D, C) une section de H, (B, A) une section de G et $f : B/A \to D/C$ un isomorphisme de groupes. Alors on a que $p_1(L_{(D,C),f,(B,A)}) = D$, $p_2(L_{(D,C),f,(B,A)}) = B$, $k_1(L_{(D,C),f,(B,A)}) = C$ et $k_2(L_{(D,C),f,(B,A)}) = A$. De plus, si $b \in B$, alors $f(bA) = dC$ si $(b, d) \in L_{(D,C),f,(B,A)}$, ce qui détermine $f : B/A \to D/C$. Ainsi les éléments D, C, B, A et f sont uniquement déterminés par $L_{(D,C),f,(B,A)}$, ce qui implique l'unicité.

□

Lemme 3.24 *Soit G et H des groupes, L un sous-groupe de $H \times G$ et soit (D, C) et (B, A) les sections de H et G respectivement et $f : B/A \xrightarrow{\cong} D/C$ l'isomorphisme de groupes tels que $L = L_{(D,C),f,(B,A)}$. Alors il existe un isomorphisme de (H, G)-ensembles*

$$(H \times G)/L \cong \mathrm{Ind}_D^H \times_D \mathrm{Inf}_{D/C}^D \times_{D/C} \mathrm{Iso}(f) \times_{B/A} \mathrm{Def}_{B/A}^B \times_B \mathrm{Res}_B^G .$$

Preuve: On pose $\Delta = (H \times G)/L$ et

$$\Gamma = \mathrm{Ind}_D^H \times_D \mathrm{Inf}_{D/C}^D \times_{D/C} \mathrm{Iso}(f) \times_{B/A} \mathrm{Def}_{B/A}^B \times_B \mathrm{Res}_B^G .$$

On définit l'application $\varphi : \Delta \to \Gamma$ par

$$\varphi((h, g)L) = (h, {}_D\, C, {}_{D/C}\, C, {}_{B/A}\, A, {}_B\, g^{-1}),$$

pour tout $(h,g) \in H \times G$. On définit l'application $\psi : \Gamma \to \Delta$ par

$$\psi((h,_D\, dC,_{D/C}\, d'C,_{B/A}\, bA,_B\, g)) = (hdd', g^{-1}b^{-1})L,$$

pour tout $h \in H$, $d, d' \in D$, $b \in B$ et $g \in G$.

- L'application φ est bien définie :
  Soit $(h,g),(k,l) \in H \times G$ tel que $(h,g)L = (k,l)L$. Donc il existe $(d,b) \in L$ tel que $(k,l) = (h,g)(d,b) = (hd, gb)$. Alors, comme $d^{-1} \in f(b^{-1}A)$

$$\begin{aligned}
\varphi((k,l)L) &= (k,_D\, C,_{D/C}\, C,_{B/A}\, A,_B\, l^{-1}) \\
&= (hd,_D\, C,_{D/C}\, C,_{B/A}\, A,_B\, b^{-1}g^{-1}) \\
&= (h,_D\, dC,_{D/C}\, C,_{B/A}\, b^{-1}A,_B\, g^{-1}) \\
&= (h,_D\, C,_{D/C}\, dd^{-1}C,_{B/A}\, A,_B\, g^{-1}) \\
&= (h,_D\, C,_{D/C}\, C,_{B/A}\, A,_B\, g^{-1}) \\
&= \varphi((h,g)L).
\end{aligned}$$

- L'application ψ est bien définie :
  Soit $h \in H$, $d, d' \in D$, $b \in B$ et soit $g \in G$. Soit, de plus, $x \in D$, $yC \in D/C$, $zA \in B/A$, $y' \in f(zA)$ et $t \in B$. On doit montrer que l'image par ψ des éléments $E = (h,_D\, dC,_{D/C}\, d'C,_{B/A}\, bA,_B\, g)$ et $F = (hx,_D\, x^{-1}dyC,_{D/C}\, y^{-1}d'y'C,_{B/A}\, z^{-1}btA,_B\, t^{-1}g)$ sont égales. Or

$$\begin{aligned}
\psi(F) &= (hxx^{-1}dyy^{-1}d'y', g^{-1}tt^{-1}b^{-1}z)L \\
&= (hdd'y', g^{-1}b^{-1}z)L \\
&= (hdd', g^{-1}b^{-1})L \\
&= \psi(E)
\end{aligned}$$

  car $(y', z) \in L$.
  De manière analogue, si $h \in H$, $d, d', \widetilde{d}, \widetilde{d'} \in D$, $b, \widetilde{b} \in B$, $g \in G$ sont tels que $dC = \widetilde{d}C$, $d'C = \widetilde{d'}C$ et $bA = \widetilde{b}A$, on peut vérifier que les images par ψ de $(h,_D\, dC,_{D/C}\, d'C,_{B/A}\, bA,_B\, g)$ et de $(h,_D\, \widetilde{d}C,_{D/C}\, \widetilde{d'}C,_{B/A}\, \widetilde{b}A,_B\, g)$ sont égales.

- L'application φ est un morphisme de (H,G)-bi-ensembles :
  Soit $(h,g) \in H \times G$, $k \in H$ et $l \in G$. Alors

$$\begin{aligned}
\varphi(k \star (h,g)L \star l) &= \varphi((kh, l^{-1}g)L) \\
&= (kh,_D\, C,_{D/C}\, C,_{B/A}\, A,_B\, g^{-1}l) \\
&= k \star (h,_D\, C,_{D/C}\, C,_{B/A}\, A,_B\, g^{-1}) \star l \\
&= k \star \varphi((h,g)L) \star l.
\end{aligned}$$

- L'application ψ est un morphisme de (H,G)-bi-ensembles :
  Soit $h \in H$, $d, d' \in D$, $b \in B$, $g \in G$, $k \in H$ et $l \in G$. Alors

$$\begin{aligned}
&\psi(k \star (h,_D dC,_{D/C} d'C,_{B/A} bA,_B g) \star l) \\
&= \psi((kh,_D dC,_{D/C} d'C,_{B/A} bA,_B gl)) \\
&= (khdd', l^{-1}g^{-1}b^{-1})L \\
&= k \star (hdd', g^{-1}b^{-1})L \star l \\
&= k \star \psi((h,_D dC,_{D/C} d'C,_{B/A} bA,_B g)) \star l.
\end{aligned}$$

- On a $\psi \circ \varphi = \mathrm{Id}_\Delta$:
  Soit $(h,g) \in H \times G$. Alors

$$\begin{aligned}
\psi \circ \varphi((h,g)L) &= \psi(h,_D C,_{D/C} C,_{B/A} A,_B g^{-1}) \\
&= (h,g)L.
\end{aligned}$$

- On a $\varphi \circ \psi = \mathrm{Id}_\Gamma$:
  Soit $h \in H$, $d, d' \in D$, $b \in B$ et $g \in G$. Alors

$$\begin{aligned}
\varphi \circ \psi((h,_D dC,_{D/C} d'C,_{B/A} bA,_B g)) &= \varphi((hdd', g^{-1}b^{-1})L) \\
&= (hdd',_D C,_{D/C} C,_{B/A} A,_B bg) \\
&= (h,_D dd'C,_{D/C} C,_{B/A} bA,_B g) \\
&= (h,_D dC,_{D/C} d'C,_{B/A} bA,_B g)
\end{aligned}$$

□

Théorème 3.25 *Soit G un groupe et (B,A), (D,C) deux sections de G. Alors il existe un isomorphisme de $(B/A, D/C)$-bi-ensemble*

$$\begin{aligned}
&\mathrm{Defres}^G_{B/A} \times_G \mathrm{Indinf}^G_{D/C} \\
&\cong \bigsqcup_{x \in [B\backslash G/D]} \mathrm{Indinf}^{B/A}_{p_{1,x}/k_{1,x}} \times_{p_{1,x}/k_{1,x}} \mathrm{Iso}(f_x) \times_{p_{2,x}/k_{2,x}} \mathrm{Defres}^{D/C}_{p_{2,x}/k_{2,x}},
\end{aligned}$$

où, pour tout $x \in [B\backslash G/D]$, f_x est l'isomorphisme canonique entre $p_{2,x}/k_{2,x}$ et $p_{1,x}/k_{1,x}$ et

$$p_{1,x} = A(B \cap {}^xD)/A, \qquad k_{1,x} = A(B \cap {}^xC)/A,$$

$$p_{2,x} = C(B^x \cap D)/C, \qquad k_{1,x} = C(A^x \cap D)/C.$$

Preuve: Par la proposition 3.17, on sait que $\mathrm{Defres}^G_{B/A} \times_G \mathrm{Indinf}^G_{D/C}$ est isomorphe à $A\backslash G/C$ comme $(B/A, D/C)$-bi-ensemble. Or $A\backslash G/C$ se décompose en une union disjointe de $(B/A, D/C)$-bi-ensembles transitifs comme suit :

$$A\backslash G/C = \bigsqcup_{x \in [B\backslash G/D]} A\backslash BxD/C.$$

On va maintenant fixer $x \in [B\backslash G/D]$ et étudier un peu $A\backslash BxD/C$. On commence par chercher le stabilisateur de AxC, que l'on va noter L.

$$\begin{aligned} L &= \{(bA, dC) \in B/A \times D/C \,\big|\, bA \star AxC = AxC \star dC\} \\ &= \{(bA, dC) \in B/A \times D/C \,\big|\, bA \star AxC \star d^{-1}C = AxC\} \\ &= \{(bA, dC) \in B/A \times D/C \,\big|\, Abxd^{-1}C = AxC\} \\ &= \{(bA, dC) \in B/A \times D/C \,\big|\, bxd^{-1} \in AxC\}. \end{aligned}$$

Alors, par la preuve du lemme 3.23, on sait que

$$L = L_{(p_1(L),k_1(L)),f_x,(p_2(L),k_2(L))},$$

où f_x est l'isomorphisme canonique entre $p_2(L)/k_2(L)$ et $p_1(L)/k_1(L)$. On a que

$$p_1(L) = \big\{bA \in B/A \,\big|\, \exists\, dC \in D/C \text{ tel que } bxd^{-1} \in AxC\big\}.$$

Ainsi, si $bA \in p_1(L)$, il existe $dC \in D/C$ tel que $bxd^{-1} \in AxC$. Donc il existe $a \in A$ et $c \in C$ tels que $bxd^{-1} = axc$ et donc $b = axcdx^{-1}$. Ainsi, comme $xcdx^{-1} = ba^{-1} \in B$, $b \in A(B \cap {}^xD)$ et donc $bA \in A(B \cap {}^xD)/A$. Réciproquement, si $bA \in A(B \cap {}^xD)/A$, alors $b \in B$ et il existe $a \in A$ et $d \in D$ tels que $b = axdx^{-1}$. Ainsi $bxd^{-1} = ax \in AxC$ et donc $bA \in p_1(L)$. Par conséquent, $p_1(L) = A(B \cap {}^xD)/A = p_{1,x}$. Par des calculs analogues, on obtient que

$$p_1(L) = A(B \cap {}^xD)/A = p_{1,x}, \qquad k_1(L) = A(B \cap {}^xC)/A = k_{1,x},$$

$$p_2(L) = C(B^x \cap D)/C = p_{2,x}, \qquad k_2(L) = C(A^x \cap D)/C = k_{2,x}.$$

On peut alors appliquer le lemme 3.10 et on a un isomorphisme de $(B/A, D/C)$-bi-ensembles

$$A\backslash BxD/C \cong (B/A \times D/C)/L.$$

Alors, par le lemme 3.24, on a un isomorphimse de $(B/A, D/C)$-bi-ensembles

$$(B/A \times D/C)/L \cong \mathrm{Indinf}^{B/A}_{p_{1,x}/k_{1,x}} \times_{p_{1,x}/k_{1,x}} \mathrm{Iso}(f_x) \times_{p_{2,x}/k_{2,x}} \mathrm{Defres}^{D/C}_{p_{2,x}/k_{2,x}}.$$

On peut maintenant remettre les résultats obtenus ensemble et on a alors un isomorphsime de $(B/A, D/C)$-bi-ensembles

$$\begin{aligned} &\mathrm{Defres}^G_{B/A} \times_G \mathrm{Indinf}^G_{D/C} \\ &\cong \bigsqcup_{x \in [B\backslash G/D]} \mathrm{Indinf}^{B/A}_{p_{1,x}/k_{1,x}} \times_{p_{1,x}/k_{1,x}} \mathrm{Iso}(f_x) \times_{p_{2,x}/k_{2,x}} \mathrm{Defres}^{D/C}_{p_{2,x}/k_{2,x}}, \end{aligned}$$

ce qui était le résultat à prouver. □

Remarque 3.26 L'article *Gluing torsion endo-permutation modules* de Serge Bouc et Jacques Thévenaz, [BT] donne une autre version de ce théorème.

3.4 Définition du groupe de Burnside

Définition 3.27 *Soit G et H des groupes finis. Le* ***groupe des bi-ensembles de Burnside*** *$B(H,G)$ est le groupe de Grothendieck de l'ensemble des classes d'isomorphisme de (H,G)-bi-ensembles finis (avec comme loi de composition l'union disjointe). Si U est un (H,G)-bi-ensemble fini, alors on note $[U]$ (ou même U) l'élément correspondant à U dans $B(H,G)$.*

Notation 3.28 *Soit G, H et K des groupes finis*

i) Il existe une unique application bilinéaire

$$\times_H : B(K,H) \times B(H,G) \to B(K,G)$$

tel que $[V] \times_H [U] = [V \times_H U]$, pour tout (H,G)-bi-ensemble fini U et pour tout (K,H)-bi-ensemble fini V.

ii) Il existe une unique application linéaire de $B(H,G)$ dans $B(G,H)$ qui envoie u sur u^{op} et qui est telle que $[U]^{\mathrm{op}} = [U^{\mathrm{op}}]$ pour tout (H,G)-bi-ensemble fini U.

Avec ces notations la proposition 3.18 induit la proposition suivante :

Proposition 3.29 *Soit G, H, K et L des groupes finis.*

i) Si $u \in B(H,G)$, $v \in B(K,H)$ et $w \in B(L,K)$ alors

$$w \times_K (v \times_H u) = (w \times_K v) \times_H u \text{ dans } B(L,G).$$

ii) Si $u \in B(H,G)$ et $v \in B(K,H)$, alors

$$(v \times_H u)^{\mathrm{op}} = u^{\mathrm{op}} \times_h v^{\mathrm{op}} \text{ dans } B(G,K).$$

iii) Si $u, u' \in B(H,G)$ et $v, v' \in B(K,H)$, alors

$$v \times_H (u + u') = (v \times_H u) + (v \times_H u')$$

$$(v + v') \times_H u = (v \times_H u) + (v' \times_H u).$$

iv) Si $u \in B(H,G)$, alors

$$[\mathrm{Id}_H] \times_H u = u = u \times_G [\mathrm{Id}_G].$$

Théorème 3.30 *Soit G un groupe fini. Alors le groupe $B(G,G)$ est un anneau si on le muni de la loi de multiplication définie par $\times_G$.*

Preuve: C'est une conséquence directe du fait que $B(G,G)$ est un groupe et de la proposition 3.29. □

3.5 Le groupe de Burnside et les KG-modules

On va maintenant revoir les définitions d'inflation, déflation, induction et restriction (ils sont définis dans les annexes : définitions B.32, B.33, B.24, B.22 et B.31) et voir le lien qu'il y a avec le groupe de Burnside et les conséquences que cela impliquent. Ce paragraphe se base sur *Biset functors for finite groups* de Serge Bouc, [Bou], pages 5-10.

Soit K un corps de caractéristique 0 et G un groupe fini.

- Si H est un sous-groupe de G et V un KG-module (de dimension finie), alors on a
$$\mathrm{Res}_H^G V \cong KG \otimes_{KG} V,$$
où KG est un (KH, KG)-bimodule pour la multiplication à gauche par les éléments de KH et la multiplication à droite par les éléments de KG.
- Si H est un sous-groupe de G et V un KH-module (de dimension finie), alors on a
$$\mathrm{Ind}_H^G V \cong KG \otimes_{KH} V,$$
où KG est un (KG, KH)-bimodule pour la multiplication à gauche par les éléments de KG et la multiplication à droite par les éléments de KH.
- Si $\varphi : G \to H$ est un isomorphisme de groupe et V un KG-module (de dimension finie), alors on a
$$\mathrm{Iso}(\varphi)V \cong KH \otimes_{KG} V,$$
où KH est un (KH, KG)-bimodule pour la multiplication à gauche par les éléments de KH et la multiplication à droite par l'image par φ des éléments de KG.
- Si N est un sous-groupe normal de G et V un $K(G/N)$-module (de dimension finie), alors on a
$$\mathrm{Inf}_{G/N}^G V \cong K(G/N) \otimes_{K(G/N)} V,$$
où $K(G/N)$ est un $(KG, K(G/N))$-bimodule pour la multiplication à gauche des projections des éléments de KG et la multiplication à droite par les éléments de $K(G/N)$.
- Soit N est un sous-groupe normal de G et si V et un KG-module (de dimension finie). Alors $\mathrm{Def}_{G/N}^G V = V^N$ et V^N est un KG-sous-module de V. Par le théorème de Maschke (théorème B.8) il existe un KG-sous-module W de V tel que $V = V^N \oplus W$. Ainsi $V^N \cong V/W$ est le plus grand quotient de V sur lequel N agit trivialement et
$$\mathrm{Def}_{G/N}^G V \cong K(G/N) \otimes_{KG} V,$$
où $K(G/N)$ est un $(K(G/N), KG)$-module pour la multiplication à gauche par les éléments de $K(G/N)$ et la multiplication à droite des projections des éléments de KG.

Ainsi chacune de ces opérations est de la forme $L \otimes_{KG} V$, où G, H sont des groupes, L un (KH, KG)-bimodule de dimension finie et V un KG-module (de dimension finie). De plus, le bimodule L est chaque fois un bimodule de permutation : il existe une base U de L qui est invariante sous l'action de G et H, c'est-à-dire $hUg = U$, pour tout $h \in H$, $g \in G$. Plus précisément, U est un (H, G)-bi-ensemble.

On va maintenant partir d'un (H, G)-bi-ensemble, où H et G sont des groupes finis, pour définir une application de $R_K(G)$ dans $R_K(H)$.

Définition 3.31 *Soit K un corps de caractéristique 0, G et H des groupes finis et U un (H, G)-bi-ensemble fini. Alors la structure de U induit une structure de (KH, KG)-bimodule à KU. On définit*

$$R_K(U) : R_K(G) \to R_K(H)$$

par

$$R_K(U)(V) = KU \otimes_{KG} V,$$

pour tout KG-module V (de dimension finie).

On peut vérifier que c'est bien défini, c'est-à-dire que $R_K(U)(V) \in R_K(H)$. On va maintenant introduire quelques propriétés de $R_K(-)$ qui seront utiles pour la suite.

Propriété 3.32 *Soit K un corps de caractéristique 0.*

i) Soit G et H des groupes finis et U_1, U_2 des (H, G)-bi-ensembles finis. Si U_1 et U_2 sont des (H, G)-bi-ensembles isomorphes, alors

$$R_K(U_1) = R_K(U_2).$$

ii) Soit G et H des groupes finis et U, U' des (H, G)-bi-ensembles finis, alors

$$R_K(U \sqcup U') = R_K(U) + R_K(U').$$

iii) Soit G, H et L des groupes finis, U un (H, G)-bi-ensemble fini et V un (L, H)-bi-ensemble fini. Alors

$$R_K(V \times_H U) = R_K(V) \circ R_K(U).$$

iv) Soit G un groupe fini, alors

$$R_K(\mathrm{Id}_G) = Id_{R_K(G)}.$$

Preuve:

i) C'est une conséquence directe du fait que KU et KU' sont isomorphes.

ii) Cela découle du fait que $K(U \sqcup U')$ et $KU \oplus KU'$ sont des (KH, KG)-bimodules isomorphes.

iii) Il suffit de vérifier que les (KL, KG)-bimodules $KV \otimes_{KH} KU$ et $K(V \times_H U)$ sont isomorphes.

iv) Si V est un KG-module (de dimension finie), alors

$$R_K(\mathrm{Id}_G)(V) = K\,\mathrm{Id}_G \otimes_{KG} V = KG \otimes_{KG} V = V.$$

Donc $R_K(\mathrm{Id}_G) = \mathrm{Id}_{R_K(G)}$.

□

Remarque 3.33 On peut remarquer que, si G est un groupe fini, H un sous-groupe et N un sous-groupe normal de G, on a que $R_K(\mathrm{Inf}_{G/N}^G) = \mathrm{Inf}_{G/N}^G$, $R_K(\mathrm{Def}_{G/N}^G) = \mathrm{Def}_{G/N}^G$, $R_K(\mathrm{Ind}_H^G) = \mathrm{Ind}_H^G$ et $R_K(\mathrm{Res}_H^G) = \mathrm{Res}_H^G$. Et si $\varphi : G \to L$ est un isomorphisme de groupes, alors on a $R_K(\mathrm{Iso}(\varphi)) = \mathrm{Iso}(\varphi)$. Ce résultat ainsi que les propriétés prouvées précédemment permettront de retrouver certaines relations entre ces opérations.

Proposition 3.34 *Soit G un groupe fini.*

i) Si L et H sont des sous-groupes de G avec $L \leq H \leq G$, alors on a des isomorphismes de (L, G)-bi-ensembles et de (G, L)-bi-ensembles respectivement

$$\mathrm{Res}_L^H \times_H \mathrm{Res}_H^G \cong \mathrm{Res}_L^G \quad et \quad \mathrm{Ind}_H^G \times_H \mathrm{Ind}_L^H \cong \mathrm{Ind}_L^G\,.$$

ii) Si $\varphi : G \to H$ et $\psi : H \to L$ sont des isomorphismes de groupes, alors on a un isomorphismes de (L, G)-bi-ensembles

$$\mathrm{Iso}(\psi) \times_H \mathrm{Iso}(\varphi) \cong \mathrm{Iso}(\psi \circ \varphi).$$

iii) Si N et M sont des sous-groupe normaux de G tels que $M \leq N$, alors on a des isomorphismes de $(G, G/M)$-bi-ensembles et respectivement de $(G/M, G)$-bi-ensembles

$$\mathrm{Inf}_{G/N}^G \times_{G/N} \mathrm{Inf}_{G/M}^{G/N} \cong \mathrm{Inf}_{G/M}^G \quad et \quad \mathrm{Def}_{G/M}^{G/N} \times_{G/N} \mathrm{Def}_{G/N}^G \cong \mathrm{Def}_{G/M}^G\,.$$

Preuve: Par exemple l'application $\alpha : \mathrm{Res}_L^H \times_H \mathrm{Res}_H^G \to \mathrm{Res}_L^G$ définie par $\alpha(h, {}_H\, g) = hg$ est un isomorphisme de (L, G)-bi-ensembles. □

Proposition 3.35: Transitivités
Soit K un corps de caractéristique 0 et G un groupe fini.

i) Si L et H sont des sous-groupes de G avec $L \leq H \leq G$, alors

$$\mathrm{Res}_L^H \circ \mathrm{Res}_H^G V = \mathrm{Res}_L^G V, \qquad \mathrm{Ind}_H^G \circ \mathrm{Ind}_L^H W = \mathrm{Ind}_L^G W$$

pour tout KG-module V (de dimension finie) et pour tout KL-module W (de dimension finie).

ii) Si $\varphi : G \to H$ et $\psi : H \to L$ sont des isomorphismes de groupes, alors

$$\mathrm{Iso}(\psi) \circ \mathrm{Iso}(\varphi)V = \mathrm{Iso}(\psi \circ \varphi)V$$

pour tout KG-module V (de dimension finie).

iii) Si N et M sont des sous-groupe normaux de G tels que $M \leq N$, alors

$$\mathrm{Inf}^G_{G/N} \circ \mathrm{Inf}^{G/N}_{G/M} V = \mathrm{Inf}^G_{G/M} V, \quad \mathrm{Def}^{G/N}_{G/M} \circ \mathrm{Def}^G_{G/N} W = \mathrm{Def}^G_{G/M} W$$

pour tout KG-module V (de dimension finie) et pour tout $K(G/M)$-module W (de dimension finie).

Preuve: Par la remarque 3.33 et les propriétés 3.32, il suffit de vérifier les relations pour les bi-ensembles correspondants, ce qui est l'objet de la proposition 3.34. □

Théorème 3.36 *Soit K un corps de caractéristique 0, G un groupe fini et (B, A), (D, C) deux sections de G. Soit V un $K(D/C)$-module (de dimension finie). Alors*

$$\mathrm{Defres}^G_{B/A} \circ \mathrm{Indinf}^G_{D/C} V \cong \bigoplus_{x \in [B\backslash G/D]} \mathrm{Indinf}^{B/A}_{p_{1,x}/k_{1,x}} \mathrm{Iso}(f_x) \, \mathrm{Defres}^{D/C}_{p_{2,x}/k_{2,x}} V,$$

où, pour tout $x \in [B\backslash G/D]$, f_x est l'isomorphisme canonique entre $p_{2,x}/k_{2,x}$ et $p_{1,x}/k_{1,x}$, et

$$p_{1,x} = A(B \cap {}^xD)/A, \qquad k_{1,x} = A(B \cap {}^xC)/A,$$

$$p_{2,x} = C(B^x \cap D)/C, \qquad k_{1,x} = C(A^x \cap D)/C.$$

Preuve: C'est une conséquence de la remarque 3.33, des propriétés 3.32 et du théorème 3.25. □

Théorème 3.37: La formule de Mackey
Soit K un corps de caractéristique 0, G un groupe fini et H, L des sous-groupes de G. Alors si V est un KL-module (de dimension finie),

$$\mathrm{Res}^G_H \circ \mathrm{Ind}^G_L V = \bigoplus_{x \in [H\backslash G/L]} \mathrm{Ind}^H_{H \cap {}^xL} \circ \mathrm{Iso}(\gamma_x) \circ \mathrm{Res}^K_{H^x \cap K} V,$$

où $[H\backslash G/L]$ est un ensemble de représentants des (H, K)-orbites de G et, pour tout $x \in [H\backslash G/L]$, $\gamma_x : H^x \cap K \to H \cap {}^xK$ est l'isomorphisme de groupes induit par la conjugaison par x.

Preuve: Il suffit d'appliquer le théorème 3.36 avec $A = C = \mathbf{1}$, $B = H$ et $D = L$. Le seul point un peu difficile est de voir que les f_x correspondent aux γ_x. □

3.6 Sections d'un groupe

Définition 3.38 *Soit G un groupe et soit (B, A) et (D, C) deux sections de G. Alors les sections (B, A) et (D, C) sont* ***liées*** *si*

$$B \cap C = D \cap A, \quad (B \cap D)A = B \quad et \quad (B \cap D)C = D.$$

On note alors (B, A) — (D, C) .

Les sections (B, A) et (D, C) sont ***liées modulo*** *G s'il existe $g \in G$ tel que (B, A) — $({}^gD, {}^gC)$. On note alors (B, A) —$_G$ (D, C).*

Remarque 3.39 On peut remarquer que la relation "être lié" ou "être lié modulo G" sont des relations réflexives et symétriques.

Proposition 3.40 *Soit G un groupe et soit (B, A) et (D, C) deux sections liées. Alors B/A et D/C sont isomorphes.*

Preuve: Par hypothèse, on sait que

$$B \cap C = D \cap A, \quad (B \cap D)A = B \quad \text{et} \quad (B \cap D)C = D.$$

Soit $b \in B$. Comme $B = (B \cap D)A$, il existe $d \in B \cap D$ et $a \in A$ tels que $b = da$. On pose $f(b) = dC$. Cela définit une application $f : B \to D/C$.

- L'application f est bien définie :
  Soit $b \in B$, $d, \widetilde{d} \in B \cap D$ et $a, \widetilde{a} \in A$ tels que $b = da = \widetilde{d}\widetilde{a}$. Alors

  $$\widetilde{d}^{-1}d = \widetilde{a}a^{-1} \in D \cap A = B \cap C \subset C.$$

  Donc $dC = \widetilde{d}C$ et donc $f(b)$ est bien défini car il ne dépend pas du choix de d et a.

- L'application f est un homomorphisme :
  Soit b et $\widetilde{b} \in B$. Il existe $d, \widetilde{d} \in B \cap D$ et $a, \widetilde{a} \in A$ tels que $b = da$ et $\widetilde{b} = \widetilde{d}\widetilde{a}$. On pose $a' = \widetilde{d}^{-1}a\widetilde{d}$. Alors a' appartient à A car $\widetilde{d} \in B$ et $A \trianglelefteq B$.

  $$b\widetilde{b} = da\widetilde{d}\widetilde{a} = d\widetilde{d}(\widetilde{d}^{-1}a\widetilde{d})\widetilde{a} = \underbrace{d\widetilde{d}}_{\in B\cap D}\ \underbrace{a'\widetilde{a}}_{\in A}.$$

  Par conséquent, on a

  $$f(b\widetilde{b}) = d\widetilde{d}C = dC\widetilde{d}C = f(b)f(\widetilde{b}).$$

- Le noyau $\operatorname{Ker} f$ est égal à A :
  Soit $b \in \operatorname{Ker} f$. Soit $d \in B \cap D$ et $a \in A$ tels que $b = da$. Alors $C = f(b) = dC$. Donc $d \in C \cap D \cap B = C \cap B = D \cap A \subset A$. Ainsi $b = da \in A$.
  Soit $a \in A$. Alors $a = 1_G a$, où $1_G \in B \cap D$. Donc $f(a) = 1_G C = C$, c'est-à-dire $a \in \operatorname{Ker} f$.

- L'homomorphisme f est surjectif :
  Soit $d \in D$. Comme $D = (B \cap D)C$, il existe $b \in B \cap D$ et $c \in C$ tels que $d = bc$. Alors $b = dc^{-1} \in D \cap B$ et donc $f(b) = bC = dc^{-1}C = dC$.

On a ainsi montré que f est un homomorphisme de groupes surjectif de noyau A. Donc, par le premier théorème d'isomorphisme, f induit un isomorphisme entre B/A et D/C. □

3.7 Sous-groupes expansifs et faiblement expansifs

Notation 3.41 *Soit G un groupe et H, K des sous-groupes de G. On note $H \overset{G}{\uparrow} K$ le sous-groupe de $N_G(K)$ défini par :*

$$H \overset{G}{\uparrow} K = \bigcap_{g \in N_G(K)} \big(H^g \cap N_G(K)\big)K.$$

Remarques 3.42 Soit G un groupe et H, K des sous-groupes de G.

i) Le sous-groupe $H \overset{G}{\uparrow} K$ est un sous-groupe normal de $N_G(K)$:
Soit $t \in N_G(K)$. Alors

$$\begin{aligned}
t(H \overset{G}{\uparrow} K)t^{-1} &= t\Big(\bigcap_{g \in N_G(K)} \big(H^g \cap N_G(K)\big)K\Big)t^{-1} \\
&= \bigcap_{g \in N_G(K)} t\Big(\big(H^g \cap N_G(K)\big)K\Big)t^{-1} \\
&= \bigcap_{g \in N_G(K)} t\big(H^g \cap N_G(K)\big)t^{-1}\underbrace{tKt^{-1}}_{=K} \\
&= \bigcap_{g \in N_G(K)} \big(tH^gt^{-1} \cap \underbrace{tN_G(K)t^{-1}}_{=N_G(K)}\big)K \\
&= \bigcap_{g \in N_G(K)} \big(H^{gt^{-1}} \cap N_G(K)\big)K \\
&= \bigcap_{g \in N_G(K)} \big(H^g \cap N_G(K)\big)K \\
&= H \overset{G}{\uparrow} K
\end{aligned}$$

Donc $t(H \overset{G}{\uparrow} K)t^{-1} = H \overset{G}{\uparrow} K$ et donc $H \overset{G}{\uparrow} K$ est normal dans $N_G(K)$.

ii) Soit $g \in N_G(K)$. Alors on a

$$\big(H^g \cap N_G(K)\big)K = H^gK \cap N_G(K) = \big\{t \in N_G(K) \,\big|\, HgKt = HgK\big\}.$$

On va prouver la seconde égalité :

$\subset$: Soit $x \in H^g K \cap N_G(K)$. Alors $x \in N_G(K)$ et il existe $h \in H, k \in K$ tels que $x = g^{-1}hgk$. Alors

$$\begin{aligned} HgKx &= Hgx\underbrace{x^{-1}Kx}_{=K} \\ &= HgxK \\ &= Hgg^{-1}hgkK \\ &= \underbrace{Hh}_{=H} g \underbrace{kK}_{=K} \\ &= HgK \end{aligned}$$

Donc $x \in \left\{ t \in N_G(K) \,\middle|\, HgKt = HgK \right\}$.

$\supset$: Soit $x \in \left\{ t \in N_G(K) \,\middle|\, HgKt = HgK \right\}$. Alors

$$g \in HgK = HgKx = Hgx\underbrace{x^{-1}Kx}_{=K} = HgxK,$$

donc il existe $h \in H$ et $k \in K$ tels que $g = hgxk$. D'où $x = g^{-1}h^{-1}gk^{-1} \in g^{-1}HgK = H^g K$ et donc $x \in H^g K \cap N_G(K)$.

En conclusion, $H \overset{G}{\uparrow} K$ est l'ensemble des éléments de $N_G(K)$ qui stabilisent pour la multiplication à droite les doubles classes HgK, pour tout $g \in N_G(K)$. Plus généralement, si $x \in G$, alors $H^x \overset{G}{\uparrow} K$ est l'ensemble des éléments de $N_G(K)$ qui stabilisent pour la multiplication à droite les doubles classes $HxgK$, pour tout $g \in N_G(K)$.

Définition 3.43 *Soit G un groupe.*

*i) Un sous-groupe H est **faiblement expansif** si $\forall\ x \in G$, les égalités*

$$H^x \overset{G}{\uparrow} H = H = {}^x H \overset{G}{\uparrow} H$$

impliquent que $x \in N_G(H)$.

*ii) Un sous-groupe H est **expansif** si $\forall\ x \in G$, l'égalité*

$$H^x \overset{G}{\uparrow} H = H$$

implique que $x \in N_G(H)$.

iii) Si K et H sont des sous-groupes de G, on écrit $H \eqslantless_G K$ s'il existe $x \in G$ tel que

$${}^x H \overset{G}{\uparrow} K = K \text{ et } K^x \overset{G}{\uparrow} H = H$$

et $H \not\eqslantless_G K$ sinon.

Proposition 3.44 *Soit G un groupe et N un sous-groupe normal de G. Alors N est expansif.*

Preuve: Si N est normal dans G, on a $N_G(N) = G$ donc si $g \in G$, on a $g \in N_G(N)$. Ainsi il est clair que N est expansif. □

Proposition 3.45 *Soit G un groupe et H, K des sous-groupes normaux de G. Alors $H \eqsim_G K$ si et seulement si $H = K$.*

Preuve:

$\Rightarrow$: Etant donné que $H \eqsim_G K$, il existe $x \in G$ tel que ${}^xH \overset{G}{\uparrow} K = K$ et $K^x \overset{G}{\uparrow} H = H$. Alors

$$K = {}^xH \overset{G}{\uparrow} K = H \overset{G}{\uparrow} K = \bigcap_{g \in G} (\underbrace{H^g}_{=H} \cap G)K = HK,$$

donc $H \subset K$. De même

$$H = K^x \overset{G}{\uparrow} H = K \overset{G}{\uparrow} H = \bigcap_{g \in G} (\underbrace{K^g}_{=K} \cap G)H = KH,$$

donc $K \subset H$. Donc on a $H = K$.

$\Leftarrow$: Si $H = K$, alors

$$H \overset{G}{\uparrow} H = \bigcap_{g \in G} (\underbrace{H^g}_{=H} \cap H)H = H,$$

donc $H \eqsim_G H$.

□

3.8 Quelques idempotents

Notation 3.46 *Soit G un groupe fini et N un sous-groupe normal de G. On note j_N^G l'élément de $B(G,G)$ défini par*

$$j_N^G = \mathrm{Inf}_{G/N}^G \times_{G/N} \mathrm{Def}_{G/N}^G .$$

Remarque 3.47 Vu l'exemple 3.13 et la proposition 3.29 2., $(j_N^G)^{\mathrm{op}} = j_N^G$ dans $B(G,G)$.

Lemme 3.48 *Soit G un groupe fini et N, M des sous-groupes normaux de G.*

i) Il existe un isomorphisme de $(G/N, G/M)$-bi-ensembles

$$\mathrm{Def}_{G/N}^G \times_G \mathrm{Inf}_{G/M}^G = \mathrm{Inf}_{G/MN}^{G/N} \times_{G/MN} \mathrm{Def}_{G/MN}^{G/M} .$$

ii) Ainsi $j_N^G \times_G j_M^G = j_{MN}^G$ et en particulier j_N^G est un idempotent de $B(G,G)$.

Preuve:

i) Il suffit de trouver un isomorphisme de $(G/N, G/M)$-bi-ensembles entre $G/N \times_G G/M$ et G/NM. On définit l'application

$$\alpha : G/N \times_G G/M \to G/NM$$

par $\alpha(gN,_G hM) = ghNM$. Il faut montrer que c'est une application bien définie, bijective et que c'est un homomorphisme de bi-ensembles.

- L'application α est bien définie :
  Soit $g, h, k, l \in G$ tels que $(gN,_G hM) = (kN,_G lM)$. On doit montrer que $ghNM = klNM$. Il existe $i \in G$ tel que $(gN, hM) = (kiN, i^{-1}lM)$, donc il existe $n \in N$ et $m \in M$ tels que $g = kin$ et $h = i^{-1}lm$. Alors

$$ghNM = kini^{-1}lmNM = kl\underbrace{(i^{-1}l)^{-1}ni^{-1}l}_{\in N}mNM = klNM.$$

- L'application α est un homomorphisme de bi-ensembles :
  Soit $(gN,_G hM) \in G/N \times_G G/M$ et $k, l \in G$. Alors

$$\begin{aligned}\alpha(kN \star (gN,_G hM) \star lM) &= \alpha(kgN,_G hlM)\\ &= kghlNM\\ &= kN \star ghNM \star lM\\ &= kN \star \alpha(gN,_G hM) \star lM.\end{aligned}$$

- L'application α est injective :
  Soit $(gN,_G hM), (kN,_G lM) \in G/N \times_G G/M$ avec $\alpha(gN,_G hM) = \alpha(kN,_G lM)$, c'est-à-dire tels que $ghNM = klNM$. Alors il existe $n \in N$ et $m \in M$ tels que $gh = klnm$ et donc $hm^{-1}l^{-1} = g^{-1}klnl^{-1}$. On pose $\widetilde{n} = lnl^{-1} \in N$ et $i = \widetilde{n}^{-1}k^{-1}g$. Alors $i^{-1} = g^{-1}k\widetilde{n} = hm^{-1}l^{-1}$ et

$$\begin{aligned}(kiN, ilM) &= (k\widetilde{n}^1k^{-1}gN, hm^{-1}l^{-1}lM)\\ &= (g\underbrace{g^{-1}k\widetilde{n}^1k^{-1}g}_{\in N}N, hM)\\ &= (gN, hM)\end{aligned}$$

  et donc $(gN,_G hM) = (kN,_G lM)$.
- L'application α est surjective :
  Soit $g \in G$. Alors $\alpha(gN,_G 1_G M) = gNM$, donc α est surjective.

ii) Il suffit de voir que, si on utilise le résultat du point *i)*,

$$\begin{aligned}j_N^G \times_G j_M^G &= \mathrm{Inf}_{G/N}^G \times_{G/N} \mathrm{Def}_{G/N}^G \times_G \mathrm{Inf}_{G/M}^G \times_{G/M} \mathrm{Def}_{G/M}^G\\ &= \mathrm{Inf}_{G/N}^G \times_{G/N} \mathrm{Inf}_{G/MN}^{G/N} \times_{G/MN} \mathrm{Def}_{G/MN}^{G/M} \times_{G/M} \mathrm{Def}_{G/M}^G\\ &\overset{(1)}{=} \mathrm{Inf}_{G/MN}^G \times_{G/MN} \mathrm{Def}_{G/MN}^G\\ &= j_{MN}^G\end{aligned}$$

où l'égalité (1) découle de la transitivité de l'inflation et de la déflation (remarque 3.34 *iii)*). □

Remarque 3.49 Le point *i)* du lemme précédent est un cas très particulier du théorème 3.25 (où $B = D = G$, $A = N$ et $C = M$).

Définition 3.50 *Soit G un groupe fini. Si N est un sous-groupe normal de G, soit f_N^G l'élément de $B(G,G)$ défini par*

$$f_N^G = \sum_{N \leq M \trianglelefteq G} \mu(N,M) j_M^G,$$

où μ est la fonction de Möbius de l'ensemble partiellement ordonné des sous-groupes normaux de G.

Remarque 3.51 Vu la remarque 3.47 et le fait que prendre l'opposé est une application linéaire dans $B(G,G)$, on a que $(f_N^G)^{\mathrm{op}} = f_N^G$.

Lemme 3.52 *Soit G un groupe fini et N est un sous-groupe normal de G. Alors*

$$j_N^G = \sum_{N \leq M \trianglelefteq G} f_M^G.$$

Preuve: C'est une conséquence directe du théorème 1.11, où P est l'ensemble des sous-groupes normaux de G, $f : P \to B(G,G)$ est défini par $f(M) = f_M^G$ et $g : P \to B(G,G)$ est défini par $g(M) = j_M^G$. □

Proposition 3.53 *Soit G un groupe fini et M, N des sous-groupes normaux de G. Alors*

i)

$$\mathrm{Def}_{G/M}^G \times_G f_N^G = \begin{cases} f_{N/M}^{G/M} \times_{G/M} \mathrm{Def}_{G/M}^G & si\ M \leq N \\ 0 & si\ M \not\leq N. \end{cases}$$

ii)

$$f_N^G \times_G \mathrm{Inf}_{G/M}^G = \begin{cases} \mathrm{Inf}_{G/M}^G \times_{G/M} f_{N/M}^{G/M} & si\ M \leq N \\ 0 & si\ M \not\leq N. \end{cases}$$

Preuve:

i) On a, en appliquant le point *i)* du lemme 3.48 et la transitivité de la

déflation (proposition 3.34 *iii)*),

$$\begin{aligned}
\mathrm{Def}^G_{G/M} \times_G f^G_N &= \mathrm{Def}^G_{G/M} \times_G \sum_{N \leq L \trianglelefteq G} \mu(N,L) j^G_L \\
&= \mathrm{Def}^G_{G/M} \times_G \sum_{N \leq L \trianglelefteq G} \mu(N,L) \, \mathrm{Inf}^G_{G/L} \times_{G/L} \mathrm{Def}^G_{G/L} \\
&= \sum_{N \leq L \trianglelefteq G} \mu(N,L) \, \mathrm{Inf}^{G/M}_{G/ML} \times_{G/ML} \mathrm{Def}^{G/L}_{G/ML} \times_{G/L} \mathrm{Def}^G_{G/L} \\
&= \sum_{N \leq L \trianglelefteq G} \mu(N,L) \, \mathrm{Inf}^{G/M}_{G/ML} \times_{G/ML} \mathrm{Def}^G_{G/ML} \\
&= \sum_{NM \leq P \trianglelefteq G} \Big(\sum_{\substack{N \leq L \trianglelefteq G \\ ML = P}} \mu(N,L) \Big) \, \mathrm{Inf}^{G/M}_{G/P} \times_{G/P} \mathrm{Def}^G_{G/P} \, .
\end{aligned}$$

On pose $s_P = \sum_{\substack{N \leq L \trianglelefteq G \\ ML = P}} \mu(N,L)$, pour tout $NM \leq P \trianglelefteq G$. On va montrer que $s_P = 0$ sauf si $N = MN$. On suppose donc que $NM \neq N$. Soit E l'ensemble des sous-groupes normaux de G muni du préordre $N \leq M$ si et seulement si N est un sous-groupe de M. Alors μ est la fonction de Möbius de E. Elle est définie comme l'inverse de la fonction $\zeta : \mathrm{int}(E) \to \mathbb{Z}$ définie par $\zeta(N,M) = 1$ pour tout $N, M \in E$ tels que $N \leq M$. Alors on a $\mu \cdot \zeta = \delta$ dans l'algèbre d'incidence $I(P, \mathbb{Z})$. Donc en particulier,

$$\begin{aligned}
0 &= \delta(N, NM) \\
&= (\mu \cdot \zeta)(N, NM) \\
&= \sum_{\substack{N \leq Q \leq NM \\ Q \trianglelefteq G}} \mu(N,Q) \zeta(Q, NM) \\
&= \sum_{\substack{N \leq Q \leq NM \\ Q \trianglelefteq G}} \mu(N,Q) \\
&= s_{NM}.
\end{aligned}$$

Ainsi on a montré que $s_{NM} = 0$. On remarque maintenant que si $NM \leq Q \trianglelefteq G$, alors on a

$$\sum_{\substack{P \trianglelefteq G \\ NM \leq P \leq Q}} s_P = \sum_{\substack{L \trianglelefteq G \\ N \leq L \leq Q}} \mu(N,L) = (\mu \cdot \zeta)(N,Q) = \delta(N,Q) = 0.$$

Mais alors, par induction, cela montre que $s_P = 0$, pour tout $NM \leq P \trianglelefteq G$. Par conséquent, $\mathrm{Def}^G_{G/M} \times_G f^G_N = 0$ sauf si $NM = N$, c'est-à-dire sauf si $M \leq N$. On peut donc maintenant supposer que

$M \leq N$. Alors $s_P = \mu(N,P)$ pour tout $NM \leq P \trianglelefteq G$ et donc

$$\begin{aligned}
\mathrm{Def}^G_{G/M} \times_G f^G_N &= \\
&= \sum_{NM \leq P \trianglelefteq G} s_P \,\mathrm{Inf}^{G/M}_{G/P} \times_{G/P} \mathrm{Def}^G_{G/P} \\
&= \sum_{N \leq P \trianglelefteq G} \mu(N,P)\,\mathrm{Inf}^{G/M}_{G/P} \times_{G/P} \mathrm{Def}^G_{G/P} \\
&= \sum_{N \leq P \trianglelefteq G} \mu(N,P)\,\mathrm{Inf}^{G/M}_{G/P} \times_{G/P} \mathrm{Def}^{G/M}_{G/P} \times_{G/M} \mathrm{Def}^G_{G/M} \\
&\overset{(1)}{=} \Big(\sum_{N/M \leq P/M \trianglelefteq G/M} \mu(N/M, P/M)\,\mathrm{Inf}^{G/M}_{G/P} \times_{G/P} \mathrm{Def}^{G/M}_{G/P} \Big) \\
&\quad \times_{G/M} \mathrm{Def}^G_{G/M} \\
&= f^{G/M}_{N/M} \times_{G/M} \mathrm{Def}^G_{G/M}
\end{aligned}$$

où l'égalité (1) découle du fait que $\mu(N,P) = \mu(N/M, P/M)$, pour tout $N/M \leq P/M \trianglelefteq G/M$ (Il suffit de regarder la définition de μ et d'utiliser la bijection entre les sous-groupes normaux de G contenant M et les sous-groupes normaux de G/M).

ii) Il suffit de considérer les bi-ensembles opposés dans l'assertion *i)* et d'utiliser la proposition 3.29 *ii)* et la remarque 3.51.

□

Proposition 3.54 *Soit G un groupe fini. Les éléments f^G_N pour $N \trianglelefteq G$ sont des idempotents orthogonaux de $B(G;G)$ et*

$$\sum_{N \trianglelefteq G} f^G_N = Id_G.$$

Preuve: Soit N et M des sous-groupes normaux de G. Alors on a

$$f^G_M \times_G f^G_N = \sum_{M \leq L \trianglelefteq G} \mu(M,L)\,\mathrm{Inf}^G_{G/L} \times_{G/L} \mathrm{Def}^G_{G/L} \times_G f^G_N.$$

Si, pour un certain $M \leq L \trianglelefteq G$, le produit $\mathrm{Def}^G_{G/L} \times_G f^G_N$ est non-nul, alors $L \leq N$ (on applique simplement la proposition 3.53 *i)*) et donc aussi $M \leq N$. Ainsi si $M \not\leq N$, on a $f^G_M \times_G f^G_N = 0$. Mais $f^G_M \times_G f^G_N = (f^G_N \times_G f^G_M)^{\mathrm{op}}$ et donc (en inversant les rôles de M et N) $f^G_M \times_G f^G_N$ est nul si $N \not\leq M$. Ainsi si on met les deux résultats ensembles on obtient que $f^G_M \times_G f^G_N = 0$ si $M \neq N$. De plus

$$\begin{aligned}
\sum_{N \trianglelefteq G} f^G_N &= \sum_{N \trianglelefteq G} \sum_{N \leq M \lhd G} \mu(N,M) j^G_M \\
&= \sum_{M \trianglelefteq G} \Big(\sum_{\substack{N \trianglelefteq G \\ \mathbf{1} \leq N \leq M}} \mu(N,M) \Big) j^G_M
\end{aligned}$$

Or, si on reprend les notations introduites à la preuve du lemme précédent,

$$\sum_{\substack{N\trianglelefteq G\\ \mathbf{1}\leq N\leq M}} \mu(N,M) = (\mu\cdot\zeta)(\mathbf{1},M) = \delta(\mathbf{1},M)$$

et donc la somme $\displaystyle\sum_{\substack{N\trianglelefteq G\\ \mathbf{1}\leq N\leq M}} \mu(N,M)$ est égale à 0, sauf si $M=\mathbf{1}$. Ainsi

$$\sum_{N\trianglelefteq G} f_N^G = j_{\mathbf{1}}^G = \mathrm{Inf}_{G/\mathbf{1}}^G \times_{G/\mathbf{1}} \mathrm{Def}_{G/\mathbf{1}}^G = \mathrm{Id}_G\,.$$

Par conséquent, pour tout $M\trianglelefteq G$,

$$f_M^G = f_M^G \times_G \Big(\sum_{N\trianglelefteq G} f_N^G\Big) = (f_M^G)^2.$$

Ainsi on a montré que les éléments f_M^G, pour $M\trianglelefteq G$, sont des idempotents orthogonaux, dont la somme vaut Id_G. □

Notation 3.55 *Soit G un groupe fini et H un sous-groupe de G. On définit les éléments $\mathcal{I}_H$ et $\mathcal{D}_H$ de $B(G,N_G(H)/H)$ et respectivement de $B(N_G(H)/H,G)$ par*

$$\mathcal{I}_H = \mathrm{Indinf}_{N_G(H)/H}^G \times_{N_G(H)/H} f_{\mathbf{1}}^{N_G(H)/H} \text{ et}$$

$$\mathcal{D}_H = \mathcal{I}_H^{op} = f_{\mathbf{1}}^{N_G(H)/H} \times_{N_G(H)/H} \mathrm{Defres}_{N_G(H)/H}^G\,.$$

Proposition 3.56 *Soit G un groupe fini.*

i) Soit H et K des sous-groupes de G tels que $H \not=_G K$. Alors

$$\mathcal{D}_K \times_G \mathcal{I}_H = 0.$$

ii) Soit H un sous-groupe faiblement expansif de G. Alors

$$\mathcal{D}_H \times_G \mathcal{I}_H = f_{\boldsymbol{1}}^{N_G(H)}.$$

iii) Soit H un sous-groupe expansif de G. Alors

$$\mathrm{Defres}_{N_G(H)/H}^G \times_G \mathcal{I}_H = f_{\boldsymbol{1}}^{N_G(H)}.$$

Preuve: Soit H et K des sous-groupes quelconques de G et on pose $S=N_G(H)$, $T=N_G(K)$. Alors par la proposition 3.17

$$\mathcal{D}_K \times_G \mathcal{I}_H = f_1^{T/K} \times_{T/K} (K\backslash G/H) \times_{S/H} f_{\mathbf{1}}^{S/H} \in B(T/K, S/H).$$

Mais alors, comme

$$G = \bigsqcup_{x\in[T\backslash G/S]} TxS = \bigsqcup_{x\in[T\backslash G/S]} \bigsqcup_{y\in[K\backslash TxS/H]} KyH$$

le $(T/K, S/H)$-bi-ensemble $K\backslash G/H$ est isomorphe à

$$K\backslash G/H \cong \bigsqcup_{x\in[T\backslash G/S]} K\backslash TxS/H.$$

Soit $x \in G$. On pose $N_x = K^x \overset{G}{\uparrow} H$. Alors, par la remarque 3.42 *ii)*, N_x/H agit trivialement à droite sur $K\backslash TxS/H$ (car si $s \in S$ et $t \in T$, alors $KtxsH = tKxsH$). Par conséquent, on a un isomorphisme de $(T/K, S/H)$-bi-ensembles

$$K\backslash TxS/H \cong (K\backslash TxS/H) \times_{S/H} \mathrm{Inf}^{S/H}_{S/N_x} \times_{S/N_x} \mathrm{Def}^{S/H}_{S/N_x}.$$

Plus précisément, si on définit

$$\varphi : K\backslash TxS/H \longrightarrow (K\backslash TxS/H) \times_{S/H} \mathrm{Inf}^{S/H}_{S/N_x} \times_{S/N_x} \mathrm{Def}^{S/H}_{S/N_x}$$

par $\varphi(KgH) = (KgH, {}_{S/H}N_x, {}_{S/N_x}N_x)$ pour tout $g \in TxS$, alors φ est un isomorphisme de $(T/K, S/H)$-biensemble. Le fait que N_x/H agit trivialement à droite sur $K\backslash TxS/H$ est utile pour montrer l'injectivité de φ.

Mais, par la proposition 3.53, $\mathrm{Def}^{S/H}_{S/N_x} \times_{S/H} f^{S/H}_{\mathbf{1}} = 0$ si $N_x/H \neq \mathbf{1}$. Cela implique que $(K\backslash TxS/H) \times_{S/H} f^{S/H}_{\mathbf{1}} = 0$ si $K^x \overset{G}{\uparrow} H \neq H$. Un argument analogue permet d'obtenir que $f^{T/K}_{\mathbf{1}} \times_{T/K} (K\backslash TxS/H) = 0$ si ${}^xH \overset{G}{\uparrow} K \neq K$. Ainsi

$$f^{T/K}_{\mathbf{1}} \times_{T/K} (K\backslash TxS/H) \times_{S/H} f^{S/H}_{\mathbf{1}} = 0,$$

sauf si ${}^xH \overset{G}{\uparrow} K = K$ et $K^x \overset{G}{\uparrow} H = H$.

i) On suppose que $H \not=_G K$. Donc en particulier, il n'existe pas de $x \in G$ tels que ${}^xH \overset{G}{\uparrow} K = K$ et $K^x \overset{G}{\uparrow} H = H$. Ainsi, par le raisonnement précédent, on obtient que

$$\mathcal{D}_K \times_G \mathcal{I}_H = 0.$$

ii) On suppose que $H = K$ et que H est un sous-groupe faiblement expansif de G. Alors, par le raisonnement fait précédemment,

$$f^{S/H}_{\mathbf{1}} \times_{S/H} (H\backslash SxS/H) \times_{S/H} f^{S/H}_{\mathbf{1}} = 0,$$

sauf si ${}^xH \overset{G}{\uparrow} H = H$ et $H^x \overset{G}{\uparrow} H = H$. Cela implique que $x \in N_G(H) = S$ et donc

$$\begin{aligned}\mathcal{D}_H \times_G \mathcal{I}_H &= f^{S/H}_{\mathbf{1}} \times_{S/H} (H\backslash S/H) \times_{S/H} f^{S/H}_{\mathbf{1}} = \\ &= f^{S/H}_{\mathbf{1}} \times_{S/H} S/H \times_{S/H} f^{S/H}_{\mathbf{1}} = \\ &= f^{S/H}_{\mathbf{1}} \times_{S/H} f^{S/H}_{\mathbf{1}} = \\ &= f^{S/H}_{\mathbf{1}}\end{aligned}$$

car $H\backslash S/H = S/H$ est le $(S/H, S/H)$-bi-ensemble identité et $f^{S/H}_{\mathbf{1}}$ est un idempotent (lemme 3.54).

iii) Par un raisonnement similaire, si H est un sous-groupe expansif, alors

$$(H\backslash S/H) \times_{S/H} f_{\mathbf{1}}^{S/H} = 0$$

sauf si $x \in N_G(H) = S$. Alors

$$\begin{aligned} \mathrm{Defres}^G_{N_G(H)/H} \times_G \mathcal{I}_H &= (H\backslash S/H) \times_{S/H} f_{\mathbf{1}}^{S/H} \\ &= S/H \times_{S/H} f_{\mathbf{1}}^{S/H} \\ &= f_{\mathbf{1}}^{N_G(H)} \end{aligned}$$

car $H\backslash S/H = S/H$ est le $(S/H, S/H)$-bi-ensemble identité.

□

Jusqu'à ici, on n'a considéré que des bi-ensembles, mais comme déjà vu précédemment, les bi-ensembles induisent des applications sur des groupes de Grothendieck des classes d'isomorphismes de KG-modules. Soit K un corps de caractéristique 0, G un groupe fini et N un sous-groupe normal. On pose $j_N^G = R_K(j_N^G)$ et $f_N^G = R_K(f_N^G)$. Ainsi les résultats précédents restent valables (si on remplace le produit $\times$ par la composition $\circ$) et par la suite, on fera appelle à ces résultats bien qu'il soit seulement énoncés pour les éléments de $B(G, G)$.

Proposition 3.57 *Soit K un corps de caractéristique 0, G un groupe fini et V un KG-module (de dimension finie) irréductible et fidèle. Alors, si N est un sous-groupe normal de G,*

$$f_N^G V = \begin{cases} V & \text{si } N = \mathbf{1} \\ \{0\} & \text{sinon.} \end{cases}$$

Preuve: Soit $N \leq M \trianglelefteq G$. Alors, si $M \neq \mathbf{1}$, alors $\mathrm{Def}^G_{G/M} V = V^M = \{0\}$ car comme V est irréductible, V^M est égal à $\{0\}$ ou V et comme V est fidèle, $V^M \neq V$. Ainsi, on a

$$\begin{aligned} f_N^G V &= \sum_{N \leq M \trianglelefteq G} \mu(N, M) j_M^G V \\ &= \sum_{N \leq M \trianglelefteq G} \mu(N, M) \, \mathrm{Inf}^G_{G/M} \circ \mathrm{Def}^G_{G/M} V \\ &= \underbrace{\mu(N, N)}_{=1} \mathrm{Inf}^G_{G/N} \circ \mathrm{Def}^G_{G/N} V \\ &= \begin{cases} V & \text{si } N = \mathbf{1} \\ \{0\} & \text{sinon.} \end{cases} \end{aligned}$$

□

Chapitre 4

Les groupes de p-rang normal 1

Pour la suite, p est un nombre premier.

On va commencer par la définition de quatre types de groupes. On va, par la suite étudier des p-groupes particuliers : ceux qui n'ont pas de sous-groupe normal isomorphe à $C_p \times C_p$. Un des premiers résultats est qu'un tel groupe est d'un de ces quatre types. La suite du chapitre sera une étude des caractères de ces groupes sur $\mathbb{Q}$. En particulier, on va prouver qu'ils possèdent un unique (à isomorphisme près) module irréductible et fidèle sur $\mathbb{Q}$.

Voici la définition des quatre types de groupes :

- C_n est le groupe cyclique d'ordre n, $n \geq 0$:

$$C_n = \langle x \,|\, x^n = 1 \rangle.$$

- Q_{2^n} est le groupe des quaternions généralisés d'ordre 2^n, $n \geq 3$:

$$Q_{2^n} = \langle x, y \,|\, x^{2^{n-1}} = 1, yxy^{-1} = x^{-1}, x^{2^{n-2}} = y^2 \rangle.$$

- D_{2^n} est le groupe diédral d'ordre 2^n, $n \geq 3$:

$$D_{2^n} = \langle x, y \,|\, x^{2^{n-1}} = y^2 = 1, yxy^{-1} = x^{-1} \rangle.$$

- SD_{2^n} est le groupe semi-diédral d'ordre 2^n, $n \geq 4$:

$$SD_{2^n} = \langle x, y \,|\, x^{2^{n-1}} = y^2 = 1, yxy^{-1} = x^{2^{n-2}-1} \rangle.$$

Définition 4.1 *Un p-groupe P fini est dit de **p-rang normal** 1 s'il ne possède pas de sous-groupe normal isomorphe à $C_p \times C_p$.*

Lemme 4.2 *Soit P un p-groupe fini, K un corps de caractéristique p et V est un KP-module de dimension finie et différent de $\{0\}$. Alors $V^P \neq \{0\}$, où $V^P = \{v \in V \,|\, gv = v, \ \forall\ g \in P\}$.*

Preuve: Soit B une base de V. Comme K est de caractéristique p, il contient $\mathbb{F}_p$. On pose

$$Y = \Big\{ \sum_{i=1}^{n} \lambda_i g_i b_i \,\Big|\, n \in \mathbb{N}^*, \lambda_i \in \mathbb{F}_p, g_i \in P, b_i \in B, \forall\ i \in \{1, \ldots, n\} \Big\}.$$

Alors Y est un P-ensemble fini et un $\mathbb{F}_p$-espace vectoriel. Alors il existe une $\mathbb{F}_p$-base $\widehat{B}$ de Y. Si on pose $m = |\widehat{B}|$, alors $|Y| = p^m$. De plus, comme $V \neq \{0\}$, on a $m \geq 1$. On considère les orbites de Y pour l'action de P : L'ensemble Y est l'union disjointe de ses orbites. Soit $x_1, \ldots x_r$ les éléments d'orbites triviales et $y_1, \ldots y_s$ des représentants des orbites non triviales. Alors

$$Y = \Big(\bigsqcup_{i=1}^{r} \{x_i\} \Big) \bigsqcup \Big(\bigsqcup_{j=1}^{r} \mathrm{Orb}_P(y_j) \Big)$$

et donc

$$|Y| = r + \sum_{j=1}^{s} |\,\mathrm{Orb}_P(y_j)|.$$

Or Y^P est l'ensemble des éléments d'orbites triviales, donc $r = |Y^P|$. Ainsi

$$|Y^P| = |Y| - \sum_{j=1}^{s} |\,\mathrm{Orb}_P(y_j)|. \tag{4.1}$$

Si une orbite est non-triviale, sa cardinalité est un multiple de p et $|Y|$ est aussi un multiple de p. Ainsi p divise le membre de droite de l'équation 4.1 et donc aussi $|Y^P|$. Ainsi Y^P possède au moins p éléments. Or $Y^P \subset V^P$, donc V^P possède au moins p éléments et donc $V^P \neq \{0\}$. □

Corollaire 4.3 *Soit P un p-groupe fini et K un corps de caractéristique p. Alors tout KP-module (de dimension finie) irréductible est isomorphe au KP-module trivial K.*

Preuve: Soit V un KP-module irréductible (de dimension finie). Alors $V \neq \{0\}$ et donc, par le lemme 4.2, $V^P \neq \{0\}$. Or V^P est un sous-module de V, donc comme V est irréductible, $V = V^P$. Ainsi P agit trivialement sur V. Mais alors, si $n = \dim_K V$,

$$V \cong \underbrace{K \oplus K \oplus \ldots \oplus K}_{n \text{ fois}}.$$

Or V doit être irréductible, donc $n = 1$ et $V \cong K$. □

Lemme 4.4 *Soit P un p-groupe fini de p-rang normal 1. Alors P ne possède pas de sous-groupe normal abélien non-cyclique.*

Preuve: Si $P = \mathbf{1}$, le résultat est vérifié. On suppose donc que $P \neq \mathbf{1}$. Soit N un sous-groupe normal abélien élémentaire d'ordre p^n, $n \geq 1$ (il suffit de prendre $b \in Z(P)$ d'ordre p, ce qui est possible car $Z(P)$ n'est pas trivial, et $N = \langle b \rangle$). On va montrer que P possède un sous-groupe normal abélien élémentaire d'ordre p^i, pour tout $1 \leq i \leq n$. Mais, si P possède un sous-groupe abélien normal non cyclique A, alors il existe des entiers naturels $r_1, \ldots r_m$ $(m \geq 2)$ tels que

$$A \cong C_{p^{r_1}} \times \ldots \times C_{p^{r_m}}.$$

Alors A contient un sous-groupe H isomorphe à

$$\underbrace{C_p \times \ldots \times C_p}_{m \text{ fois}}.$$

Or ce sous-groupe H est caractéristique dans A et donc normal dans P. Ainsi, on aura obtenu que si P est de p-rang normal 1, P ne possède pas de sous-groupe normal abélien non-cyclique car sinon il posséderait un sous-groupe normal abélien élémentaire d'ordre p^n, $n \geq 2$ et donc aussi un sous-groupe normal isomorphe à $C_p \times C_p$.
On va étudier N :

$$N \cong \underbrace{C_p \times C_p \times \ldots \times C_p}_{n \text{ fois}} = (C_p)^n.$$

Or, par le théorème A.9, $(C_p)^n$ est un $\mathbb{F}_p$-espace vectoriel de dimension n (où l'addition correspond à la multiplication dans $(C_p)^n$) muni d'une action de P (la conjugaison) et on peut vérifier que c'est un $\mathbb{F}_p P$-module. On va construire une suite de $\mathbb{F}_p P$-modules

$$N = N_0 \supset N_1 \supset N_2 \supset \ldots \supset N_n = \{0\}$$

tel que N_i/N_{i+1} est irréductible, pour tout $0 \leq i \leq n-1$. Pour cela, on va faire une récurrence sur n qui correspond à la dimension de N. Si $n = 1$, alors N est irréductible. Donc il suffit de prendre la suite $N = N_0 \supset N_1 = \{0\}$. On suppose maintenant le résultat vrai pour $n-1$ avec $n \geq 2$. Alors comme $|N| > p$, N n'est pas irréductible (corollaire 4.3). Donc il existe un sous-module irréductible M de N. Par le corollaire 4.3, M est isomorphe à $\mathbb{F}_p$ et est donc de dimension 1. On considère $H = N/M$, c'est un $\mathbb{F}_p$-module de dimension $n-1$. Par hypothèse de récurrence, il existe une suite

$$H = H_0 \supset H_1 \supset \ldots \supset H_{n-1} = \{0\}$$

telle que H_i/H_{i+1} est irréductible pour tout $0 \leq i \leq n-2$. Alors soit $\pi : N \to N/M$ la projection canonique. On pose $N_i = \pi^{-1}(H_i)$ pour tout $0 \leq i \leq n-1$ et $N_n = \{0\}$. Alors on a bien

$$N = N_0 \supset N_1 \supset N_2 \supset \ldots \supset N_{n-1} \supset N_n = \{0\}.$$

De plus $N_{n-1}/N_n \cong M$ est irréductible et si $0 \leq i \leq n-2$, alors par le troisième théorème d'isomorphisme. $N_i/N_{i+1} \cong H_i/H_{i+1}$ est irréductible. Ainsi on a montré le résultat et on a bien une suite

$$N = N_0 \supset N_1 \supset N_2 \supset \ldots \supset N_n = \{0\}$$

tels que N_i/N_{i+1} est irréductible, pour tout $0 \leq i \leq n-1$. On va maintenant étudier à quoi correspondent les N_i dans P. Soit $1 \leq i \leq n$. Alors N_i est un sous-groupe de N, donc aussi abélien élémentaire, d'ordre p^i. Il reste à voir que N_i est normal dans P. Or N_i est un $\mathbb{F}_pP$-module, donc en particulier, $gN_ig^{-1} = N_i$ pour tout $g \in P$, c'est-à-dire que N_i est normal dans P. □

Théorème 4.5 *Soit P un p-groupe fini de p-rang normal 1. Alors soit P est cyclique, soit $p = 2$ et P est isomorphe à Q_{2^n} pour $n \geq 3$, D_{2^n} pour $n \geq 4$ ou SD_{2^n} pour $n \geq 4$.*

Preuve: Le groupe P ne possède pas de sous-groupe normal abélien non-cyclique (lemme 4.4). Ainsi, on peut appliquer le théorème 4.10 du chapitre 5, page 199 de *Finite groups* de Daniel Gorenstein, [Gor68] : Si P est un p-groupe qui ne possède pas de sous-groupe abélien normal non-cyclique, alors soit $p \neq 2$ et P est cyclique, soit $p = 2$ et P est isomorphe à un des groupes C_{2^n} pour $n \geq 0$, Q_{2^n} pour $n \geq 3$, D_{2^n} pour $n \geq 4$ ou SD_{2^n} pour $n \geq 4$. □

Lemme 4.6 *Soit P un p-groupe fini de p-rang normal 1 non-cyclique. Alors $p = 2$ et P a exactement 3 sous-groupes maximaux A, B et C. Le groupe C est cyclique et de plus :*

i) Si $P \cong Q_8$, alors A et B sont cycliques.

ii) Si P est diédral, alors A et B sont diédraux.

iii) Si P est quaternionien généralisé d'ordre au moins 16, alors A et B sont quaternionien généralisé.

iv) Si P est semi-diédral, alors A est diédral et B est quaternionien généralisé.

Preuve: Par le théorème 4.5, on sait que P est isomorphe à un groupe diédral, semi-diédral ou quaternionien généralisé. Alors, par la proposition A.11, on sait que $\Phi(P) = \langle x^2 \rangle$. Ainsi on a que $P/\Phi(P)$ est isomorphe à $C_2 \times C_2$. Or les sous-groupes maximaux de P sont en bijections avec les sous-groupes maximaux de $P/\Phi(P)$, donc avec ceux de $C_2 \times C_2$ et donc il y en a exactement 3. Or les sous-groupes suivants sont d'ordre 2^{n-1} et sont donc maximaux dans P :

$$A = \langle x^2, y \rangle, \qquad B = \langle x^2, xy \rangle \quad \text{et} \quad C = \langle x \rangle.$$

Il est clair que C est cyclique.

i) Si P est isomorphe à Q_8, alors on a :

$$A = \langle y \rangle, \qquad B = \langle xy \rangle \quad \text{et} \quad C = \langle x \rangle$$

qui sont bien des sous-groupes cycliques.

ii) Si P est diédral, on peut voir qu'alors A et B sont aussi diédraux.

iii) Si P est quaternionien généralisé (d'ordre au moins 16), on peut voir que A et B sont aussi quaternionien généralisé.

iv) Si P est semi-diédral, on peut voir alors que A est diédral et B est quaternionien généralisé.

□

Lemme 4.7 *Soit P un p-groupe fini de p-rang normal 1. Si Q est un sous-groupe de P tel que $Q \cap Z(P) = \mathbf{1}$, alors $Q = \mathbf{1}$ si P est cyclique ou quaternionien généralisé et $|Q| \leq 2$ si P est diédral ou semi-diédral.*

Preuve: Si P est trivial, le résultat est clair. Si P est non trivial et que P est cyclique ou quaternionien généralisé, alors P possède un unique sous-groupe d'ordre p qui intersecte non trivialement le centre (théorème A.12) et donc Q est trivial (car sinon Q contient un sous-groupe d'ordre p et qui alors intersecte non trivialement le centre, ce qui est impossible). On suppose maintenant que P est diédral ou semi-diédral. Alors comme P est non trivial, $Q \neq P$, donc Q est contenu dans un sous-groupe maximal M non cyclique (si Q est contenu dans le sous-groupe maximal cyclique, alors il contient le centre et donc l'intersecte non trivialement). De plus, le centre de P est alors aussi le centre de M, qui est diédral, semi-diédral ou quaternionien généralisé. Ainsi Q est un sous-groupe de M tel que $Q \cap Z(M) = \mathbf{1}$. On peut alors prouver le résultat par un argument d'induction sur l'ordre de P. □

On va maintenant montrer qu'un p-groupe fini P de p-rang normal 1 possède un unique $\mathbb{Q}P$-module irréductible fidèle. Pour ce faire, on va utiliser le théorème 4.5 et traiter séparément les cas cyclique, diédral, semi-diédral et quaternionien généralisé.

Théorème 4.8 *Soit $n \in \mathbb{N}^*$.Alors le groupe cyclique C_{p^n} possède un unique $\mathbb{Q}C_{p^n}$-module irréductible fidèle (de dimension finie).*

Preuve: Soit $P = C_{p^n} = \langle x \mid x^{p^n} = 1 \rangle$.
Pour le cas $n = 0$, il y a un seul $\mathbb{Q}\mathbf{1}$-module irréductible (le module trivial) qui est fidèle.
On suppose maintenant que $n \geq 1$. On sait que C_{p^n} possède $n+1$ sous-groupes cycliques (à conjugaison près) et donc, par le corollaire 2.10, P possède $n+1$ $\mathbb{Q}P$-modules irréductibles. Le groupe C_{p^n} possède un sous-groupe isomorphe à C_p : $\langle x^{p^{n-1}} \rangle$. Or on sait que C_p possède deux caractères

irréductibles qui apparaissent chacun une fois dans le caractère régulier (exemple 2.11). Donc C_p possède deux $\mathbb{Q}C_p$-modules irréductibles, qui apparaissent chacun une fois dans le $\mathbb{Q}C_p$-module régulier. Or $\mathbb{Q}C_p = \mathbb{Q} \oplus \Omega_{C_p}$, où Ω_{C_p} est le noyau de l'homomorphisme d'augmentation $\mathbb{Q}C_p \to \mathbb{Q}$. Ainsi les deux $\mathbb{Q}C_p$-modules irréductibles sont $\mathbb{Q}$ et Ω_{C_p}. Alors on a que

$$\begin{aligned}
\mathbb{Q}C_{p^n} &\overset{(1)}{=} \mathrm{Ind}_{C_p}^{C_{p^n}} \mathbb{Q}C_p \\
&= \mathrm{Ind}_{C_p}^{C_{p^n}} \mathbb{Q} \oplus \mathrm{Ind}_{C_p}^{C_{p^n}} \Omega_{C_p} \\
&\overset{(2)}{=} \mathrm{Inf}_{C_{p^n}/C_p}^{C_{p^n}} \mathbb{Q}(C_{p^n}/C_p) \oplus \mathrm{Ind}_{C_p}^{C_{p^n}} \Omega_{C_p} \\
&= \mathrm{Inf}_{C_{p^{n-1}}}^{C_{p^n}} \mathbb{Q}C_{p^{n-1}} \oplus \mathrm{Ind}_{C_p}^{C_{p^n}} \Omega_{C_p},
\end{aligned}$$

où l'égalité (1) découle de la proposition B.25 et l'égalité (2) de la proposition B.40. On sait aussi (par le corollaire 2.10), que $C_{p^{n-1}}$ possède n $\mathbb{Q}C_{p^{n-1}}$-modules irréductibles. Donc $\mathrm{Inf}_{C_{p^{n-1}}}^{C_{p^n}} \mathbb{Q}C_{p^{n-1}}$ donne n $\mathbb{Q}P$-modules irréductibles non-fidèles de P. Il reste un $\mathbb{Q}P$-modules irréductible à trouver et voir qu'il est fidèle. On va montrer que $V = \mathrm{Ind}_{C_p}^{C_{p^n}} \Omega_{C_p}$ est un $\mathbb{Q}P$-modules irréductible et fidèle. On note ψ le caractère associé à Ω_{C_p} et χ le caractère associé à V. On sait que, si $g = x^{p^{n-1}}$

$$\psi(g^i) = \begin{cases} p-1 & \text{si } i = 0 \\ -1 & \text{si } i \neq 0 \end{cases},$$

pour tout $i \in \{0, \ldots, p-1\}$. Alors, en utilisant la formule B.27, on obtient :

$$\chi(x^j) = \begin{cases} p^{n-1}(p-1) & \text{si } j = 0 \\ -p^{n-1} & \text{si } j \neq 0 \text{ et } p^{n-1} | j \\ 0 & \text{si } p^{n-1} \nmid j \end{cases},$$

pour tout $j \in \{0, \ldots, p^n - 1\}$. Ainsi on voit que χ est un caractère fidèle et donc $\mathrm{Ind}_{C_p}^{C_{p^n}} \Omega_{C_p}$ est un module fidèle.

On connaît la table de caractère de P sur $\mathbb{C}$ (exemple B.51) :

	1	x	$\cdots$	x^k	$\cdots$	x^{p^n-1}
$\psi_0 = \mathbf{1}_P$	1	1	$\cdots$	1	$\cdots$	1
ψ_j	1	ξ^j	$\ldots$	$(\xi^j)^k$	$\ldots$	$(\xi^j)^{p^n-1}$

$0 \leq j \leq p^n - 1$ et ξ est une racine p^n-ième primitive de l'unité.

Mais χ est aussi un caractère de P sur $\mathbb{C}$, donc on peut trouver sa

décomposition en caractères irréductibles de $\mathbb{C}$. Soit $0 \leq i \leq p^n - 1$.

$$\begin{aligned}
\langle \psi_i, \chi \rangle_P &= \frac{1}{|P|} \sum_{g \in P} \psi_i(g)\overline{\chi(g)} \\
&= \frac{1}{p^n} \sum_{j=0}^{p^n-1} \psi_i(x^j)\chi(x^j) \\
&= \frac{1}{p^n} \left(p^{n-1}(p-1) - p^{n-1} \sum_{k=1}^{p-1} (\xi^i)^{kp^{n-1}} \right) \\
&= \frac{1}{p^n} \left(p^{n-1}(p-1) - p^{n-1} \sum_{k=1}^{p-1} \left((\xi^{p^{n-1}})^i \right)^k \right)
\end{aligned}$$

On remarque que $\xi^{p^{n-1}}$ est une racine $p^{\text{ième}}$ primitive de l'unité. Alors il y a deux cas à distinguer :

- Si $\text{pgcd}(i, p) = 1$, alors $(\xi^{p^{n-1}})^i$ est aussi une racine $p^{\text{ième}}$ primitive de l'unité et $\sum_{k=1}^{p-1} \left((\xi^{p^{n-1}})^i \right)^k = -1$ d'où :

$$\begin{aligned}
\langle \psi_i, \chi \rangle_P &= \frac{1}{p^n} \Big(p^{n-1}(p-1) - p^{n-1} \sum_{k=1}^{p-1} \left((\xi^{p^{n-1}})^i \right)^k \Big) \\
&= \frac{1}{p^n} \big(p^{n-1}(p-1) + p^{n-1} \big) \\
&= \frac{p^n}{p^n} = 1
\end{aligned}$$

- Si $\text{pgcd}(i, p) \neq 1$, alors $(\xi^{p^{n-1}})^i = 1$ et donc :

$$\begin{aligned}
\langle \psi_i, \chi \rangle_P &= \frac{1}{p^n} (p^{n-1}(p-1) - p^{n-1} \sum_{k=1}^{p-1} \left((\xi^{p^{n-1}})^i \right)^k) \\
&= \frac{1}{p^n} \big(p^{n-1}(p-1) - p^{n-1} \sum_{k=1}^{p-1} 1 \big) \\
&= \frac{1}{p^n} \big(p^{n-1}(p-1) - p^{n-1}(p-1) \big) = 0
\end{aligned}$$

On a ainsi obtenu que $\langle \psi_i, \chi \rangle_P$ est égal à 1 si $\text{pgcd}(i, p) = 1$ et est égal à 0 sinon. Donc χ est la somme des caractères irréductibles ψ_i tels que $\text{pgcd}(i, p) = 1$.

Soit W un $\mathbb{Q}P$-sous-module irréductible de V et soit η le caractère associé à W. Alors W possède sur $\mathbb{C}$ au moins un sous-module irréductible comme facteur de composition (un de ceux de V) et donc il existe $j \in \{0, \ldots, p^n - 1\}$ avec $\text{pgcd}(p, j) = 1$ tel que $\langle \psi_j, \eta \rangle_P \neq 0$. Mais alors $\langle \psi_j, \eta \rangle_P = 1$.

On pose $G = \mathrm{Gal}(\mathbb{Q}(\xi), \mathbb{Q})$, le groupe de Galois de $\mathbb{Q}(\xi)$ sur $\mathbb{Q}$. On sait que si $\varphi \in G$, alors $\varphi \circ \psi_j$ est un caractère irréductible de P sur $\mathbb{C}$, et il existe $0 \leq i \leq p^n - 1$ avec $\mathrm{pgcd}(i,p) = 1$ tel que $\varphi \circ \psi_j = \psi_i$. Ainsi

$$\{\varphi \circ \psi_j \,\big|\, \varphi \in G\} = \{\psi_i \,\big|\, 0 \leq i \leq p^n - 1, \mathrm{pgcd}(i,p) = 1\}.$$

On a, si $\varphi \in G$

$$\begin{aligned}
\langle \varphi \circ \psi_j, \eta \rangle_P &= \frac{1}{|P|} \sum_{h \in P} \varphi\big(\psi_j(h)\big)\overline{\eta(h)} \\
&\overset{\eta(h) \in \mathbb{Q}}{=} \frac{1}{|P|} \sum_{h \in P} \varphi\left(\psi_j(h)\overline{\eta(h)}\right) \\
&= \frac{1}{|P|} \varphi\Big(\sum_{h \in P} \psi_j(h)\overline{\eta(h)}\Big) \\
&= \varphi\Big(\frac{1}{|P|} \sum_{h \in P} \psi_j(h)\overline{\eta(h)}\Big) \\
&= \varphi\big(\langle \psi_j, \eta \rangle_P\big) \\
&= \varphi(1) = 1.
\end{aligned}$$

Donc W contient 1 fois chacun des $\mathbb{C}P$-modules irréductibles ψ_i tel que $\mathrm{pgcd}(p,i) = 1$ et donc $V \subset W$. Or $W \subset V$, donc $V = W$ et V est irréductible. □

Remarque 4.9 Cette preuve se base sur la preuve du lemme 2 de l'article *A remark on a theorem of Ritter and Segal* de Serge Bouc, [Bou01].

Théorème 4.10 *Soit $n \in \mathbb{N}$, $n \geq 3$. Le groupe diédral D_{2^n} possède un unique $\mathbb{Q}D_{2^n}$-module irréductible fidèle (de dimension finie). De même, si $n \geq 4$, alors le groupe semi-diédral SD_{2^n} possède un unique $\mathbb{Q}SD_2$-module irréductible fidèle (de dimension finie).*

Preuve: Soit P l'un des groupes suivants :

$$D_{2^n} = \langle x, y \,\big|\, x^{2^{n-1}} = y^2 = 1, yxy^{-1} = x^{-1} \rangle$$

ou

$$SD_{2^n} = \langle x, y \,\big|\, x^{2^{n-1}} = y^2 = 1, yxy^{-1} = x^{2^{n-2}-1} \rangle.$$

Le groupe P possède un sous-groupe isomorphe à C_2 : Le sous-groupe $C = \langle x^{2^{n-2}} \rangle$. Les deux $\mathbb{Q}C_2$-modules irréductibles sont $\mathbb{Q}$ et Ω_{C_2}, et $\mathbb{Q}C_2 = \mathbb{Q} \oplus \Omega_{C_2}$ (voir la preuve du théorème 4.8). Alors on a

$$\begin{aligned}
\mathbb{Q}P &\overset{(1)}{=} \mathrm{Ind}_C^P \mathbb{Q}C \\
&= \mathrm{Ind}_C^P \mathbb{Q} \oplus \mathrm{Ind}_C^P \Omega_C \\
&\overset{(2)}{=} \mathrm{Inf}_{P/C}^P \mathbb{Q}(P/C) \oplus \mathrm{Ind}_C^P \Omega_C \\
&= \mathrm{Inf}_{D_{2^{n-1}}}^P \mathbb{Q}D_{2^{n-1}} \oplus \mathrm{Ind}_C^P \Omega_C
\end{aligned}$$

où l'égalité (1) découle de la proposition B.25 et l'égalité (2) de la proposition B.40. Le terme $\mathrm{Inf}_{D_{2^{n-1}}}^{P} \mathbb{Q}D_{2^{n-1}}$ donne des $\mathbb{Q}P$-modules irréductibles non-fidèles. Contrairement à C_{p^n}, le $\mathbb{Q}P$-module $V = \mathrm{Ind}_{C}^{P} \Omega_C$ n'est pas irréductible, comme on va le voir un peu plus loin.

On pose $D = \langle y \rangle$ et $D' = \langle x^{2^{n-2}} y \rangle$. Alors $N = N_P(D) = N_P(D') = \{1, y, x^{2^{n-2}}, x^{2^{n-2}} y\} \cong C_2 \times C_2$. Or on connaît les caractères de $C_2 \times C_2$ (exemple 2.13) : il y a le caractère trivial et trois caractères qui sont l'inflation des caractères non-triviaux des quotients de $C_2 \times C_2$ par les sous-groupes d'ordre 2. Ainsi on connaît les $\mathbb{Q}(C_2 \times C_2)$-modules irréductibles et

$$\begin{aligned}
\mathbb{Q}P &= \mathrm{Ind}_{N}^{P} \mathbb{Q}N \\
&= \mathrm{Ind}_{N}^{P} \mathbb{Q} \oplus \mathrm{Ind}_{N}^{P} \mathrm{Inf}_{N/C}^{N} \Omega_{N/C} \\
&\quad \oplus \mathrm{Ind}_{N}^{P} \mathrm{Inf}_{N/D}^{N} \Omega_{N/D} \oplus \mathrm{Ind}_{N}^{P} \mathrm{Inf}_{N/D'}^{N} \Omega_{N/D'}
\end{aligned}$$

De plus, on a :

$$\begin{aligned}
\mathrm{Inf}_{D_{2^{n-1}}}^{P} \mathbb{Q}D_{2^{n-1}} &\overset{(1)}{=} \mathrm{Ind}_{C}^{P} \mathbb{Q} \\
&= \mathrm{Ind}_{N}^{P} \mathrm{Ind}_{C}^{N} \mathbb{Q} \\
&\overset{(2)}{=} \mathrm{Ind}_{N}^{P} \mathrm{Inf}_{N/C}^{N} \mathbb{Q}(N/C) \\
&= \mathrm{Ind}_{N}^{P} \mathrm{Inf}_{N/C}^{N} \mathbb{Q} \oplus \mathrm{Ind}_{N}^{P} \mathrm{Inf}_{N/C}^{N} \Omega_{N/C} \\
&= \mathrm{Ind}_{N}^{P} \mathbb{Q} \oplus \mathrm{Ind}_{N}^{P} \mathrm{Inf}_{N/C}^{N} \Omega_{N/C},
\end{aligned}$$

où l'égalité (1) découle, par la proposition B.43, de

$$\mathrm{Inf}_{D_{2^{n-1}}}^{P} \mathbb{Q}D_{2^{n-1}} = \mathrm{Inf}_{P/C}^{P} \mathbb{Q}(P/C) = \mathbb{Q}(P/C) = \mathrm{Ind}_{C}^{P} \mathbb{Q}$$

et l'égalité (2), par la proposition B.43, de

$$\mathrm{Ind}_{C}^{N} \mathbb{Q} = \mathbb{Q}(N/C) = \mathrm{Inf}_{N/C}^{N} \mathbb{Q}(N/C).$$

Ainsi, en résumé, on a :

$$\begin{aligned}
\mathbb{Q}P \cong\ & \mathrm{Ind}_{N}^{P} \mathbb{Q} \oplus \mathrm{Ind}_{N}^{P} \mathrm{Inf}_{N/C}^{N} \Omega_{N/C} \\
& \oplus \mathrm{Ind}_{N}^{P} \mathrm{Inf}_{N/D}^{N} \Omega_{N/D} \oplus \mathrm{Ind}_{N}^{P} \mathrm{Inf}_{N/D'}^{N} \Omega_{N/D'}
\end{aligned}$$

et

$$\mathbb{Q}P \cong \mathrm{Ind}_{N}^{P} \mathbb{Q} \oplus \mathrm{Ind}_{N}^{P} \mathrm{Inf}_{N/C}^{N} \Omega_{N/C} \oplus \mathrm{Ind}_{C}^{P} \Omega_C$$

donc $\mathrm{Ind}_{C}^{P} \Omega_C \cong \mathrm{Ind}_{N}^{P} \mathrm{Inf}_{N/D}^{N} \Omega_{N/D} \oplus \mathrm{Ind}_{N}^{P} \mathrm{Inf}_{N/D'}^{N} \Omega_{N/D'}$, qui n'est pas irréductible. On pose

$$W_1 = \mathrm{Ind}_{N}^{P} \mathrm{Inf}_{N/D}^{N} \Omega_{N/D} \text{ et } W_2 = \mathrm{Ind}_{N}^{P} \mathrm{Inf}_{N/D'}^{N} \Omega_{N/D'}.$$

Comme D et D' sont conjugués (par $x^{2^{n-3}}$) on a que W_1 et W_2 sont isomorphes (proposition B.46). On pose $W = W_1 (\cong W_2)$. On va montrer que

W est un $\mathbb{Q}P$-module irréductible et fidèle. Alors on aura trouvé tous les $\mathbb{Q}P$-modules de P car $\mathbb{Q}P = \mathrm{Inf}_{D_{2^{n-1}}}^{P} \mathbb{Q}D_{2^{n-1}} \oplus W_1 \oplus W_2$ et de plus, on sait déjà que les modules irréductibles différents de W ne sont pas fidèles (car ils sont inflatés depuis $D_{2^{n-1}}$). On note ψ le caractère associé à $V = \mathrm{Ind}_{C}^{P} \Omega_C$ et χ le caractère associé à W. On sait que $V \cong W \oplus W$, donc $\psi = 2\chi$ et donc $\chi = \frac{1}{2}\psi$. Or, en utilisant la formule B.27, on obtient,

$$\psi(g) = \begin{cases} 2^{n-1} & \text{si } g = 1 \\ -2^{n-1} & \text{si } g = x^{2^{n-2}} \\ 0 & \text{sinon} \end{cases}$$

pour tout $g \in P$ et donc

$$\chi(g) = \begin{cases} 2^{n-2} & \text{si } g = 1 \\ -2^{n-2} & \text{si } g = x^{2^{n-2}} \\ 0 & \text{sinon} \end{cases}$$

pour tout $g \in P$. Ainsi on voit que χ est un caractère fidèle et donc W est un $\mathbb{Q}P$-module fidèle.

On connait la table de caractère de D_{2^n} sur $\mathbb{C}$ (exemple B.54) :

	1	$x^{2^{n-2}}$	x^k $1 \leq k \leq 2^{n-2}-1$	y	xy
η_1	1	1	1	1	1
η_2	1	1	1	-1	-1
η_3	1	1	$(-1)^k$	-1	1
η_4	1	1	$(-1)^k$	1	-1
ψ_j	2	$(-1)^j 2$	$\omega^{jk} + \omega^{-jk}$	0	0

$1 \leq j \leq 2^{n-2} - 1$, ω est une racine 2^{n-1}-ième primitive de l'unité (par exemple $\omega = \exp(\frac{2\pi\imath}{2^{n-1}})$).

De même, on connait la table de caractère de SD_{2^n} sur $\mathbb{C}$ (exemple B.55) :

	1	$x^{2^{n-2}}$	x^{2k} $1 \leq k \leq 2^{n-3}-1$	x^{2k+1} $1 \leq k \leq 2^{n-3}-1$	y	xy
$\widetilde{\psi_1}$	1	1	1	1	1	1
$\widetilde{\psi_2}$	1	1	1	1	-1	-1
$\widetilde{\psi_3}$	1	1	1	-1	1	-1
$\widetilde{\psi_4}$	1	1	1	-1	-1	1
ψ_j	2	$(-1)^j 2$	$\omega^{jk} + \omega^{-jk}$	$\omega^{jk} - \omega^{-jk}$	0	0

$1 \leq j \leq 2^{n-2} - 1$, ω est une racine 2^{n-1}-ième primitive de l'unité (par exemple $\omega = \exp(\frac{2\pi\imath}{2^{n-1}})$).

Mais χ est aussi un caractère de P sur $\mathbb{C}$, donc on peut trouver sa décomposition en caractères irréductibles de $\mathbb{C}$. On commence par les caractères linéaires. Soit $i \in \{1,2,3,4\}$:

$$\begin{aligned}\langle \eta_i, \chi \rangle_P &= \frac{1}{|P|} \sum_{h \in P} \eta_i(h)\overline{\chi(h)} \\ &= \frac{1}{2^n}(2^{n-2} - 2^{n-2}) = 0\end{aligned}$$

Soit maintenant $1 \leq j \leq 2^{n-2} - 1$:

$$\begin{aligned}\langle \psi_j, \chi \rangle_P &= \frac{1}{|P|} \sum_{h \in P} \psi_i(h)\overline{\chi(h)} \\ &= \frac{1}{2^n}(2 \cdot 2^{n-2} - (-1)^j 2 \cdot 2^{n-2}) \\ &= 1 - (-1)^j = \begin{cases} 0 & \text{si } j \text{ est pair} \\ 1 & \text{si } j \text{ est impair.} \end{cases}\end{aligned}$$

On a ainsi obtenu que $\langle \psi_j, \chi \rangle_P$ est égal à 1 si $\text{pgcd}(j,2) = 1$ et à 0 sinon. Donc χ est la somme des caractères irréductibles ψ_j tel que $\text{pgcd}(j,2) = 1$.

Soit U un $\mathbb{Q}P$-sous-module irréductible de W et soit η le caractère associé à U. Alors U possède sur $\mathbb{C}$ au moins un sous-module irréductible comme facteur de composition (un de ceux de U) et donc il existe $j \in \{0, \ldots, 2^{n-2} - 1\}$ avec $\text{pgcd}(2,j) = 1$ tel que $\langle \psi_j, \eta \rangle_P \neq 0$, d'où $\langle \psi_j, \eta \rangle_P = 1$. On pose $G = \text{Gal}(\mathbb{Q}(\omega), \mathbb{Q})$. Si $\varphi \in G$, alors $\varphi \circ \psi_j$ est un caractère irréductible de P sur $\mathbb{C}$, et il existe $0 \leq i \leq 2^{n-2} - 1$ avec $\text{pgcd}(2,i) = 1$ tel que $\varphi \circ \psi_j = \psi_i$. Alors

$$\{\varphi \circ \psi_j \,\big|\, \varphi \in G\} = \{\psi_i \,\big|\, 0 \leq i \leq 2^{n-2} - 1, \text{pgcd}(i,2) = 1\}.$$

On a, si $\varphi \in G$

$$\begin{aligned}\langle \varphi \circ \psi_j, \eta \rangle_P &= \frac{1}{|P|} \sum_{h \in P} \varphi(\psi_j(h))\overline{\eta(h)} \\ &\overset{\overline{\eta(h)} \in \mathbb{Q}}{=} \frac{1}{|P|} \sum_{h \in P} \varphi(\psi_j(h)\overline{\eta(h)}) \\ &= \frac{1}{|P|} \varphi\Big(\sum_{h \in P} \psi_j(h)\overline{\eta(h)} \Big) \\ &= \varphi\Big(\frac{1}{|P|} \sum_{h \in P} \psi_j(h)\overline{\eta(h)}\Big) \\ &= \varphi(\langle \psi_j, \eta \rangle_P) \\ &= \varphi(1) = 1\end{aligned}$$

Donc U contient chacun des $\mathbb{C}P$-modules irréductibles ψ_i tel que $\text{pgcd}(p,i) = 1$ et donc $W \subset U$. Donc $W = U$ et W est irréductible. $\square$

Théorème 4.11 *Soit $n \in \mathbb{N}$, $n \geq 3$. Le groupe des quaternions généralisés Q_{2^n} possède un unique $\mathbb{Q}Q_{2^n}$-module irréductible fidèle.*

Preuve: Soit $P = Q_{2^n} = \langle x, y \,\big|\, x^{2^{n-1}} = 1, y^2 = x^{2^{n-2}}, yxy^{-1} = x^{-1} \rangle$. Le groupe Q_{2^n} possède un sous-groupe isomorphe à C_2 : Le sous-groupe $\langle x^{2^{n-2}} \rangle$. Les deux $\mathbb{Q}C_2$-modules irréductibles sont $\mathbb{Q}$ et Ω_{C_2} et $\mathbb{Q}C_2 = \mathbb{Q} \oplus \Omega_{C_2}$. Alors on a

$$\begin{aligned}
\mathbb{Q}Q_{2^n} &\overset{(1)}{=} \mathrm{Ind}_{C_2}^{Q_{2^n}} \mathbb{Q}C_2 \\
&= \mathrm{Ind}_{C_2}^{Q_{2^n}} \mathbb{Q} \oplus \mathrm{Ind}_{C_2}^{Q_{2^n}} \Omega_{C_2} \\
&\overset{(2)}{=} \mathrm{Inf}_{Q_{2^n}/C_2}^{Q_{2^n}} \mathbb{Q}(Q_{2^n}/C_2) \oplus \mathrm{Ind}_{C_2}^{Q_{2^n}} \Omega_{C_2} \\
&= \mathrm{Inf}_{D_{2^{n-1}}}^{Q_{2^n}} \mathbb{Q}D_{2^{n-1}} \oplus \mathrm{Ind}_{C_2}^{Q_{2^n}} \Omega_{C_2},
\end{aligned}$$

où l'égalité (1) découle de la proposition B.25 et l'égalité (2) de la proposition B.40. Le terme $\mathrm{Inf}_{D_{2^{n-1}}}^{Q_{2^n}} \mathbb{Q}D_{2^{n-1}}$ donne des $\mathbb{Q}P$-modules irréductibles non-fidèles. On va montrer que $V = \mathrm{Ind}_{C_2}^{Q_{2^n}} \Omega_{C_2}$ est un $\mathbb{Q}P$-module irréductible et fidèle. Alors on aura trouvé tous les $\mathbb{Q}P$-modules irréductibles car $\mathbb{Q}Q_{2^n} = \mathrm{Inf}_{D_{2^{n-1}}}^{Q_{2^n}} \mathbb{Q}D_{2^{n-1}} \oplus \mathrm{Ind}_{C_2}^{Q_{2^n}} \Omega_{C_2}$ et de plus, on sait déjà que tous les modules irréductibles différents de V ne sont pas fidèles (ils sont inflatés depuis un quotient). On note ψ le caractère associé à Ω_{C_2} et χ le caractère associé à V. On sait que,

$$\psi(h) = \begin{cases} 1 & \text{si } h = 1 \\ -1 & \text{si } h = x^{2^{n-2}}. \end{cases}$$

Alors, en utilisant la formule B.27, on obtient :

$$\chi(g) = \begin{cases} 2^{n-1} & \text{si } g = 1 \\ -2^{n-1} & \text{si } g = x^{2^{n-2}} \\ 0 & \text{sinon.} \end{cases}$$

Ainsi on voit que χ est un caractère fidèle et donc $\mathrm{Ind}_{C_2}^{Q_{2^n}} \Omega_{C_2}$ est un module fidèle. Il reste à voir que V est un module irréductible. On a

$$V = \mathrm{Ind}_{C_2}^{Q_{2^n}} \Omega_{C_2} = \mathbb{Q}Q_{2^n} \otimes_{\mathbb{Q}C_2} \Omega_{C_2}.$$

On pose $A = \langle x \rangle$, c'est un sous-groupe de Q_{2^n} d'ordre 2^{n-1}. Alors $\mathbb{Q}A$ et $\mathbb{Q}Ay$ sont des $\mathbb{Q}C_2$-modules et $\mathbb{Q}Q_{2^n} = \mathbb{Q}A \oplus \mathbb{Q}Ay$. Ainsi on a

$$V = (\mathbb{Q}A \otimes_{\mathbb{Q}C_2} \Omega_{C_2}) \oplus (\mathbb{Q}Ay \otimes_{\mathbb{Q}C_2} \Omega_{C_2})$$

comme $\mathbb{Q}C_2$-modules. On va commencer à étudier $\mathbb{Q}A \otimes_{\mathbb{Q}C_2} \Omega_{C_2}$. On pose

$$K = \mathbb{Q}[X]/\langle \Phi_{2^{n-1}}(X) \rangle = \mathbb{Q}[X]/\langle \Phi_2(X^{2^{n-2}}) \rangle = \mathbb{Q}[X]/\langle X^{2^{n-2}} + 1 \rangle,$$

où Φ_n est le $n^{\text{ième}}$ polynôme cyclotomique. Or $\Phi_{2^{n-1}}(X)$ est un polynôme irréductible dans $\mathbb{Q}[X]$ donc K est un corps et $[K:\mathbb{Q}] = 2^{n-2}$. On va munir le corps K d'une structure de $\mathbb{Q}A$-module : L'élément x^i agit sur K comme la multiplication par $\overline{X}^i$, pour tout $x^i \in A$. On peut vérifier que l'action est bien définie et muni K d'une structure de $\mathbb{Q}A$-module.

En appliquant la proposition B.29, on a

$$\dim_{\mathbb{Q}} \mathbb{Q}A \otimes_{\mathbb{Q}C_2} \Omega_{C_2} = |A:C| \dim_{\mathbb{Q}} \Omega_{C_2} = 2^{n-2}.$$

Ainsi $\mathbb{Q}A \otimes_{\mathbb{Q}C_2} \Omega_{C_2}$ et K sont des $\mathbb{Q}$-espaces vectoriels de même dimension. On va montrer qu'ils sont isomorphes comme $\mathbb{Q}A$-modules.

Comme $\mathbb{Q}$-espace vectoriel, Ω_{C_2} est isomorphe à $\mathbb{Q}$. Le groupe C_2 agit sur $\mathbb{Q}$, où la multiplication par $x^{2^{n-2}}$ correspond à la multiplication par -1. Alors $\mathbb{Q}$ et Ω_{C_2} sont isomorphes comme $\mathbb{Q}C_2$-modules. Ainsi, par la suite, on va identifier Ω_{C_2} avec $\mathbb{Q}$.

On définit alors l'application $\varphi : \mathbb{Q}A \times \Omega_{C_2} \to K$ par

$$\varphi\Big(\sum_{i=0}^{2^{n-1}-1} q_i x^i, r\Big) = \sum_{i=0}^{2^{n-1}-1} r q_i \overline{X}^i.$$

Alors un petit calcul nous donne que

$$\varphi(a+b,c) = \varphi(a,c) + \varphi(b,c) \text{ et } \varphi(a,c+d) = \varphi(a,c) + \varphi(a,d),$$

pour tout $a, b \in \mathbb{Q}A$ et pour tout $c, d \in \Omega_{C_2}$. On peut de plus remarquer que dans $K = \mathbb{Q}[X]/\langle X^{2^{n-2}} + 1\rangle$,

$$\overline{X}^{2^{n-2}} = -1 \quad \text{et} \quad \overline{X}^{2^{n-1}} = 1.$$

Soit $a = \sum_{i=0}^{2^{n-1}-1} q_i x^i \in \mathbb{Q}A$, $r \in \Omega_{C_2}$ et $\lambda + \mu x^{2^{n-2}} \in \mathbb{Q}C_2$. Alors

$$\begin{aligned}
\varphi\big(a \cdot (\lambda + \mu x^{2^{n-2}}), r\big) &= \varphi\Big(\sum_{i=0}^{2^{n-1}-1} q_i \lambda x^i + \sum_{i=0}^{2^{n-1}-1} q_i \mu x^{2^{n-2}+i}, r\Big) \\
&= \varphi\Big(\sum_{i=0}^{2^{n-1}-1} q_i \lambda x^i, r\Big) + \varphi\Big(\sum_{i=0}^{2^{n-2}-1} q_i \mu x^{2^{n-2}+i}, r\Big) \\
&\quad + \varphi\Big(\sum_{i=2^{n-2}}^{2^{n-1}-1} q_i \mu x^{2^{n-2}+i}, r\Big)
\end{aligned}$$

$$\begin{aligned}
\varphi\big(a\cdot(\lambda+\mu x^{2^{n-2}}),r\big) &= \varphi\Big(\sum_{i=0}^{2^{n-1}-1} q_i\lambda x^i, r\Big) + \varphi\Big(\sum_{i=0}^{2^{n-2}-1} q_i\mu x^{2^{n-2}+i}, r\Big)\\
&\quad + \varphi\Big(\sum_{i=0}^{2^{n-2}-1} q_i\mu x^i, r\Big)\\
&= \sum_{i=0}^{2^{n-1}-1} rq_i\lambda\overline{X}^i + \sum_{i=0}^{2^{n-2}-1} rq_i\mu\overline{X}^{2^{n-2}+i}\\
&\quad + \sum_{i=0}^{2^{n-2}-1} rq_i\mu\overline{X}^i\\
&= \lambda\sum_{i=0}^{2^{n-1}-1} rq_i\overline{X}^i + \mu\sum_{i=0}^{2^{n-2}-1} rq_i\overline{X}^{2^{n-2}}\overline{X}^i\\
&\quad + \mu\sum_{i=0}^{2^{n-2}-1} rq_i\overline{X}^{2^{n-2}}\overline{X}^{2^{n-2}+i}\\
&= \lambda\sum_{i=0}^{2^{n-1}-1} rq_i\overline{X}^i - \mu\sum_{i=0}^{2^{n-2}-1} rq_i\overline{X}^i - \mu\sum_{i=2^{n-2}}^{2^{n-1}-1} rq_i\overline{X}^i\\
&= \lambda\sum_{i=0}^{2^{n-1}-1} rq_i\overline{X}^i - \mu\sum_{i=0}^{2^{n-1}-1} rq_i\overline{X}^i\\
&= (\lambda-\mu)\sum_{i=0}^{2^{n-1}-1} rq_i\overline{X}^i\\
&= \sum_{i=0}^{2^{n-1}-1} (\lambda r-\mu r)\, q_i\overline{X}^i\\
&= \varphi\Big(\sum_{i=0}^{2^{n-1}-1} q_i\overline{X}^i, \lambda r-\mu r\Big)\\
&= \varphi\big(a,(\lambda+\mu x^{2^{n-2}})\cdot r\big)
\end{aligned}$$

Ainsi on a que $\varphi(a\cdot c,b)=\varphi(a,c\cdot b)$, pour tout $a\in\mathbb{Q}A$, $b\in\Omega_{C_2}$ et $c\in\mathbb{Q}C_2$. Donc il existe un unique homomorphisme de groupes $\widetilde{\varphi}:\mathbb{Q}A\otimes_{\mathbb{Q}C_2}\Omega_{C_2}\to K$ tel que $\widetilde{\varphi}\,(a\otimes b)=\varphi(a,b)$, pour tout $a\in\mathbb{Q}A$ et $b\in\Omega_{C_2}$. On peut de plus vérifier que $\widetilde{\varphi}$ est une application $\mathbb{Q}$-linéaire surjective. Or on a déjà vu que $\mathbb{Q}A\otimes_{\mathbb{Q}C_2}\Omega_{C_2}$ et K sont des $\mathbb{Q}$-espaces vectoriels de même dimension donc $\widetilde{\varphi}$ est un isomorphisme de $\mathbb{Q}$-espaces vectoriels. On va maintenant montrer que c'est même un isomorphisme de $\mathbb{Q}A$-modules. Il suffit de vérifier que $\widetilde{\varphi}\,(x(a\otimes r))=x\widetilde{\varphi}\,(a\otimes r)$ pour tout $a\in\mathbb{Q}A$ et $r\in\Omega_{C_2}$. Soit

$a = \sum_{i=0}^{2^{n-1}-1} q_i x^i \in \mathbb{Q}A$ et $r \in \Omega_{C_2}$. Alors

$$\begin{aligned}
\widetilde{\varphi}\big(x \cdot (a \otimes r)\big) &= \widetilde{\varphi}\Big(\Big(\sum_{i=0}^{2^{n-1}-1} q_i x^{i+1}\Big) \otimes r\Big) \\
&= \widetilde{\varphi}\Big(\Big(q_{2^{n-1}-1} + \sum_{i=0}^{2^{n-1}-2} q_i x^{i+1}\Big) \otimes r\Big) \\
&= r q_{2^{n-1}-1} + \sum_{i=0}^{2^{n-1}-2} r q_i \overline{X}^{i+1} \\
&= r q_{2^{n-1}-1} \overline{X}^{2^{n-1}} + \sum_{i=0}^{2^{n-1}-2} r q_i \overline{X}^{i+1} \\
&= \sum_{i=0}^{2^{n-1}-1} r q_i \overline{X}^{i+1} \\
&= \overline{X} \sum_{i=0}^{2^{n-1}-1} r q_i \overline{X}^{i} \\
&= \overline{X} \widetilde{\varphi}\Big(\Big(\sum_{i=0}^{2^{n-1}-1} q_i \overline{X}^{i}\Big) \otimes r\Big) \\
&= x \cdot \widetilde{\varphi}(a \otimes r).
\end{aligned}$$

En résumé, on a obtenu que $\mathbb{Q}A \otimes_{\mathbb{Q}C_2} \Omega_{C_2}$ et K sont des $\mathbb{Q}A$-modules isomorphes.

On remarque que tout élément de $\mathbb{Q}A \otimes_{\mathbb{Q}C_2} \Omega_{C_2}$ peut s'écrire sous la forme $d \otimes 1$, où $d \in \mathbb{Q}A$:

$$\begin{aligned}
\sum_{j=1}^{m} \Big(\Big(\sum_{i=0}^{2^{n-1}-1} q_{ij} x^i\Big) \otimes r_j\Big) &= \sum_{j=1}^{m} \Big(\Big(\sum_{i=0}^{2^{n-1}-1} q_{ij} r_j x^i\Big) \otimes 1\Big) \\
&= \Big(\sum_{j=1}^{m} \sum_{i=0}^{2^{n-1}-1} q_{ij} r_j x^i\Big) \otimes 1 \\
&= \underbrace{\Big(\sum_{i=0}^{2^{n-1}-1} \Big(\sum_{j=1}^{m} q_{ij} r_j\Big) x^i\Big)}_{\in \mathbb{Q}A} \otimes 1
\end{aligned}$$

Soit $K \oplus KY$ le K-espace vectoriel de base $(1, Y)$. On définit l'application $f : V \to K \oplus KY$ par

$$f(v) = \widetilde{\varphi}(d \otimes 1) \oplus \widetilde{\varphi}\Big(\widetilde{d} \otimes 1\Big) Y,$$

où $v \in V$ et $d, \widetilde{d} \in \mathbb{Q}A$ sont tels que $v = (d \otimes 1) \oplus (\widetilde{d}y \otimes 1)$. Par le fait que φ est un isomorphisme de $\mathbb{Q}$-espaces vectoriels, f est un aussi un isomorphisme de $\mathbb{Q}$-espaces vectoriels. On va montrer que f est un isomorphisme de $\mathbb{Q}P$-modules. Pour cela, il va falloir munir $K \oplus KY$ d'une structure de $\mathbb{Q}P$-module. On définit maintenant l'automorphisme de corps $\sigma : K \to K$ par $\sigma(\overline{X}) = \overline{X}^{-1}$. Alors on définit sur $K \oplus KY$ l'action de x par la multiplication par $\overline{X}$ et celle de y par

$$y \cdot (a + bY) = -\sigma(b) + \sigma(a)Y, \text{ pour tout } a, b \in K$$

(ainsi l'action de A correspond à la restriction de l'action de P sur K au sous-groupe A). On peut alors vérifier que $K \oplus KY$ est un $\mathbb{Q}P$-module.

On va maintenant étudier $f : V \to K \oplus KY$. Soit $v \in V$ et $d = \sum_{i=0}^{2^{n-1}-1} q_i x^i, \widetilde{d} = \sum_{i=0}^{2^{n-1}-1} \widetilde{q}_i x^i \in \mathbb{Q}A$ tels que $v = (d \otimes 1) \oplus \Big(\widetilde{d}y \otimes 1\Big)$. Alors

$$\begin{aligned}
f\left(x \cdot v\right) &= f\Big(x\big(d \otimes 1\big) \oplus \big((x\widetilde{d})y \otimes 1\big)\Big) \\
&= \widetilde{\varphi}\big(x(d \otimes 1)\big) \oplus \widetilde{\varphi}\big(x(\widetilde{d} \otimes 1)\big)Y \\
&= \overline{X}\widetilde{\varphi}(d \otimes 1) \oplus \overline{X}\widetilde{\varphi}(\widetilde{d} \otimes 1)Y \\
&= \overline{X}\big(\widetilde{\varphi}(d \otimes 1) \oplus \widetilde{\varphi}(\widetilde{d} \otimes 1)Y\big) \\
&= \overline{X}\Big(f\big((d \otimes 1) \oplus (\widetilde{d}y \otimes 1)\big)\Big) \\
&= x \cdot \big(f(v)\big)
\end{aligned}$$

et

$$\begin{aligned}
f(y \cdot v) &= f\Bigg(\Big(y \sum_{i=0}^{2^{n-1}-1} q_i x^i \otimes 1\Big) \oplus \Big(y \sum_{i=0}^{2^{n-1}-1} \widetilde{q}_i x^i y \otimes 1\Big)\Bigg) \\
&= f\Bigg(\Big(\sum_{i=0}^{2^{n-1}-1} q_i \underbrace{yx^iy^{-1}}_{=\, x^{-i}} y \otimes 1\Big) \oplus \Big(\sum_{i=0}^{2^{n-1}-1} \widetilde{q}_i \underbrace{yx^iy^{-1}}_{=\, x^{-i}} \underbrace{y^2}_{=\, x^{2^{n-2}}} \otimes 1\Big)\Bigg) \\
&= f\Bigg(\Big(x^{2^{n-2}} \sum_{i=0}^{2^{n-1}-1} \widetilde{q}_i x^{2^{n-1}-i} \otimes 1\Big) \oplus \Big(\sum_{i=0}^{2^{n-1}-1} q_i x^{2^{n-1}-i} y \otimes 1\Big)\Bigg) \\
&= \widetilde{\varphi}\Big(x^{2^{n-2}} \sum_{i=0}^{2^{n-1}-1} \widetilde{q}_i x^{2^{n-1}-i} \otimes 1\Big) \oplus \widetilde{\varphi}\Big(\sum_{i=0}^{2^{n-1}-1} q_i x^{2^{n-1}-i} \otimes 1\Big)Y \\
&= x^{2^{n-2}} \cdot \widetilde{\varphi}\Big(\sum_{i=0}^{2^{n-1}-1} \widetilde{q}_i x^{2^{n-1}-i} \otimes 1\Big) \oplus \widetilde{\varphi}\Big(\sum_{i=0}^{2^{n-1}-1} q_i x^{2^{n-1}-i} \otimes 1\Big)Y
\end{aligned}$$

$$
\begin{aligned}
f(y\cdot v) &= -\sum_{i=0}^{2^{n-1}-1}\widetilde{q_i}\overline{X}^{2^{n-1}-i}\oplus\sum_{i=0}^{2^{n-1}-1}q_i\overline{X}^{2^{n-1}-i}Y\\
&= -\sum_{i=0}^{2^{n-1}-1}\widetilde{q_i}\overline{X}^{-i}\oplus\sum_{i=0}^{2^{n-1}-1}q_i\overline{X}^{-i}Y\\
&= -\sigma\Big(\sum_{i=0}^{2^{n-1}-1}\widetilde{q_i}\overline{X}^{i}\Big)\oplus\sigma\Big(\sum_{i=0}^{2^{n-1}-1}q_i\overline{X}^{i}\Big)Y\\
&= y\cdot\Big(\sum_{i=0}^{2^{n-1}-1}q_i\overline{X}^{i}\oplus\sum_{i=0}^{2^{n-1}-1}\widetilde{q_i}\overline{X}^{i}Y\Big)\\
&= y\cdot\left(\widetilde{\varphi}\Big(\sum_{i=0}^{2^{n-1}-1}q_ix^i\otimes 1\Big)\oplus\widetilde{\varphi}\Big(\sum_{i=0}^{2^{n-1}-1}\widetilde{q_i}x^i\otimes 1\Big)Y\right)\\
&= y\cdot\left(f\Big(\Big(\sum_{i=0}^{2^{n-1}-1}q_ix^i\otimes 1\Big)\oplus\Big(\sum_{i=0}^{2^{n-1}-1}\widetilde{q_i}x^iy\otimes 1\Big)\Big)\right)\\
&= y\cdot f\big((d\otimes 1)\oplus(\widetilde{d}y\otimes 1)\big) = y\cdot f\left(v\right).
\end{aligned}
$$

Donc f est bien un isomorphisme de $\mathbb{Q}P$-modules et on peut identifier V à $K\oplus KY$.

On va maintenant munir V d'une structure de $\mathbb{Q}$-algèbre : On définit la multiplication dans V par :

$$(a+bY)(c+dY) = ac - b\sigma(d) + (ad+b\sigma(c))Y, \quad \forall\ a,b,c,d\in K.$$

Alors V est bien une $\mathbb{Q}$-algèbre et de plus, l'action de x et et celle de y correspondent respectivement à la multiplication par $\overline{X}$ et Y dans V. Ainsi, si on montre que V est un corps gauche, cela prouvera que c'est un $\mathbb{Q}P$-module irréductible (car comme toute multiplication à gauche correspond à l'action d'un élément de $\mathbb{Q}P$, un $\mathbb{Q}P$-sous-module de V est un idéal de V). Soit $a,b\in K$. Alors

$$(a+bY)(\sigma(a)-bY) = a\sigma(a)+b\sigma(b)\in K$$

et donc $(a+bY)$ est inversible si $a\sigma(a)+b\sigma(b)$ est inversible ce qui est le cas si et seulement si $a\sigma(a)-b\sigma(b)$ est non-nul dans K. Or si $a=\sum_{i=0}^{2^{n-1}-1}a_ix^i$ et $b=\sum_{j=0}^{2^{n-1}-1}b_jx^j$, alors le coefficient de $1=x^0$ dans $a\sigma(a)+b\sigma(b)$ est

$$\sum_{i=0}^{2^{n-1}-1}a_i^2+\sum_{j=0}^{2^{n-1}-1}b_j^2$$

et est donc non-nul si $a+bY$ est non-nul. Ainsi on a obtenu que si $a+bY\in V$ est non-nul alors $a+bY$ est inversible, c'est-à-dire que V est un corps gauche et donc qu'il est irréductible. □

Remarques 4.12

i) La preuve de ce théorème se base sur la fin de la preuve du théorème 1 de l'article *A remark on a theorem of Ritter and Segal* de Serge Bouc, [Bou01].

ii) Dans la preuve du théorème 4.11, on n'utilise pas la même méthode que pour les deux théorèmes précédents (théorèmes 4.8 et 4.10). Cela vient du fait que vu dans $\mathbb{C}$, l'unique $\mathbb{Q}Q_{2^n}$-module irréductible et fidèle est la somme de deux fois certains des $\mathbb{C}Q_{2^n}$-modules irréductibles et non pas seulement une fois. Cela fait que l'on ne peut pas appliquer la théorie de Galois pour ce cas.

Théorème 4.13 *Soit P un p-groupe fini de p-rang normal 1, ou P est le groupe diédral D_8. Alors P possède un unique $\mathbb{Q}P$-module irréductible et fidèle, noté Φ_P , dont le caractère χ_P est donnée par :*

- *Si $P = C_{p^n} = \langle x \,|\, x^{p^n} = 1\rangle$, alors*

$$\chi_P(x^i) = \begin{cases} (p-1)p^{n-1} & si\ i = 0 \\ -p^{n-1} & si\ p^{n-1} \mid i\ et\ i \neq 0 \\ 0 & sinon, \end{cases}$$

  pour tout $0 \leq i \leq p^n - 1$.

- *Si $P = Q_{2^n} = \langle x, y \,|\, x^{2^{n-1}} = 1, x^{2^{n-2}} = y^2, yxy = x^{-1}\rangle$, alors*

$$\chi_P(g) = \begin{cases} 2^{n-1} & si\ g = 1 \\ -2^{n-1} & si\ g = x^{2^{n-2}} \\ 0 & sinon, \end{cases}$$

  pour tout $g \in Q_{2^n}$.

- *Si $P = D_{2^n} = \langle x, y \,|\, x^{2^{n-1}} = y^2 = 1, yxy = x^{-1}\rangle$, alors*

$$\chi_P(g) = \begin{cases} 2^{n-2} & si\ g = 1 \\ -2^{n-2} & si\ g = x^{2^{n-2}} \\ 0 & sinon, \end{cases}$$

  pour tout $g \in D_{2^n}$.

- *Si $P = SD_{2^n} = \langle x, y \,|\, x^{2^{n-1}} = y^2 = 1, yxy = x^{2^{n-2}-1}\rangle$, alors*

$$\chi_P(g) = \begin{cases} 2^{n-2} & si\ g = 1 \\ -2^{n-2} & si\ g = x^{2^{n-2}} \\ 0 & sinon, \end{cases}$$

  pour tout $g \in SD_{2^n}$.

Preuve: C'est une conséquence du théorème 4.5 et des preuves des théorèmes 4.8, 4.11 et 4.10. □

Corollaire 4.14 *Soit P un p-groupe fini de p-rang normal 1 d'ordre p^n ou P est le groupe diédral D_8. Alors*

$$\dim_{\mathbb{Q}} \Phi_P = \begin{cases} (p-1)p^{n-1} & \text{si } P \cong C_{p^n} \text{ ou } P \cong Q_{2^n} \\ 2^{n-2} & \text{si } P \cong D_{2^n} \text{ ou } P \cong SD_{2^n} \end{cases}.$$

Preuve: C'est une conséquence du fait que $\dim_{\mathbb{Q}} \Phi_P = \chi_P(1_P)$ et du théorème 4.13. □

Proposition 4.15 *Soit P un p-groupe fini de p-rang normal 1 ou P est le groupe diédral D_8. Alors*

$$\langle \chi_P, \chi_P \rangle_P = \begin{cases} p^{n-1}(p-1) & \text{si } P \cong C_{p^n} \text{ ou } P \cong Q_{2^n} \\ 2^{n-3} & \text{si } P \cong D_{2^n} \text{ ou } P \cong SD_{2^n} \end{cases}.$$

Preuve: Par le théorème 4.5, il y a quatre cas à traiter :

- Il existe $n \in \mathbb{N}$ tel que $P = C_{p^n}$. Alors, par le théorème 4.13,

$$\begin{aligned} \langle \chi_P, \chi_P \rangle_P &= \frac{1}{|P|} \sum_{g \in P} \chi(g)\overline{\chi(g)} \\ &= \frac{1}{p^n} \sum_{i=0}^{p^n-1} \chi(x^i)\chi(x^i) \\ &= \frac{1}{p^n} \left((p-1)^2 p^{2(n-1)} + \sum_{i=1}^{p-1} p^{2(n-1)} \right) \\ &= \frac{p^{2n-2}}{p^n}(p^2 - 2p + 1 + p - 1) \\ &= p^{n-2}(p^2 - p) = p^{n-1}(p-1). \end{aligned}$$

- Il existe $n \in \mathbb{N}$, $n \geq 3$ tel que $P = Q_{2^n}$. Alors, par le théorème 4.13,

$$\begin{aligned} \langle \chi_P, \chi_P \rangle_P &= \frac{1}{|P|} \sum_{g \in P} \chi(g)\overline{\chi(g)} \\ &= \frac{1}{2^n} \left(2^{2(n-1)} + 2^{2(n-1)} \right) \\ &= \frac{2^{2n-1}}{2^n} = 2^{n-1}. \end{aligned}$$

- Il existe $n \in \mathbb{N}$, $n \geq 3$ (pour inclure le cas où $P = D_8$) tel que $P = D_{2^n}$. Alors, par le théorème 4.13,

$$\begin{aligned} \langle \chi_P, \chi_P \rangle_P &= \frac{1}{|P|} \sum_{g \in P} \chi(g)\overline{\chi(g)} \\ &= \frac{1}{2^n} \left(2^{2(n-2)} + 2^{2(n-2)} \right) \\ &= \frac{2^{2n-3}}{2^n} = 2^{n-3}. \end{aligned}$$

- Il existe $n \in \mathbb{N}$, $n \geq 4$ tel que $P = SD_{2^n}$. Alors, par le théorème 4.13,

$$\begin{aligned}\langle \chi_P, \chi_P \rangle_P &= \frac{1}{|P|} \sum_{g \in P} \chi(g)\overline{\chi(g)} \\ &= \frac{1}{2^n}\left(2^{2(n-2)} + 2^{2(n-2)}\right) \\ &= \frac{2^{2n-3}}{2^n} = 2^{n-3}.\end{aligned}$$

□

Lemme 4.16 *Soit P un p-groupe fini et non-trivial de p-rang normal 1 et H un sous-groupe maximal de P. Alors :*

i) $\mathrm{Res}_H^P \Phi_P = (p-1)\Phi_H$ *si* $|P| = p$.

ii) $\mathrm{Res}_H^P \Phi_P = p\Phi_H$ *si P est cyclique ou quaternionien généralisé.*

iii) $\mathrm{Res}_H^P \Phi_P = 2\Phi_H$ *si P est diédral ou semi-diédral et H est diédral.*

iv) $\mathrm{Res}_H^P \Phi_P = \Phi_H$ *si P est diédral ou semi-diédral et H est cyclique ou quaternionien généralisé.*

Preuve: Il suffit de montrer ces relations pour les caractères. Pour cela, on va utiliser le théorème 4.13.

i) Si $|P| = p$, alors $P \cong C_p$ et $H = \{1\}$. On a

$$\chi_P(g) = \begin{cases} p-1 & \text{si } g = 1 \\ -1 & \text{sinon} \end{cases}$$

Ainsi $\chi_P(1) = p - 1 = (p-1)\chi_H(1)$ et donc $\mathrm{Res}_H^P \chi_P = (p-1)\chi_H$.

ii) On suppose maintenant que P est isomorphe à $C_{p^n} = \langle x \,\big|\, x^{p^n} = 1 \rangle$, $n \geq 2$. Alors $H = \langle x^p \rangle$ est un groupe cyclique d'ordre p^{n-1}. On a

$$\chi_P(x^i) = \begin{cases} (p-1)p^{n-1} & \text{si } i = 0 \\ -p^{n-1} & \text{si } p^{n-1} \mid i \text{ et } i \neq 0 \\ 0 & \text{sinon} \end{cases},$$

pour tout $0 \leq i \leq p^n - 1$. Ainsi, si $y = x^p$ et $0 \leq j \leq p^n - 1$,

$$\chi_P(y^j) = \left\{ \begin{array}{ll} (p-1)p^{n-1} & \text{si } j = 0 \\ -p^{n-1} & \text{si } p^{n-2} \mid j \text{ et } j \neq 0 \\ 0 & \text{sinon} \end{array} \right\} = p\chi_H(y^j).$$

Donc $\mathrm{Res}_H^P \chi_P = p\chi_H$.

On suppose maintenant que P est le groupe des quaternions $Q_8 = \langle x, y \,\big|\, x^4 = 1, x^2 = y^2, yxy^{-1} = x^{-1} \rangle$. Alors H est l'un des trois sous-groupes cycliques d'ordre 4 suivants :

$$H_1 = \langle x \rangle \qquad H_2 = \langle y \rangle \qquad H_2 = \langle xy \rangle.$$

Par le théorème 4.13, on a

$$\chi_P(g) = \begin{cases} 2^{n-1} & \text{si } g = 1 \\ -2^{n-1} & \text{si } g = x^2 \\ 0 & \text{sinon} \end{cases},$$

$g \in Q_8$. On voit alors facilement que $\mathrm{Res}^P_{H_i} \chi_P = 2\chi_{H_i}$, pour tout $i = 1, 2, 3$.

On suppose pour finir que P est un groupe des quaternions généralisés $Q_{2^n} = \langle x, y \,\big|\, x^{2^{n-1}} = 1, y^2 = x^{2^{n-2}}, yxy^{-1} = x^{-1} \rangle$, $n \geq 4$. On a

$$\chi_P(g) = \begin{cases} 2^{n-1} & \text{si } g = 1 \\ -2^{n-1} & \text{si } g = x^{2^{n-2}} \\ 0 & \text{sinon} \end{cases},$$

$g \in Q_{2^n}$. Par le lemme 4.6, il y a trois possibilités pour H :

- Le groupe cyclique $H_1 = \langle x \rangle$ d'ordre 2^{n-1} : Soit $0 \leq i \leq 2^{n-1} - 1$, alors

$$\chi_P(x^i) = \left\{ \begin{array}{ll} 2^{n-1} & \text{si } i = 0 \\ -2^{n-1} & \text{si } 2^{n-2} | i \text{ et } i \neq 0 \\ 0 & \text{sinon} \end{array} \right\} = 2\chi_{H_1}(x^i),$$

  donc $\mathrm{Res}^P_{H_1} \chi_P = 2\chi_{H_1}$.

- Le groupe des quaternions généralisés $H_2 = \langle x^2, y \rangle$ d'ordre 2^{n-1} : Soit $g \in H_2$, alors

$$\chi_P(g) = \left\{ \begin{array}{ll} 2^{n-1} & \text{si } g = 1 \\ -2^{n-1} & \text{si } g = (x^2)^{2^{n-3}} \\ 0 & \text{sinon} \end{array} \right\} = 2\chi_{H_2}(g),$$

  donc $\mathrm{Res}^P_{H_2} \chi_P = 2\chi_{H_2}$.

- Le groupe des quaternions généralisés $H_3 = \langle x^2, xy \rangle$ d'ordre 2^{n-1} : Soit $g \in H_3$, alors

$$\chi_P(g) = \left\{ \begin{array}{ll} 2^{n-1} & \text{si } g = 1 \\ -2^{n-1} & \text{si } g = (x^2)^{2^{n-3}} \\ 0 & \text{sinon} \end{array} \right\} = 2\chi_{H_3}(g),$$

  donc $\mathrm{Res}^P_{H_3} \chi_P = 2\chi_{H_3}$.

iii) On suppose que P est le groupe diédral

$$D_{2^n} = \langle x, y \,\big|\, x^{2^{n-1}} = y^2 = 1, yxy = x^{-1} \rangle,$$

$n \geq 4$ et H est aussi un groupe diédral. Alors par le théorème 4.13, on a

$$\chi_P(g) = \begin{cases} 2^{n-2} & \text{si } g = 1 \\ -2^{n-2} & \text{si } g = x^{2^{n-2}} \\ 0 & \text{sinon} \end{cases},$$

$g \in D_{2^n}$. Il y a deux possibilités pour H :

- Le groupe diédral $H_1 = \langle x^2, y\rangle$ d'ordre 2^{n-1} : Soit $g \in H_1$, alors

$$\chi_P(g) = \left\{ \begin{array}{ll} 2^{n-2} & \text{si } g = 1 \\ -2^{n-2} & \text{si } g = (x^2)^{2^{n-3}} \\ 0 & \text{sinon} \end{array} \right\} = 2\chi_{H_1}(g).$$

  Donc $\mathrm{Res}^P_{H_1} \chi_P = 2\chi_{H_1}$.
- Le groupe diédral $H_2 = \langle x^2, yx\rangle$ d'ordre 2^{n-1} : Soit $g \in H_2$, alors

$$\chi_P(g) = \left\{ \begin{array}{ll} 2^{n-2} & \text{si } g = 1 \\ -2^{n-2} & \text{si } g = (x^2)^{2^{n-3}} \\ 0 & \text{sinon} \end{array} \right\} = 2\chi_{H_2}(g).$$

  Donc $\mathrm{Res}^P_{H_2} \chi_P = 2\chi_{H_2}$.

On suppose que P est le groupe semi-diédral

$$SD_{2^n} = \langle x, y \,\big|\, x^{2^{n-1}} = y^2 = 1, yxy = x^{2^{n-2}-1}\rangle,$$

$n \geq 4$ et H est un groupe diédral. Alors par le théorème 4.13, on a

$$\chi_P(g) = \left\{ \begin{array}{ll} 2^{n-2} & \text{si } g = 1 \\ -2^{n-2} & \text{si } g = x^{2^{n-2}} \\ 0 & \text{sinon} \end{array} \right. ,$$

$g \in D_{2^n}$. Il y a une seule possibilité pour H : C'est le groupe diédral $\langle x^2, y\rangle$ d'ordre 2^{n-1}. Soit $g \in H$, alors

$$\chi_P(g) = \left\{ \begin{array}{ll} 2^{n-2} & \text{si } g = 1 \\ -2^{n-2} & \text{si } g = (x^2)^{2^{n-3}} \\ 0 & \text{sinon} \end{array} \right\} = 2\chi_H(g).$$

Donc $\mathrm{Res}^P_H \chi_P = 2\chi_H$.

iv) On suppose que P est le groupe diédral

$$D_{2^n} = \langle x, y \,\big|\, x^{2^{n-1}} = y^2 = 1, yxy = x^{-1}\rangle,$$

$n \geq 4$ et H est aussi un groupe cyclique. Alors par le théorème 4.13, on a

$$\chi_P(g) = \left\{ \begin{array}{ll} 2^{n-2} & \text{si } g = 1 \\ -2^{n-2} & \text{si } g = x^{2^{n-2}} \\ 0 & \text{sinon} \end{array} \right. ,$$

$g \in D_{2^n}$. Il y a une seule possibilité pour H : C'est le groupe cyclique $\langle x\rangle$ d'ordre 2^{n-1}. Soit $0 \leq i \leq 2^{n-1} - 1$, alors

$$\chi_P(x^i) = \left\{ \begin{array}{ll} 2^{n-2} & \text{si } i = 0 \\ -2^{n-2} & \text{si } 2^{n-2} | i \text{ et } i \neq 0 \\ 0 & \text{sinon} \end{array} \right\} = \chi_H(x^i).$$

Donc $\mathrm{Res}_H^P \chi_P = \chi_H$.
On suppose que P est le groupe semi-diédral

$$SD_{2^n} = \langle x, y \,\big|\, x^{2^{n-1}} = y^2 = 1, yxy = x^{2^{n-2}-1} \rangle$$

$n \geq 4$ et H est un groupe cyclique ou quaternionien généralisé. Alors par le théorème 4.13, on a

$$\chi_P(g) = \begin{cases} 2^{n-2} & \text{si } g = 1 \\ -2^{n-2} & \text{si } g = x^{2^{n-2}} \\ 0 & \text{sinon} \end{cases},$$

$g \in D_{2^n}$. Il y a deux possibilités pour H :

- Le groupe cyclique $H_1 = \langle x \rangle$ d'ordre 2^{n-1} : Soit $0 \leq i \leq 2^{n-1} - 1$, alors

  $$\chi_P(x^i) = \left\{ \begin{array}{ll} 2^{n-2} & \text{si } i = 0 \\ -2^{n-2} & \text{si } 2^{n-2} | i \text{ et } i \neq 0 \\ 0 & \text{sinon} \end{array} \right\} = \chi_{H_1}(x^i).$$

  Donc $\mathrm{Res}_{H_1}^P \chi_P = \chi_{H_1}$.
- Le groupe des quaternions généralisés $H_2 = \langle x^2, yx \rangle$ d'ordre 2^{n-1} : Soit $g \in H_2$, alors

  $$\chi_P(g) = \left\{ \begin{array}{ll} 2^{n-2} & \text{si } g = 1 \\ -2^{n-2} & \text{si } g = (x^2)^{2^{n-3}} \\ 0 & \text{sinon} \end{array} \right\} = \chi_{H_2}(g).$$

  Donc $\mathrm{Res}_{H_2}^P \chi_P = \chi_{H_2}$.

□

Chapitre 5

Les sous-groupes génétiques

On a maintenant introduit toutes les notions nécessaires pour prouver le théorème de Roquette et introduire la notion de sous-groupe génétique. On va ensuite prouver plusieurs lemmes techniques qui vont permettre de donner une description des sous-groupes génétiques qui n'utilise que des propriétés sur les groupes et non plus des propriétés sur les $\mathbb{Q}G$-modules. On va finir sur un théorème qui donne des conditions pour que deux sous-groupes génétiques donnent le même $\mathbb{Q}G$-module, ce qui va permettre d'introduire la notion de base génétique.

5.1 Le théorème de Roquette et ses conséquences

Lemme 5.1 *Soit G un groupe fini, (T,S) une section de G, W un $\mathbb{Q}(T/S)$-module (de dimension finie) et $V = \mathrm{Indinf}_{T/S}^{G} W$. Soit χ le caractère de W et $\eta = \mathrm{Indinf}_{T/S}^{G} \chi$ le caractère de V. Alors on a un isomorphisme de $\mathbb{Q}$-algèbres*

$$\mathrm{Hom}_{\mathbb{Q}G}(V,V) \cong \mathrm{Hom}_{\mathbb{Q}(T/S)}(W,W)$$

si et seulement si

$$\langle \eta, \eta \rangle_G = \langle \chi, \chi \rangle_{T/S}$$

.

Preuve:

$\Leftarrow$: On définit l'application

$$\alpha : \mathrm{Hom}_{\mathbb{Q}(T/S)}(W,W) \to \mathrm{Hom}_{\mathbb{Q}(T/S)}(\mathrm{Inf}_{T/S}^{T} W, \mathrm{Inf}_{T/S}^{T} W)$$

où $\alpha(f) : \mathrm{Inf}_{T/S}^{T} W \to \mathrm{Inf}_{T/S}^{T} W$ est définie par $\alpha(f)(w) = f(w)$, pour tout $w \in \mathrm{Inf}_{T/S}^{T} W$ et $f \in \mathrm{Hom}_{\mathbb{Q}(T/S)}(W,W)$ (où on identifie W et $\mathrm{Inf}_{T/S}^{T} W$ comme $\mathbb{Q}$-espaces vectoriels). Un peu de calcul permet de vérifier que c'est un homomorphisme de $\mathbb{Q}$-algèbres injectif.

On définit aussi l'application

$$\beta : \mathrm{Hom}_{\mathbb{Q}T}(\mathrm{Inf}_{T/S}^{T} W, \mathrm{Inf}_{T/S}^{T} W) \to \mathrm{Hom}_{\mathbb{Q}G}(V, V)$$

où $\beta(f) : V \to V$ est définie par $\beta(f)(x \otimes w) = x \otimes f(w)$, pour tout $x \in \mathbb{Q}G$, $w \in \mathrm{Inf}_{T/S}^{T} W$ et $f \in \mathrm{Hom}_{\mathbb{Q}T}(\mathrm{Inf}_{T/S}^{T} W, \mathrm{Inf}_{T/S}^{T} W)$, où $V = \mathbb{Q}G \otimes_{\mathbb{Q}T} \mathrm{Inf}_{T/S}^{T} W$. On peut vérifier que c'est une application bien définie et que de plus, c'est un homomorphisme de $\mathbb{Q}$-algèbres injectif. Pour finir, on définit l'application

$$\varphi : \mathrm{Hom}_{\mathbb{Q}(T/S)}(W, W) \to \mathrm{Hom}_{\mathbb{Q}G}(V, V)$$

par $\varphi = \beta \circ \alpha$. C'est un homomorphisme de $\mathbb{Q}$-algèbres injectif de $\mathrm{Hom}_{\mathbb{Q}(T/S)}(W, W)$ dans $\mathrm{Hom}_{\mathbb{Q}P}(V, V)$. Si on montre que $\mathrm{Hom}_{\mathbb{Q}(T/S)}(W, W)$ et $\mathrm{Hom}_{\mathbb{Q}G}(V, V)$ sont de même dimension sur $\mathbb{Q}$, alors φ sera un isomorphisme. Or, par le lemme B.18,

$$\begin{aligned} \dim_{\mathbb{Q}} \mathrm{Hom}_{\mathbb{Q}G}(V, V) &= \langle \eta, \eta \rangle_G \\ &= \langle \chi, \chi \rangle_{T/S} \\ &= \dim_{\mathbb{Q}} \mathrm{Hom}_{\mathbb{Q}(T/S)}(W, W) \end{aligned}$$

ce qui permet de conclure que φ est un isomorphisme de $\mathbb{Q}$-algèbres.

$\Rightarrow$: Par le lemme B.18, on a

$$\begin{aligned} \langle \eta, \eta \rangle_G &= \dim_{\mathbb{Q}} \mathrm{Hom}_{\mathbb{Q}G}(V, V) \\ &= \dim_{\mathbb{Q}} \mathrm{Hom}_{\mathbb{Q}(T/S)}(W, W) \\ &= \langle \chi, \chi \rangle_{T/S} \end{aligned}$$

□

Théorème 5.2: Théorème de Roquette ([Bou], théorème 9.4.1, page 173)
Soit P un p-groupe fini et V un $\mathbb{Q}P$-module irréductible (de dimension finie). Alors il existe une section (T, S) de P et un $\mathbb{Q}(T/S)$-module W (de dimension finie) irréductible et fidèle tels que :

i) Le module V est isomorphe à $\mathrm{Indinf}_{T/S}^{P} W$.

ii) Cette isomorphisme induit un isomorphisme de $\mathbb{Q}$-algèbres

$$\mathrm{Hom}_{\mathbb{Q}P}(V, V) \cong \mathrm{Hom}_{\mathbb{Q}(T/S)}(W, W).$$

iii) Le groupe T/S est de p-rang normal 1.

Preuve: On va faire une preuve par récurrence sur P.

- Si $|P| = 1$, il suffit de prendre $T = S = 1$.

- Si $|P| = p$, alors $P = C_p$ et on connaît la table de caractère de P sur $\mathbb{Q}$ (exemple 2.11). Il y a deux cas :
  i) Soit V est le $\mathbb{Q}P$-module trivial et on peut prendre $T = S = P$. Alors $T/S = \mathbf{1}$ est bien un groupe de p-rang normal 1, $V = \mathbb{Q} = \mathrm{Indinf}_{T/S}^{P} \mathbb{Q}$, et $\mathbb{Q}$ est l'unique module irréductible et fidèle du groupe $\mathbf{1}$. De plus, comme $\langle \mathbb{Q}, \mathbb{Q} \rangle_{\mathbf{1}} = 1 = \langle V, V \rangle_P$, par le lemme 5.1, on a bien que $\mathrm{Hom}_{\mathbb{Q}P}(V, V) = \mathrm{Hom}_{\mathbb{Q}\mathbf{1}}(\mathbb{Q}, \mathbb{Q})$.
  ii) Soit V est le seul $\mathbb{Q}P$-module irréductible et fidèle et on peut prendre $T = P$ et $S = 1_P$. Alors $T/S = P = C_p$ est un groupe de p-rang normal 1, $V = \mathrm{Indinf}_{T/S}^{P} V$ et $\mathrm{Hom}_{\mathbb{Q}P}(V, V) = \mathrm{Hom}_{\mathbb{Q}(T/S)}(V, V)$.
- On suppose maintenant que $|P| \geq p^2$ et que le résultat est vérifié pour tout p-groupe d'ordre $< |P|$. On va considérer deux cas :
  i) Le $\mathbb{Q}P$-module V n'est pas fidèle. Soit χ le caractère de V. On pose $N = \mathrm{Ker}\, \chi \neq \mathbf{1}$. Alors il existe un $\mathbb{Q}(P/N)$-module irréductible et fidèle $\widetilde{V}$ tel que $V = \mathrm{Inf}_{P/N}^{P} \widetilde{V}$. Or $|P/N| < |P|$ donc par hypothèse de récurrence, il existe une section $(\widetilde{T}, \widetilde{S})$ de P/N et W un $\mathbb{Q}(\widetilde{T}/\widetilde{S})$-module irréductible et fidèle tels que
     (a) Le module $\widetilde{V}$ est isomorphe à $\mathrm{Indinf}_{\widetilde{T}/\widetilde{S}}^{P/N} W$.
     (b) Cette isomorphisme induit un isomorphisme de $\mathbb{Q}$-algèbres
     $$\mathrm{Hom}_{\mathbb{Q}(P/N)}(\widetilde{V}, \widetilde{V}) \cong \mathrm{Hom}_{\mathbb{Q}(\widetilde{T}/\widetilde{S})}(W, W).$$
     (c) Le groupe $\widetilde{T}/\widetilde{S}$ est de p-rang normal 1.

     Soit $\pi : P \to P/N$ la projection canonique. On pose $T = \pi^{-1}(\widetilde{T})$ et $S = \pi^{-1}(\widetilde{S})$. Alors $\widetilde{T} = T/N$, $\widetilde{S} = S/N$ et
     $$\begin{aligned} V &= \mathrm{Inf}_{P/N}^{P} \widetilde{V} \\ &= \mathrm{Inf}_{P/N}^{P} \mathrm{Ind}_{T/N}^{P/N} \mathrm{Inf}_{(T/N)/(S/N)}^{T/N} W \\ &\overset{(1)}{=} \mathrm{Ind}_{T}^{P} \mathrm{Inf}_{T/N}^{T} \mathrm{Inf}_{(T/N)/(S/N)}^{T/N} W \\ &\overset{(2)}{=} \mathrm{Ind}_{T}^{P} \mathrm{Inf}_{T/S}^{T} W \end{aligned}$$
     où l'égalité (1) découle de la proposition B.40 et l'égalité (2) de la transitivité de l'inflation (proposition B.34). De plus T/S est isomorphe à $\widetilde{T}/\widetilde{S}$ ($3^{\text{ème}}$ théorème d'isomorphisme) et est donc de p-rang normal 1.

     Il reste à voir que $\mathrm{Hom}_{\mathbb{Q}P}(V, V) \cong \mathrm{Hom}_{\mathbb{Q}(T/S)}(W, W)$. Or on a $\mathrm{Hom}_{\mathbb{Q}P}(V, V) \cong \mathrm{Hom}_{\mathbb{Q}(P/N)}(\widetilde{V}, \widetilde{V})$ (par le lemme 5.1 et le lemme B.37) et $\mathrm{Hom}_{\mathbb{Q}(P/N)}(\widetilde{V}, \widetilde{V}) \cong \mathrm{Hom}_{\mathbb{Q}(\widetilde{T}/\widetilde{S})}(W, W)$, et donc on a bien $\mathrm{Hom}_{\mathbb{Q}P}(V, V) \cong \mathrm{Hom}_{\mathbb{Q}(T/S)}(W, W)$.

ii) Le $\mathbb{Q}P$-module V est fidèle. Si P est de p-rang normal 1, il suffit de prendre $T = P$ et $S = 1$. On peut donc supposer que P possède un sous-groupe normal E isomorphe à $C_p \times C_p$. Soit V_1 une composante homogène de $\mathrm{Res}^P_E V$. Soit $I = \{x \in P \,\big|\, {}^xV_1 \cong V_1\}$. Alors, par le théorème B.49, V_1 est un $\mathbb{Q}I$-module irréductible et on a $V \cong \mathrm{Ind}^P_I V_1$.
On va commencer par étudier un peu plus I. Si $x \in C_P(E)$, alors ${}^xV_1 \cong V_1$ car ${}^xV_1$ et V_1 sont toujours isomorphes en tant qu'espaces vectoriels et comme x commute avec tous les éléments de E c'est même un isomorphisme de $\mathbb{Q}E$-modules. Ainsi $x \in I$ et donc $C_P(E) \subset I$. On définit l'application $\varphi : P \to \mathrm{Aut}(E)$ par $\varphi(z) = \gamma_z$, où $\gamma_z : E \to E$ est définie par $\gamma_z(e) = zez^{-1}$ pour tout $e \in E$ et pour tout $z \in P$. Si $z \in P$ alors comme $E \trianglelefteq P$, on a bien $\gamma_z \in \mathrm{Aut}(E)$ et donc φ est bien définie. De plus, on peut vérifier que φ est un homomorphisme de groupes et que $\mathrm{Ker}\,\varphi = C_P(E)$. Donc, par le 1$^{\text{er}}$ théorème d'isomorphisme, $P/C_P(E)$ est isomorphe à un sous-groupe de $\mathrm{Aut}(E)$. Or $\mathrm{Aut}(E) = \mathrm{Aut}(C_p \times C_p) \cong \mathrm{Gl}_n(\mathbb{F}_p)$ ([Rot95], exemple 7.4, page 157) et de plus $|\,\mathrm{Gl}_n(\mathbb{F}_p)| = p(p^2-1)(p-1)$. Ainsi $|\,\mathrm{Aut}(E)| = p(p^2-1)(p-1)$ et $|P/C_P(E)|$ est une puissance de p qui divise $|\,\mathrm{Aut}(E)|$ et donc $|P/C_P(E)|$ est égal à 1 ou p. Or $|C_P(E)|$ divise la cardinalité de I donc $|P/I|$ divise $|P/C_P(E)|$. Ainsi P/I est de cardinalité 1 ou p.
On suppose que $I = P$. Alors $V = \mathrm{Ind}^P_I V_1 = V_1$ donc V_1 est un $\mathbb{Q}I$-module fidèle et donc V_1 est aussi un $\mathbb{Q}E$-module fidèle. Or $V_1 = \oplus_{i=1}^s L$, où L est un $\mathbb{Q}E$-sous-module irréductible de $\mathrm{Res}^P_E V$. Donc L est un $\mathbb{Q}E$-module irréductible et fidèle. Cela est impossible car E ne possède pas de module irréductible et fidèle (exemple 2.14). Donc $I \neq P$ et $|P : I| = p$. Alors $I \lhd P$ et on peut appliquer l'hypothèse de récurrence : Il existe une section (T, S) de I et un $\mathbb{Q}(T/S)$-module W irréductible et fidèle tels que :

(a) Le module V_1 est isomorphe à $\mathrm{Indinf}^I_{T/S} W$.

(b) Cette isomorphisme induit un isomorphisme de $\mathbb{Q}$-algèbres

$$\mathrm{Hom}_{\mathbb{Q}I}(V_1, V_1) \cong \mathrm{Hom}_{\mathbb{Q}(T/S)}(W, W).$$

(c) Le groupe T/S est de p-rang normal 1.

Or (T, S) est aussi une section de P et, par la transitivité de l'induction (proposition B.26),

$$\begin{aligned} V &= \mathrm{Ind}^P_I V_1 \\ &= \mathrm{Ind}^P_I \mathrm{Ind}^I_T \mathrm{Inf}^T_{T/S} W \\ &= \mathrm{Ind}^P_T \mathrm{Inf}^T_{T/S} W \end{aligned}$$

Il reste à voir que $\mathrm{Hom}_{\mathbb{Q}P}(V, V) \cong \mathrm{Hom}_{\mathbb{Q}(T/S)}(W, W)$. Comme on sait déjà que $\mathrm{Hom}_{\mathbb{Q}I}(V_1, V_1) \cong \mathrm{Hom}_{\mathbb{Q}(T/S)}(W, W)$, il suffit de

montrer que $\mathrm{Hom}_{\mathbb{Q}P}(V,V) \cong \mathrm{Hom}_{\mathbb{Q}I}(V_1,V_1)$ et alors, par le lemme 5.1, il suffit de voir que $\langle V,V\rangle_P = \langle V_1,V_1\rangle_I$. Soit η le caractère associé au $\mathbb{Q}I$-module V_1 et χ le caractère associé au $\mathbb{Q}P$-module V. Alors, par le théorème de réciprocité de Frobenius (théorème B.30) on a

$$\begin{aligned}
\langle \chi,\chi\rangle_P &= \langle \mathrm{Ind}_I^P \eta, \mathrm{Ind}_I^P \eta\rangle_P \\
&= \langle \eta, \mathrm{Res}_I^P \mathrm{Ind}_I^P \eta\rangle_I \\
&\overset{(1)}{=} \langle \eta, \bigoplus_{x\in[I\backslash P/I]} \mathrm{Ind}^I_{\underbrace{I\cap {}^xI}_{=I}} \mathrm{Iso}(\gamma_x)\,\mathrm{Res}^I_{\underbrace{I\cap {}^xI}_{=I}} \eta\rangle_I \quad \text{car } I \lhd P \\
&= \langle \eta, \bigoplus_{x\in[I\backslash P/I]} \mathrm{Iso}(\gamma_x)\eta\rangle_I \\
&= \langle \eta,\eta\rangle_I + \sum_{\substack{x\in[I\backslash P/I]\\ x\notin I}} \langle \eta, \mathrm{Iso}(\gamma_x)\eta\rangle_I \\
&\overset{(2)}{=} \langle \eta,\eta\rangle_I
\end{aligned}$$

où l'égalité (1) découle de la formule de Mackey (théorème 3.37). L'égalité (2) découle du fait que si $x \in [I\backslash P/I]$ et $x \notin I$, alors $\mathrm{Iso}(\gamma_x)\eta = {}^x\eta$ et η ne sont pas égaux et donc, comme ce sont des caractères irréductibles, cela implique que leur produit scalaire vaut 0.

□

Remarque 5.3 ([Bou], remarque 9.4.2, page 174)

- Dans le théorème précédent, T/S est de p-rang normal 1 et W est un $\mathbb{Q}(T/S)$-module irréductible et fidèle. Or, par le théorème 4.13, T/S possède un unique $\mathbb{Q}(T/S)$-module fidèle et irréductible, $\Phi_{T/S}$. Donc W est isomorphe à $\Phi_{T/S}$.
- Dans la partie *ii)*, comme V et W sont des modules irréductibles, $\mathrm{Hom}_{\mathbb{Q}P}(V,V)$ et $\mathrm{Hom}_{\mathbb{Q}(T/S)}(W,W)$ sont des corps gauches (Lemme de Schur : lemme B.10).
- Réciproquement au théorème, soit (T,S) une section de P, W un $\mathbb{Q}(T/S)$-module (de dimension finie) et $V = \mathrm{Indinf}^P_{T/S} W$. Cela induit un homomorphisme de $\mathbb{Q}$-algèbres injectif de $\mathrm{Hom}_{\mathbb{Q}(T/S)}(W,W)$ dans $\mathrm{Hom}_{\mathbb{Q}P}(V,V)$ (voir la preuve du lemme 5.1). Pour que cela soit un isomorphisme, il suffit d'avoir $\langle V,V\rangle_P = \langle W,W\rangle_{T/S}$. Cela implique, si W est irréductible, que $\mathrm{Hom}_{\mathbb{Q}(T/S)}(W,W) \cong \mathrm{Hom}_{\mathbb{Q}P}(V,V)$ est un corps gauche. Ainsi V est un module irréductible (car $\mathbb{Q}$ est de caractéristique 0).

Lemme 5.4 ([Bou], lemme 9.4.3, page 174) *Soit P un p-groupe fini et (T/S) une section de P telle que :*

i) Le groupe T/S est de p-rang normal 1.
ii) Soit $V = \mathrm{Indinf}_{T/S}^{P} \Phi_{T/S}$. *On a* $\langle V, V\rangle_P = \langle \Phi_{T/S}, \Phi_{T/S}\rangle_{T/S}$.
Alors $T = N_P(S)$.

Preuve: On note $N_P(T,S)$ le normalisateur de S et T, c'est-à-dire que

$$N_P(T,S) = \big\{ g \in P \,\big|\, gTg^{-1} = T, gSg^{-1} = S \big\}.$$

En particulier, c'est le normalisateur de T dans le groupe $N_P(S)$. Si $x \in T$, alors on note $\overline{x}$ l'élément xS de T/S.

En utilisant le théorème de réciprocité de Frobenius (théorème B.30) et la formule de Mackey (théorème 3.37), on a

$$\begin{aligned}
\langle V,V\rangle_P &= \langle \mathrm{Ind}_T^P \mathrm{Inf}_{T/S}^T \Phi_{T/S}, \mathrm{Ind}_T^P \mathrm{Inf}_{T/S}^T \Phi_{T/S}\rangle_P \\
&= \langle \mathrm{Inf}_{T/S}^T \Phi_{T/S}, \mathrm{Res}_T^P \mathrm{Ind}_T^P \mathrm{Inf}_{T/S}^T \Phi_{T/S}\rangle_T \\
&= \langle \mathrm{Inf}_{T/S}^T \Phi_{T/S}, \bigoplus_{x\in[T\backslash P/T]} \mathrm{Ind}_{T\cap {}^xT}^T \mathrm{Iso}(\gamma_x) \mathrm{Res}_{T\cap {}^xT}^T \mathrm{Inf}_{T/S}^T \Phi_{T/S}\rangle_T \\
&= \sum_{x\in[T\backslash P/T]} \langle \mathrm{Inf}_{T/S}^T \Phi_{T/S}, \mathrm{Ind}_{T\cap {}^xT}^T \mathrm{Iso}(\gamma_x) \mathrm{Res}_{T\cap {}^xT}^T \mathrm{Inf}_{T/S}^T \Phi_{T/S}\rangle_T \\
&\geq \sum_{x\in[N_P(T,S)/T]} \langle \mathrm{Inf}_{T/S}^T \Phi_{T/S}, \mathrm{Ind}_{\underbrace{T\cap {}^xT}_{=T}}^T \mathrm{Iso}(\gamma_x) \mathrm{Res}_{\underbrace{T\cap {}^xT}_{=T}}^T \mathrm{Inf}_{T/S}^T \Phi_{T/S}\rangle_T \\
&= \sum_{x\in[N_P(T,S)/T]} \langle \mathrm{Inf}_{T/S}^T \Phi_{T/S}, \underbrace{\mathrm{Iso}(\gamma_x) \mathrm{Inf}_{T/S}^T \Phi_{T/S}}_{=\mathrm{Inf}_{T/S}^T \mathrm{Iso}(\gamma_{\overline{x}})\Phi_{T/S}}\rangle_T \\
&\overset{(1)}{=} \sum_{x\in[N_P(T,S)/T]} \langle \mathrm{Inf}_{T/S}^T \Phi_{T/S}, \mathrm{Inf}_{T/S}^T \Phi_{T/S}\rangle_T \\
&= |N_P(T,S)/T| \langle \mathrm{Inf}_{T/S}^T \Phi_{T/S}, \mathrm{Inf}_{T/S}^T \Phi_{T/S}\rangle_T \\
&\overset{(2)}{=} |N_P(T,S)/T| \langle \Phi_{T/S}, \Phi_{T/S}\rangle_{T/S} \\
&= |N_P(T,S)/T| \langle V,V\rangle_P
\end{aligned}$$

où on utilise pour l'égalité (1) que $\mathrm{Iso}(\gamma_{\overline{x}})\Phi_{T/S}$ est un $\mathbb{Q}(T/S)$-module irréductible et fidèle et est donc isomorphe à $\Phi_{T/S}$ par le théorème 4.13. Pour l'égalité (2), on utilise simplement la proposition B.37. On a ainsi obtenu que

$$\langle V,V\rangle_P \geq |N_P(T,S)/T| \langle V,V\rangle_P.$$

Or $\langle V,V\rangle_P$ est un entier naturel différent de 0, donc $1 \geq |N_P(T,S)/T|$ et donc $N_P(T,S) = T$. Ainsi, dans $N_P(S)$, T est son propre normalisateur. Or $N_P(S)$ est un p-groupe, donc par la proposition A.6, on a $N_P(S) = T$. □

Définition 5.5 ([Bou], Définition et notation 9.4.5, page 175)
Soit P un p-groupe fini. Un sous-groupe S de P est dit ***génétique*** *s'il satisfait les deux conditions suivantes :*

i) Le groupe $N_P(S)/S$ est de p-rang normal 1.

ii) On pose $V(S) = \mathrm{Indinf}_{N_P(S)/S}^{P} \Phi_{N_P(S)/S}$. *Alors*

$$\langle V(S), V(S)\rangle_P = \langle \Phi_{N_P(S)/S}, \Phi_{N_P(S)/S}\rangle_{N_P(S)/S}.$$

Si S est un sous-groupe génétique de P, on définit l'entier d_S par

$$d_S = \begin{cases} 1 & \text{si } N_P(S)/S \text{ est cyclique ou quaternionien généralisé} \\ 2 & \text{si } N_P(S)/S \text{ est diédral ou semi-diédral.} \end{cases}$$

Remarque 5.6

i) Soit P un p-groupe fini et S un sous-groupe génétique. Alors d_S correspond au nombre de fois qu'apparaît le module irréductible $\Phi_{N_P(S)/S}$ dans $\mathbb{Q}N_P(S)/S$, c'est-à-dire $d_S = m(\Phi_{N_P(S)/S}, \mathbb{Q}N_P(S)/S)$ (c'est une conséquence des preuves des théorèmes 4.8, 4.10 et 4.11).

ii) Par les remarques 5.3 , le module $V(S)$ est irréductible.

Corollaire 5.7 ([Bou], corollaire 9.4.5, page 175) *Soit P un p-groupe fini et V un $\mathbb{Q}P$-module irréductible (de dimension finie). Alors il existe un sous-groupe génétique S de P tel que $V \cong V(S)$.*

Preuve: C'est une conséquence du théorème 5.2, du lemme 5.4 et de la définition 5.5. □

Lemme 5.8 ([Bou], lemme 9.4.6, page 176) *Soit P un p-groupe fini et S un sous-groupe génétique de P. Alors le noyau de la représentation irréductible associé à $V(S)$ est égal à l'intersection de tous les conjugués de S dans P, c'est-à-dire à*

$$\bigcap_{x\in P} S^x.$$

En particulier, $V(S) \cong \mathbb{Q}$ si et seulement si $S = P$.

Preuve: On pose $T = N_P(S)$. On note η le caractère de $V(S)$ et ψ est le caractère de $\mathrm{Inf}_{T/S}^{T} \Phi_{T/S}$. Alors le noyau de la représentation irréductible $V(S)$ est égal à $\mathrm{Ker}\,\eta = \{g \in P \,|\, \eta(g) = \eta(1)\}$ et $\eta = \mathrm{Indinf}_{T/S}^{P} \chi_{T/S} = \mathrm{Ind}_T^P \psi$. Soit $g \in P$. Alors, par la formule B.27, on a

$$\eta(g) = \frac{1}{|T|} \sum_{x\in P} \dot{\psi}(xgx^{-1}),$$

où $\dot{\psi} : P \to \mathbb{Q}$ est définie par

$$\dot{\psi}(h) = \begin{cases} \psi(h) & \text{si } h \in T \\ 0 & \text{sinon.} \end{cases}$$

Par la même formule,

$$\eta(1) = \frac{1}{|T|} \sum_{x \in P} \psi(1).$$

Alors $\eta(g) = \eta(1)$ si et seulement si

$$\frac{1}{|T|} \sum_{x \in P} \dot{\psi}(xgx^{-1}) = \frac{1}{|T|} \sum_{x \in P} \psi(1)$$

ce qui est équivalent à

$$\sum_{x \in P} \big(\psi(1) - \dot{\psi}(xgx^{-1})\big) = 0.$$

Or, pour tout $h \in T$, on a que $|\psi(h)| \leq \psi(1)$ et $0 < \psi(1)$ donc pour tout $h \in P$, $|\dot{\psi}(h)| \leq \psi(1)$. Ainsi pour tout $h \in P$, on a $\psi(1) - \dot{\psi}(xgx^{-1}) \geq 0$, donc l'égalité

$$\sum_{x \in P} \big(\psi(1) - \dot{\psi}(xgx^{-1})\big) = 0$$

est équivalente à $\dot{\psi}(xgx^{-1}) = \psi(1) > 0$ pour tout $x \in P$. Ceci est équivalent à $xgx^{-1} \in T \cap \operatorname{Ker} \psi$, pour tout $x \in P$. Or ici $\psi = \operatorname{Inf}_{T/S}^{T} \chi_{T/S}$, donc comme $\chi_{T/S}$ est fidèle, $\operatorname{Ker} \chi_{T/S} = \{1_{T/S}\}$ et donc $\operatorname{Ker} \psi = S$. Ainsi, on a obtenu que $\eta(g) = \eta(1)$ si et seulement si $xgx^{-1} \in S \cap T = S$ pour tout $x \in P$, c'est-à-dire si et seulement si $g \in S^x$ pour tout $x \in P$.

En résumé, on a montré que $\operatorname{Ker} \eta = \bigcap_{x \in P} S^x$, ce qui est équivalent au résultat à démontrer. □

5.2 Les sous-groupes génétiques

Notation 5.9 ([Bou], notation 9.3.1, page 176) *Soit P un p-groupe fini. Si S est un sous-groupe de P, on note $Z_P(S)$ la préimage dans $N_P(S)$ du centre de $N_P(S)/S$, c'est-à-dire le sous-groupe défini par $S \leq Z_P(S) \leq N_P(S)$ et*

$$Z_P(S)/S = Z(N_P(S)/S).$$

On note $\widehat{S}$ la préimage dans $N_P(S)$ du plus grand sous-groupe abélien élémentaire central de $N_P(S)/S$.

Lemme 5.10 ([Bou], lemme 9.5.2, page 176) *Soit P un groupe fini.*

i) Soit S et T des sous-groupes de P. Alors

$$S \overset{P}{\uparrow} T = T \text{ si et seulement si } S \cap Z_P(T) \leq T.$$

En particulier,

$$S \eqslantless_P T \iff \exists\, x \in P \text{ tel que } S^x \cap Z_P(T) \leq T \text{ et } {}^xT \cap Z_P(S) \leq S.$$

ii) Soit S un sous-groupe de P. Alors les conditions suivantes sont équivalentes :

(a) Le sous-groupe S est un sous-groupe expansif de P.

(b) Si $x \in P$ est tel que $S^x \cap Z_P(S) \leq S$, alors $S^x = S$.

Similairement, les conditions suivantes sont équivalentes :

(a) Le sous-groupe S est un sous-groupe faiblement expansif de P.

(b) Si $x \in P$ est tel que ${}^xS \cap Z_P(S) \leq S$ et $S^x \cap Z_P(S) \leq S$, alors $S^x = S$.

Preuve: Le groupe $S \overset{P}{\uparrow} T$ est un sous-groupe normal de $N_P(T)$, donc $(S \overset{P}{\uparrow} T)/T$ est un sous-groupe normal de $N_P(T)/T$. Alors, par la proposition A.7, $(S \overset{P}{\uparrow} T)/T$ est non trivial si et seulement si il intersecte le centre de $N_P(T)/T$ non trivialement, ce qui est équivalent à $(S \overset{P}{\uparrow} T) \cap Z_P(T) \neq T$ car $Z(N_P(T)/T) = Z_P(T)/T$. Mais on a

$$\begin{aligned}
(S \overset{P}{\uparrow} T) \cap Z_P(T) &= \Big(\bigcap_{g \in N_P(T)} \big(S^g \cap N_P(T)\big)T \Big) \cap Z_P(T) \\
&\overset{(1)}{=} \bigcap_{g \in N_P(T)} \big(S^g \cap N_P(T) \cap Z_P(T)\big)T \\
&= \bigcap_{g \in N_P(T)} \big(S^g \cap Z_P(T)\big)T \\
&\overset{(2)}{=} \big(S \cap Z_P(T)\big)T.
\end{aligned}$$

Donc $T < S \overset{P}{\uparrow} T$ si et seulement si $(S \cap Z_P(T))T \neq T$, c'est-à-dire si et seulement si $S \cap Z_P(T) \not\leq T$ et donc $S \overset{P}{\uparrow} T = T$ si et seulement si $S \cap Z_P(T) \leq T$.

Il reste à prouver les égalités (1) et (2). L'égalité (1) est une conséquence du fait que $Z_P(T)$ contient T. On va montrer l'égalité (2) par double inclusion. L'inclusion

$$\bigcap_{g \in N_P(T)} \big(S^g \cap Z_P(T)\big)T \subset \big(S \cap Z_P(T)\big)T$$

est claire car le terme de droite est un terme de l'intersection.

Soit $x \in (S \cap Z_P(T))T$. Alors il existe $y \in S \cap Z_P(T)$ et $t \in T$ tels que $x = yt$. Soit $g \in N_P(T)$. Alors $\overline{g^{-1}yg} = \overline{y}$ dans $N_P(T)/T$ car $\overline{y} \in Z_P(T)/T = Z(N_P(T)/T)$. Donc il existe $\widetilde{t} \in T$ tel que $g^{-1}yg = y\widetilde{t}$. Alors $y\widetilde{t} = g^{-1}yg \in S^g$ et $y\widetilde{t} \in Z_P(T)T = Z_P(T)$, donc $y\widetilde{t} \in S^g \cap Z_P(T)$. Ainsi

$$x = yt = (y\widetilde{t}) \underbrace{\widetilde{t}^{-1}t}_{\in T} \in (S^g \cap Z_P(T))T.$$

Mais ceci est vrai pour tout $g \in N_P(T)$ donc

$$x \in \bigcap_{g \in N_P(T)} (S^g \cap Z_P(T))T.$$

□

Lemme 5.11 ([Bou], lemme 9.5.3, page 177) *Soit P un p-groupe fini et S une sous-groupe génétique de P. Si Y est un sous-groupe de P, on définit les entiers a_Y et b_Y par*

$$a_Y = \big|\{x \in [N_P(S)\backslash P/Y] \,\big|\, N_P(S) \cap {}^xY \leq S\}\big|$$
$$b_Y = \big|\{x \in [N_P(S)\backslash P/Y] \,\big|\, |I_x(S,Y)| = p, I_x(S,Y) \not\leq Z(N_P(S)/S)\}\big|,$$

où $I_x(S,Y) = (N_P(S) \cap {}^xY)S/S$. Alors

$$m\big(V(S), \mathbb{Q}(P/Y)\big) = d_S a_Y + b_Y.$$

En particulier, les conditions suivantes sont équivalentes :

i) Le module irréductible $V(S)$ est un facteur de composition de $\mathbb{Q}(P/Y)$.

ii) Il existe $x \in P$ tel que ${}^xY \cap Z_P(S) \leq S$.

Preuve: On commence par remarquer que si $S = P$, alors $V(S) = \mathbb{Q}$ (lemme 5.8) et par l'exemple B.21, $\mathbb{Q}$ est contenu exactement une fois dans $\mathbb{Q}(P/Y)$. Or si $S = P$, alors $a_Y = 1$, $d_S = 1$ et $b_Y = 0$. Donc on a bien $m(V(S), \mathbb{Q}(P/Y)) = d_S a_Y + b_Y$.
On suppose maintenant que $S \neq P$. On pose $T = N_P(S)$. Soit η le caractère associé à $\mathbb{Q}(P/Y)$ et $\chi = \mathrm{Indinf}_{T/S}^P \chi_{T/S}$ (où $\chi_{T/S}$ est le caractère associé au $\mathbb{Q}(T/S)$-module $\Phi_{T/S}$). Alors, par le théorème de Frobenius (théorème B.30) et le théorème B.39, on a

$$\begin{aligned} m(V(S), \mathbb{Q}(P/Y))\langle\chi,\chi\rangle_P &= \langle \mathrm{Indinf}_{T/S}^P \chi_{T/S}, \eta\rangle_P \\ &= \langle \chi_{T/S}, \mathrm{Defres}_{T/S}^P \eta\rangle_{T/S} \\ &= m\big(\Phi_{T/S}, \mathrm{Defres}_{T/S}^P \mathbb{Q}(P/Y)\big) \\ &\quad \cdot \langle \chi_{T/S}, \chi_{T/S}\rangle_{T/S} \end{aligned}$$

Mais S est un sous-groupe génétique de P, donc $\langle\chi,\chi\rangle_P = \langle\chi_{T/S}, \chi_{T/S}\rangle_{T/S}$ est non-nul et donc $m(V(S), \mathbb{Q}(P/Y)) = m(\Phi_{T/S}, \mathrm{Defres}_{T/S}^P \mathbb{Q}(P/Y))$.
On va montrer que $\mathrm{Defres}_{T/S}^P \mathbb{Q}(P/Y)$ est isomorphe au $\mathbb{Q}(T/S)$-module de permutation associé à l'action de T/S sur $S\backslash P/Y$. Le sous-groupe S agit sur P/Y. Soit $x_1Y, \ldots, x_mY$ un ensemble de représentants des orbites. Soit $1 \leq i \leq m$. Il existe $s_{i1}, \ldots s_{ir_i} \in S$ tel que

$$\mathrm{Orb}_S(x_iY) = \{s_{ij}x_iY \,\big|\, 1 \leq j \leq r_i\}.$$

Alors $\{s_{ij}x_i \,\big|\, 1 \leq i \leq m, 1 \leq j \leq r_i\}$ est un ensemble de représentants des classes à gauche modulo Y dans P. On pose

$$b_i = \sum_{j=1}^{r_i} s_{ij}x_iY$$

pour tout $1 \leq i \leq m$. Alors $B = \{b_i \,\big|\, 1 \leq i \leq m\}$ est une base du $\mathbb{Q}(T/S)$-module $\mathrm{Defres}^P_{T/S}\,\mathbb{Q}(P/Y)$: on peut vérifier que tout élément de $\mathrm{Defres}^P_{T/S}\,\mathbb{Q}(P/Y)$ est une combinaison $\mathbb{Q}$-linéaire des éléments de B et que S agit trivialement sur B et donc aussi sur toute combinaison $\mathbb{Q}$-linéaire d'éléments de B. De plus, on peut remarquer que

$$\bigsqcup_{j=1}^{r_i} s_{ij}x_iY = Sx_iY, \qquad \text{pour tout } 1 \leq i \leq m$$

et donc

$$P = \bigsqcup_{i=1}^{m}\bigsqcup_{j=1}^{r_i} s_{ij}x_iY = \bigsqcup_{i=1}^{m} Sx_iY.$$

Ainsi $x_1, \ldots, x_m$ est un ensemble de représentants des classes de $S\backslash P/Y$. On définit alors l'application $\varphi : \mathrm{Defres}^P_{T/S}\,\mathbb{Q}(P/Y) \to \mathbb{Q}(S\backslash P/Y)$ par

$$\varphi\Big(\sum_{i=1}^{m} q_ib_i\Big) = \sum_{i=1}^{m} q_iSx_iY,$$

pour tout $\sum_{i=1}^{m} q_ib_i \in \mathrm{Defres}^P_{T/S}\,\mathbb{Q}(P/Y)$. C'est une application $\mathbb{Q}$-linéaire bijective. Il reste à vérifier que c'est un homomorphisme de $\mathbb{Q}(T/S)$-modules. Soit $\sum_{i=1}^{m} q_ib_i \in \mathrm{Defres}^P_{T/S}\,\mathbb{Q}(P/Y)$ et $t \in T$. Alors pour tout $1 \leq i \leq m$ et $1 \leq j \leq r_i$

$$t(s_{ij}x_iY) = ts_{ij}t^{-1}tx_iY$$

ainsi la multiplication par t permute les orbites de l'action de S sur P/Y. Plus précisément, la multiplication par t envoie l'orbite $\mathrm{Orb}_S(x_iY)$ sur l'orbite $\mathrm{Orb}_S(tx_iY)$. Soit $1 \leq t_i \leq m$ tel que $tx_iY = x_{t_i}Y$. Alors

$$\begin{aligned}
\varphi\Big(tS \cdot \sum_{i=1}^{m} q_ib_i\Big) &= \varphi\Big(t\sum_{i=1}^{m} q_ib_i\Big) = \varphi\Big(\sum_{i=1}^{m} q_itb_i\Big) \\
&= \varphi\Big(\sum_{i=1}^{m} q_ib_{t_i}\Big) = \sum_{i=1}^{m} q_iSx_{t_i}Y \\
&= \sum_{i=1}^{m} q_iStx_iY = \sum_{i=1}^{m} q_itSx_iY \\
&= tS \cdot \sum_{i=1}^{m} q_iSx_iY = tS \cdot \varphi\Big(\sum_{i=1}^{m} q_ib_i\Big).
\end{aligned}$$

Ainsi φ est un isomorphisme de $\mathbb{Q}(T/S)$-modules et donc

$$\mathrm{Defres}^P_{T/S}\,\mathbb{Q}(P/Y) \cong \mathbb{Q}S\backslash P/Y.$$

On va maintenant étudier un peut $S\backslash P/Y$. On a

$$P = \bigsqcup_{x\in[T\backslash P/Y]} TxY = \bigsqcup_{x\in[T\backslash P/Y]} \bigsqcup_{y\in[S\backslash TxY/Y]} SyY$$

donc

$$S\backslash P/Y = \bigsqcup_{x\in[T\backslash P/Y]} S\backslash TxY/Y.$$

Soit $x \in P$. Alors T/S agit sur $S\backslash TxY/Y$:

$$tS \cdot SzY = tSzY = StzY \in S\backslash TxY/Y, \qquad \forall\ t \in T,\ \forall z \in TxY,$$

car S est un sous-groupe normal de T. De plus, cette action est transitive : Soit $u, v \in TxY$. Alors il existe $t_u, t_v \in T$ et $y_u, y_v \in Y$ tels que $u = t_u x y_u$ et $v = t_v x y_v$. On pose $t = t_v t_u^{-1}$, alors

$$tS \cdot SuY = StuY = St_v t_u^{-1} t_u x y_u Y = St_v xY = St_v x y_v Y = SvY.$$

Alors le stabilisateur de SxY par l'action de T/S est

$$\begin{aligned}
\{tS \in T/S \,\big|\, tS \cdot SxY = SxY\} &= \{tS \in T/S \,\big|\, StxY = SxY\} \\
&= \{tS \in T/S \,\big|\, tx \in SxY\} \\
&= \{tS \in T/S \,\big|\, t \in SxYx^{-1}\} \\
&= \{tS \in T/S \,\big|\, t \in S({}^xY \cap T)\} \\
&= \{tS \in T/S \,\big|\, t \in ({}^xY \cap T)S\} \\
&= I_x(S,Y)
\end{aligned}$$

Ainsi $S\backslash TxY/Y$ et $(T/S)/I_x(S,Y)$ sont isomorphes en tant que T/S-ensembles. En résumé, on a obtenu

$$\begin{aligned}
\mathrm{Defres}^P_{T/S}\,\mathbb{Q}(P/Y) &\cong \mathbb{Q}(S\backslash P/Y) \\
&\cong \bigoplus_{x\in[T\backslash P/Y]} \mathbb{Q}(S\backslash TxY/Y) \\
&\cong \bigoplus_{x\in[T\backslash P/Y]} \mathbb{Q}\big((T/S)/I_x(S,Y)\big)
\end{aligned}$$

comme $\mathbb{Q}(T/S)$-modules. Ainsi

$$\begin{aligned}
m\big(V(S), \mathbb{Q}(P/Y)\big) &= m\big(\Phi_{T/S}, \mathrm{Defres}^P_{T/S}\,\mathbb{Q}(P/Y)\big) \\
&= \sum_{x\in[T\backslash P/Y]} m\big(\Phi_{T/S}, \mathbb{Q}\big((T/S)/I_x(S,Y)\big)\big).
\end{aligned}$$

On va donc étudier $m(\Phi_{T/S}, \mathbb{Q}((T/S)/I_x(S,Y)))$. Si le groupe $I_x(S,Y)$ intersecte $Z(T/S)$ non trivialement, alors le noyau du module $\mathbb{Q}((T/S)/I_x(S,Y))$ est non-trivial et ce module est inflaté depuis un quotient propre de T/S. Mais alors, si on décompose $\mathbb{Q}((T/S)/I_x(S,Y))$ en une somme directe de $\mathbb{Q}(T/S)$-modules irréductibles, chacun de ces modules irréductibles est aussi inflaté depuis un quotient propre de T/S et est donc non-fidèle. Ainsi $\mathbb{Q}((T/S)/I_x(S,Y))$ ne possède pas comme facteur de composition un module irréductible et fidèle, d'où $m(\Phi_{T/S}, \mathbb{Q}((T/S)/I_x(S,Y))) = 0$. Ainsi il reste à traiter le cas où $I_x(S,Y) \cap Z(T/S) = \mathbf{1}$. Il y a deux cas à distinguer (lemme 4.7) :

- Soit $I_x(S,Y) = \mathbf{1}$, et alors on cherche $m(\Phi_{T/S}, \mathbb{Q}(T/S))$, c'est-à-dire le nombre de fois qu'apparaît l'unique $\mathbb{Q}(T/S)$-module irréductible fidèle dans le $\mathbb{Q}(T/S)$-module régulier. Or d_S est égal au nombre de fois qu'apparaît l'unique $\mathbb{Q}(T/S)$-module irréductible fidèle dans $\mathbb{Q}(T/S)$ (remarque 5.6, *i)*). Il reste à voir combien de $x \in [T\backslash P/Y]$ sont tels que $I_x(S,Y) = \mathbf{1}$, c'est-à-dire tel que $T \cap {}^xY \leq S$: Il y en a exactement a_Y.
- Soit $p = 2$, P est un groupe diédral ou semi-diédral et $|I_x(S,Y)| = 2$. Soit ϕ le caractère associé au $\mathbb{Q}(T/S)$-module $\mathbb{Q}((T/S)/I_x(S,Y))$. On va calculer les valeurs de ϕ en 1 et z, où z est l'élément non-trivial du centre de P. Si $|T/S| = 2^n$, on a $\phi(1) = |(T/S)/I_x(S,Y)| = 2^{n-1}$ et

$$\phi(z) = |\operatorname{fix}(z)| = |\{x \in (T/S)/I_x(S,Y) \,\big|\, \overline{z}x = x\}| = 0$$

  car $z \notin I_x(S,Y)$. Alors, comme $\chi_{T/S}$ est nul sauf pour 1 et z (théorème 4.13), on peut calculer le produit scalaire de $\chi_{T/S}$ et ϕ :

$$\begin{aligned}\langle \chi_{T/S}, \phi \rangle_{T/S} &= \frac{1}{|T/S|} \sum_{g \in T/S} \chi_{T/S}(g)\overline{\phi(g)} \\ &= 2^{-n}2^{n-2}2^{n-1} = 2^{n-3}\end{aligned}$$

  Or $\langle \chi_{T/S}, \chi_{T/S} \rangle_{T/S} = 2^{n-3}$ (proposition 4.15) et donc

$$m\big(\Phi_{T/S}, \mathbb{Q}\big((T/S)/I_x(S,Y)\big)\big) = \frac{\langle \chi_{T/S}, \phi \rangle_{T/S}}{\langle \chi_{T/S}, \chi_{T/S} \rangle_{T/S}} = 1.$$

  Il reste à voir combien de $x \in [T\backslash P/Y]$ sont tels que $|I_x(S,Y)| = 2$ et $I_x(S,Y) \cap Z(T/S) = \mathbf{1}$, c'est-à-dire tel que $|I_x(S,Y)| = 2$ et $I_x(S,Y) \not\leq Z(T/S)$: Il y en a b_Y.

Il reste à remettre tous ces résultats ensemble :

$$m\big(V(S), \mathbb{Q}(P/Y)\big) = \sum_{x \in [T\backslash P/Y]} m\big(\Phi_{T/S}, \mathbb{Q}\big((T/S)/I_x(S,Y)\big)\big) = a_Y d_S + b_Y.$$

Une conséquence de ce résultat est que $V(S)$ est un facteur de composition de $\mathbb{Q}(P/Y)$ si et seulement si $a_Y + b_Y \neq 0$. On va étudier un peu $a_Y + b_Y$:

On pose

$$A_Y = \{TxY \in T\backslash P/Y \,\big|\, T \cap {}^xY \leq S\}$$
$$B_Y = \{TxY \in T\backslash P/Y \,\big|\, |I_x(S,Y)| = p, I_x(S,Y) \not\leq Z(T/S)\}$$
$$C_Y = \{TxY \in T\backslash P/Y \,\big|\, Z_P(S) \cap {}^xY \leq S\}$$

On peut vérifier que ces ensembles sont bien définis, c'est-à-dire qu'ils ne dépendent pas du choix des représentants. On va montrer que C_Y est l'union disjointe de A_Y est B_Y.

$\subset$: Soit $TxY \in C_Y$. Alors $Z_P(S) \cap (T \cap {}^xY) = Z_P(S) \cap {}^xY \leq S$, donc $I_x(S,Y) \cap Z(T/S) = \mathbf{1}$. Ainsi, par le lemme 4.7, soit $I_x(S,Y) = \mathbf{1}$, c'est-à-dire que ${}^xY \cap T \leq S$ et $TxY \in A_Y$, soit $|I_x(S,Y)| = p$ et $I_x(S,Y) \not\leq Z(T/S)$, c'est-à-dire que $TxY \in B_Y$.

$\supset$: Soit $TxY \in A_Y$. Alors $Z_P(S) \cap {}^xY \leq T \cap {}^xY \leq S$ donc $TxY \in C_Y$. Soit $TxY \in B_Y$, alors $|I_x(S,Y)| = p$ et $I_x(S,Y) \not\leq Z(T/S)$ donc $I_x(S,Y) \cap Z(T/S) = \mathbf{1}$ et donc $Z_P(S) \cap {}^xY = Z_P(S) \cap (T \cap {}^xY) \leq S$, c'est-à-dire que $TxY \in C_Y$.

Mais alors $a_Y + b_Y = |A_Y| + |B_Y| = |C_Y|$ et donc $a_Y + b_Y \neq 0$ si et seulement si il existe $x \in P$ tel que ${}^xY \cap Z_P(S) \leq S$. □

Théorème 5.12 *Soit P un p-groupe fini. Si V est un $\mathbb{Q}P$-module irréductible non-trivial (de dimension finie), alors il existe des sous-groupes R et Q de P tels que $Q \subset R$ et $|R : Q| = p$ et un isomorphisme de $\mathbb{Q}P$-modules*

$$V \cong \mathrm{Indinf}_{R/Q}^{P} \Omega_{R/Q}$$

où $\Omega_{R/Q}$ est l'idéal d'augmentation de l'algèbre de groupe $\mathbb{Q}(R/Q)$.

Preuve: On va commencer par prouver le résultat pour certains cas particuliers avant de faire le cas général : Soit V un $\mathbb{Q}P$-module irréductible non-trivial. Pour les cas particuliers, on suppose de plus que V est un module fidèle.

- Le groupe P est isomorphe à C_p^n pour un certain $n \geq 1$:
  Par le théorème 4.13, on sait que $V \cong \Phi_P$. Or, par la preuve du théorème 4.8, on a que $\Phi_P = \mathrm{Ind}_{C_p}^{C_{p^n}} \Omega_{C_p}$. Ainsi il suffit de prendre $R = C_p$ et $Q = \mathbf{1}$.
- Le groupe P est isomorphe à D_{2^n} pour un certain $n \geq 4$:
  On a $D_{2^n} = \langle x, y \,\big|\, x^{2^{n-1}} = y^2 = 1, yxy^{-1} = x^{-1}\rangle$. Par le théorème 4.13, on sait que $V \cong \Phi_P$. Or, par la preuve du théorème 4.10, on a que $\Phi_P = \mathrm{Indinf}_{N/D}^{D_{2^n}} \Omega_{N/D}$, où $N = \langle x^{2^{n-2}}, y\rangle$ et $D = \langle y\rangle$. Ainsi il suffit de prendre $R = N$ et $Q = D$.
- Le groupe P est isomorphe à SD_{2^n} pour un certain $n \geq 4$:
  On a $SD_{2^n} = \langle x, y \,\big|\, x^{2^{n-1}} = y^2 = 1, yxy^{-1} = x^{2^{n-2}-1}\rangle$. Par le théorème 4.13, on sait que $V \cong \Phi_P$. Or, par la preuve du théorème 4.10, on a que $\Phi_P = \mathrm{Indinf}_{N/D}^{SD_{2^n}} \Omega_{N/D}$, où $N = \langle x^{2^{n-2}}, y\rangle$ et $D = \langle y\rangle$. Ainsi il suffit de prendre $R = N$ et $Q = D$.

- Le groupe P est isomorphe à Q_{2^n} pour un certain $n \geq 3$:
  On a $Q_{2^n} = \langle x, y \,\big|\, x^{2^{n-1}} = 1, y^2 = x^{2^{n-2}}, yxy^{-1} = x^{-1} \rangle$. Par le théorème 4.13, on sait que $V \cong \Phi_P$. Or, par la preuve du théorème 4.11, on a que $\Phi_P = \mathrm{Ind}_{C_2}^{Q_{2^n}} \Omega_{C_2}$. Ainsi il suffit de prendre $R = C_2 = \langle x^{2^{n-2}} \rangle$ et $Q = \mathbf{1}$.

On va maintenant prouver le résultat en général, par récurrence sur l'ordre de P. Si $P = \mathbf{1}$, il n'y a rien à faire, car il n'y a pas de $\mathbb{Q}P$-module non-trivial. Si $|P| = p$, alors P est isomorphe à C_p pour lequel le résultat a déjà été prouvé dans les cas particuliers.

On suppose maintenant le résultat vrai pour tout groupe de cardinalité $< |P|$. Si V est un module non-fidèle, alors il existe un sous-groupe propre et normal N de P et W un $\mathbb{Q}(P/N)$-module irréductible (et fidèle) tel que

$$V \cong \mathrm{Inf}_{P/N}^{P} W.$$

Comme V est un $\mathbb{Q}P$-module non-trivial, W est aussi non-trivial. Par hypothèse d'induction, il existe alors des sous-groupes R/N et Q/N de P/N tel que $Q/N \subset R/N$ et $|R/N : Q/N| = p$ et

$$W \cong \mathrm{Indinf}_{(R/N)/(Q/N)}^{P/N} \Omega_{(R/N)/(Q/N)}.$$

Ainsi, on a

$$\begin{aligned} V &= \mathrm{Inf}_{P/N}^{P} W \\ &= \mathrm{Inf}_{P/N}^{P} \mathrm{Ind}_{R/N}^{P/N} \mathrm{Inf}_{(R/N)/(Q/N)}^{R/N} \Omega_{(R/N)/(Q/N)} \\ &\overset{(1)}{=} \mathrm{Ind}_{R}^{P} \mathrm{Inf}_{R/N}^{R} \mathrm{Inf}_{(R/N)/(Q/N)}^{R/N} \Omega_{(R/N)/(Q/N)} \\ &\overset{(2)}{=} \mathrm{Ind}_{R}^{P} \mathrm{Inf}_{R/Q}^{R} \Omega_{R/Q}, \end{aligned}$$

où l'égalité (1) découle de la proposition B.40 et l'égalité (2) de la transitivité de l'inflation (proposition B.34). Les groupes R, Q sont des sous-groupes de P avec $Q \subset R$ et $|R : Q| = p$. Ainsi, si V n'est pas fidèle, on a prouvé le résultat. On peut donc maintenant supposer que V est fidèle. Il y a alors deux cas à distinguer :

- Il existe un sous-groupe normal E de P qui est isomorphe à $C_p \times C_p$. Soit L un $\mathbb{Q}E$-module irréductible qui est un facteur de composition de $\mathrm{Res}_E^P V$ et on pose $I = \{x \in P \,\big|\, {}^x L \cong L\}$ (le sous-groupe d'inertie de L dans P). Alors, par la théorie de Clifford (théorème B.49), si $\widetilde{L}$ est la composante homogène de $\mathrm{Res}_E^P V$ qui possède L comme facteur de composition, $\widetilde{L}$ est un $\mathbb{Q}I$-module irréductible et

  $$V \cong \mathrm{Ind}_I^P \widetilde{L}.$$

  Or, comme dans le théorème de Roquette (théorème 5.2), on peut montrer que $C_P(E)$ est contenu dans I, que $P/C_P(E)$ est un p-sous-groupe

du groupe des automorphismes de E qui est d'ordre $p(p-1)(p^2-1)$. Donc I est un sous-groupe de P d'indice 1 ou p. Comme pour le théorème de Roquette (théorème 5.2), on peut aussi montrer que si $I = P$, alors L est un $\mathbb{Q}E$-module irréductible et fidèle, ce qui est impossible car E n'en possède pas (exemple 2.14). Ainsi on a que $|P : I| = p$ et en particulier I est un sous-groupe normal propre de P. Le $\mathbb{Q}I$-module $\widetilde{L}$ ne peut pas être trivial car sinon $V \cong \mathrm{Ind}_I^P \mathbb{Q} \cong \mathbb{Q}(P/I)$ qui n'est pas un module irréductible. Alors, par hypothèse de récurrence, il existe des sous-groupes R et Q de I tels que $Q \subset R$, $|R : Q| = p$ et

$$\widetilde{L} \cong \mathrm{Indinf}_{R/Q}^I \Omega_{R/Q}.$$

Mais alors, par transitivité de l'induction (proposition B.26),

$$V \cong \mathrm{Ind}_I^P \mathrm{Ind}_R^I \mathrm{Inf}_{R/Q}^R \Omega_{R/Q} = \mathrm{Ind}_R^P \mathrm{Inf}_{R/Q}^R \Omega_{R/Q}.$$

- Le groupe P ne possède pas de sous-groupe normal isomorphe à $C_p \times C_p$, c'est-à-dire P est de p-rang normal 1. Mais alors, par le théorème 4.5, P est isomorphe à un groupe cyclique, diédral, semi-diédral ou quaternionien généralisé et donc le résultat à déjà été prouvé dans un des cas particuliers.

□

Remarque 5.13 La preuve du théorème précédent se base sur la preuve du théorème 1 de l'article *A remark on a theorem of Ritter and Segal* de Serge Bouc, [Bou01].

Lemme 5.14 *Soit K un corps, G un groupe fini et A, B des sous-groupes de G. Alors*

$$\langle \mathrm{Ind}_A^G \mathbf{1}_A, \mathrm{Ind}_B^G \mathbf{1}_B \rangle_G = |A\backslash G/B|.$$

Preuve: Par les théorèmes de Frobenius et Mackey (théorèmes B.30 et 3.37), on a

$$\begin{aligned}
\langle \mathrm{Ind}_A^G \mathbf{1}_A, \mathrm{Ind}_B^G \mathbf{1}_B \rangle_G &= \langle \mathbf{1}_A, \mathrm{Res}_A^G \mathrm{Ind}_B^G \mathbf{1}_B \rangle_A \\
&= \langle \mathbf{1}_A, \bigoplus_{x \in [A\backslash G/B]} \mathrm{Ind}_{A \cap {}^x B}^A \underbrace{\mathrm{Iso}(\gamma_x) \mathrm{Res}_{A^x \cap B}^B \mathbf{1}_B}_{= \mathbf{1}_{A \cap {}^x B}} \rangle_A \\
&= \sum_{x \in [A\backslash G/B]} \langle \mathbf{1}_A, \mathrm{Ind}_{A \cap {}^x B}^A \mathbf{1}_{A \cap {}^x B} \rangle_A \\
&\overset{(1)}{=} \sum_{x \in [A\backslash G/B]} \langle \mathbb{Q}, \mathbb{Q}\big(A/(A \cap {}^x B)\big) \rangle_A \\
&\overset{(2)}{=} \sum_{x \in [A\backslash G/B]} 1 \\
&= |A\backslash G/B|,
\end{aligned}$$

où l'égalité (1) découle de la proposition B.43 et l'égalité (2) de l'exemple B.21. □

Lemme 5.15 *Soit P un p-groupe fini. Soit R et Q des sous-groupes de P tels que $Q \subset R$ et $|R : Q| = p$. Soit la projection $p : \mathbb{Q}(P/Q) \to \mathbb{Q}(P/R)$ et W le noyau de p. On a alors la suite exacte*

$$0 \longrightarrow W \overset{\iota}{\hookrightarrow} \mathbb{Q}(P/Q) \overset{p}{\twoheadrightarrow} \mathbb{Q}(P/R) \longrightarrow 0.$$

Si W est irréductible, alors $N_P(Q)/Q$ possède un unique sous-groupe d'ordre p.

Preuve: Comme $|R : Q| = p$, Q est un sous-groupe maximal de R et en particulier $Q \lhd R$ (théorème A.6). On a la suite exacte

$$0 \longrightarrow \Omega_{R/Q} \hookrightarrow \mathbb{Q}(R/Q) \twoheadrightarrow \mathbb{Q} \longrightarrow 0,$$

où $\Omega_{R/Q}$ est le noyau de l'homomorphisme d'augmentation de $\mathbb{Q}R/Q$ dans $\mathbb{Q}$. On applique $\mathrm{Ind}_R^P \mathrm{Inf}_{R/Q}^R$ à cette suite exacte et, par les propositions B.41, B.42 et B.43 cela donne la suite exacte suivante :

$$0 \longrightarrow \mathrm{Indinf}_{R/Q}^P \Omega_{R/Q} \hookrightarrow \mathbb{Q}(P/Q) \twoheadrightarrow \mathrm{Ind}_R^P \mathbb{Q} \longrightarrow 0.$$

Or, par la proposition B.43,

$$\mathrm{Ind}_R^P \mathbb{Q} = \mathrm{Indinf}_{R/R}^P \mathbb{Q} = \mathrm{Indinf}_{R/R}^P \mathbb{Q}(R/R) = \mathbb{Q}(P/R).$$

Ainsi on a les deux suites exactes suivantes :

$$0 \longrightarrow \mathrm{Indinf}_{R/Q}^P \Omega_{R/Q} \hookrightarrow \mathbb{Q}(P/Q) \twoheadrightarrow \mathbb{Q}(P/R) \longrightarrow 0$$

et

$$0 \longrightarrow W \overset{\iota}{\hookrightarrow} \mathbb{Q}(P/Q) \overset{p}{\twoheadrightarrow} \mathbb{Q}(P/R) \longrightarrow 0.$$

En particulier, cela implique que $\mathbb{Q}(P/Q)$ est isomorphe à $\mathbb{Q}(P/R) \oplus \mathrm{Indinf}_{R/Q}^P \Omega_{R/Q}$ et à $\mathbb{Q}(P/R) \oplus W$. Ainsi, on a que $W \cong \mathrm{Indinf}_{R/Q}^P \Omega_{R/Q}$ et donc $\mathrm{Indinf}_{R/Q}^P \Omega_{R/Q}$ est un $\mathbb{Q}P$-module irréductible.
On va maintenant montrer que si S est un sous-groupe de P tel que $R \cap S \subset Q$, alors $|S| < |R|$:
Le caractère de W est orthogonal (pour le produit scalaire) aux caractères des $\mathbb{Q}P$-modules irréductibles $S_{U,V} = \mathrm{Indinf}_{U/V}^P \Omega_{U/V}$, où U et V sont des sous-groupes de P tels que $V \subset U$, $|U : V| = p$ et $|U| > |R|$ (ils sont forcément distincts de W par dimension). On définit N comme le sous-groupe de $R_{\mathbb{Q}}(P)$ généré par $\mathbb{Q}$ et l'ensemble des $\mathbb{Q}P$-modules irréductibles $S_{U,V}$, où U et V sont des sous-groupes de P tels que $V \subset U$, $|U : V| = p$ et $|U| > |R|$ et on définit M comme le sous-groupe de $R_{\mathbb{Q}}(P)$ généré par l'ensemble des modules de permutations $\mathbb{Q}(P/S)$, où S est un sous-groupe de P tel que $|S| \geq |R|$. On va montrer que $N = M$. Soit U et V des sous-groupes

de P tels que $V \subset U$, $|U : V| = p$ et $|U| > |R|$. Alors, par un raisonnement analogue au début de la preuve pour R et Q, on obtient la suite exacte

$$0 \longrightarrow \mathrm{Indinf}_{U/V}^{P} \Omega_{U/V} \hookrightarrow \mathbb{Q}(P/V) \twoheadrightarrow \mathbb{Q}(P/U) \longrightarrow 0$$

donc $S_{U,V} = \mathbb{Q}(P/V) - \mathbb{Q}(P/U)$ appartient à M car $|U| > |R|$ et $|V| \geq |R|$. Ainsi on a bien que N est un sous-groupe de M. Soit maintenant S un sous-groupe de P tel que $|S| \geq |R|$. On décompose $\mathbb{Q}(P/S)$ en $\mathbb{Q}P$-modules irréductibles :

$$\mathbb{Q}(P/S) = \mathbb{Q} \oplus W_1 \oplus \ldots \oplus W_r.$$

Alors, par le théorème 5.12, pour tout $1 \leq i \leq r$, il existe des sous-groupes U_i et V_i de P tels que $U_i \subset V_i$ et $|V_i : U_i| = p$ et un isomorphisme de $\mathbb{Q}P$-modules

$$W_i \cong \mathrm{Indinf}_{V_i/U_i}^{P} \Omega_{V_i/U_i} = S_{U_i,V_i}.$$

Ainsi $\mathbb{Q}(P/S) = \mathbb{Q} \oplus S_{U_1,V_1} \oplus \ldots \oplus S_{U_r,V_r}$. Soit $1 \leq i \leq r$. Il reste à montrer que $|U_i| > |R|$. Or

$$\begin{aligned} \dim_{\mathbb{Q}} S_{U_i,V_i} &= \dim_{\mathbb{Q}} \mathbb{Q}(P/V_i) - \dim_{\mathbb{Q}} \mathbb{Q}(P/U_i) \\ &= |P : V_i| - |P : U_i| \\ &= |P : U_i| \cdot |U_i : V_i| - |P : U_i| \\ &= (p-1)|P : U_i| \end{aligned}$$

et donc

$$|P : U_i| \leq (p-1)|P : U_i| = \dim_{\mathbb{Q}} S_{U_i,V_i} < \dim_{\mathbb{Q}} \mathbb{Q}(P/S) = |P : S|.$$

Par conséquent, on a $|R| \leq |S| < |U_i|$, ce qui implique que $S_{U_i,V_i} \in N$. Ainsi, on a bien que $\mathbb{Q}(P/S) \in N$ et M est un sous-groupe de N.
En résumé, on a montré que $M = N$. Or le caractère de W est orthogonal aux générateurs de N, donc avec tous les éléments de N. Ainsi le caractère de W est orthogonal à l'ensemble des $\mathbb{Q}P$-modules de M, donc en particulier à $\mathrm{Ind}_S^P \mathbb{Q}$, pour tout sous-groupe S de P tel que $|S| \geq |R|$.

Soit S un sous-groupe de P tel que $|S| \geq |R|$. Comme $W \oplus \mathbb{Q}(P/R) = \mathbb{Q}(P/Q)$, c'est-à-dire $W \oplus \mathrm{Ind}_R^P \mathbb{Q} = \mathrm{Ind}_Q^P \mathbb{Q}$, le caractère de W est égal à $\mathrm{Ind}_Q^P \mathbf{1}_P - \mathrm{Ind}_R^P \mathbf{1}_R$. Or si A et B sont des sous-groupes de P, alors $\langle \mathrm{Ind}_A^P \mathbf{1}_A, \mathrm{Ind}_B^P \mathbf{1}_B \rangle_P = |A\backslash P/B|$ (lemme 5.14). Donc ici, on obtient que

$$|Q\backslash P/S| = |R\backslash P/S|.$$

Or si $x \in P$, comme $QxS \subset RxS$, cela implique $QxS = RxS$, ou de manière équivalente que $R \subset Q \cdot {}^xS$ (si $QxS = RxS$, alors $Rx \subset RxS = QxS$, donc $R \subset QxSx^{-1}$; et réciproquement si $R \subset QxSx^{-1}$, alors $Rx \subset QxS$ et donc $RxS \subset QxS$ et comme on a déjà $QxS \subset RxS$, cela implique l'égalité). Mais comme $Q \subset R$, c'est équivalent à $R \subset Q(R \cap {}^xS)$ et donc à $R \cap {}^xS \not\subset Q$ car

$|R : Q| = p$. Donc, pour tout $x \in P$, on a $R \cap {}^xS \not\subset Q$ et donc en particulier $R \cap S \not\subset Q$. Donc si on a un sous-groupe S de P tel que $R \cap S \subset Q$, alors $|S| < |R|$.
On va maintenant utiliser ce résultat pour prouver que $N_P(Q)/Q$ possède un unique sous-groupe d'ordre p :
Soit S un sous-groupe de P contenant Q mais pas R. Alors $Q \leq R \cap S < R$ donc comme Q est un sous-groupe maximal de R, on a $R \cap S = Q$. Alors, par le résultat qu'on vient de montrer, on a $|S| < |R|$ et donc en particulier $|S| \leq |Q|$. Or, comme $Q \subset S$, on a aussi $|Q| \leq |S|$ et donc on a $S = Q$. Ainsi tout sous-groupe de P contenant Q mais différent de Q contient aussi R. Ainsi R est le seul sous-groupe de P tel que $|R : Q| = p$ et donc R/Q est le seul sous-groupe d'ordre p de $N_P(Q)/Q$. □

Remarque 5.16 La preuve du lemme précédent se base sur la preuve de la proposition 4 (1. implique 2. et 2. implique 3.) de l'article *A remark on a theorem of Ritter and Segal* de Serge Bouc, [Bou01].

Lemme 5.17 ([Bou], lemme 9.5.4, page 179) *Soit P un p-groupe fini, et S un sous-groupe génétique propre de P. Alors $|\widehat{S} : S| = p$ et*

i) Le noyau de la projection $\mathbb{Q}(P/S) \to \mathbb{Q}(P/\widehat{S})$ est isomorphe à la somme directe de d_S copies de $V(S)$.

ii) Le module $V(S)$ n'est pas un facteur de composition de $\mathbb{Q}(P/\widehat{S})$.

Preuve:

i) On a que $|\widehat{S} : S|$ est égal à la cardinalité de $\widehat{S}/S$. Or $\widehat{S}/S$ est le plus grand sous-groupe central abélien élémentaire de $N_P(S)/S$ (qui est de p-rang normal 1) et $N_P(S)/S$ n'est pas le groupe trivial $\mathbf{1}$ car S est un sous-groupe propre de P. Ainsi, il suffit de vérifier le résultat pour les groupes cycliques (différents du groupe trivial), diédraux, semi-diédraux et quaternionien généralisé. Or, pour ces groupes, le résultat est vrai : $|\widehat{S} : S| = p$.
On pose $T = N_P(S)$ et $Z = \widehat{S}/S$. On sait déjà que le nombre de fois que $\Phi_{T/S}$ est un facteur de composition de $\mathbb{Q}(T/S)$ est égal à d_S. Le $\mathbb{Q}(T/S)$-module $\mathbb{Q}((T/S)/Z)$ est inflaté du $\mathbb{Q}((T/S)/Z)$-module $\mathbb{Q}((T/S)/Z)$, donc en particulier, tous les $\mathbb{Q}(T/S)$-modules irréductibles facteurs de $\mathbb{Q}((T/S)/Z)$ sont inflatés depuis des $\mathbb{Q}((T/S)/Z)$-modules irréductible. Or $Z \neq \mathbf{1}$, donc cela implique que tous les $\mathbb{Q}(T/S)$-modules irréductibles facteurs de $\mathbb{Q}((T/S)/Z)$ sont non-fidèles et ne peuvent donc être isomorphes à $\Phi_{T/S}$. Ainsi on a obtenu que $\Phi_{T/S}$ n'est pas un facteur de composition de $\mathbb{Q}((T/S)/Z)$. On a la suite suivante :

$$0 \longrightarrow d_S\Phi_{T/S} \overset{\iota}{\hookrightarrow} \mathbb{Q}(T/S) \overset{p}{\twoheadrightarrow} \mathbb{Q}((T/S)/Z) \longrightarrow 0$$

où ι est l'inclusion de $d_S\Phi_{T/S}$ dans $\mathbb{Q}(T/S)$ et p la projection de $\mathbb{Q}(T/S)$ dans $\mathbb{Q}((T/S)/Z)$. C'est une suite exacte si on prouve que $\operatorname{Ker} p = \operatorname{Im} \iota$.

Or $\mathbb{Q}(T/S) \cong \operatorname{Ker} p \oplus \operatorname{Im} p$ et $\Phi_{T/S}$ n'est pas un facteur de composition de $\mathbb{Q}((T/S)/Z)$, donc ce n'est pas non plus un facteur de composition de $\operatorname{Im} p$. Ainsi $\operatorname{Ker} p$ contient d_S fois $\Phi_{T/S}$ comme facteur de composition, c'est-à-dire que $\operatorname{Im} \iota \subset \operatorname{Ker} p$. Or en utilisant le corollaire 4.14, si $|T/S| = p^n$, on a

$$\begin{aligned}
\dim_{\mathbb{Q}} \operatorname{Ker} p &= \dim_{\mathbb{Q}} \mathbb{Q}(T/S) - \dim_{\mathbb{Q}} \operatorname{Im} p \\
&= p^n - \dim_{\mathbb{Q}} \mathbb{Q}((T/S)/Z) \\
&= p^n - p^{n-1} \\
&= p^{n-1}(p-1) \\
&= d_S \dim_{\mathbb{Q}} \Phi_{T/S} \\
&= \dim_{\mathbb{Q}} \operatorname{Im} \iota
\end{aligned}$$

et donc $\operatorname{Im} \iota = \operatorname{Ker} p$. Ainsi on a la suite exacte

$$0 \longrightarrow d_S \Phi_{T/S} \overset{\iota}{\hookrightarrow} \mathbb{Q}(T/S) \overset{p}{\twoheadrightarrow} \mathbb{Q}((T/S)/Z) \longrightarrow 0.$$

On applique alors $\operatorname{Indinf}_{T/S}^{P}$ à cette suite et, par les propositions B.41, B.42 et B.43, on obtient la suite exacte

$$0 \longrightarrow d_S V(S) \hookrightarrow \mathbb{Q}(P/S) \twoheadrightarrow \operatorname{Indinf}_{T/S}^{P} \mathbb{Q}((T/S)/Z) \longrightarrow 0.$$

Or on a, par la transitivité de l'inflation (proposition B.34) et la proposition B.43, que

$$\begin{aligned}
\operatorname{Ind}_T^P \operatorname{Inf}_{T/S}^T \mathbb{Q}((T/S)/Z) &= \operatorname{Ind}_T^P \operatorname{Inf}_{T/S}^T \operatorname{Inf}_{(T/S)/Z}^{T/S} \mathbb{Q}((T/S)/Z) \\
&= \operatorname{Ind}_T^P \operatorname{Inf}_{T/\widehat{S}}^T \mathbb{Q}(T/\widehat{S}) \\
&= \mathbb{Q}(P/\widehat{S}).
\end{aligned}$$

Ainsi, en résumé, on a obtenu la suite exacte

$$0 \longrightarrow d_S V(S) \hookrightarrow \mathbb{Q}(P/S) \twoheadrightarrow \mathbb{Q}(P/\widehat{S}) \longrightarrow 0.$$

De plus, l'application entre $\mathbb{Q}(P/S)$ et $\mathbb{Q}(P/\widehat{S})$ correspond à la projection. Ainsi on a obtenu le résultat cherché.

ii) On pose $T = N_P(S)$ et $p^n = |T/S|$. Par le lemme 5.8, on sait que $V(S)$ n'est pas isomorphe à $\mathbb{Q}$. On commence par calculer la dimension de

$V(S)$:

$$\begin{aligned}
\dim_{\mathbb{Q}} V(S) &= \dim_{\mathbb{Q}} \operatorname{Ind}_T^P \operatorname{Inf}_{T/S}^T \Phi_{T/S} \\
&= |P:T| \dim_{\mathbb{Q}} \operatorname{Inf}_{T/S}^T \Phi_{T/S} \\
&= |P:T| \dim_{\mathbb{Q}} \Phi_{T/S} \\
&= |P:T| \frac{p^{n-1}(p-1)}{d_S} \\
&= |P:T| \cdot |T:S| \frac{p-1}{pd_S} \\
&= |P:\widehat{S}| \frac{|\widehat{S}:S|(p-1)}{pd_S} \\
&= |P:\widehat{S}| \frac{p-1}{d_S}.
\end{aligned} \tag{5.1}$$

On suppose, par l'absurde, que $V(S)$ est un facteur de composition de $\mathbb{Q}(P/\widehat{S})$. Alors, comme $\mathbb{Q}$ est aussi un facteur de composition de $\mathbb{Q}(P/\widehat{S})$, on a que $\dim_{\mathbb{Q}} V(S) < \dim_{\mathbb{Q}} \mathbb{Q}(P/\widehat{S})$ et donc

$$|P:\widehat{S}| \frac{p-1}{d_S} < |P:\widehat{S}|.$$

Ainsi, on a $p-1 < d_S$ et donc $p \leq d_S$. Ainsi la seule possibilité est que $p=2$ et $d_S = 2$. Cela implique que T/S est diédral ou semi-diédral. Alors $|T:S| \geq 16$, ce qui implique en particulier que $|T:\widehat{S}| \geq 8$. Ainsi on peut trouver un sous-groupe S' de T qui contient $\widehat{S}$ et tel que $|S':\widehat{S}| = 2$: Le sous-groupe $\widehat{S}$ est normal dans T et $T/\widehat{S}$ est un 2-groupe non-trivial. Donc on peut trouver un sous-groupe de $T/\widehat{S}$ d'ordre 2. Sa préimage par l'application $\pi : T \to T/\widehat{S}$ donne S'.
Soit la projection $p : \mathbb{Q}(P/\widehat{S}) \to \mathbb{Q}(P/S')$ et W le noyau de p. Alors, si on reprend la dimension de $V(S)$ (équation 5.1), on a

$$\dim_{\mathbb{Q}} V(S) = \frac{|P:\widehat{S}|}{2} = \frac{|P:S'| \cdot |S':\widehat{S}|}{2} = |P:S'|.$$

Ainsi en particulier $V(S)$ n'est pas un facteur de composition de $\mathbb{Q}(P/S')$ car $\mathbb{Q}(P/S')$ contient aussi $\mathbb{Q}$ et alors il ne reste plus assez de place pour $V(S)$ vu les dimensions. Ainsi, comme $V(S)$ est un facteur de composition de $\mathbb{Q}(P/\widehat{S})$, il est aussi un facteur de composition de W. Or on a

$$\begin{aligned}
\dim_{\mathbb{Q}} W &= \dim_{\mathbb{Q}} \mathbb{Q}(P/\widehat{S}) - \dim_{\mathbb{Q}} \mathbb{Q}(P/S') \\
&= |P:\widehat{S}| - |P:S'| \\
&= |P:S'| \cdot |S':\widehat{S}| - |P:S'| \\
&= 2|P:S'| - |P:S'| \\
&= |P:S'| = \dim_{\mathbb{Q}} V(S)
\end{aligned}$$

et donc W est isomorphe à $V(S)$ et est en particulier irréductible. Alors, par le lemme 5.15, $N_P(\widehat{S})/\widehat{S}$ possède un unique sous-groupe d'ordre p. Cela implique, par la proposition A.12, que $N_P(\widehat{S})/\widehat{S}$ est un groupe cyclique ou quaternionien généralisé. Or $\widehat{S}$ est un sous-groupe normal de T et donc $T/\widehat{S}$ est un sous-groupe de $N_P(\widehat{S})/\widehat{S}$. Or, par le troisième théorème d'isomorphisme, $T/\widehat{S}$ est isomorphe à $(T/S)/(\widehat{S}/S)$ qui est un groupe diédral ou semi-diédral car T/S est diédral ou semi-diédral. Donc on a un groupe cyclique ou quaternionien généralisé qui contient un groupe diédral ou semi-diédral, ce qui est une contradiction. Ainsi l'hypothèse de départ que $V(S)$ est un facteur de composition de $\mathbb{Q}(P/\widehat{S})$ est fausse, et donc $V(S)$ n'est pas un facteur de composition de $\mathbb{Q}(P/\widehat{S})$, ce qui était le résultat à prouver.

□

Corollaire 5.18 ([Bou], corollaire 9.5.5, page 181) *Soit P un p-groupe fini, et S un sous-groupe génétique de P.*

i) Si $x \in P$ et $N_P(S) \cap {}^xS \leq S$, alors ${}^xS = S$.

ii) Si $x \in P$, alors $(N_P(S) \cap {}^xS)S/S$ ne peut pas être un sous-groupe non central d'ordre p de $N_P(S)/S$.

iii) Si $x \in P$ et $Z_P(S) \cap {}^xS \leq S$, alors ${}^xS = S$. En d'autres mots, S est un sous-groupe expansif de P (lemme 5.10).

Preuve: Si $S = P$, alors les trois résultats sont clairs. On suppose donc que $S \neq P$. On pose $T = N_P(S)$. On sait, par le lemme 5.17, que la multiplicité de $\Phi_{T/S}$ dans $\mathbb{Q}(P/S)$ est égale à d_S. Or par le lemme 5.11 (et en reprenant les notations du lemme et de sa preuve), cette multiplicité est égale à $a_S d_S + b_S$. Donc $a_S d_S + b_S = d_S$ et donc $d_S(a_S - 1) + b_S = 0$. Or $a_S \geq 1$ (car $N_P(S)1_P S \in \{N_P(S)xS \in N_P(S)\backslash P/S \,\big|\, N_P(S) \cap {}^xS \leq S\} = A_S$) et $b_S \geq 0$, donc $a_S = 1$ et $b_S = 0$.

i) Soit $x \in P$ tel que $T \cap {}^xS \leq S$. Alors comme $a_S = 1$, $TxS = T1_P S = T$. Donc $x \in T$, c'est-à-dire que ${}^xS = S$.

ii) Soit $x \in P$. Alors $(T \cap {}^xS)S/S$ ne peut pas être un sous-groupe non central d'ordre p de T/S, car sinon $b_S \geq 1$ ce qui contredirait $b_S = 0$.

iii) Soit $x \in P$ tel que $Z_P(S) \cap {}^xS \leq S$. Alors (en reprenant les notations de la preuve du lemme 5.11) $TxS \in C_S = A_S \bigsqcup B_S$. Or on sait que $B_S = \emptyset$ car $b_S = 0$. Donc $TxS \in A_S$. Or $a_S = 1$ et le seul élément de A_S est $T1_P S = T$. Donc $TxS = T$, c'est-à-dire que $x \in T$ et donc ${}^xS = S$.

□

Théorème 5.19 ([Bou], théorème 9.5.6, page 181) *Soit P un p-groupe fini et S un sous-groupe de P, tel que $N_P(S)/S$ est de p-rang normal 1. Alors les conditions suivantes sont équivalentes :*

i) Le sous-groupe S est un sous-groupe génétique de P.

ii) Si $x \in P$ est tel que ${}^xS \cap Z_P(S) \leq S$, alors ${}^xS = S$. En d'autres mots, S est un sous-groupe expansif de P (lemme 5.10).

iii) Si $x \in P$ est tel que ${}^xS \cap Z_P(S) \leq S$ et $S^x \cap Z_P(S) \leq S$, alors ${}^xS = S$. En d'autres mots, S est un sous-groupe faiblement expansif de P (lemme 5.10).

Preuve:

- *i) $\Rightarrow$ ii)* : Si S est un sous-groupe génétique de P, alors par le corollaire 5.18, S est expansif.
- *ii) $\Rightarrow$ iii)* : Si S est expansif, clairement S est aussi faiblement expansif.
- *iii) $\Rightarrow$ i)* : On suppose que S est faiblement expansif. On pose $T = N_P(S)$. Alors comme $\Phi_{T/S}$ est irréductible et fidèle, $f_{\mathbf{1}}^{T/S}\Phi_{T/S} = \Phi_{T/S}$ (lemme 3.57) et donc

$$V(S) = \mathrm{Indinf}_{T/S}^P \Phi_{T/S} = \mathrm{Indinf}_{T/S}^P f_{\mathbf{1}}^{T/S}\Phi_{T/S} = \mathcal{I}_S\Phi_{T/S}. \qquad (5.2)$$

Alors, par le théorème de réciprocité de Frobenius (théorèmes B.30) et le théorème B.39,

$$\begin{aligned}
\langle V(S), V(S)\rangle_P &= \langle \mathrm{Indinf}_{T/S}^P \Phi_{T/S}, V(S)\rangle_P \\
&= \langle \Phi_{T/S}, \mathrm{Defres}_{T/S}^P V(S)\rangle_{T/S} \\
&= \langle \Phi_{T/S}, \mathrm{Defres}_{T/S}^P \mathcal{I}_S\Phi_{T/S}\rangle_{T/S} \\
&= \langle f_{\mathbf{1}}^{T/S}\Phi_{T/S}, \mathrm{Defres}_{T/S}^P \mathcal{I}_S\Phi_{T/S}\rangle_{T/S} \\
&= \langle \Phi_{T/S}, f_{\mathbf{1}}^{T/S}\,\mathrm{Defres}_{T/S}^P \mathcal{I}_S\Phi_{T/S}\rangle_{T/S} \\
&= \langle \Phi_{T/S}, \mathcal{D}_S\mathcal{I}_S\Phi_{T/S}\rangle_{T/S} \\
&= \langle \Phi_{T/S}, \Phi_{T/S}\rangle_{T/S}
\end{aligned}$$

car, par le théorème 3.56 *ii)*, $\mathcal{D}_S\mathcal{I}_S\Phi_{T/S} = f_{\mathbf{1}}^{T/S}\Phi_{T/S} = \Phi_{T/S}$. Ainsi on a montré que $\langle V(S), V(S)\rangle_P = \langle \Phi_{T/S}, \Phi_{T/S}\rangle_{T/S}$ et donc S est un sous-groupe génétique de P.

□

5.3 Les bases génétiques

Théorème 5.20 ([Bou], théorème 9.6.1, page 182) *Soit P un p-groupe fini. Si S et T sont des sous-groupes génétiques de P, alors les conditions suivantes sont équivalentes :*

i) Les $\mathbb{Q}P$-modules $V(S)$ et $V(T)$ sont isomorphes.

ii) Il existe $x, y \in P$ tels que ${}^xT \cap Z_P(S) \leq S$ et ${}^yS \cap Z_P(T) \leq T$.

iii) Il existe $x \in P$ tel que ${}^xT \cap Z_P(S) \leq S$ et $S^x \cap Z_P(T) \leq T$. En d'autres termes, $S \widehat{\ }_P\, T$ (lemme 5.10).

iv) Les sections $(N_P(S), S)$ *et* $(N_P(T), T)$ *de* P *sont liées modulo* P.

Si ces conditions sont satisfaites, on a, en particulier, que les groupes $N_P(S)/S$ *et* $N_P(T)/T$ *sont isomorphes.*

Preuve:

- *iv)* $\Rightarrow$ *iii)* : Les sections $(N_P(S), S)$ et $(N_P(T), T)$ de P sont liées modulo P, donc il existe $x \in P$ tel que $(N_P(S), S)$ — $({}^xN_P(T), {}^xT)$. Alors

$$ {}^xT \cap N_P(S) = S \cap {}^xN_P(T). $$

Donc on a

$$ {}^xT \cap Z_P(S) \leq {}^xT \cap N_P(S) = S \cap {}^xN_P(T) \leq S $$

c'est-à-dire ${}^xT \cap Z_P(S) \leq S$. De même

$$ S \cap {}^xZ_P(T) \leq S \cap {}^xN_P(T) = {}^xT \cap N_P(S) \leq {}^xT, $$

d'où $S \cap {}^xZ_P(T) \leq {}^xT$ et donc $S^x \cap Z_P(T) \leq T$.

- *iii)* $\Rightarrow$ *ii)* : On sait qu'il existe $x \in P$ tel que ${}^xT \cap Z_P(S) \leq S$ et $S^x \cap Z_P(T) \leq T$. Il suffit alors de prendre $y = x^{-1}$ et on obtient le résultat cherché.

- *ii)* $\Rightarrow$ *i)* : On commence par supposer que $S = P$. Alors la condition ${}^yS \cap Z_P(T) \leq T$ implique que $Z_P(T) = T$, c'est-à-dire que $Z(N_P(T)/T) = \mathbf{1}$. Donc $N_P(T)/T$ est un p-groupe de centre trivial et donc $N_P(T)/T = \mathbf{1}$ (théorème A.6). Or cela implique que $N_P(T) = T$ et donc, comme P est un p-groupe, cela implique que $T = P$ (théorème A.6). Mais alors on a bien $V(S) \cong \mathbb{Q} \cong V(T)$.
  De la même manière, on peut montrer que si $T = P$, alors $V(T) \cong \mathbb{Q} \cong V(S)$.
  On peut maintenant supposer que S et T sont des sous-groupes propres de P. On pose $N = N_P(S)$ et $M = N_P(T)$. Par le lemme 5.8, $V(S)$ et $V(T)$ ne sont pas isomorphes à $\mathbb{Q}$. On va supposer par l'absurde que $V(S)$ et $V(T)$ ne sont pas isomorphes. Par les hypothèses du point *ii)* et par le lemme 5.11, on sait que $V(S)$ est un facteur de composition de $\mathbb{Q}(P/T)$ et $V(T)$ est un facteur de composition de $\mathbb{Q}(P/S)$. Par le lemme 5.17, on sait aussi que $\mathbb{Q}(P/S) \cong d_S V(S) \oplus \mathbb{Q}(P/\widehat{S})$ et $\mathbb{Q}(P/T) \cong d_T V(T) \oplus \mathbb{Q}(P/\widehat{T})$, donc $V(S)$ est un facteur de composition de $\mathbb{Q}(P/\widehat{T})$ et $V(T)$ est un facteur de composition de $\mathbb{Q}(P/\widehat{S})$. Or on a,

en utilisant la proposition B.29 et le corollaire 4.14 et si $|N : S| = p^n$,

$$\begin{aligned}
\dim_{\mathbb{Q}} V(S) &= \dim_{\mathbb{Q}} \operatorname{Ind}_N^P \operatorname{Inf}_{N/S}^N \Phi_{N/S} \\
&= |P : N| \dim_{\mathbb{Q}} \operatorname{Inf}_{N/S}^N \Phi_{N/S} \\
&= |P : N| \dim_{\mathbb{Q}} \Phi_{N/S} \\
&= |P : N| \frac{p^{n-1}(p-1)}{d_S} \\
&= |P : N| \frac{p^n(p-1)}{pd_S} \\
&= |P : N| \cdot |N : S| \frac{p-1}{pd_S} \\
&= |P : S| \frac{p-1}{pd_S}.
\end{aligned} \tag{5.3}$$

Ainsi, comme $\mathbb{Q}$ est aussi un facteur de composition de $\mathbb{Q}(P/\widehat{T})$, on a que $\dim_{\mathbb{Q}} V(S) < \dim_{\mathbb{Q}} \mathbb{Q}(P/\widehat{T})$ et donc

$$|P : S| \frac{p-1}{pd_S} < |P : \widehat{T}| = \frac{|P : T|}{p}.$$

En réarrangeant l'équation, on obtient que

$$|P : S|(p-1) < |P : T| d_S. \tag{5.4}$$

Par symétrie, on a aussi

$$|P : T|(p-1) < |P : S| d_T. \tag{5.5}$$

On multiplie les deux équations :

$$|P : S| \cdot |P : T|(p-1)^2 < |P : T| \cdot |P : S| d_S d_T.$$

En divisant par $|P : S| \cdot |P : T|$, on a alors que $(p-1)^2 < d_S d_T \leq 4$. Cela implique que $p = 2$ et d_S ou d_T est égal à 2. Alors les équations 5.4 et 5.5 deviennent

$$|P : S| < |P : T| d_S \quad \text{et} \quad |P : T| < |P : S| d_T \tag{5.6}$$

et donc on a $|P : S| \leq |P : T|$ et $|P : T| \leq |P : S|$, c'est-à-dire que $|P : T| = |P : S|$ et donc $|T| = |S|$. De plus, les équations 5.6 impliquent alors aussi que $d_S = d_T = 2$, donc N/S et M/T sont des groupes diédraux ou semi-diédraux et $|P : S| = |P : T| \geq 16$.
Comme $|M : \widehat{T}| \geq 8$, on peut trouver un sous-groupe T' de M contenant $\widehat{T}$ et tel que $|T' : \widehat{T}| = 2$: Cela est possible car $\widehat{T}$ est normal dans M et $M/\widehat{T}$ est un 2-groupe non-trivial, donc il existe un sous-groupe de $M/\widehat{T}$ d'ordre 2. Il suffit de prendre pour T' la préimage par $\pi : M \to M/\widehat{T}$ de ce sous-groupe.

Soit la projection $p : \mathbb{Q}(P/\widehat{T}) \to \mathbb{Q}(P/T')$ et $W = \operatorname{Ker} p$. On a la suite exacte

$$0 \longrightarrow W \hookrightarrow \mathbb{Q}(P/\widehat{T}) \twoheadrightarrow \mathbb{Q}(P/T') \longrightarrow 0.$$

Alors on a, si on reprend le résultat 5.3, on a que

$$\begin{aligned}
\dim_{\mathbb{Q}} V(S) &= \frac{|P:S|}{4} \\
&= \frac{|P:T|}{4} \\
&= \frac{|P:T'| \cdot |T':\widehat{T}| \cdot |\widehat{T}:T|}{2 \cdot 2} \\
&= |P:T'| \\
&= \dim_{\mathbb{Q}} \mathbb{Q}P/T'.
\end{aligned}$$

Ainsi $V(S)$ n'est pas un facteur de composition de $\mathbb{Q}P/T'$ car $\mathbb{Q}$ est déjà un facteur de composition de $\mathbb{Q}P/T'$ et ainsi, vu les dimensions, il n'y a plus de place pour $V(S)$. Mais alors, comme $V(S)$ est un facteur de composition de $\mathbb{Q}P/\widehat{T}$, $V(S)$ est un facteur de composition de W. Or on a

$$\begin{aligned}
\dim_{\mathbb{Q}} W &= \dim_{\mathbb{Q}} \mathbb{Q}(P/\widehat{T}) - \dim_{\mathbb{Q}} \mathbb{Q}(P/T') \\
&= |P:\widehat{T}| - |P:T'| \\
&= |P:T'| \cdot |T':\widehat{T}| - |P:T'| \\
&= 2|P:T'| - |P:T'| \\
&= |P:T'| = \dim_{\mathbb{Q}} V(S).
\end{aligned}$$

Ainsi W est isomorphe à $V(S)$ et est en particulier irréductible. Alors, par le lemme 5.15, $N_P(\widehat{T})/\widehat{T}$ possède un unique sous-groupe d'ordre p. Cela implique, par la proposition A.12, que $N_P(\widehat{T})/\widehat{T}$ est un groupe cyclique ou quaternionien généralisé. Or $\widehat{T}$ est un sous-groupe normal de M et donc $M/\widehat{T}$ est un sous-groupe de $N_P(\widehat{T})/\widehat{T}$. Or, par le troisième théorème d'isomorphisme, $M/\widehat{T}$ est isomorphe à $(M/T)/(\widehat{T}/T)$ qui est un groupe diédral ou semi-diédral car M/T est diédral ou semi-diédral. Donc on a un groupe cyclique ou quaternionien généralisé qui contient un groupe diédral ou semi-diédral, ce qui est une contradiction. Ainsi l'hypothèse de départ que $V(S)$ et $V(T)$ ne sont pas isomorphes est fausse et donc $V(S)$ et $V(T)$ sont isomorphes, ce qui était le résultat à prouver.

- *i) ⇒ iv)* : On suppose que $V(S) \cong V(T)$. Si $V(S) \cong \mathbb{Q}$, alors, par le lemme 5.8, S et T sont égaux à P et la condition 4. est vérifiée. On peut donc supposer que $V(S) \ncong \mathbb{Q} \ncong V(T)$, c'est-à-dire que S et T sont des sous-groupes génétiques propres de P. On pose $N = N_P(S)$ et $M = N_P(T)$. Comme $V(S) = \mathcal{I}_S\Phi_{N/S}$ (voir la preuve du théorème

5.19, équation 5.2) et comme S est un sous-groupe expansif de P, la proposition 3.56 montre que

$$\mathrm{Defres}^P_{N/S} V(S) = \mathrm{Defres}^P_{N/S} \mathcal{I}_S \Phi_{N/S} = f_{\mathbf{1}}^{N/S} \Phi_{N/S} = \Phi_{N/S}$$

($\Phi_{N/S}$ est un $\mathbb{Q}(N/S)$-module irréductible et fidèle et on applique le lemme 3.57). Comme $V(S) \cong V(T)$, cela implique que

$$\mathrm{Defres}^P_{N/S} V(T) \cong \Phi_{N/S}.$$

Alors, si on applique le théorème 3.36, on a

$$\begin{aligned}\Phi_{N/S} &\cong \mathrm{Defres}^P_{N/S} \mathrm{Indinf}^P_{M/T} \Phi_{M/T} \\ &\cong \bigoplus_{x \in [N\backslash P/M]} \mathrm{Indinf}^{N/S}_{p_{1,x}/k_{1,x}} \mathrm{Iso}(f_x) \mathrm{Defres}^{M/T}_{p_{2,x}/k_{2,x}} \Phi_{M/T},\end{aligned}$$

où, pour tout $x \in [N\backslash P/M]$, f_x est l'isomorphisme canonique entre $p_{2,x}/k_{2,x}$ et $p_{1,x}/k_{1,x}$ et

$$p_{1,x} = S(N \cap {}^x M)/S, \qquad k_{1,x} = S(N \cap {}^x T)/S, \tag{5.7}$$

$$p_{2,x} = T(N^x \cap M)/T, \qquad k_{2,x} = T(M \cap S^x)/T. \tag{5.8}$$

Or $\Phi_{N/S}$ est un $\mathbb{Q}(N/S)$-module irréductible, donc il existe un unique $x \in [N\backslash P/M]$ tel que le facteur correspondant est non-nul dans la partie droite de l'équation précédente, et

$$\Phi_{N/S} \cong \mathrm{Indinf}^{N/S}_{p_{1,x}/k_{1,x}} \mathrm{Iso}(f_x) \mathrm{Defres}^{M/T}_{p_{2,x}/k_{2,x}} \Phi_{M/T}. \tag{5.9}$$

En particulier, pour tout $y \in [N\backslash P/M] - \{x\}$,

$$\langle \Phi_{N/S}, \mathrm{Indinf}^{N/S}_{p_{1,y}/k_{1,y}} \mathrm{Iso}(f_y) \mathrm{Defres}^{M/T}_{p_{2,y}/k_{2,y}} \Phi_{M/T} \rangle_{N/S} = 0,$$

c'est-à-dire, par le théorème de Frobenius (théorème B.30) et le théorème B.39,

$$\langle \mathrm{Defres}^{N/S}_{p_{1,y}/k_{1,y}} \Phi_{N/S}, \mathrm{Iso}(f_y) \mathrm{Defres}^{M/T}_{p_{2,y}/k_{2,y}} \Phi_{M/T} \rangle_{p_{1,y}/k_{1,y}} = 0. \tag{5.10}$$

Par symétrie de S et T, on peut faire le même raisonnement pour $\Phi_{M/T}$. De plus, si l'on étudie la décomposition, on voit apparaît f_y^{-1}, $p_{1,y}$, $k_{1,y}$, $p_{2,x}$ et $k_{2,x}$:

$$\Phi_{M/T} \cong \bigoplus_{y \in [N\backslash P/M]} \mathrm{Indinf}^{M/T}_{p_{2,y}/k_{2,y}} \mathrm{Iso}(f_y^{-1}) \mathrm{Defres}^{N/S}_{p_{1,x}/k_{1,y}} \Phi_{N/S}.$$

Comme avant, il existe un unique élément $x' \in [N\backslash P/M]$ tel que

$$\Phi_{M/T} \cong \mathrm{Indinf}^{M/T}_{p_{2,x'}/k_{2,x'}} \mathrm{Iso}(f_{x'}^{-1}) \mathrm{Defres}^{N/S}_{p_{1,x'}/k_{1,x'}} \Phi_{N/S}, \tag{5.11}$$

et pour tout $y \in [N\backslash P/M] - \{x'\}$

$$\langle \mathrm{Iso}\, f_y^{-1} \,\mathrm{Defres}^{N/S}_{p_{1,y}/k_{1,y}} \Phi_{N/S}, \mathrm{Defres}^{M/T}_{p_{2,y}/k_{2,y}} \Phi_{M/T} \rangle_{p_{1,y}/k_{1,y}} = 0. \quad (5.12)$$

Or pour tout y, les équations 5.10 et 5.12 sont équivalentes, ce qui implique que $x = x'$ (car si $y = x$ alors le produit scalaire dans l'équation 5.10 n'est pas nul et si $y = x'$ alors le produit scalaire dans l'équation 5.12 est aussi non-nul).

On pose $W = \mathrm{Iso}(f_x)\,\mathrm{Defres}^{M/T}_{p2,x/k_{2,x}} \Phi_{M/T}$. Alors comme $\mathrm{Indinf}^{N/S}_{p_{1,x}/k_{1,x}} W = \Phi_{N/S}$ est irréductible, cela implique que W est aussi irréductible. De plus, on a, si on utilise le théorème de Frobenius (théorème B.30) et la formule de Mackey (théorème 3.37),

$$\begin{aligned}
&\langle \Phi_{N/S}, \Phi_{N/S} \rangle_{N/S} \\
&= \langle \mathrm{Indinf}^{N/S}_{p_{1,x}/k_{1,x}} W, \mathrm{Indinf}^{N/S}_{p_{1,x}/k_{1,x}} W \rangle_{N/S} \\
&= \langle \mathrm{Inf}^{p_{1,x}}_{p_{1,x}/k_{1,x}} W, \mathrm{Res}^{N/S}_{p_{1,x}} \mathrm{Indinf}^{N/S}_{p_{1,x}/k_{1,x}} W \rangle_{p_{1,x}} \\
&= \langle \mathrm{Inf}^{p_{1,x}}_{p_{1,x}/k_{1,x}} W, \bigoplus_{y \in [p_{1,x}\backslash (N/S)/p_{1,x}]} \mathrm{Ind}^{p_{1,x}}_{p_{1,x} \cap {}^y p_{1,x}} \mathrm{Iso}(\gamma_y)\, \mathrm{Res}^{p_{1,x}}_{(p_{1,x})^y \cap p_{1,x}} \mathrm{Inf}^{p_{1,x}}_{p_{1,x}/k_{1,x}} W \rangle_{p_{1,x}} \\
&= \sum_{y \in [p_{1,x}\backslash (N/S)/p_{1,x}]} \langle \mathrm{Inf}^{p_{1,x}}_{p_{1,x}/k_{1,x}} W, \mathrm{Ind}^{p_{1,x}}_{p_{1,x} \cap {}^y p_{1,x}} \mathrm{Iso}(\gamma_y)\, \mathrm{Res}^{p_{1,x}}_{(p_{1,x})^y \cap p_{1,x}} \mathrm{Inf}^{p_{1,x}}_{p_{1,x}/k_{1,x}} W \rangle_{p_{1,x}} \\
&\geq \langle \mathrm{Inf}^{p_{1,x}}_{p_{1,x}/k_{1,x}} W, \mathrm{Ind}^{p_{1,x}}_{p_{1,x} \cap {}^{1_G} p_{1,x}} \mathrm{Iso}(\gamma_{1_G})\, \mathrm{Res}^{p_{1,x}}_{(p_{1,x})^{1_G} \cap p_{1,x}} \mathrm{Inf}^{p_{1,x}}_{p_{1,x}/k_{1,x}} W \rangle_{p_{1,x}} \\
&= \langle \mathrm{Inf}^{p_{1,x}}_{p_{1,x}/k_{1,x}} W, \mathrm{Inf}^{p_{1,x}}_{p_{1,x}/k_{1,x}} W \rangle_{p_{1,x}} \\
&= \langle W, W \rangle_{p_{1,x}/k_{1,x}}
\end{aligned}$$

où la dernière égalité découle de la proposition B.37.

On pose $W' = \mathrm{Defres}^{M/T}_{p_{2,x}/k_{2,x}} \Phi_{M/T}$. Alors comme $\mathrm{Iso}(f_x)W' = W$ est irréductible, W' est aussi irréductible et de plus, par le théorème de Frobenius (théorème B.30) et le théorème B.39,

$$\begin{aligned}
\langle W, W \rangle_{p_{1,x}/k_{1,x}} &= \langle W', W' \rangle_{p_{2,x}/k_{2,x}} \\
&= \langle \mathrm{Defres}^{M/T}_{p_{2,x}/k_{2,x}} \Phi_{M/T}, W' \rangle_{p_{2,x}/k_{2,x}} \\
&= \langle \Phi_{M/T}, \mathrm{Indinf}^{M/T}_{p_{2,x}/k_{2,x}} W' \rangle_{M/T} \\
&= m(\Phi_{M/T}, \mathrm{Indinf}^{M/T}_{p_{2,x}/k_{2,x}} W') \langle \Phi_{M/T}, \Phi_{M/T} \rangle_{M/T}.
\end{aligned}$$

Or $\langle W, W \rangle_{p_{1,x}/k_{1,x}}$ est différent de 0, donc le module $\Phi_{M/T}$ est un facteur de composition de $\mathrm{Indinf}^{M/T}_{p_{2,x}/k_{2,x}} W'$. Donc $\langle W, W \rangle_{p_{1,x}/k_{1,x}}$ est plus

grand ou égal à $\langle \Phi_{M/T}, \Phi_{M/T} \rangle_{M/T}$. Ainsi on a

$$\begin{aligned}\langle V(S), V(S) \rangle_P &= \langle \Phi_{N/S}, \Phi_{N/S} \rangle_{N/S} \\ &\geq \langle W, W \rangle_{p_{1,x}/k_{1,x}} \\ &\geq \langle \Phi_{M/T}, \Phi_{M/T} \rangle_{M/T} \\ &= \langle V(T), V(T) \rangle_P.\end{aligned}$$

Or on sait que $\langle V(S), V(S) \rangle_P = \langle V(T), V(T) \rangle_P$ car $V(S)$ et $V(T)$ sont isomorphes. Donc

$$\begin{aligned}\langle V(S), V(S) \rangle_P &= \langle \Phi_{N/S}, \Phi_{N/S} \rangle_{N/S} \\ &= \langle W, W \rangle_{p_{1,x}/k_{1,x}} \\ &= \langle \Phi_{M/T}, \Phi_{M/T} \rangle_{M/T} \\ &= \langle V(T), V(T) \rangle_P.\end{aligned}$$

On suppose maintenant, par l'absurde, que $p_{2,x} \neq M/T$ et on choisit un sous-groupe maximal H de M/T qui contient $p_{2,x}$. Par le lemme 4.16, la restriction de $\Phi_{M/T}$ à H est égal à $m\Phi_H$, pour un certain entier positif m. Or, par transitivité de la restriction (proposition B.23),

$$\begin{aligned}W' &= \operatorname{Defres}^{M/T}_{p_{2,x}/k_{2,x}} \Phi_{M/T} \\ &= \operatorname{Defres}^{H}_{p_{2,x}/k_{2,x}} \operatorname{Res}^{M/T}_{H} \Phi_{M/T} \\ &= \operatorname{Defres}^{H}_{p_{2,x}/k_{2,x}} m\Phi_H\end{aligned}$$

ne peut être irréductible que si $m = 1$. Or ceci n'est possible que si $p = 2$ et $|M/T| = 2$ ou si M/T est diédral ou semi-diédral et H est cyclique ou quaternionien généralisé.
Si $|M/T| = 2$, alors comme $p_{2,x} \leq M/T$, $p_{2,x} = \mathbf{1} = k_{2,x}$ et par conséquent, $W' = \operatorname{Res}^{M/T}_{\mathbf{1}} \Phi_{M/T} = \Phi_{\mathbf{1}} = \mathbb{Q}$. Ainsi on a aussi que $W \cong \mathbb{Q}$, et donc $\Phi_{N/S} = \operatorname{Indinf}^{N/S}_{p_{2,x}/k_{2,x}} \mathbb{Q} \cong \mathbb{Q}((N/S)/k_{2,x})$ (lemme B.43). Ainsi $\mathbb{Q}$ est un facteur de composition de $\Phi_{N/S}$, ce qui implique que $\Phi_{N/S} \cong \mathbb{Q}$, ce qui est impossible car S est différent de P (lemme 5.8). Par conséquent $|M/T| \neq 2$.
Si M/T est diédral ou semi-diédral et si H est cyclique ou quaternionien généralisé, alors $\operatorname{Res}^{M/T}_{H} \Phi_{M/T} = \Phi_H$. Si $p_{2,x} \neq H$, alors soit L un sous-groupe maximal de H qui contient $p_{2,x}$. Par le lemme 4.16, on a $\operatorname{Res}^{H}_{L} \Phi_H = 2\Phi_L$ et donc

$$W' = \operatorname{Defres}^{L}_{p_{2,x}/k_{2,x}} \operatorname{Res}^{H}_{L} \Phi H = \operatorname{Defres}^{L}_{p_{2,x}/k_{2,x}} 2\Phi_L$$

n'est pas irréductible, ce qui est une contradiction. Donc $p_{2,x} = H$. De plus, comme Φ_H est irréductible, toute déflation de Φ_H à un quotient propre de H est égale à 0. Par conséquent, vu que $W' = \operatorname{Def}^{H}_{H/k_{2,x}} \Phi_H$

est irréductible donc non-nul, $k_{2,x} = \mathbf{1}$ et $W' = \Phi_H$. Mais alors, si $|M/T| = 2^n$, $n \geq 4$ (et donc $|H| = 2^{n-1}$), par le lemme 4.15, on a $\langle \Phi_{M/T}, \Phi_{M/T} \rangle_{M/T} = 2^{n-3}$ et $\langle W', W' \rangle_H = \langle \Phi_H, \Phi_H \rangle_H = 2^{n-4}$. Cela est impossible car on sait que $\langle \Phi_{M/T}, \Phi_{M/T} \rangle_{M/T} = \langle W', W' \rangle_H$. Par conséquent $p_{2,x} = M/T$. Mais alors $W' = \mathrm{Def}^{M/T}_{(M/T)/k_{2,x}} \Phi_{M/T}$ est irréductible et toute déflation de $\Phi_{M/T}$ à un quotient propre de M/T est égale à 0, donc $k_{2,x} = \mathbf{1}$, et $W' = \Phi_{M/T}$.
Par symétrie de S et T et comme $x = x'$, on a aussi que $p_{1,x} = N/S$ et $k_{1,x} = \mathbf{1}$. Par conséquent, les équations 5.7 et 5.8 deviennent (sans les quotients)

$$N = S(N \cap {}^x M), \qquad S = S(N \cap {}^x T), \tag{5.13}$$

$$M = T(N^x \cap M), \qquad T = T(M \cap S^x). \tag{5.14}$$

En appliquant la conjugaison par x à l'équation 5.14, on obtient

$${}^x M = {}^x T({}^x N \cap {}^x M), \qquad {}^x T = {}^x T({}^x M \cap S). \tag{5.15}$$

Comme ${}^x T \subset {}^x M$ et par l'équation 5.13, on a $N \cap {}^x T \subset S \cap {}^x M$ et de même, comme $S \subset N$ et par l'équation 5.15, $S \cap {}^x M \subset N \cap {}^x T$. Mais alors, on a que $S \cap {}^x M = N \cap {}^x T$, $N = (N \cap {}^x M)S$ et ${}^x M = (N \cap {}^x M)\,{}^x T)$ (équations 5.13 et 5.15), c'est-à-dire

$$(N, S) \text{ — } ({}^x M, {}^x T)$$

ou encore

$$(N, S) \text{ —}_P (M, T),$$

ce qui est le résultat cherché.

Si les conditions 1. à 4. sont satisfaites, alors par la proposition 3.40, $N_P(S)/S$ et $N_P(T)/T$ sont isomorphes. □

Corollaire 5.21 *Soit P un p-groupe fini. Alors la relation —$_P$ sur l'ensemble des sections $(N_P(S), S)$ où S est un sous-groupe génétique de P est une relation d'équivalence. De même la relation $\widehat{=}_P$ sur l'ensemble des sous-groupes génétiques de P est une relation d'équivalence.*

Preuve: C'est une conséquence du théorème 5.20 et du fait que la relation "être isomorphe" est une relation d'équivalence. □

Définition 5.22 ([Bou], définition 9.6.11, page 189) *Soit P un p-groupe fini. Par le corollaire 5.21, la relation $\widehat{=}_P$ est une relation d'équivalence sur l'ensemble des sous-groupes génétiques. Une **base génétique de** P est un ensemble de représentants des classes d'équivalences des sous-groupes génétiques de P.*

Remarque 5.23 Si $\mathcal{G}$ est une base génétique de P, alors l'ensemble des $\mathbb{Q}P$-modules $V(S)$ pour $S \in \mathcal{G}$ est un ensemble complet de représentants des $\mathbb{Q}P$-modules irréductibles (de dimension finie).

Chapitre 6

Applications à quelques p-groupes particuliers

On va maintenant chercher les sous-groupes génétiques de certains groupes finis. On va commencer par le cas des p-groupes abéliens finis, puis les p-groupes finis extra-spéciaux et pour finir les groupes $C_{p^r} \rtimes C_{p^m}$, où C_{p^m} agit fidèlement sur C_{p^r}.

Avant de commencer les applications, on va prouver deux petits résultats qui seront utiles par la suite :

Proposition 6.1 *Soit P un p-groupe fini, A un sous-groupe normal de P et C un sous-groupe de P. On pose $D = N_P(C)$. Alors (P, A) — (D, C) si et seulement si $A = C$.*

Preuve:

$\Rightarrow$: On a les relations suivantes :

$$P \cap C = D \cap A \qquad (P \cap D)A = P \quad \text{et} \quad (P \cap D)C = D.$$

Comme A est normal dans P,

$$N_P(D) \subset N_P(D \cap A) = N_P(C \cap P) = N_P(C) = D.$$

Donc D est son propre normalisateur dans P et donc $D = P$ (théorème A.6). Mais alors $C = P \cap C = P \cap A = A$.

$\Leftarrow$: On a $D = N_P(C) = N_P(A) = P$ car A est normal dans P. Comme la relation — est une relation réflexive, il est clair que (P, A) — (P, C).

□

Proposition 6.2 *Soit P un p-groupe fini, S un sous-groupe de P et N un sous-groupe normal de P tel que $N \subset S$. Alors S est un sous-groupe expansif de P si et seulement si S/N est un sous-groupe expansif de P/N.*

En particulier, S est un sous-groupe génétique de P si et seulement si S/N est un sous-groupe génétique de P/N.

Preuve: Soit $\pi : P \to P/N$ la projection canonique. On va commencer par montrer que $Z_{P/N}(S/N) = Z_P(S)/N$. Comme $N_{P/N}(S/N) = N_P(S)/N$,

$$\begin{aligned} Z_{P/N}(S/N) &= Z\big(N_{P/N}(S/N)/(S/N)\big) \\ &= \big\{x \in N_{P/N}(S/N) \,\big|\, xyx^{-1}y^{-1} \in S/N,\ \forall\ y \in N_{P/N}(S/N)\big\} \\ &= \big\{xN \in N_P(S)/N \,\big|\, xyx^{-1}y^{-1} \in S,\ \forall\ y \in N_P(S)\big\} \\ &= Z_P(S)/N. \end{aligned}$$

Alors, par le lemme 5.10, S/N est expansif si et seulement si pour tout $x \in P/N$ tel que $(S/N)^x \cap Z_{P/N}(S/N) \leq S/N$, on a $x \in N_{P/N}(S/N)$. Cela est équivalent à dire que pour tout $x \in P$ tel que $(S^x)/N \cap Z_P(S)/N \leq S/N$, on a $x \in N_P(S)$, ce qui est aussi équivalent à dire que pour tout $x \in P$ tel que $(S^x) \cap Z_P(S) \leq S$, on a $x \in N_P(S)$, c'est-à-dire que S est expansif.

Pour la deuxième partie, on sait déjà que S est expansif si et seulement si S/N est expansif. Or, par le $3^{\text{ième}}$ théorème d'isomorphisme, $N_P(S)/S$ et $N_{P/N}(S/N)/(S/N)$ sont isomorphes, donc S est un sous-groupe génétique de P si et seulement si S/N est un sous-groupe génétique de P/N. □

6.1 Bases génétiques des p-groupes abéliens

On va commencer par faire le cas général puis illustrer ce cas général par quelques exemples.
Soit P un p-groupe abélien fini. Alors si S est un sous-groupe de P, S est normal dans P donc expansif (proposition 3.44). De plus, le quotient P/S est de p-rang normal 1 si et seulement si il est cyclique (car il est abélien). Donc pour trouver les sous-groupes génétiques de P, il suffit de trouver les sous-groupes S de P tels que P/S est cyclique. De plus, si S et S' sont deux sous-groupes génétiques de P, alors par la proposition 3.45, $S \eqsim_P S'$ si et seulement si $S = S'$. Ainsi, la seule base génétique de P est l'ensemble des sous-groupes génétiques de P.

Exemple 6.3: Le groupe cyclique C_{p^n}
Le groupe C_{p^n} possède $n+1$ sous-groupes cycliques donc, par le corollaire 2.10, le groupe C_{p^n} a $n+1$ $\mathbb{Q}C_{p^n}$-modules irréductibles et donc une base génétique possède $n+1$ éléments. Or tout quotient de C_{p^n} est cyclique donc tout sous-groupe de C_{p^n} est un sous-groupe génétique. Ainsi la seule base génétique de C_{p^n} est l'ensemble des sous-groupes de C_{p^n}.

Exemple 6.4: Le groupe $C_p \times C_p$
Le groupe $C_p \times C_p$ possède $p+2$ sous-groupes cycliques donc, par le corollaire 2.10, $C_p \times C_p$ possède $p+2$ $\mathbb{Q}(C_p \times C_p)$-modules irréductibles et donc une base génétique possède $p+2$ éléments. Or tout quotient de $C_p \times C_p$ par un sous-groupe propre est cyclique donc tout sous-groupe propre de $C_p \times C_p$ est un sous-groupe génétique. Si $C_p = \langle x \rangle$, alors la seule base génétique est :

$$\big\{P, \langle (x,1) \rangle\big\} \cup \big\{\langle (x^i, x) \rangle \,\big|\, 0 \leq i \leq p-1\big\}.$$

Exemple 6.5: Le groupe $C_p \times C_p \times C_p$
Un peu de calcul permet d'obtenir que le groupe $C_p \times C_p \times C_p$ possède p^2+p+2 sous-groupes cycliques, donc par le corollaire 2.10, $C_p \times C_p \times C_p$ possède p^2+p+2 $\mathbb{Q}(C_p \times C_p \times C_p)$-modules irréductibles et donc une base génétique possède p^2+p+2 éléments. Tout quotient de $C_p \times C_p \times C_p$ est abélien élémentaire, donc les sous-groupes génétiques sont les sous-groupes d'ordre p^2 et p^3. La base génétique de $C_p \times C_p \times C_p$ est l'ensemble des sous-groupes de $C_p \times C_p \times C_p$ d'ordre p^2 et $C_p \times C_p \times C_p$.

Exemple 6.6: Le groupe $C_{p^2} \times C_p$
Un peu de calcul permet d'obtenir que le groupe $C_{p^2} \times C_p$ possède $2p+2$ sous-groupes cycliques, donc par le corollaire 2.10, $C_{p^2} \times C_p$ possède $2p+2$ $\mathbb{Q}(C_{p^2} \times C_p)$-modules irréductibles et donc une base génétique possède $2p+2$ éléments. On pose $C_{p^2} = \langle x \rangle$ et $C_p = \langle y \rangle$. Quelques autres calculs permettent d'obtenir que l'ensemble

$$\big\{\langle (x^p, y^i)\rangle \,\big|\, 1 \leq i \leq p-1\big\} \cup \big\{\langle (x, y^i)\rangle \,\big|\, 0 \leq i \leq p-1\big\} \cup \big\{\langle (1,y)\rangle, C_p \times C_p, C_{p^2} \times C_p\big\}$$

est une base génétique de $C_{p^2} \times C_p$.

6.2 Les p-groupes extra-spéciaux

6.2.1 Définition et propriétés des p-groupes extra-spéciaux

Définition 6.7 *Soit P un p-groupe fini. On dit que P est un p-groupe* ***extra-spécial*** *si les conditions suivantes sont satisfaites :*

i) $[P,P] = Z(P) = \Phi(P)$ *;*

ii) $|Z(P)| = p$.

Propriété 6.8 *Soit P un p-groupe fini extra-spécial. Alors*

i) P est non-abélien.

ii) le groupe P est de classe 2 (où la classe désigne la longueur de la plus courte suite centrale).

iii) $P/Z(P)$ est abélien élémentaire.

Preuve:

i) Le groupe dérivé $[P,P] \neq \mathbf{1}$ donc P n'est pas abélien.

ii) La suite $P \trianglerighteq [P,P] \trianglerighteq \mathbf{1}$ est une suite centrale donc P est de classe au plus 2. Mais P n'est pas abélien donc sa classe n'est pas 1.

iii) C'est une conséquence du fait que $Z(P) = \Phi(P)$ et de la proposition A.10.

□

On va maintenant faire une classification des p-groupes extra-spéciaux. Soit

P un p-groupe fini extra-spécial et soit $n \in \mathbb{N}$ tel que $|P| = p^n$. Le quotient $P/Z(P)$ est abélien élémentaire (propriété 6.8 *iii)*) :

$$P/Z(P) \cong \underbrace{C_p \times C_p \times \ldots \times C_p}_{n-1 \text{ fois}}.$$

Ainsi c'est un $\mathbb{F}_p$-espace vectoriel que l'on va noter $(V, +, \cdot)$, où l'addition dans V correspond à la multiplication dans le quotient $P/Z(P)$. De plus, $Z(P) \cong C_p \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ et si on choisit $z \in Z(P) - \{1\}$, alors l'homomorphisme $f : (Z(P), \cdot) \to (\mathbb{F}_p, +)$ tel que $f(z) = 1$ est un isomorphisme de groupes. Ainsi on peut identifier $\mathbb{F}_p$ à $Z(P)$. On définit l'application $\beta : V \times V \to \mathbb{F}_p$ par $\beta(v_1, v_2) = f([x_1, x_2])$, où $v_1, v_2 \in V$ et $x_1, x_2 \in P$ sont tels que $v_1 = x_1 Z(P)$ et $v_2 = x_2 Z(P)$.

Lemme 6.9 *L'application β est une application bien définie. De plus, c'est une forme bilinéaire symplectique non-dégénérée.*

Preuve:

- L'application β est bien définie :
  Soit $x_1, x_2, y_1, y_2 \in P$ tels que $x_1 Z(P) = y_1 Z(P)$ et $x_2 Z(P) = y_2 Z(P)$. Il faut vérifier que $[x_1, x_2] = [y_1, y_2]$. Il existe $z_1, z_2 \in Z(P)$ tels que $y_1 = x_1 z_1$ et $y_2 = x_2 z_2$. Alors

$$\begin{aligned}
[y_1, y_2] &= y_1 y_2 y_1^{-1} y_2^{-1} \\
&= x_1 z_1 x_2 z_2 z_1^{-1} x_1^{-1} z_2^{-1} x_2^{-1} \\
&= x_1 x_2 x_1^{-1} x_2^{-1} \underbrace{z_1 z_1^{-1} z_2 z_2^{-1}}_{= 1_G} \\
&= [x_1, x_2].
\end{aligned}$$

  De plus, si $v_1, v_2 \in V$ et $x_1, x_2 \in P$ sont tels que $v_1 = x_1 Z(P)$ et $v_2 = x_2 Z(P)$ alors $[x_1, x_2] \in Z(P)$ car $Z(P) = [P, P]$. Donc $\beta(v_1, v_2)$ est bien définie.

- L'application β est bilinéaire :
  Soit $v_1, v_2, v \in V$ et $x_1, x_2, x \in P$ tels que $v_1 = x_1 Z(P), v_2 = x_2 Z(P)$

et $v = xZ(P)$. Alors $v_1 + v_2 = x_1Z(P)x_2Z(P) = x_1x_2Z(P)$ et on a

$$\begin{aligned}
\beta(v_1, v) + \beta(v_2, v) &= f([x_1, x]) + f([x_2, x]) \\
&= f([x_1, x][x_2, x]) \\
&= f(x_1 x x_1^{-1} x^{-1} \underbrace{[x_2, x]}_{\in\, Z(P)}) \\
&= f(x_1 [x_2, x] x x_1^{-1} x^{-1}) \\
&= f(x_1 x_2 x x_2^{-1} \underbrace{x^{-1}x}_{=\, 1_G} x_1^{-1} x^{-1}) \\
&= f(x_1 x_2 x \underbrace{x_2^{-1} x_1^{-1}}_{=\, (x_1x_2)^{-1}} x^{-1}) \\
&= f([x_1 x_2, x]) \\
&= \beta(v_1 + v_2, v)
\end{aligned}$$

et de même

$$\begin{aligned}
\beta(v, v_1) + \beta(v, v_2) &= f([x, x_1]) + f([x, x_2]) \\
&= f([x, x_1][x, x_2]) \\
&= f(x x_1 x^{-1} x_1^{-1} \underbrace{[x, x_2]}_{\in\, Z(P)}) \\
&= f(x x_1 x^{-1} [x, x_2] x_1^{-1}) \\
&= f(x x_1 \underbrace{x^{-1}x}_{=\, 1_G} x_2 x^{-1} x_2^{-1} x_1^{-1}) \\
&= f(x x_1 x_2 x^{-1} \underbrace{x_2^{-1} x_1^{-1}}_{=\, (x_1x_2)^{-1}}) \\
&= f([x, x_1 x_2]) \\
&= \beta(v, v_1 + v_2).
\end{aligned}$$

On a ainsi montré que $\beta(v_1+v_2, v) = \beta(v_1, v)+\beta(v_2, v)$ et $\beta(v, v_1+v_2) = \beta(v, v_1) + \beta(v, v_2)$.
Soit $v, w \in V$ et $\lambda \in \mathbb{F}_p$. Par ce qui précède, répété λ fois, on a $\beta(\lambda \cdot v, w) = \lambda\beta(v, w) = \beta(v, \lambda \cdot w)$. On a ainsi montré que β est une application bilinéaire.

- L'application bilinéaire β est symplectique :
  Soit $v \in V$ et $x \in P$ tel que $v = xZ(P)$. Alors

$$\beta(v, v) = f([x, x]) = f(1) = 0$$

  et donc β est une application bilinéaire symplectique.

- L'application β est une application bilinéaire non-dégénérée. Soit $v \in V$ tel que $\beta(v, w) = 0$, pour tout $w \in V$. On doit montrer que $v = 0$. Soit

$x \in P$ tel que $v = xZ(P)$. Alors pour tout $y \in P$, $f([x,y]) = 0$, donc pour tout $y \in P$, $[x,y] = 1_P$ et donc $x \in Z(P)$. Ainsi

$$v = xZ(P) = Z(P) = 0.$$

□

Alors, par la proposition C.10, il existe une base symplectique $B = \{v_1, w_1, v_2, w_2, \dots v_m, w_m\}$ de V tel que $\beta(v_i, w_i) = 1$ pour tout $1 \leq i \leq m$, $\beta(v_i, v_j) = \beta(w_i, w_j) = 0$ pour tout $1 \leq i, j \leq m$ et $\beta(v_i, w_j) = 0$ pour tout $1 \leq i, j \leq m$ tels que $i \neq j$. En particulier, $n - 1 = \dim_{\mathbb{F}_p} V = 2m$ pour un certain $m \in \mathbb{N}^*$ (la cardinalité de P est supérieur ou égal à p^3 car sinon P est abélien). Soit $x_1, x_2, \dots, x_m, y_1, y_2, \dots, y_m \in P$ tels que $v_i = x_i Z(P)$ et $w_i = y_i Z(P)$ pour tout $1 \leq i \leq m$. Alors, on a $[x_i, y_i] = z$ pour tout $1 \leq i \leq m$, $[x_i, x_j] = [y_i, y_j] = 1$ pour tout $1 \leq i, j \leq m$ et $[x_i, y_j] = 1$ pour tout $1 \leq i, j \leq m$ tels que $i \neq j$. En particulier, x_i et x_j commutent entre eux pour tout $1 \leq i, j \leq m$, y_i et y_j commutent entre eux pour tout $1 \leq i, j \leq m$ et x_i et y_j commutent entre eux pour tout $1 \leq i, j \leq m$ tels que $i \neq j$. Alors $P/Z(P)$ est engendré par $\{x_1 Z(P), \dots, x_m Z(P), y_1 Z(P), \dots y_m Z(P)\}$ et $Z(P)$ est engendré par z, donc $P = \langle x_1, y_1, x_2, y_2, \dots x_m, y_m, z \rangle$.

On va maintenant étudier l'ordre des éléments de P. On peut déjà remarquer que comme $P/Z(P)$ est abélien élémentaire, pour tout $x \in P$, $x^p \in Z(P)$. Or $Z(P)$ est cyclique d'ordre p donc pour tout $x \in P$, $x^{p^2} = 1_P$. Ainsi tout élément de P est d'ordre 1, p ou p^2. On définit alors l'application $\alpha : V \to \mathbb{F}_p$ par $\alpha(v) = f(x^p)$ où $v \in V$ et $x \in P$ est tel que $v = xZ(P)$.

Lemme 6.10 *L'application α est bien définie et si p est impair, c'est une application $\mathbb{F}_p$-linéaire.*

Preuve: On va commencer par montrer que l'application α est bien définie. Soit $x, y \in P$ tels que $xZ(P) = yZ(P)$. Il faut vérifier qu'on a alors $x^p = y^p$. Or, comme $xZ(P) = yZ(P)$, il existe $t \in Z(P)$ tel que $y = xt$. Alors $y^p = (xt)^p = x^p t^p = x^p$ car t commute avec x et t est d'ordre au plus p (le groupe $Z(P)$ est d'ordre p). Ainsi $\alpha(v)$ ne dépend pas du choix de $x \in P$ tel que $v = xZ(P)$. De plus, on sait déjà que pour tout $x \in P$, $x^p \in Z(P)$, donc $f(x^p)$ a bien un sens.

On suppose maintenant que p est impair et on va montrer que α est une application $\mathbb{F}_p$-linéaire. Soit $v_1, v_2 \in V$ et $x_1, x_2 \in P$ tels que $v_1 = x_1 Z(P)$ et $v_2 = x_2 Z(P)$. Alors $v_1 + v_2 = x_1 Z(P) x_2 Z(P) = x_1 x_2 Z(P)$. Donc

$$\begin{aligned} \alpha(v_1 + v_2) &= f\big((x_1 x_2)^p\big) \\ &\overset{(1)}{=} f(x_1^p x_2^p) \\ &= f(x_1^p) + f(x_2^p) \\ &= \alpha(v_1) + \alpha(v_2), \end{aligned}$$

où l'égalité (1) découle du lemme A.4 ($[x_1, x_2]$ appartient à $Z(P)$, de plus p est impair, donc p divise $\binom{p}{2}$ et donc $[x_1, x_2]^{\binom{p}{2}} = 1_P$).

Soit $v \in V$, $\lambda \in \mathbb{F}_p$ et $x \in P$ tel que $v = xZ(P)$. alors

$$\lambda \cdot v = \underbrace{v + v + \ldots + v}_{\lambda \text{ fois}} = \underbrace{xZ(P) \cdot xZ(P) \cdot \ldots \cdot xZ(P)}_{\lambda \text{ fois}} = x^\lambda Z(P).$$

Alors on a

$$\begin{aligned} \alpha(\lambda \cdot v) &= f((x^\lambda)^p) \\ &= f((x^p)^\lambda) \\ &= \lambda f(x^p) \\ &= \lambda \alpha(v) \end{aligned}$$

□

On suppose maintenant que p est impair. Alors, vu le lemme précédent, α est une application linéaire. En particulier,

$$\dim_{\mathbb{F}_p} V = \dim_{\mathbb{F}_p} \operatorname{Ker} \alpha + \dim_{\mathbb{F}_p} \operatorname{Im} \alpha$$

et donc $\dim_{\mathbb{F}_p} \operatorname{Ker} \alpha$ est égal à $n-2$ ou $n-1$ ($\dim_{\mathbb{F}_p} \operatorname{Im} \alpha$ est égal à 0 ou 1). Ainsi il y a deux cas possibles :

- 1^{er} cas : On a $\alpha \equiv 0$. Alors tout élément de P est d'ordre p. Ainsi on a

$$\begin{aligned} P = \langle z, x_1, \ldots, x_m, y_1, \ldots, y_m \,\big|\, & x_i^p = y_i^p = z^p = 1_P, \forall\ 1 \leq i \leq m, \\ & [x_i, z] = [y_i, z] = 1_P, \forall\ 1 \leq i \leq m, \\ & [x_i, y_i] = z, \forall\ 1 \leq i \leq m, \\ & [x_i, y_j] = 1_P, \forall\ 1 \leq i, j \leq m \text{ avec } i \neq j, \\ & [x_i, x_j] = [y_i, y_j] = 1_P, \forall\ 1 \leq i, j \leq m \rangle. \end{aligned}$$

- $2^{\text{ème}}$ cas : On a $\alpha \not\equiv 0$. Alors $\operatorname{Im} \alpha = \mathbb{F}_p$. On peut supposer que $x_1^p = z$, $y_1^p = 1_P$ et que $x_i^p = y_i^p = 1_P$ pour tout $2 \leq i \leq m$ (on peut modifier ou construire la base symplectique de telle sorte qu'elle satisfasse ces propriétés). Ainsi on a

$$\begin{aligned} P = \langle z, x_1, \ldots, x_m, y_1, \ldots, y_m \,\big|\, & x_1^p = z, y_1^p = z^p = 1_P, \\ & x_i^p = y_i^p = 1_P, \forall\ 2 \leq i \leq m, \\ & [x_i, z] = [y_i, z] = 1_P, \forall\ 1 \leq i \leq m, \\ & [x_i, y_i] = z, \forall\ 1 \leq i \leq m, \\ & [x_i, y_j] = 1_P, \forall\ 1 \leq i, j \leq m \text{ avec } i \neq j, \\ & [x_i, x_j] = [y_i, y_j] = 1_P, \forall\ 1 \leq i, j \leq m \rangle. \end{aligned}$$

Les deux cas nous donnent bien des groupes non-isomorphes car dans le premier cas, tous les éléments sont d'ordre 1 ou p, alors que dans le second, il existe des éléments d'ordre p^2.

On va maintenant traiter le cas où $p = 2$. Pour cela, on va commencer par étudier l'application α.

Lemme 6.11 *Si $p = 2$, alors l'application α est une forme quadratique et sa forme polaire associée est β.*

Preuve:

- Pour tout $\lambda \in \mathbb{F}_2$ et pour tout $v \in V$, on a $\alpha(\lambda \cdot v) = \lambda^2\alpha(v)$:
  Le corps $\mathbb{F}_2$ ne contient que deux éléments : 0 et 1. Or si λ est égal à 0 ou 1, il est clair que l'on a $\alpha(\lambda \cdot v) = \lambda^2\alpha(v)$, pour tout $v \in V$.

- L'application $(v, w) \mapsto \alpha(v+w)-\alpha(v)-\alpha(w)$ est une forme bilinéaire :
  Soit $v, w \in V$. Il existe $x, y \in P$ tel que $v = xZ(P)$ et $w = yZ(P)$. Alors $v + w = xZ(P)yZ(P) = xyZ(P)$. Donc on a

$$\begin{aligned}\alpha(v + w) - \alpha(v) - \alpha(w) &= f((xy)^2) - f(x^2) - f(y^2)\\ &= f(xyxy \underbrace{x^{-2}}_{\in\, Z(P)} y^{-2})\\ &= f(xyx^{-2}xyy^{-2})\\ &= f(xyx^{-1}y^{-1})\\ &= f([x, y]) = \beta(v, w).\end{aligned}$$

  Ainsi l'application $(v, w) \mapsto \alpha(v + w) - \alpha(v) - \alpha(w)$ est une forme bilinéaire et plus précisément, c'est même la forme bilinéaire β.

□

On va maintenant utiliser un théorème de classification des formes quadratiques pour certains corps de caractéristique 2 (théorème C.13). Si on applique ce théorème à notre cas, comme on sait déjà que $\dim_{\mathbb{F}_2} V = n-1 = 2m$, $m \in \mathbb{N}^*$, on se trouve dans le second cas du théorème C.13 et de plus δ ne peut prendre que deux valeurs : 0 ou 1. Ainsi il y a deux cas à considérer :

- Il existe une base $\{b_1, b_2, \ldots, b_n\}$ de V telle que

$$\alpha\Big(\sum_{i=1}^{n} \xi_i b_i\Big) = \sum_{i=1}^{m} \xi_i \xi_{m+i}.$$

Alors, si $x = \sum_{i=1}^{n} \lambda_i b_i$, $y = \sum_{j=1}^{n} \mu_j b_j \in V$,

$$\begin{aligned}
\beta(x,y) &= \alpha(x+y) - \alpha(x) - \alpha(y) \\
&= \sum_{i=1}^{m} (\lambda_i + \mu_i)(\lambda_{m+i} + \mu_{m+i}) - \sum_{j=1}^{m} \lambda_j \lambda_{m+j} - \sum_{k=1}^{m} \mu_k \mu_{m+k} \\
&= \sum_{i=1}^{m} (\lambda_i \lambda_{m+i} + \lambda_i \mu_{m+i} + \mu_i \lambda_{m+i} + \mu_i \mu_{m+i}) \\
&\quad - \sum_{j=1}^{m} \lambda_j \lambda_{m+j} - \sum_{k=1}^{m} \mu_k \mu_{m+k} \\
&= \sum_{i=1}^{m} (\lambda_i \mu_{m+i} + \mu_i \lambda_{m+i}).
\end{aligned}$$

On pose $v_i = b_i$ et $w_i = b_{m+i}$ pour tout $1 \leq i \leq m$. Alors $\{v_1, w_1, v_2, w_2, \ldots, v_m, w_m\}$ est une base de V et par le calcul précédent on a

$$\beta(v_i, w_j) = \delta_{ij}, \quad \beta(v_i, v_j) = 0 \quad \text{et} \quad \beta(w_i, w_j) = 0$$

pour tout $1 \leq i, j \leq m$. Par conséquent $\{v_1, w_1, v_2, w_2, \ldots, v_m, w_m\}$ est une base symplectique pour la forme β. Soit maintenant, pour tout $1 \leq i \leq m$, $x_i, y_i \in P$ tel que $v_i = x_i Z(P)$ et $w_i = y_i Z(P)$. Alors $\{x_1, \ldots, x_m, y_1, \ldots, y_m, z\}$ est un ensemble générateur de P et on a

$$[x_i, y_j] = \begin{cases} z & \text{si } i = j \\ 1_P & \text{sinon} \end{cases}, \quad [x_i, x_j] = 1_P \quad \text{et} \quad [y_i, y_j] = 1_P,$$

pour tout $1 \leq i, j \leq m$. De plus, $x_i^2 = f^{-1}(\alpha(v_i)) = f^{-1}(0) = 1$ et $y_i^2 = f^{-1}(\alpha(w_i)) = f^{-1}(0) = 1$, pour tout $1 \leq i \leq m$. Ainsi on peut résumer ces calculs par

$$\begin{aligned}
P = \langle z, x_1, \ldots, x_m, y_1, \ldots, y_m \,\big|\, & x_i^2 = y_i^2 = z^2 = 1_P, \forall\ 1 \leq i \leq m, \\
& [x_i, z] = [y_i, z] = 1_P, \forall\ 1 \leq i \leq m, \\
& [x_i, y_i] = z, \forall\ 1 \leq i \leq m, \\
& [x_i, y_j] = 1_P, \forall\ 1 \leq i, j \leq m \text{ avec } i \neq j, \\
& [x_i, x_j] = [y_i, y_j] = 1_P, \forall\ 1 \leq i, j \leq m \rangle.
\end{aligned}$$

- Il existe une base $\{b_1, b_2, \ldots, b_n\}$ de V tel que

$$\alpha\Big(\sum_{i=1}^{n} \xi_i b_i\Big) = \sum_{i=1}^{m} \xi_i \xi_{m+i} + \xi_m^2 + \xi_{2m}^2.$$

Alors, si $x = \sum_{i=1}^{n} \lambda_i b_i$, $y = \sum_{j=1}^{n} \mu_j b_j \in V$,

$$\begin{aligned}
\beta(x,y) &= \alpha(x+y) - \alpha(x) - \alpha(y) \\
&= \sum_{i=1}^{m} (\lambda_i + \mu_i)(\lambda_{m+i} + \mu_{m+i}) - \sum_{j=1}^{m} \lambda_j \lambda_{m+j} - \sum_{k=1}^{m} \mu_k \mu_{m+k} \\
&\quad + (\lambda_m + \mu_m)^2 + (\lambda_{2m} + \mu_{2m})^2 - \lambda_m^2 - \lambda_{2m}^2 - \mu_m^2 - \mu_{2m}^2 \\
&= \sum_{i=1}^{m} (\lambda_i \lambda_{m+i} + \lambda_i \mu_{m+i} + \mu_i \lambda_{m+i} + \mu_i \mu_{m+i}) \\
&\quad - \sum_{j=1}^{m} \lambda_j \lambda_{m+j} - \sum_{k=1}^{m} \mu_k \mu_{m+k} + \lambda_m^2 + \mu_m^2 + \underbrace{2\lambda_m \mu_m}_{=\,0 \,\in\, \mathbb{F}_2} \\
&\quad + \lambda_{2m}^2 + \mu_{2m}^2 + \underbrace{2\lambda_{2m}\mu_{2m}}_{=\,0 \,\in\, \mathbb{F}_2} - \lambda_m^2 - \lambda_{2m}^2 - \mu_m^2 - \mu_{2m}^2 \\
&= \sum_{i=1}^{m} (\lambda_i \mu_{m+i} + \mu_i \lambda_{m+i}).
\end{aligned}$$

On pose $v_i = b_i$ et $w_i = b_{m+i}$ pour tout $1 \leq i \leq m$. Alors $\{v_1, w_1, v_2, w_2, \ldots, v_m, w_m\}$ est une base de V et par le calcul précédent on a

$$\beta(v_i, w_j) = \delta_{ij}, \quad \beta(v_i, v_j) = 0 \quad \text{et} \quad \beta(w_i, w_j) = 0$$

pour tout $1 \leq i, j \leq m$. Par conséquent $\{v_1, w_1, v_2, w_2, \ldots, v_m, w_m\}$ est une base symplectique pour la forme β. Soit maintenant, pour tout $1 \leq i \leq m$, $x_i, y_i \in P$ tel que $v_i = x_i Z(P)$ et $w_i = y_i Z(P)$. Alors $\{x_1, \ldots, x_m, y_1, \ldots, y_m, z\}$ est un ensemble générateur de P et on a

$$[x_i, y_j] = \begin{cases} z & \text{si } i = j \\ 1_P & \text{sinon} \end{cases}, \quad [x_i, x_j] = 1_P \quad \text{et} \quad [y_i, y_j] = 1_P,$$

pour tout $1 \leq i, j \leq m$. De plus, $x_i^2 = f^{-1}(\alpha(v_i)) = f^{-1}(0) = 1$ et $y_i^2 = f^{-1}(\alpha(w_i)) = f^{-1}(0) = 1$, pour tout $1 \leq i \leq m-1$ et $x_m^2 = f^{-1}(\alpha(v_m)) = f^{-1}(1) = z$, $y_m^2 = f^{-1}(\alpha(w_m)) = f^{-1}(1) = z$. Ainsi on peut résumer ces calculs par

$$\begin{aligned}
P = \langle z, x_1, \ldots, x_m, y_1, \ldots, y_m \,\big|\, & x_m^2 = y_m^2 = z, z^2 = 1_P \\
& x_i^2 = y_i^2 = 1_P, \forall\ 1 \leq i \leq m-1, \\
& [x_i, z] = [y_i, z] = 1_P, \forall\ 1 \leq i \leq m, \\
& [x_i, y_i] = z, \forall\ 1 \leq i \leq m, \\
& [x_i, y_j] = 1_P, \forall\ 1 \leq i, j \leq m \text{ avec } i \neq j, \\
& [x_i, x_j] = [y_i, y_j] = 1_P, \forall\ 1 \leq i, j \leq m \rangle.
\end{aligned}$$

Les deux cas nous donnent bien des groupes non-isomorphes car dans le second cas, excepté les éléments 1_P et z, tous les éléments sont d'ordre 4, ce qui n'est pas le cas dans le premier cas.

Ainsi, dans chacun des cas, on a trouvé une description de P. Pour $|P| = p^{2m+1}$, $m \in \mathbb{N}^*$, il y a exactement deux groupes extra-spéciaux, à isomorphisme près. Avant d'étudier P pour trouver tous ses sous-groupes génétiques et une base génétique, on va faire quelques remarques sur sa structure.

Remarque 6.12

i) Etant donné que $P/Z(P)$ est abélien élémentaire, tout élément de ce quotient est d'ordre 1 ou p. Par conséquent, si $x \in P$, alors $x^p \in Z(P)$ et donc, comme $Z(P)$ est d'ordre p, $x^{p^2} = 1_P$. Ainsi tout élément de P est d'ordre 1, p ou p^2.

ii) Vu les descriptions de P, on peut remarquer que tout élément de P s'écrit de manière unique comme $x_1^{\alpha_1} \cdot \ldots \cdot x_m^{\alpha_m} y_1^{\beta_1} \cdot \ldots \cdot y_m^{\beta_m} z^{\gamma}$, avec $0 \leq \alpha_i, \beta_i \leq p-1$ pour tout $1 \leq i \leq m$ et $0 \leq \gamma \leq p-1$.

iii) Vu les relations entre les x_i, les y_j et z et la remarque précédent, la conjugaison revient à la multiplication par un élément de $Z(P)$.

6.2.2 Bases génétiques des p-groupes extra-spéciaux

On va commencer par deux exemples particuliers : Le groupe diédral D_8 et le groupe des quaternions Q_8, qui sont des 2-groupes extra-spéciaux (les seuls d'ordre 8 à isomorphisme près).

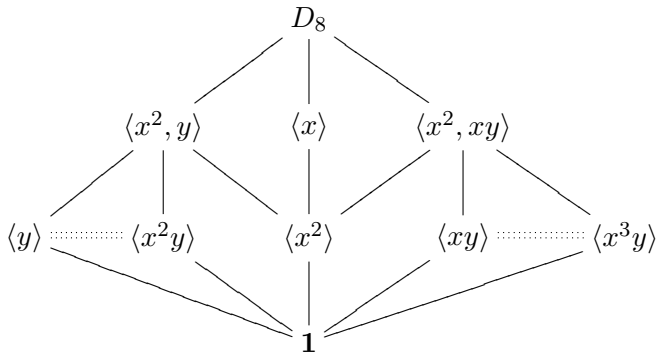
Exemple 6.13: Le groupe diédral D_8
On va étudier le groupe $D_8 = \langle x, y \,|\, x^4 = y^2 = 1, yxy = x^{-1} \rangle$. Il possède trois sous-groupes maximaux (lemme 4.6) :

$$\langle x \rangle, \qquad \langle x^2, y \rangle \quad \text{et} \quad \langle x^2, xy \rangle.$$

Ses autres sous-groupes sont :

$$D_8, \qquad \mathbf{1}, \qquad \langle x^2 \rangle, \qquad \langle y \rangle, \qquad \langle xy \rangle, \qquad \langle x^2 y \rangle \quad \text{et} \quad \langle x^3 y \rangle.$$

Voici un diagramme des sous-groupes de D_8 :



Ainsi, on peut voir que D_8 possède exactement 7 sous-groupes cycliques. Mais $\langle y \rangle$ et $\langle x^2 y \rangle$ sont conjugués par x et de même $\langle xy \rangle$ et $\langle x^3 y \rangle$ sont

conjugués par x. Il n'y a pas d'autres sous-groupes cycliques qui sont conjugués donc il y a, à conjugaison près, 5 sous-groupes cycliques et donc par le corollaire 2.10, il y a exactement 5 $\mathbb{Q}D_8$-modules irréductibles non-isomorphes et une base génétique de D_8 doit posséder 5 éléments.

On va montrer que les groupes $\langle y\rangle$, $\langle xy\rangle$, $\langle x^2y\rangle$ et $\langle x^3y\rangle$ sont expansifs. Par le lemme 5.10, un sous-groupe S de D_8 est expansif si et seulement si on a pour tout $z \in D_8$ tel que $S^z \cap Z_{D_8}(S) \leq S$, alors $z \in N_{D_8}(S)$. Si $S = \langle y\rangle$, alors $Z_{D_8}(S) = \langle x^2, y\rangle$. Soit $z \in D_8$ tel que $S^z \cap Z_{D_8}(S) \leq S$. Or $S^y = S$, $S^x = \langle x^2y\rangle$ et $S^{xy} = S^x$, donc pour tout $0 \leq i \leq 4$, pour tout $0 \leq i \leq 1$, $S^{x^iy^j}$ est égal à S ou à S^x qui sont les deux inclus dans $Z_{D_8}(S)$. Donc $S^z \cap Z_{D_8}(S) = S^z \leq S$, d'où comme S est fini, $S^z = S$. Ce qui implique que z appartient $N_{D_8}(S)$. Un raisonnement analogue permet de montrer que les trois autres sous-groupes ($\langle xy\rangle$, $\langle x^2y\rangle$ et $\langle x^3y\rangle$) sont aussi expansifs. Les autres sous-groupes de D_8 sont normaux dans D_8, donc expansifs (lemme 3.44). Alors, quelques calculs permettent d'obtenir le tableau suivant :

	H	$N_{D_8}(H)$	$N_{D_8}(H)/H$	Expansif	Génétique
$i)$	$\mathbf{1}$	D_8	D_8	oui	non
$ii)$	$\langle y\rangle$	$\langle x^2, y\rangle$	C_2	oui	oui
$iii)$	$\langle xy\rangle$	$\langle x^2, xy\rangle$	C_2	oui	oui
$iv)$	$\langle x^2y\rangle$	$\langle x^2, y\rangle$	C_2	oui	oui
$v)$	$\langle x^3y\rangle$	$\langle x^2, xy\rangle$	C_2	oui	oui
$vi)$	$\langle x^2\rangle$	D_8	$C_2 \times C_2$	oui	non
$vii)$	$\langle x\rangle$	D_8	C_2	oui	oui
$viii)$	$\langle x^2, y\rangle$	D_8	C_2	oui	oui
$ix)$	$\langle x^2, xy\rangle$	D_8	C_2	oui	oui
$x)$	D_8	D_8	$\mathbf{1}$	oui	oui

Ainsi on sait quels sont les sous-groupes génétiques de D_8. Il reste à voir ceux qui sont liés modulo D_8 entre eux (il doit y en avoir car on sait qu'il y a 5 éléments dans une base génétique et on a 8 sous-groupes génétiques). Or, par la proposition 6.1, ceux qui sont normaux ne peuvent pas être liés modulo D_8 avec un autre sous-groupe génétique (normal ou pas). Donc les seuls qui peuvent être liés modulo D_8 sont $ii)$, $iii)$, $iv)$ et $v)$. De plus, on sait déjà que $ii)$ et $iv)$ sont conjugués donc

$$(\langle x^2, y\rangle, \langle y\rangle) \text{—}_{D_8} (\langle x^2, y\rangle, \langle x^2y\rangle).$$

De même, on sait aussi que $iii)$ et $v)$ sont conjugués donc

$$(\langle x^2, xy\rangle, \langle xy\rangle) \text{—}_{D_8} (\langle x^2, xy\rangle, \langle x^3y\rangle).$$

On va montré $ii)$ et $iii)$ sont liés modulo D_8. On pose $A = \langle y\rangle$, $B = \langle x^2, y\rangle$, $C = \langle xy\rangle$ et $D = \langle x^2, xy\rangle$. Alors on a $B \cap C = \mathbf{1} = A \cap D$. De plus, $B \cap D = \langle x^2\rangle$, donc $(B \cap D)A = B$ et $(B \cap D)C = D$. Ainsi on a obtenu que (B, A) — (D, C) et donc aussi (B, A) —$_{D_8}$ (D, C). Par conséquent, pour la

relation —_{D_8}, les sections associés aux points $ii)$, $iii)$, $iv)$ et $v)$ sont dans la même classe d'équivalence. Ainsi $\{\langle y\rangle, \langle x\rangle, \langle x^2, y\rangle, \langle x^2, xy\rangle, D_8\}$ est une base génétique de D_8.

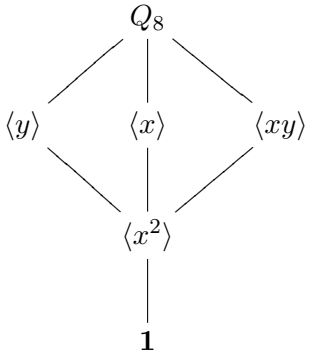
Exemple 6.14: Le groupe des quaternions Q_8
On va étudier le groupe $Q_8 = \langle x, y \,|\, x^4 = 1, y^2 = x^2, yxy = x^{-1}\rangle$. Il possède trois sous-groupes maximaux (lemme 4.6) :

$$\langle x\rangle, \qquad \langle y\rangle \quad \text{et} \quad \langle xy\rangle.$$

Ses autres sous-groupes sont :

$$Q_8, \qquad \mathbf{1} \quad \text{et} \quad \langle x^2\rangle.$$

Voici un diagramme des sous-groupes de Q_8 :



Ainsi, on peut voir que Q_8 possède exactement 5 sous-groupes cycliques. Il n'y a pas de sous-groupes cycliques qui sont conjugués donc il y a, à conjugaison près, 5 sous-groupes cycliques et donc par le corollaire 2.10, il y a exactement 5 $\mathbb{Q}Q_8$-modules irréductibles non-isomorphes et une base génétique de Q_8 doit possèder 5 éléments. Quelques calculs permettent d'obtenir le tableau suivant :

	H	$N_{Q_8}(H)$	$N_{Q_8}(H)/H$	Expansif	Génétique
$i)$	$\mathbf{1}$	Q_8	Q_8	oui	oui
$ii)$	$\langle x^2\rangle$	Q_8	$C_2 \times C_2$	oui	non
$iii)$	$\langle y\rangle$	Q_8	C_2	oui	oui
$iv)$	$\langle xy\rangle$	Q_8	C_2	oui	oui
$v)$	$\langle x\rangle$	Q_8	C_2	oui	oui
$vi)$	Q_8	Q_8	$\mathbf{1}$	oui	oui

Ainsi on sait quels sont les sous-groupes génétiques de Q_8. De plus, les sections $(N_{Q_8}(H), H)$ ne sont pas liées entre elles car tous les sous-groupes sont normaux. Ainsi $\{\mathbf{1}, \langle x\rangle, \langle y\rangle, \langle xy\rangle, Q_8\}$ est une base génétique de Q_8.

On va maintenant faire le cas général. Soit P un p-groupe fini extra-spécial, d'ordre p^{2m+1}. On pose $Z = Z(P)(= \Phi(P) = [P, P])$.

Tout élément de P est d'ordre divisant p^2 (remarque 6.12). Ceci reste valable pour tout quotient T/S, où (T, S) est une section de P. Comme les groupes D_{2n}, $n \geq 4$, SD_{2n}, $n \geq 4$ et Q_{2n}, $n \geq 3$ possède tous au moins un élément d'ordre au moins 8, un quotient T/S, où (T, S) est une section de P, est de p-rang normal 1 si et seulement si il est cyclique.

Ainsi on cherche les sous-groupes S de P qui sont expansifs et tels que $N_P(S)/S$ est cyclique.

On va utiliser la proposition 6.2 pour trouver tous les sous-groupes génétiques de P contenant Z : Soit $\pi : P \to P/Z$ la projection canonique. On sait que

$$P/Z \cong \underbrace{C_p \times \ldots \times C_p}_{2m \text{ fois}} = E$$

est un groupe abélien élémentaire. Or dans la section 6.1, on a déjà trouvé tous les sous-groupes génétiques des p-groupes abéliens. Ainsi il suffit de prendre leur préimage par π pour obtenir tous les sous-groupes génétiques de P contenant Z.

On va étudier un peu plus les sous-groupes génétiques de E, en particulier pour trouver combien il y en a. Tout sous-groupe de E est normal et expansif. Donc S est un sous-groupe génétique de E si et seulement si E/S est de p-rang normal 1. Or E/S est abélien élémentaire, donc de p-rang normal 1 si et seulement si $|E/S| \in \{1, p\}$. Donc on cherche les sous-groupes S de E d'ordre p^{2m-1} (le seul sous-groupe d'ordre p^{2m} de E est E lui-même). Or si l'on considère E comme un $\mathbb{F}_p$ espace-vectoriel, cela revient à chercher les sous-espaces vectoriels de dimension $2m-1$. Pour trouver le nombre de sous-espaces vectoriels de dimension $2m-1$, on va trouver le nombre de base à $2m-1$ éléments que l'on peut former avec les éléments de E puis diviser ce résultat par le nombre de bases d'un espace vectoriel de dimension $2m-1$.

Nombre de bases : $p^{\binom{2m-1}{2}} \prod_{i=2}^{2m} (p^i - 1)$

Nombre de bases qui donnent le même sous-espace : $p^{\binom{2m-1}{2}} \prod_{i=1}^{2m-1} (p^i - 1)$

Nombre de sous-groupes génétiques propres : $\dfrac{p^{2m}-1}{p-1} = \sum_{i=0}^{2m-1} p^i$.

Ainsi E possède $\sum_{i=0}^{2m-1} p^i + 1$ sous-groupes génétiques et donc P possède $\sum_{i=0}^{2m-1} p^i + 1$ sous-groupes génétiques contenant Z.

Comme tous les sous-groupes génétiques de E sont normaux de E, tous les sous-groupes génétiques de P contenant Z sont normaux dans P. En particulier, cela implique qu'ils ne peuvent pas être liés (modulo P) avec un autre sous-groupe génétique distinct (lemme 6.1).

Une dernière remarque sur ces sous-groupes génétiques : l'ensemble des sous-groupes génétiques propres de E est égal à l'ensemble des sous-groupes maximaux de E. Or l'ensemble des sous-groupes maximaux de E est en

bijection (via π) avec l'ensemble des sous-groupes maximaux de P. Ainsi l'ensemble des sous-groupes génétiques de P contenant Z est égal à l'ensemble des sous-groupes maximaux de P auquel on rajoute P.

Il reste maintenant à trouver les sous-groupes génétiques de P ne contenant pas Z. Soit H un sous-groupe de P ne contenant pas Z, c'est-à-dire tel que $H \cap Z = \mathbf{1}$. Alors pour tout $x, y \in H$, $[x, y] \in H \cap Z = \mathbf{1}$ et donc H est un groupe abélien. De plus, tout élément de H est d'ordre p (ou 1) car si $x \in H$, alors $x^p \in H \cap Z$. Donc H est abélien élémentaire.

Par le deuxième théorème d'isomorphisme, H est isomorphe à HZ/Z. De plus HZ/Z est un sous-groupe de P/Z, donc un sous-espace vectoriel de V. Comme H est abélien, HZ/Z est un sous-espace totalement isotrope (pour la forme bilinéaire symplectique non-dégénérée β ou pour la forme quadratique α). Or la dimension d'un sous-espace totalement isotrope est au plus $1/2 \dim_{\mathbb{F}_p} V = m$ (proposition C.10) et donc H est d'ordre au plus p^m.

Comme $H \cap Z = \mathbf{1}$ et comme la conjugaison correspond à la multiplication par un élément de Z (remarque 6.12), le normalisateur de H est égal au centralisateur de H. De plus, le centralisateur de H est égal au centralisateur de HZ dans P. Donc $N_P(H) = \{x \in P \,\big|\, [x, y] = 1 \ \forall\ y \in HZ\}$. Ainsi $N_P(H)/Z$ est égal (vu comme un sous-espace vectoriel de V) à $H^\perp$. Or, si $|H| = p^h$ (où $h \leq m$), par la proposition C.7,

$$\dim_{\mathbb{F}_p} H^\perp = \dim_{\mathbb{F}_p} V - \dim_{\mathbb{F}_p} H = 2m - h.$$

Donc $|N_P(H)/H| = p^{2m-h}$ et donc $|N_P(H)| = p^{2m-h+1}$.

Pour que $N_P(H)/H$ puisse être cyclique, comme tout élément de ce quotient est d'ordre 1, p ou p^2, il faut que $N_P(H)/H$ soit d'ordre au plus p^2. Or $|N_P(H)/H| = p^{2m-h+1}/p^h = p^{2(m-h)+1} \leq p^2$ si et seulement si $m = h$. Ainsi si H est un sous-groupe génétique ne contenant pas Z, alors $|H| = p^m$. On va montrer la réciproque, c'est-à-dire que si H est un sous-groupe de P d'ordre p^m ne contenant pas Z, alors H est un sous-groupe génétique de P. On va donc maintenant supposer que $|H| = p^m$. On peut remarquer que $HZ \subset N_P(H)$ et $|HZ| = p^{m+1} = |N_P(H)|$, donc $N_P(H) = HZ$. De plus, on a $|N_P(H)/H| = p$, donc $N_P(H)/H$ est de p-rang normal 1.

Il reste donc à montrer que H est un sous-groupe expansif. On doit montrer que si $x \in P$ est tel que ${}^xH \cap Z_P(H) \leq H$, alors $x \in N_P(H)$ (lemme 5.10). Or comme $N_P(H)/H \cong C_p$, $Z_P(H) = N_P(H) = HZ$. Donc on doit montrer que si $x \in P$ est tel que ${}^xH \cap HZ \leq H$, alors $x \in N_P(H)$. Or comme déjà dit, la conjugaison correspond à la multiplication par un élément de Z, donc ${}^xH$ est un sous-groupe de HZ. Donc on doit montrer que si $x \in P$ est tel que ${}^xH \leq H$, c'est-à-dire tel que ${}^xH = H$, alors $x \in N_P(H)$, ce qui est clair par définition du normalisateur $N_P(H)$.

Pour résumé tous ces calculs...

Théorème 6.15 *Soit P un p-groupe fini extra-spécial d'ordre p^{2m+1}. Alors les sous-groupes génétiques de P sont :*

- *le groupe P,*
- *les sous-groupes maximaux de P,*
- *les sous-groupes de P d'ordre p^m qui ne contiennent pas Z.*

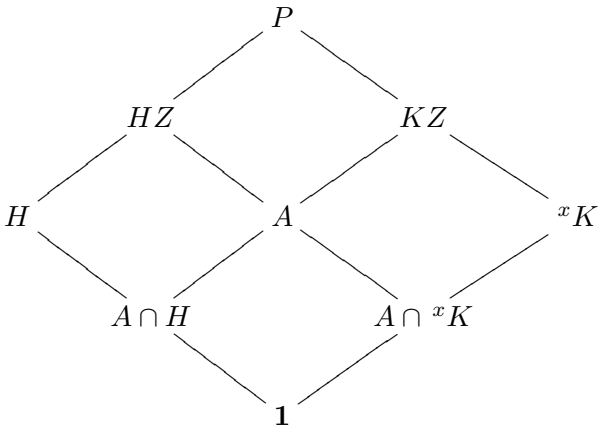
Pour trouver une base génétique, il faut encore trouver les sous-groupes génétiques qui sont liés (modulo P). Vu le lemme 6.1, les seuls sous-groupes génétiques de P qui peuvent être liés (modulo P) sont les sous-groupes de P d'ordre p^m qui ne contiennent pas Z.

Une première méthode est de compter le nombre de sous-groupes cycliques de P à conjugaison près et d'utiliser le corollaire 2.10 pour avoir le nombre d'éléments que comporte une base génétique. Si l'on fait les calculs, on constate que P possède exactement $2+\sum_{i=0}^{2m-1} p^i$ sous-groupes cycliques à conjugaison près et donc qu'une base génétique doit posséder $2+\sum_{i=0}^{2m-1} p^i$ éléments. Cela implique que tous les sous-groupes de P d'ordre p^m qui ne contiennent pas Z doivent être liés (modulo P).

On va ici montrer directement que tous ces groupes doivent être liés (modulo P). Soit H et K deux sous-groupes de P d'ordre p^m ne contenant pas Z. Alors, $N_P(H) = HZ$ et $N_P(K) = HZ$. On pose $A = HZ \cap KZ$. On doit trouver $x \in P$ tel que $(HZ, H) \text{—} (KZ, {}^xK)$, c'est-à-dire tel que

$$HZ \cap {}^xK = KZ \cap H, \qquad (HZ \cap KZ)H = HZ \quad \text{et} \quad (HZ \cap KZ)\,{}^xK = KZ.$$

Etant donné que $HZ \cap KZ$ contient Z, les deux dernières égalités sont toujours satisfaites, quelques soit $x \in P$. Ainsi on cherche $x \in P$ tel que $HZ \cap {}^xK = KZ \cap H$. Or $H = H \cap HZ$ et ${}^xK = {}^xK \cap KZ$, donc on cherche $x \in P$ tel que $A \cap {}^xK = A \cap H$. On a le diagramme suivant :



Comme $A \subset HZ$ est abélien et $Z \subset A$, A/Z est un sous-espace totalement isotrope de V. Les espaces vectoriels HZ/Z et KZ/Z sont des espaces totalement isotropes maximaux. On peut alors trouver une base symplectique $\{v_1, w_1, \ldots, v_r, w_r, \widehat{v}_{r+1}, \widehat{w}_{r+1} \ldots, \widehat{v}_m, \widehat{w}_m\}$ de V telle que $\{v_1, \ldots, v_r\}$ soit une base de A/Z et $\{v_1, \ldots, v_r, \widehat{v}_{r+1}, \ldots, \widehat{v}_m\}$ soit une base de HZ/Z.

De même, on peut alors trouver une base sympletique $\{v_1, w_1, \ldots, v_r, w_r, \widetilde{v}_{r+1}, \widetilde{w}_{r+1} \ldots, \widetilde{v}_m, \widetilde{w}_m\}$ de V telle que $\{v_1, \ldots, v_r\}$ soit une base de A/Z et $\{v_1, \ldots, v_r, \widetilde{v}_{r+1}, \ldots, \widetilde{v}_m\}$ soit une base de KZ/Z.

Pour tout $1 \leq i \leq r$, on peut trouver $x_i \in H \cap A$ tel que $v_i = x_i Z$ et $y_i \in P$ tel que $w_i = y_i Z$; de même pour tout $r+1 \leq i \leq m$, on peut trouver $\widehat{x}_i \in H$ tel que $\widehat{v}_i = \widehat{x}_i Z$. Il faut maintenant faire attention : pour $1 \leq i \leq r$, x_i n'appartient pas forcément à K. C'est pourquoi on va devoir introduire un conjugué de K.

Soit $1 \leq i \leq r$. Comme $x_i \in A \subset KZ$, il existe $u_i \in Z$ et $k_i \in K$ tels que $x_i = k_i u_i$. Or on peut trouver $0 \leq \alpha_i \leq p-1$ tel que $y_i^{-\alpha_i} x_i y_i^{\alpha_i} = k_i \in K$ (on peut trouver un α_i tel que la conjugaison par $y_i^{-\alpha_i}$ correspond à la multiplication par u_i^{-1}). On pose $x = y_1^{\alpha_1} \cdot \ldots \cdot y_r^{\alpha_r}$. Alors on peut voir que pour tout $1 \leq i \leq r$, $x^{-1} x_i x = k_i \in K$ et donc $x_i \in {}^x K$. On a trouvé l'élément x qui va permettre de montrer que $(HZ, H) \text{ — } (KZ, {}^x K)$. Pour tout $r+1 \leq i \leq m$, on peut trouver $\widetilde{x}_i \in {}^x K$ ($KZ = {}^x KZ$) tel que $\widetilde{v}_i = \widetilde{x}_i Z$.

On va maintenant utiliser les x_i, $\widehat{x}_i$ et $\widetilde{x}_i$ pour trouver des générateurs de H, ${}^x K$ et A. L'ensemble $\{x_1, \ldots, x_r, \widehat{x}_{r+1}, \ldots, \widehat{x}_m, z\}$ (où z est un générateur de Z, qui correspond à 1 dans $\mathbb{F}_p$) est un système de générateurs de HZ. Or $H \cap Z = \mathbf{1}$, donc $x_1, \ldots, x_r, \widehat{x}_{r+1}, \ldots, \widehat{x}_m$ est un système de générateurs de H :

$$H = \langle x_1, \ldots, x_r, \widehat{x}_{r+1}, \ldots, \widehat{x}_m \rangle.$$

De même, $x_1, \ldots, x_r, \widetilde{x}_{r+1}, \ldots, \widetilde{x}_m$ est un système de générateurs de ${}^x K$:

$${}^x K = \langle x_1, \ldots, x_r, \widetilde{x}_{r+1}, \ldots, \widetilde{x}_m \rangle.$$

De plus, on a aussi que

$$A = \langle x_1, \ldots, x_r, z \rangle.$$

Alors, on a clairement que $\langle x_1, \ldots, x_r \rangle \subset A \cap H$. Si $t \in A \cap H \subset A$, alors il existe $h \in \langle x_1, \ldots, x_r \rangle \subset H$ et $u \in Z$ tels que $t = hu$. Alors on a $u = h^{-1} t \in H \cap Z = \mathbf{1}$, donc $u = 1_P$ et donc $t = h \in \langle x_1, \ldots, x_r \rangle$. Ainsi $A \cap H = \langle x_1, \ldots, x_r \rangle$. De même, on peut montrer que $A \cap {}^x K = \langle x_1, \ldots, x_r \rangle$. Ainsi on a montré que $A \cap H = A \cap {}^x K$ et par conséquent $(HZ, H) \text{ — } (KZ, {}^x K)$, c'est-à-dire que $(HZ, Z) \text{ —}_P (KZ, K)$.

On peut résumer ceci par...

Théorème 6.16 *Soit P un p-groupe fini extra-spécial d'ordre p^{2m+1}. Alors l'ensemble des sous-groupes suivants est une base génétique de P :*

- *le groupe P,*
- *les sous-groupes maximaux de P,*
- *un sous-groupe de P d'ordre p^m qui ne contient pas Z.*

6.3 Les groupes $C_{p^r} \rtimes C_{p^m}$

Soit p un nombre premier différent de 2 et $m, n \in \mathbb{N}^*$. On va étudier un peu les groupes $C_{p^r} \rtimes C_{p^m}$, où C_{p^m} agit fidèlement sur C_{p^r}. On va montrer que les sous-groupes C_{p^m} et C_{p^r} sont des sous-groupes génétiques.

Soit $P = C_{p^r} \rtimes C_{p^m}$, où C_{p^m} agit fidèlement sur C_{p^r}. Soit a un générateur de C_{p^r} et b un générateur de C_{p^m}. Soit l'homomorphisme $\varphi : C_{p^m} \to \mathrm{Aut}(C_{p^r})$ qui donne l'action de C_{p^m} sur C_{p^r}. Etant donné que C_{p^m} et C_{p^r} sont cycliques, l'application φ est entièrement définie par la valeur de $\varphi(b)(a)$. Comme $\varphi(b)$ est un automorphisme de C_{p^r}, il doit envoyer un générateur de C_{p^r} sur un générateur de C_{p^r}. Il existe donc $0 \leq k \leq p^r - 1$, $\mathrm{pgcd}(p, k) = 1$ tel que $\varphi(b)(a) = a^k$. Alors, étant donné que φ et $\varphi(b^j)$ sont des homomorphismes, on a que

$$\varphi(b^j)(a^i) = a^{ik^j},$$

pour tout $0 \leq j \leq p^m - 1$ et pour tout $0 \leq i \leq p^r - 1$.

L'action de C_{p^m} sur C_{p^r} doit être fidèle, donc φ doit être injective. Ainsi, pour tout $0 \leq j \leq p^m - 1$, $\varphi(b^j)(a) \neq a$. Donc $a^{k^j} \neq a$ pour tout $0 \leq j \leq p^m - 1$. De plus $b^{p^m} = 1_P$, donc $\varphi(b^{p^m}) = \varphi(1_P) = \mathrm{Id}_{C_{p^r}}$, ce qui implique que $a^{k^{p^m}} = a$. Ainsi, si l'on considère k comme un élément de $(\mathbb{Z}/p^r\mathbb{Z})^*$, k doit être un élément d'ordre p^m. L'ordre de k divise la cardinalité de $(\mathbb{Z}/p^r\mathbb{Z})^*$, c'est-à-dire divise $p^{r-1}(p-1)$, donc $m \leq r - 1$ et donc $m < r$.

Lemme 6.17 *Soit p un nombre premier impair. Soit $u, l \in \mathbb{N}$ tel que $u \neq 0$ et $\mathrm{pgcd}(u, p) = 1$. La plus grande puissance de p divisant $k^{up^l} - 1$ est p^{r-m+l}. En particulier, la plus grande puissance divisant $k - 1$ est p^{r-m}.*

Preuve: Soit $c \in \mathbb{N}$ tel que p^c soit la plus grande puissance de p divisant $k - 1$ (k est différent de 1, donc c existe). On va commencer par remarquer que $c \geq 1$:
On peut montrer que $(\mathbb{Z}/p^r\mathbb{Z})^*$ est un groupe cyclique d'ordre $p^{r-1}(p-1)$. De plus, le groupe engendré par $p+1$ est d'ordre p^{r-1} et contient donc tous les éléments d'ordre une puissance de p. Ainsi il existe $1 \leq n \leq p^{r-1} - 1$ tel que $k \equiv (p+1)^n \pmod{p^r}$. Mais alors

$$\begin{aligned} k - 1 &\equiv (p+1)^n - 1 \pmod{p^r} \\ &\equiv \sum_{i=1}^{n} \binom{n}{i} p^i \pmod{p^r} \\ &\equiv p \cdot \sum_{i=1}^{n} \binom{n}{i} p^{i-1} \pmod{p^r}, \end{aligned}$$

donc p divise $k - 1$ et donc $c \geq 1$.
On va montrer que la plus grande puissance de p divisant $k^{up^l} - 1$ est p^{c+l}. On commence par prouver le résultat pour $u = 1$, par récurrence sur l.

- Par définition de c, p^c est la plus grande puissance de p divisant $k-1$.
- Soit $l \geq 1$. On suppose maintenant que p^{c+l-1} est la plus grande puissance de p divisant $k^{p^{l-1}} - 1$. Donc il existe $t \in \mathbb{N}^*$ avec $\text{pgcd}(t,p) = 1$ et tel que $k^{p^{l-1}} - 1 = p^{c+l-1}t$. Alors

$$\begin{aligned} k^{p^l} - 1 &= (k^{p^{l-1}})^p - 1 \\ &= (p^{c+l-1}t + 1)^p - 1 \\ &= \sum_{i=1}^{p} \binom{p}{i} p^{i(c+l-1)} t^i \\ &= p^{c+l}t + \sum_{i=2}^{p} \binom{p}{i} p^{i(c+l-1)} t^i. \end{aligned}$$

  Or $\binom{p}{2}$ est divisible par p, donc comme $c+l-1 \geq 1$ (car $c \geq 1$), p^{c+l+1} divise $\sum_{i=2}^{p} \binom{p}{i} p^{i(c+l-1)} t^i$. De plus, p^{c+l} divise $p^{c+l}t$, donc on a bien que p^{c+l} divise $k^{p^l} - 1$. Il reste à voir que c'est la plus grande puissance de p qui le fait. Or si p^{c+l+1} divise $k^{p^l} - 1$, alors comme il divise aussi $\sum_{i=2}^{p} \binom{p}{i} p^{i(c+l-1)} t^i$, il devrait aussi diviser $p^{c+l}t$. Cela implique que p devrait diviser t, ce qui est impossible car $\text{pgcd}(p,t) = 1$. Ainsi p^{c+l} est bien la plus grande puissance de p divisant $k^{p^l} - 1$.

On va maintenant faire le cas général. Par le cas précédent, on sait qu'il existe $t \in \mathbb{N}^*$ avec $\text{pgcd}(p,t) = 1$ et tel que $k^{p^l} - 1 = p^{c+l}t$. Alors

$$\begin{aligned} k^{p^l u} - 1 &= (k^{p^l})^u - 1 \\ &= (p^{c+l}t + 1)^u - 1 \\ &= \sum_{i=1}^{u} \binom{u}{i} p^{i(c+l)} t^i \\ &= up^{c+l}t + \sum_{i=2}^{u} \binom{u}{i} p^{i(c+l)} t^i. \end{aligned}$$

Donc p^{c+l} divise bien $k^{p^l u} - 1$. De plus, si p^{c+l+1} divisait $k^{p^l u} - 1$, alors comme p^{c+l+1} divise aussi $\sum_{i=2}^{u} \binom{u}{i} p^{u(c+l)} t^u$, p^{c+l+1} devrait aussi diviser $up^{c+l}t$, c'est-à-dire que p devrait diviser u ou t. Cela est impossible car $\text{pgcd}(p,t) = \text{pgcd}(p,u) = 1$. Ainsi p^{c+l+1} est bien la plus grande puissance de p divisant $k^{p^l u} - 1$.
Il reste maintenant à montrer que $c = r - m$. On sait que, dans $(\mathbb{Z}/p^r\mathbb{Z})^*$, k est un élément d'ordre p^m. Donc p^r divise $k^{p^m} - 1$. Or p^{c+m} est la plus grande puissance de p divisant $k^{p^m} - 1$, donc $r \leq c+m$ et donc $c \geq r-m$. De plus, $k^{p^{m-1}}$ ne doit pas être égal à 1 dans $(\mathbb{Z}/p^r\mathbb{Z})^*$, donc, p^{c+m-1} étant la plus grande puissance de p divisant $k^{p^{m-1}} - 1$, on a $c+m-1 < r$ et donc $c < r-m+1$, c'est-à-dire $c \leq r-m$. Ainsi on a obtenu $c = r-m$ et donc la plus grande puissance de p divisant $k^{p^l u} - 1$ est égale à p^{r-m+l}. □

Remarque 6.18 Le résultat du lemme précédent n'est pas toujours valable si $p = 2$. Cela vient du fait que p ne divise pas $\binom{p}{2}$ si $p = 2$. C'est pourquoi on s'est restreint au cas où p est impair.

Le produit dans $C_{p^r} \rtimes C_{p^m}$ est défini, si $x, y \in C_{p^r}$ et $s, t \in C_{p^m}$, par

$$(x, s) \cdot (y, t) = (x\varphi(s)(y), st).$$

Par conséquent, si $0 \leq i, n \leq p^r - 1$ et $0 \leq j, l \leq p^m - 1$,

$$(a^i, b^j) \cdot (a^n, b^k) = (a^{i+nk^j}, b^{j+k}).$$

En particulier, si $0 \leq i \leq p^r$, $0 \leq j \leq p^m$ et $n \in \mathbb{N}^*$,

$$(a^i, b^j)^n = (a^{i\sum_{s=0}^{n-1} k^{sj}}, b^{nj})$$

et

$$(a^i, b^j)^{-1} = (a^{-ik^{-j}}, b^{-j}),$$

où k^{-j} n'est pas l'inverse de k^j dans $\mathbb{R}$ mais un représentant de l'inverse de k^j dans $(\mathbb{Z}/p^r\mathbb{Z})^*$.

Lemme 6.19 *Soit p un nombre premier impair et soit $0 \leq i \leq p^r - 1$ et $0 \leq j \leq p^m - 1$. Si $p^{\widetilde{i}}$ est la plus grande puissance de p divisant i (si $i = 0$, alors on prend $\widetilde{i} = r$) et $p^{\widetilde{j}}$ la plus grande puissance de p divisant j (si $j = 0$, alors on prend $\widetilde{j} = m$), alors l'ordre de (a^i, b^j) est $p^{\max\{r-\widetilde{i}, m-\widetilde{j}\}}$. En d'autres mots, l'ordre de (a^i, b^j) dans $C_{p^r} \rtimes C_{p^m}$ est égal à l'ordre de (a^i, b^j) dans $C_{p^r} \times C_{p^m}$.*

Preuve: Si i ou j est nul, alors le résultat se vérifie facilement. On peut donc supposer que i et j sont différents de 0. Soit $n \in \mathbb{N}$ et $\widetilde{n} \in \mathbb{N}$ tel que $p^{\widetilde{n}}$ soit la plus grande puissance de p divisant n. Pour prouver le résultat, il suffit de montrer que la plus grande puissance de p divisant $\sum_{s=0}^{n-1} k^{sj}$ est égale à $p^{\widetilde{n}}$. Or

$$\sum_{s=0}^{n-1} k^{sj} = \frac{(k^j)^n - 1}{k^j - 1},$$

donc il suffit de trouver la plus grande puissance de p qui divise $(k^{jn} - 1)/(k^j - 1)$. Mais, par le lemme 6.17, la plus grande puissance de p divisant $k^{jn} - 1$ est $p^{r-m+\widetilde{j}+\widetilde{n}}$ et la plus grande puissance de p divisant $k^j - 1$ est $p^{r-m+\widetilde{j}}$, donc la plus grande puissance de p divisant $\sum_{s=0}^{n-1} k^{sj}$ est $p^{\widetilde{n}}$.

La plus grande puissance de p divisant $i\sum_{s=0}^{n-1} k^{sj}$ est $p^{\widetilde{n}+\widetilde{i}}$ et la plus grande puissance de p divisant jn est $p^{\widetilde{n}+\widetilde{j}}$. Mais alors $(a^i, b^j)^n = 1_P$ si et seulement si p^r divise $p^{\widetilde{n}+\widetilde{i}}$ et p^m divise $p^{\widetilde{n}+\widetilde{j}}$, c'est-à-dire si et seulement si

$\widetilde{n} \geq r - \widetilde{\imath}$ et $\widetilde{n} \geq m - \widetilde{\jmath}$. En particulier, le plus petit n qui satisfasse cela est $p^{\max\{r-\widetilde{\imath}, m-\widetilde{\jmath}\}}$, qui est donc bien l'ordre de (a^i, b^j). □

On a maintenant tous les résultats nécessaires pour montrer que C_{p^r} et C_{p^m} sont des sous-groupes génétiques de P.

Proposition 6.20 *Soit p un nombre premier impair. Le sous-groupe C_{p^r} est un sous-groupe génétique de $P = C_{p^r} \rtimes C_{p^m}$.*

Preuve: Dans un produit semi-direct $N \rtimes K$, le sous-groupe N est un sous-groupe normal de $N \rtimes K$ (où $N = \{(n,k) \in N \rtimes K \,\big|\, k = 1_K\}$). Donc ici le sous-groupe C_{p^r} est un sous-groupe normal de $P = C_{p^r} \rtimes C_{p^m}$ et est donc un sous-groupe expansif (lemme 3.44). Il faut donc juste montrer que P/C_{p^r} est un groupe de p-rang normal 1. Si $x \in P$, on note $\overline{x}$ l'élément xC_{p^r} de P/C_{p^r}. Si $0 \leq i \leq p^r - 1$ et $0 \leq j \leq p^m - 1$, on a

$$\overline{(a^i, b^j)} = \overline{(a^i, 1)(1, b^j)} = \overline{(1, b^j)} = \overline{(1, b)}^j.$$

Donc $P/C_{p^r} = \langle \overline{(1,b)} \rangle$. Or $(1,b)^j = (1, b^j) \in C_{p^r}$ si et seulement si $b^j = 1$, donc $\overline{(1,b)}$ est d'ordre p^m et donc $P/C_{p^r} \cong C_{p^m}$ est de p-rang normal 1. □

Proposition 6.21 *Soit p un nombre premier impair. Le sous-groupe C_{p^m} est un sous-groupe génétique de $P = C_{p^r} \rtimes C_{p^m}$.*

Preuve: On pose $H = C_{p^m}$. On va commencer par calculer $N_P(H)$. Or $x \in N_P(H)$ si et seulement si ${}^x(1,b) \in H$. Soit $0 \leq i \leq p^r - 1$ et $0 \leq j \leq p^m - 1$. On a

$$\begin{aligned}(a^i, b^j)(1,b)(a^i, b^j)^{-1} &= (a^i, b^{j+1})(a^{-ik^{-j}}, b^{-j}) \\ &= (a^{i - ik^{-j}k^{j+1}}, b) \\ &= (a^{i(1-k)}, b).\end{aligned}$$

Pour que (a^i, b^j) appartiennent à $N_P(H)$, il faut que $(a^{i(1-k)}, b)$ appartienne à H, c'est-à-dire que p^r diviser $i(1-k)$. Or la plus grande puissance de p qui divise $1 - k = -1(k-1)$ est p^{r-m} (lemme 6.17), donc il faut que p^m divise i. Ainsi on a

$$N_P(H) = \big\{(a^i, b^j) \in P \,\big|\, 0 \leq i \leq p^{r-m} - 1, 0 \leq j \leq p^m - 1, p^m \text{ divise } i\big\}.$$

On va maintenant montrer que $N_P(H)/H$ est de p-rang normal 1. Si $x \in N_P(H)$, on note $\overline{x}$ l'élément xH de $N_P(H)/H$. Si $0 \leq i \leq p^{r-m} - 1$ et $0 \leq j \leq p^m - 1$, on a

$$\overline{(a^{ip^m}, b^j)} = \overline{(a^{ip^m}, 1)(1, b^j)} = \overline{(a^{ip^m}, 1)} = \overline{(a, 1)}^{ip^m}.$$

Donc $N_P(H)/H = \langle \overline{(a^{p^m}, 1)} \rangle$. Or $(a^{p^m}, 1)^i = (a^{ip^m}, 1) \in H$ si et seulement si $a^{ip^m} = 1$, donc $\overline{(a^{p^m}, 1)}$ est d'ordre p^{r-m} et donc $N_P(H)/H \cong C_{p^{r-m}}$ est de p-rang normal 1.

On va pour finir montrer que H est un sous-groupe expansif. Par le lemme 5.10, il faut montrer que si $x \in P$ est tel que $H^x \cap Z_P(H) \leq H$, alors $x \in N_P(H)$. Comme $x \in N_P(H)$ si et seulement si $x^{-1} \in N_P(H)$, cela est équivalent à montrer que si $x \in P$ est tel que ${}^xH \cap Z_P(H) \leq H$, alors $x \in N_P(H)$. Comme $N_P(H)/H \cong C_{p^{r-m}}$ est abélien, $Z_P(H) = N_P(H)$. Soit $x \in P - \{1_P\}$ tel que $H^x \cap Z_P(H) \leq H$. Soit $0 \leq i \leq p^r - 1$ et $0 \leq j \leq p^m - 1$ tels que $x = (a^i, b^j)$. Alors, pour tout $1 \leq l \leq p^m - 1$,

$$\begin{aligned} {}^x(1, b^l) &= (a^i, b^j)(1, b^l)(a^i, b^j)^{-1} \\ &= (a^i, b^{j+l})(a^{-ik^{-j}}, b^{-j}) \\ &= (a^{i-ik^{-j}k^{j+l}}, b^l) \\ &= (a^{i(1-k^l)}, b^l). \end{aligned}$$

Si $i = 0$, il est clair que $x \in N_P(H)$, donc on peut supposer que $i \neq 0$. Soit $\widetilde{\imath} \in \mathbb{N}$ tel que $p^{\widetilde{\imath}}$ soit la plus grande puissance de p divisant i. Si $\widetilde{l} \in \mathbb{N}$ tel que $p^{\widetilde{l}}$ soit la plus grande puissance de p divisant l, alors ${}^x(1, b^l)$ appartient à $N_P(H)$ si et seulement si p^m divise $i(1 - k^l)$, c'est à dire si et seulement si $m \leq \widetilde{\imath} + r - m + \widetilde{l}$, ce qui est équivalent à $\widetilde{l} \geq 2m - r - \widetilde{\imath}$. On va maintenant distinguer deux cas :

- On suppose que $2m - r - \widetilde{\imath} > 0$. On remarque que

  $$2m - r - \widetilde{\imath} \leq 2m - r = m - (r - m) \leq m - 1.$$

  On pose $\widetilde{l} = 2m - r - \widetilde{\imath}$ et $l = p^{\widetilde{l}}$. Alors $1 \leq l \leq p^{m-1} \leq p^m - 1$ et $(a^{i(1-k^l)}, b^l)$ appartient à ${}^xH \cap N_P(H)$ et donc appartient aussi à H. Par conséquent p^r divise $i(1 - k^l)$. Or la plus grande puissance de p divisant $i(1 - k^l)$ est $p^{\widetilde{\imath}+r-m+\widetilde{l}} = p^m$, donc $r \leq m$, ce qui est impossible car $r > m$.

- On suppose que $2m - r - \widetilde{\imath} \leq 0$. Alors

  $${}^xH \cap N_P(H) = \left\{ (a^{i(1-k^l)}, b^l) \in P \,\middle|\, 0 \leq l \leq p^m - 1 \right\} \subset H.$$

  Or alors $(a^{i(1-k)}, b)$ appartient à ${}^xH \cap N_P(H)$ et donc appartient aussi à H. Par conséquent p^r divise $i(1 - k)$. Or la plus grande puissance de p divisant $i(1 - k)$ est $p^{\widetilde{\imath}+r-m}$, donc $r \leq \widetilde{\imath} + r - m$, c'est-à-dire $\widetilde{\imath} \leq m$. Par suite, p^m divise i et donc x appartient à $N_P(H)$.

Ainsi on a montré que H est un sous-groupe expansif et donc H est un sous-groupe génétique de P. □

Conclusion

Ce travail m'a permis d'étudier et de comprendre des notions importantes sur la théorie des sous-groupes génétiques. Le fait d'avoir pu étudier et modifier les preuves de certains résultats introduits dans les chapitres 4 et 5 a constitué un travail intéressant de comparaison et de réflexion. J'ai également découvert de nombreuses notions, comme la formule d'inversion de Möbius, les (H, G)-bi-ensembles et leurs propriétés, et de nouveaux résultats sur les KG-modules.

Dans le dernier chapitre sur les applications, j'ai donné quelques exemples de p-groupes finis pour lesquels j'ai essayé de trouver les sous-groupes génétiques et les bases génétiques. Pour le dernier exemple sur les groupes $C_{p^r} \rtimes C_{p^m}$, je n'ai donné que deux sous-groupes génétiques et seulement dans le cas où C_{p^m} agit fidèlement sur C_{p^r} et où p est un nombre premier impair. On peut continuer l'étude de ces groupes pour trouver les autres sous-groupes génétiques et pour généraliser les résultats à un groupe $C_{p^r} \rtimes C_{p^m}$ quelconque. Une autre continuation possible est d'étudier des p-groupes finis différents.

Annexe A

Rappels sur les groupes

Dans ce chapitre, on rappelle quelques définitions et théorèmes qui sont utiles dans ce projet. La plupart de ces théorèmes seront énoncés sans démonstration.

Voici la définition de quelques groupes :

Définition A.1

i) Soit $n \geq 0$. Le ***groupe cyclique*** C_n ***d'ordre*** n *est défini par :*

$$C_n = \langle x \,|\, x^n = 1 \rangle.$$

ii) Soit $n \geq 3$. Le ***groupe des quaternions généralisés*** Q_{2^n} ***d'ordre*** 2^n *est défini par :*

$$Q_{2^n} = \langle x, y \,|\, x^{2^{n-1}} = 1, yxy^{-1} = x^{-1}, x^{2^{n-2}} = y^2 \rangle.$$

iii) Soit $n \geq 3$. Le ***groupe diédral*** D_{2^n} ***d'ordre*** 2^n *est défini par :*

$$D_{2^n} = \langle x, y \,|\, x^{2^{n-1}} = y^2 = 1, yxy^{-1} = x^{-1} \rangle.$$

iv) Soit $n \geq 4$. Le ***groupe semi-diédral*** SD_{2^n} ***d'ordre*** 2^n *est défini par :*

$$SD_{2^n} = \langle x, y \,|\, x^{2^{n-1}} = y^2 = 1, yxy^{-1} = x^{2^{n-2}-1} \rangle.$$

Définition A.2 *Soit $(G, \cdot)$ un groupe. On définit le* ***groupe opposé*** $(G^{op}, \star)$ *par $G^{op} = G$ comme ensemble et la loi de multiplication est définie par $g \star h = h \cdot g$, pour tout $g, h \in G^{op}$.*

Définition A.3 *Soit G un groupe. On définit* ***le sous-groupe de Frattini de*** G*, noté $\Phi(G)$, par l'intersection de tous les sous-groupes maximaux de G.*

Lemme A.4 ([Rot95], lemme 5.42, page 119) *Soit G un groupe et a, $b \in G$. On suppose que $[a, b] = z$ est central dans G.*

i) On a $[a^i, b^j] = z^{ij}$, pour tout $i, j \in \mathbb{N}^*$.

ii) Si $n \in \mathbb{N}$, alors $(ab)^n = z^{-\binom{n}{2}} a^n b^n$.

A.1 Rappels sur les p-groupes fini

Pour cette section, p désigne un nombre premier

Définition A.5 *Un groupe fini P est un **p-groupe fini** s'il existe $n \in \mathbb{N}$ tel que $|P| = p^n$.*

Théorème A.6 ([Tsu82], page 99, théorème 2.5) *Soit P un p-groupe fini non trivial. Alors :*

i) $Z(P) \neq \mathbf{1}$.

ii) Si H est un sous-groupe propre de P, alors $H \subsetneq N_P(H)$.

iii) Si H est un sous-groupe maximal de P, alors H est normal dans P et $|P : H| = p$.

iv) Tout groupe d'ordre p^2 est abélien.

Proposition A.7 ([Ré89], page 98, Bemerkung 1.4) *Soit G un p-groupe fini et N un sous-groupe normal non trivial de G. Alors l'intersection de N avec le centre de G est non trivial :*

$$N \cap Z(G) \neq \mathbf{1}.$$

Définition A.8 *Soit P un p-groupe fini. Alors P est un **groupe abélien élémentaire** s'il existe $n \in \mathbb{N}^*$ tel que*

$$P \cong \underbrace{C_p \times \ldots \times C_p}_{n \text{ fois}}.$$

Théorème A.9 ([Gor68], théorème 3.2, page 10) *Un p-groupe fini abélien élémentaire d'ordre p^n est isomorphe à un espace vectoriel de dimension n sur le corps $\mathbb{F}_p$.*

Théorème A.10 ([Gor68], théorème 1.3, page 174) *Soit P un p-groupe fini. Alors le facteur de Frattini $P/\Phi(P)$ est un p-groupe abélien élémentaire.*

Propriété A.11 *Si G est l'un des groupes suivant :*

i) Le groupe des quaternions généralisés Q_{2^n} pour $n \geq 3$,

ii) Le groupe diédral D_{2^n} pour $n \geq 3$,

iii) Le groupe semi-diédral SD_{2^n} pour $n \geq 4$,

alors $[G, G] = \Phi(G) = \langle x^2 \rangle$ et $Z(G) = \langle x^{2^{n-2}} \rangle$. De plus, on a

$$Q_{2^n}/Z(Q_{2^n}) \cong D_{2^n}/Z(D_{2^n}) \cong SD_{2^n}/Z(SD_{2^n}) \cong D_{2^{n-1}}.$$

Preuve: On suppose que G est le groupe diédral

$$D_{2^n} = \langle x, y \,\big|\, x^{2^{n-1}} = y^2 = 1, yxy^{-1} = x^{-1} \rangle.$$

On commence par remarquer que tout élément de G s'écrit de manière unique comme $x^i y^j$ avec $0 \leq i \leq 2^{n-1} - 1$ et $0 \leq j \leq 1$.

On va commencer par calculer le centre de G. Il est facile de voir que 1_G et $x^{2^{n-2}}$ appartiennent à $Z(G)$. Il faut voir qu'il n'y a pas d'autres éléments dans le centre. Or $yxy^{-1} = x^{-1}$, donc $yx^i y^{-1} = x^{-i}$, pour tout $0 \leq i \leq 2^{n-1} - 1$. Ainsi $yx^i y^{-1} \neq x^i$ sauf si $i = 0$ ou $i = 2^{n-2}$ et donc y et x^i n'appartiennent pas à $Z(G)$, pour tout $1 \leq i \leq 2^{n-1} - 1$ tel que $i \neq 2^{n-2}$ Si $0 \leq i \leq 2^{n-1} - 1$, alors $y(x^i y)y^{-1}(x^i y)^{-1} = yx^i y^{-1} x^{-i} = x^{-2i} \neq 1_G$ sauf si $i = 0$ ou 2^{n-1}. Ainsi si $1 \leq i \leq 2^{n-1}$ tel que $i \neq 2^{n-2}$ alors $x^i y$ appartient pas à $Z(G)$. Il ne reste plus qu'à voir que $x^{n-2}y$ n'appartient pas à $Z(G)$. Or si $x^{n-2}y$ appartient $Z(G)$, alors, comme x^{n-2} appartient aussi à $Z(G)$, cela implique que y appartient à $Z(G)$, ce qui n'est pas le cas. Ainsi, on a vu que les seuls éléments de $Z(G)$ sont 1_G et $x^{2^{n-2}}$ et donc $Z(G) = \langle x^{2^{n-2}} \rangle$.

On va maintenant calculer le groupe dérivé $[G, G]$. Soit $0 \leq i, k \leq 2^{n-1}-1$ et $0 \leq j, l \leq 1$. On va calculer $[x^i y^j, x^k y^l]$. Il faut distinguer quatre cas.

- $j = l = 0$: Alors $[x^i y^j, x^k y^l] = 1_G$.
- $j = 1$ et $l = 0$: Alors $[x^i y^j, x^k y^l] = x^i y x^k y^{-1} x^{-i} x^{-k} = x^{-2k}$.
- $j = 0$ et $l = 1$: Alors $[x^i y^j, x^k y^l] = x^i x^k y x^{-i} y^{-1} x^{-k} = x^{2i}$.
- $j = l = 1$: Alors $[x^i y^j, x^k y^l] = x^i y x^k y y^{-1} x^{-i} y^{-1} x^{-k} = x^{2(i-k)}$.

Ainsi $[G, G] \subset \langle x^2 \rangle$. De plus, $x^2 = xy^{-1}x^{-1}y = [x, y^{-1}] \in [G, G]$, donc $[G, G] = \langle x^2 \rangle$.

Il reste à calculer $\Phi(G)$. Les sous-groupes $\langle x \rangle$, $\langle x^2, y \rangle$ et $\langle x^2, xy \rangle$ sont des sous-groupes maximaux de G. Ainsi $\Phi(G)$ est un sous-groupe de l'intersection de ces trois groupes, c'est-à-dire de $\langle x^2 \rangle$. Or G est un 2-groupe, donc $G/\Phi(G)$ est un 2-groupe abélien élémentaire (théorème A.10). Or si H est un sous-groupe propre de $\langle x^2 \rangle$, alors G/H n'est pas abélien élémentaire, donc $\Phi(G) = \langle x^2 \rangle$.

Les cas des groupes Q_{2^n} et SD_{2n} se traitent de manière analogue. □

Proposition A.12 ([Rob82], résultat 5.3.6, page 138) *Soit P un p-groupe fini. Alors P possède un unique sous-groupe cyclique d'ordre p si et seulement si P est cyclique ou quaternionien généralisé.*

Annexe B

Rappels sur les KG-modules

Dans ce chapitre, on rappelle quelques définitions et théorèmes sur les KG-modules (de dimension finie) qui sont utiles dans ce projet. La plupart de ces théorèmes seront énoncés sans démonstration.

B.1 Rappels de quelques définitions et propriétés

Pour la section B.1, sauf mention contraire, K est un corps et G un groupe fini. Pour plus de détails sur les KG-modules, voir les livres *Representations and characters of Groups* de Gordon James et Martin Liebeck, [JL06] et *Representation theory of finite groups and associative algebras* de Charles W. Curtis et Irving Reiner, [CR66].

Définition B.1 *Une* ***représentation (linéaire) matricielle de*** G ***sur*** K *est un homomorphisme* $\rho : G \to GL_n(K)$ *pour un certain* $n \in \mathbb{N}^*$. *Le* ***degré*** *de* ρ *est l'entier* n.

Définition B.2 *La représentation* $\rho : G \to GL_1(K)$ *définie par* $\rho(g) = 1$ *pour tout* $g \in G$ *est appelé la* ***représentation triviale*** *de* G.

Définition B.3 *Une représentation* $\rho : G \to GL_n(K)$ *de* G *est dite* ***fidèle*** *si* $\operatorname{Ker} \rho = \{1_G\}$.

Définition B.4 *Soit* V *un* K*-espace vectoriel de dimension finie. Alors* V *est un* KG***-module*** *(de dimension finie) si* V *est muni d'une loi* $\cdot : G \times V \to V$ *qui satisfait les propriétés suivantes :*

i) $g \cdot v \in V$, *pour tout* $g \in G$ *et* $v \in V$,

ii) $h \cdot (g \cdot v) = (hg) \cdot v$, *pour tout* $h, g \in G$ *et* $v \in V$,

iii) $1_G \cdot v = v$, *pour tout* $v \in V$ *et où* 1_G *est l'élément neutre de* G,

iv) $\lambda(g \cdot v) = g \cdot (\lambda v)$, *pour tout* $v \in V$, $g \in G$ *et* $\lambda \in K$,

v) $g \cdot (u + v) = g \cdot u + g \cdot v$, *pour tout* $u, v \in V$, *pour tout* $g \in G$.

Par la suite, on notera en général gv à la place de $g \cdot v$.

*Le **degré** du KG-module V est la dimension de V comme K-espace vectoriel.*

Définition B.5 *Soit G un groupe fini et V un K-espace vectoriel ayant comme base $\{v_g\}_{g\in G}$. On le munit d'une structure de KG-module (de dimension finie) avec*

$$h \star v_g = v_{hg}, \qquad \forall\ h, g \in G.$$

*Alors on appelle V le KG-**module régulier** et on le note KG.*

Définition B.6

*i) Le KG-**module trivial** est le K-espace vectoriel V de dimension 1 (isomorphe à K) avec $gv = v$ pour tout $g \in G$ et $v \in V$.*

*ii) Un KG-module V (de dimension finie) est **fidèle** si l'élément neutre de G est le seul élément g de G tel que $gv = v$ pour tout $v \in V$.*

Il existe une correspondance entre les représentations de G sur K et les KG-modules (de dimension finie), comme suit :

i) Soit $\rho : G \to GL_n(K)$ une représentation de G. Alors K^n est un KG-module (de dimension finie) si on définit

$$g \cdot v = \rho(g)(v) \text{ pour tout } v \in K^n \text{ et } g \in G.$$

ii) Soit V un KG-module (de dimension finie) de degré n et soit B une K-base de V. Alors l'application $\rho : G \to GL_n(K)$ est définie par $\rho(g)$ est la matrice de l'endomorphisme $v \mapsto gv$ de V par rapport à la base B, pour tout $g \in G$.

Définition B.7

*i) Soit V un KG-module (de dimension finie). Un sous-ensemble W est un KG-**sous-module de** V si W est un sous-espace vectoriel de V et si $gw \in W$ pour tout $w \in W$ et $g \in G$.*

*ii) Un KG-module V (de dimension finie) est dit **irréductible** si V est différent de $\{0\}$ et si les seuls sous-modules de V sont $\{0\}$ et V.*

Théorème B.8: Théorème de Maschke
Soit G un groupe fini et K un corps de caractéristique première à $|G|$ et V un KG-module (de dimension finie). Si U est un KG-sous-module de V, alors il existe un KG-sous-module W de V tel que

$$V = U \oplus W.$$

Preuve: Une preuve de ce théorème pour le cas où $K = \mathbb{C}$ ou $\mathbb{R}$ se trouve dans [JL06], page 70, théorème 8.1. Pour la preuve dans le cas général, voir [CR66], page 41, théorème 10.8. □

Corollaire B.9 *Soit G un groupe fini et K un corps de caractéristique première à $|G|$. Alors tout KG-module (de dimension finie) non-nul se décompose en une somme directe de KG-modules irréductibles.*

Preuve: C'est une conséquence du théorème B.8. □

Lemme B.10: Lemme de Schur ([NT89], théorème 5.1, page 23) *Soit K un corps et G un groupe fini. Soit V et W deux KG-modules (de dimension finie) irréductibles. Si $\theta : V \to W$ est un homomorphisme de KG-modules, alors $\theta = 0$ ou θ est un isomorphisme.*

Théorème B.11 *Soit K un corps de caractéristique 0 et G un groupe fini. On décompose l'algèbre de groupe KG en une somme directe de KG-modules irréductibles :*

$$KG = V_1 \oplus V_2 \oplus \ldots \oplus V_m.$$

Alors pour tout KG-module irréductible U, il existe $1 \leq i \leq m$ tel que U est isomorphe à V_i.

Preuve: Une preuve de ce théorème pour le cas où $K = \mathbb{C}$ se trouve dans *Representations and characters of groups* de Gordon James et Martin Liebeck, [JL06], théorème 10.5, page 91. On peut modifier cette preuve ainsi que les résultats préparatoires qui y sont relatifs pour obtenir une preuve pour un corps K de caractéristique 0. □

Proposition B.12 *Soit K un corps de caractéristique 0 et G un groupe fini. On décompose l'algèbre de groupe KG en une somme directe de KG-modules irréductibles :*

$$KG = V_1 \oplus V_2 \oplus \ldots \oplus V_m.$$

Soit U un KG-module irréductible. Alors la cardinalité de l'ensemble

$$\left\{ V_i \,\middle|\, 1 \leq i \leq m, V_i \cong U \right\}$$

est inférieure ou égale à $\dim_K U$.

Preuve: Une preuve de ce théorème pour le cas où $K = \mathbb{C}$ se trouve dans *Representations and characters of groups* de Gordon James et Martin Liebeck, [JL06], théorème 11.9, page 100. On peut modifier cette preuve ainsi que les résultats préparatoires qui y sont relatifs pour obtenir une preuve pour un corps K de caractéristique 0. □

Définition B.13 *Soit V un KG-module (de dimension finie) et B une K-base de V. Soit ρ la représentation matricielle de V associé à la base B. Le* ***caractère de*** *V est la fonction $\chi : G \to K$ définie par*

$$\chi(g) = \mathrm{Tr}(\rho(g)), \text{ pour tout } g \in G.$$

On peut montrer que la définition du caractère de V ne dépend pas du choix de la base.

Définition B.14 *On dit que χ est un **caractère de** G si c'est le caractère d'un certain KG-module (de dimension finie). Un caractère χ est **irréductible** si c'est le caractère d'un KG-module irréductible (de dimension finie).*

Notation B.15 *On note $\mathbf{1}_G$ le caractère associé au KG-module trivial et χ_{reg} le caractère associé au KG-module régulier.*

Propriétés B.16 *Soit K un corps et G un groupe fini.*

i) Des KG-modules (de dimension finie) isomorphes ont le même caractère.

ii) Si x et y sont des éléments conjugués de G, alors

$$\chi(x) = \chi(y),$$

pour tout caractère χ de G.

iii) Soit V un KG-module (de dimension finie) et χ son caractère. Alors

$$\chi(1) = \dim_K V.$$

iv) Le caractère régulier χ_{reg} de G a comme valeur

$$\chi_{reg}(g) = \begin{cases} |G| & si\ g = 1_G \\ 0 & sinon \end{cases}$$

pour tout $g \in G$. Le caractère trivial de G a comme valeur

$$\mathbf{1}_G(g) = 1, \qquad \forall\ g \in G.$$

Définition B.17 *Soit K un corps de caractéristique 0, G un groupe fini. Si χ et η sont des caractères de G sur K, alors on définit*

$$\langle \chi, \eta \rangle_G = \frac{1}{|G|} \sum_{g \in G} \chi(g)\eta(g^{-1}).$$

Si K est un sous-corps de $\mathbb{C}$, on peut prolonger la définition : On définit le produit scalaire $\langle -, - \rangle_G : C_K(G) \times C_K(G) \to K$ par

$$\langle f, h \rangle_G = \frac{1}{|G|} \sum_{g \in G} f(g)\overline{h(g)},$$

pour tout $f, h \in C_K(G)$ ($C_K(G)$ est l'ensemble des fonctions centrales de G dans K). C'est bien un prolongement de la définition précédente car si χ est un caractère de G sur K, alors $\chi(g^{-1}) = \overline{\chi(g)}$. On peut montrer que c'est bien un produit scalaire.

Maintenant K est un corps quelconque de caractéristique 0. Si V et W sont des KG-modules (de dimension finie) et φ, η sont leurs caractères respectifs, alors on pose $\langle V, W \rangle_G = \langle \varphi, \eta \rangle_G$.

Lemme B.18 ([Kar92], théorème 2.11, page 750) *Soit K un corps de caractéristique 0 et G un groupe fini. Si V et W sont des KG-modules (de dimension finie), alors*

$$\langle V, W\rangle_G = \dim_K \mathrm{Hom}_{KG}(V, W).$$

Définition B.19 *Soit K un corps, G un groupe fini et V, W des KG-modules (de dimension finie) tels que V soit irréductible. Alors on note $m(V, W)$ le nombre de fois que V est contenu dans W. Si χ et η sont les caractères de V et W respectivement, alors*

$$m(V, W) = \frac{\langle \chi, \eta\rangle_G}{\langle \chi, \chi\rangle_G}.$$

Théorème B.20 ([Ser78], théorème 6, page 32) *Soit G un groupe fini et $\chi_1, \chi_2, \ldots, \chi_s$ un ensemble complet de caractères irréductibles de G sur $\mathbb{C}$. Alors $\{\chi_1, \chi_2, \ldots, \chi_s\}$ est une base orthonormale (pour le produit scalaire $\langle -, -\rangle_G$) du $\mathbb{C}$-espace vectoriel $C_{\mathbb{C}}(G)$. En particulier l'ensemble $\{\chi_1, \chi_2, \ldots, \chi_s\}$ est linéairement indépendant sur $\mathbb{C}$ ou sur tout sous-corps de $\mathbb{C}$.*

Exemple B.21 Soit K un corps, G un groupe fini et H un sous-groupe. Soit V le K-espace vectoriel de base $\{v_{xH} \,\big|\, xH \in G/H\}$. Alors V est un KG-module si on le munit de l'action suivante :

$$g \cdot v_{xH} = v_{gxH} \qquad \text{pour tout } g \in G \text{ et } xH \in G/H.$$

On va montrer que V contient exactement une fois le KG-module trivial. Soit χ le caractère associé à V. Si $g \in G$, on peut calculer la valeur du caractère χ en g : On a $\chi(g) = |\,\mathrm{fix}(g)|$, où $\mathrm{fix}(g)$ est l'ensemble

$$\{v_{xH} \,\big|\, xH \in G/H \text{ et } g \cdot v_{xH} = v_{xH}\}.$$

Alors le nombre de fois qu'apparaît le module trivial comme facteur dans V

est égal à

$$\begin{aligned}
\frac{\langle \chi, \mathbf{1}_G\rangle_G}{\langle \mathbf{1}_G, \mathbf{1}_G\rangle_G} &= \langle \chi, \mathbf{1}_G\rangle_G = \frac{1}{|G|}\sum_{g\in G}\chi(g)\overline{\mathbf{1}_G(g)} \\
&= \frac{1}{|G|}\sum_{g\in G}\chi(g) = \frac{1}{|G|}\sum_{g\in G}|\operatorname{fix}(g)| \\
&= \frac{1}{|G|}\sum_{g\in G}\big|\{v_{xH} \,\big|\, xH \in G/H \text{ et } g\cdot v_{xH} = v_{xH}\}\big| \\
&= \frac{1}{|G|}\sum_{g\in G}\big|\{xH \in G/H \,\big|\, gxH = xH\}\big| \\
&= \frac{1}{|G|}\sum_{g\in G}\big|\{xH \in G/H \,\big|\, x^{-1}gx \in H\}\big| \\
&= \frac{1}{|G|}\sum_{g\in G}\frac{1}{|H|}\big|\{x \in G \,\big|\, x^{-1}gx \in H\}\big| \\
&= \frac{1}{|G|\cdot|H|}\sum_{g\in G}\big|\{x \in G \,\big|\, x^{-1}gx \in H\}\big| \\
&= \frac{1}{|G|\cdot|H|}\sum_{x\in G}\big|\{g \in G \,\big|\, x^{-1}gx \in H\}\big| \\
&= \frac{1}{|G|\cdot|H|}\sum_{x\in G}|H| \\
&= \frac{1}{|G|\cdot|H|}|G|\cdot|H| = 1.
\end{aligned}$$

On note $K(G/H)$ le KG-module V.

B.2 La restriction, l'induction, l'inflation et la déflation

Dans cette section, on va rappeler la définition de la restriction, l'induction, l'inflation ou la déflation d'un KG-module (de dimension finie). Puis on va étudier les liens entre ces opérations.

Définition B.22 *Soit K un corps, G un groupe fini et H un sous-groupe de G. Soit V un KG-module (de dimension finie). Alors, comme H est un sous-ensemble de G, V est aussi un KH-module, que l'on note $\operatorname{Res}^G_H V$. On appelle le KH-module Res^G_H la **restriction de V à H** . Le caractère de $\operatorname{Res}^G_H V$ est obtenu à partir du caractère χ de V en n'évaluant χ que sur les éléments de H. On note $\operatorname{Res}^G_H\chi$ le caratère de Res^G_H, c'est la **restriction du caractère χ à H** .*

Propriété B.23: Transitivité de la restriction
Soit K un corps, G un groupe fini et H, L des sous-groupes de G tels que

$H \subset L$. Alors, si V est un KG-module (de dimension finie),

$$\mathrm{Res}_H^L \mathrm{Res}_L^G V = \mathrm{Res}_H^G V.$$

Soit χ un caractère de G. Alors, de même

$$\mathrm{Res}_H^L \mathrm{Res}_L^G \chi = \mathrm{Res}_H^G \chi.$$

Preuve: C'est une conséquence de la définition de la restriction. □

Définition B.24 *Soit K un corps, G un groupe fini et H un sous-groupe de G. Soit V un KH-module (de dimension finie). Alors on définit le KG-module $\mathrm{Ind}_H^G V$ par*

$$\mathrm{Ind}_H^G V = KG \otimes_{KH} V.$$

*On dit que $\mathrm{Ind}_H^G V$ est **l'induction de V à G** . Si χ est le caractère de KH, alors on note $\mathrm{Ind}_H^G \chi$ le caractère associé à $\mathrm{Ind}_H^G V$.*

Proposition B.25 *Soit K un corps, G un groupe fini et H un sous-groupe de G. Alors*

$$\mathrm{Ind}_H^G KH = KG.$$

Preuve: Il suffit de voir que, par les propriétés du produit tensoriel,

$$\mathrm{Ind}_H^G KH = KG \otimes_{KH} KH = KG.$$

□

Propriété B.26: Transitivité de l'induction ([Kar92], proposition 1.5, page 673 et proposition 1.4, page 736)
Soit K un corps, G un groupe fini et H, L des sous-groupes de G tels que $H \subset L$. Soit V un KH-module (de dimension finie). Alors

$$\mathrm{Ind}_L^G \mathrm{Ind}_H^L V = \mathrm{Ind}_H^G V.$$

Soit χ le caractère de V. Alors

$$\mathrm{Ind}_L^G \mathrm{Ind}_H^L \chi = \mathrm{Ind}_H^G \chi.$$

Proposition B.27 ([Kar92], proposition 1.2, page 734) *Soit K un corps, G un groupe fini et H un sous-groupe de G. Soit χ un caractère de H. Alors*

$$\mathrm{Ind}_H^G \chi(g) = \frac{1}{|H|} \sum_{t \in G} \dot{\chi}(t^{-1}gt),$$

pour tout $g \in G$, où $\dot{\chi} : G \to K$ est défini par

$$\dot{\chi}(g) = \begin{cases} \chi(g) & si\ g \in H \\ 0 & sinon \end{cases}$$

pour tout $g \in G$.

Définition B.28 *Soit K un corps, G un groupe fini et H un sous-groupe de G. Soit f une fonction centrale de G sur K. Alors on définit la fonction centrale* $\mathrm{Ind}_H^G f : G \to K$ *par*

$$\mathrm{Ind}_H^G f(g) = \frac{1}{|H|} \sum_{t \in G} \dot{f}(t^{-1}gt),$$

pour tout $g \in G$, où $\dot{f} : G \to K$ est défini par

$$\dot{f}(g) = \begin{cases} \chi(g) & \text{si } g \in H \\ 0 & \text{sinon} \end{cases}$$

pour tout $g \in G$. Alors si f est une combinaison K-linéaire de caractères de H, alors $\mathrm{Ind}_H^G f$ *est une combinaison K-linéaire de caractères de G.*

Corollaire B.29 *Soit K un corps, G un groupe fini et H un sous-groupe de G. Soit V un KH-module (de dimension finie) et $W = \mathrm{Ind}_H^G V$. Alors*

$$\dim_K W = |G : H| \dim_K V.$$

Preuve: Soit χ le caractère de V. Alors, par la proposition B.27,

$$\begin{aligned} \dim_K W &= \mathrm{Ind}_H^G \chi(1_G) \\ &= \frac{1}{|H|} \sum_{t \in G} \dot{\chi}(t^{-1}1_G t) \\ &= \frac{1}{|H|} \sum_{t \in G} \dot{\chi}(1_G) \\ &= \frac{1}{|H|} \sum_{t \in G} \dim_K V \\ &= \frac{1}{|H|} |G| \dim_K V = |G : H| \dim_K V, \end{aligned}$$

où $\dot{\chi} : G \to K$ est défini par

$$\dot{\chi}(g) = \begin{cases} \chi(g) & \text{si } g \in H \\ 0 & \text{sinon} \end{cases}$$

pour tout $g \in G$. □

Théorème B.30: Le théorème de réciprocité de Frobenius ([Kar92], corollaire 2.12, page 751)
Soit K un corps, G un groupe fini et H un sous-groupe de G. Soit V un KG-module (de dimension finie) et W un KH-module (de dimension finie). Alors on a

$$\langle V, \mathrm{Ind}_H^G W \rangle_G = \langle \mathrm{Res}_H^G V, W \rangle_H.$$

Définition B.31 *Soit K un corps, G et H des groupes finis et $\varphi : G \to H$ un isomorphisme de groupe. Si V est un KG-module (de dimension finie), alors on définit le KH-module* $\mathrm{Iso}(\varphi)V$ *ainsi :* $\mathrm{Iso}(\varphi)V$ *est égal à V comme K-espace vectoriel et l'action de H sur V est définie par*

$$h \star v = \varphi^{-1}(h) \cdot v \text{ dans } V, \qquad \forall\ h \in H,\ \forall\ v \in V.$$

Si χ est le caractère associé à V, alors on note $\mathrm{Iso}(\varphi)\chi$ *le caractère de* $\mathrm{Iso}(\varphi)V$.

Définition B.32 *Soit K un corps, G un groupe fini et N un sous-groupe normal de G. Si V est un $K(G/N)$-module (de dimension finie), alors on définit le KG-module* $\mathrm{Inf}_{G/N}^{G} V$ *ainsi :* $\mathrm{Inf}_{G/N}^{G} V$ *est égal à V comme K-espace vectoriel et l'action de G sur V est définie par*

$$g \star v = gN \cdot v \text{ dans } V, \qquad \forall\ g \in G,\ \forall\ v \in V.$$

On appelle le KG-module $\mathrm{Inf}_{G/N}^{G} V$ *le* ***module inflaté de*** V *. Si χ est le caractère associé à V, alors on note* $\mathrm{Inf}_{G/N}^{G} \chi$ *le caractère de* $\mathrm{Inf}_{G/N}^{G} V$ *.*

Définition B.33 *Soit K un corps de caractéristique 0, G un groupe fini et N un sous-groupe normal. Soit V un KG-module (de dimension finie). Soit V^N l'ensemble des points fixés par N dans V. C'est un $K(G/N)$-module. On pose* $\mathrm{Def}_{G/N}^{G} V = V^N$*, c'est le $K(G/N)$-**module déflaté de** V **sur** G/N . Si χ est le caractère associé à V, alors on note* $\mathrm{Def}_{G/N}^{G} \chi$ *le caractère associé à* $\mathrm{Def}_{G/N}^{G} V$ *.*

Propriété B.34: Transitivité de l'inflation
Soit K un corps, G un groupe fini et N, M des sous-groupes normaux de G tels que $N \subset M$. Alors si V est un $K(M/N)$-module (de dimension finie)

$$\mathrm{Inf}_{G/N}^{G} \mathrm{Inf}_{G/M}^{G/N} V = \mathrm{Inf}_{G/M}^{G} V.$$

Soit χ un caractère de M/N. Alors, de même

$$\mathrm{Inf}_{G/N}^{G} \mathrm{Inf}_{G/M}^{G/N} \chi = \mathrm{Inf}_{G/M}^{G} \chi.$$

Preuve: Cela découle de la définition de l'inflation. □

Propriété B.35: Transitivité de la déflation
Soit K un corps de caractéristique 0, G un groupe fini et N, M des sous-groupes normaux de G tels que $N \subset M$. Alors si V est un KG-module (de dimension finie)

$$\mathrm{Def}_{G/M}^{G/N} \mathrm{Def}_{G/N}^{G} V = \mathrm{Def}_{G/M}^{G} V.$$

Soit χ un caractère de G. Alors, de même

$$\mathrm{Def}_{G/M}^{G/N} \mathrm{Def}_{G/N}^{G} \chi = \mathrm{Def}_{G/M}^{G} \chi.$$

Preuve: Cela découle de la définition de l'inflation. □

Notation B.36 *Soit K un corps de caractéristique 0, G un groupe fini et (T,S) une section de G. Si V est un KG-module (de dimension finie) et W un $K(T/S)$-module (de dimension finie), alors on pose*

$$\mathrm{Defres}^G_{T/S} V = \mathrm{Def}^T_{T/S} \mathrm{Res}^G_T V \quad et \quad \mathrm{Indinf}^G_{T/S} W = \mathrm{Ind}^G_T \mathrm{Inf}^T_{T/S} W.$$

Proposition B.37 *Soit K un sous-corps de $\mathbb{C}$. Soit G un groupe fini et N un sous-groupe normal de G. Soit χ et μ des caractères de G/N. Alors $\langle \mathrm{Inf}^G_{G/N} \chi, \mathrm{Inf}^G_{G/N} \mu \rangle_G = \langle \chi, \mu \rangle_{G/N}$.*

Preuve: Soit $\{g_1, \ldots, g_s\}$ un ensemble complet de représentants des classes à droite modulo N. Alors

$$\begin{aligned}
\langle \mathrm{Inf}^G_{G/N} \chi, \mathrm{Inf}^G_{G/N} \mu \rangle_G &= \frac{1}{|G|} \sum_{g \in G} \mathrm{Inf}^G_{G/N} \chi(g) \overline{\mathrm{Inf}^G_{G/N} \mu(g)} \\
&= \frac{1}{|G|} \sum_{g \in G} \chi(gN) \overline{\mu(gN)} \\
&= \frac{1}{|G|} \sum_{i=1}^{s} |N| \chi(g_i N) \overline{\mu(g_i N)} \\
&= \frac{|N|}{|G|} \sum_{gN \in G/N} \chi(gN) \overline{\mu(gN)} \\
&= \frac{1}{|G/N|} \sum_{gN \in G/N} \chi(gN) \overline{\mu(gN)} \\
&= \langle \chi, \mu \rangle_{G/N}
\end{aligned}$$

□

Proposition B.38 *Soit K un corps de caractéristique 0, G un groupe fini et N un sous-groupe normal de G. Soit V un $K(G/N)$-module (de dimension finie). Alors $V \cong \mathrm{Def}^G_{G/N} \mathrm{Inf}^G_{G/N} V$.*

Preuve: Soit $v \in V$ et $n \in N$. Alors, dans $\mathrm{Inf}^G_{G/N}$, $n \star v = nN \cdot v = N \cdot v = v$ et donc $(\mathrm{Inf}^G_{G/N} V)^N = \mathrm{Inf}^G_{G/N} V = V$ comme K-espace vectoriel. D'où

$$\mathrm{Def}^G_{G/N} \mathrm{Inf}^G_{G/N} V = (\mathrm{Inf}^G_{G/N} V)^N = V$$

comme K-espace vectoriel. De plus, l'action de G/N est aussi la même donc $V = \mathrm{Def}^G_{G/N} \mathrm{Inf}^G_{G/N} V$ comme KG-module. □

On a un résultat analogue au théorème de réciprocité de Frobenius pour l'inflation et la déflation :

Proposition B.39 *Soit K un corps de caractéristique 0, G un groupe fini et N un sous-groupe normal de G. Soit V un KG-module (de dimension finie) et W un $K(G/N)$-module (de dimension finie). Alors on a*

$$\langle V, \mathrm{Inf}_{G/N}^{G} W\rangle_G = \langle \mathrm{Def}_{G/N}^{G} V, W\rangle_{G/N}.$$

Preuve: On va commencer par supposer que V et W sont irréductibles. Alors $\mathrm{Def}_{G/N} V = V^N$ est le plus grand KG-sous-module de V sur lequel N agit trivialement. Or V est irréductible, donc $V^N = V$ ou $V^N = \{0\}$. On a alors deux cas :

- 1^{er} cas : On suppose que $V^N = \{0\}$. Alors $\langle \mathrm{Def}_{G/N}^{G} V, W\rangle_{G/N} = 0$. On doit montrer que $\langle V, \mathrm{Inf}_{G/N}^{G} W\rangle_G = 0$. Or l'inflation préserve la propriété "être irréductible" donc $\mathrm{Inf}_{G/N}^{G} W$ est un KG-module irréductible. Ainsi

$$\langle V, \mathrm{Inf}_{G/N}^{G} W\rangle_G = \begin{cases} \langle V, V\rangle_G & \text{si } V \cong \mathrm{Inf}_{G/N}^{G} W \\ 0 & \text{sinon} \end{cases}.$$

  Or si $V \cong \mathrm{Inf}_{G/N}^{G} W$, alors N agit trivialement sur V, c'est-à-dire que $V = V^N = \{0\}$, ce qui est impossible car V est irréductible. Donc $V \ncong \mathrm{Inf}_{G/N}^{G} W$ et

$$\langle V, \mathrm{Inf}_{G/N}^{G} W\rangle_G = 0 = \langle \mathrm{Def}_{G/N}^{G} V, W\rangle_{G/N}.$$

- $2^{\text{ème}}$ cas : On suppose maintenant que $V^N = V$. Alors, par un raisonnement analogue à la preuve de la proposition B.38, on a que $\mathrm{Inf}_{G/N}^{G} \mathrm{Def}_{G/N}^{G} V = V$. Alors on a, en utilisant la proposition B.37

$$\begin{aligned} \langle \mathrm{Def}_{G/N}^{G} V, W\rangle_{G/N} &= \langle \mathrm{Inf}_{G/N}^{G} \mathrm{Def}_{G/N}^{G} V, \mathrm{Inf}_{G/N}^{G} W\rangle_G \\ &= \langle V, \mathrm{Inf}_{G/N}^{G} W\rangle_G \end{aligned}$$

Ainsi, si V et W sont irréductibles, on sait que le résultat est vrai. On va maintenant faire le cas général. Il existe des KG-modules irréductibles $V_1, V_2, \ldots, V_r$ et des $K(G/N)$-modules irréductibles $W_1, W_2, \ldots, W_s$ tels que

$$V = V_1 \oplus V_2 \oplus \ldots \oplus V_r \text{ et } W = W_1 \oplus W_2 \oplus \ldots \oplus W_s.$$

On a, en utilisant le cas particulier,

$$\begin{aligned}\langle V, \operatorname{Inf}_{G/N}^G W\rangle_G &= \langle V_1 \oplus \ldots \oplus V_r, \operatorname{Inf}_{G/N}^G W_1 \oplus \ldots \oplus \operatorname{Inf}_{G/N}^G W_s\rangle_G \\ &= \sum_{i=1}^{r}\sum_{j=1}^{s}\langle V_i, \operatorname{Inf}_{G/N}^G W_j\rangle_G \\ &= \sum_{i=1}^{r}\sum_{j=1}^{s}\langle \operatorname{Def}_{G/N}^G V_i, W_j\rangle_{G/N} \\ &= \langle \operatorname{Def}_{G/N}^G V_1 \oplus \ldots \oplus \operatorname{Def}_{G/N}^G V_r, W_1 \oplus \ldots \oplus W_s\rangle_{G/N} \\ &= \langle \operatorname{Def}_{G/N}^G V, W\rangle_{G/N}\end{aligned}$$

ce qui est le résultat cherché. □

Proposition B.40 *Soit K un corps, G un groupe fini, H un sous-groupe de G et N un sous-groupe normal de G tel que $N \subset H$. Alors*

$$\operatorname{Ind}_H^G \operatorname{Inf}_{H/N}^H V = \operatorname{Inf}_{G/N}^G \operatorname{Ind}_{H/N}^{G/N} V,$$

pour tout $K(H/N)$-module V (de dimension finie).

Preuve: On peut voir $\operatorname{Ind}_H^G \operatorname{Inf}_{H/N}^H V$ comme le KG-module $KG \otimes_{KH} V$, où V est le KH-module $\operatorname{Inf}_{H/N}^H V$. De même, on peut voir $\operatorname{Inf}_{G/N}^G \operatorname{Ind}_{H/N}^{G/N} V$ comme le KG-module $K(G/N) \otimes_{K(H/N)} V$.

Soit $g_1, \ldots, g_s$ un ensemble de représentant des classes à droites modulo H de G et $v_1, \ldots, v_n$ une base de V. Alors $g_1N, \ldots, g_sN$ est un ensemble de représentant des classes à droites modulo H/N de G/N. L'ensemble $\{g_i \otimes v_j \,\big|\, 1 \leq i \leq s, 1 \leq j \leq n\}$ est une base de $KG \otimes_{KH} V$ et l'ensemble $\{g_iN \otimes v_j \,\big|\, 1 \leq i \leq s, 1 \leq j \leq n\}$ est une base de $K(G/N) \otimes_{K(H/N)} V$.

On définit l'application K-linéaire $\alpha : KG \otimes_{KH} V \to K(G/N) \otimes_{K(H/N)} V$ par

$$\alpha(g_i \otimes v_j) = g_iN \otimes v_j,$$

pour tout $1 \leq i \leq s$ et $1 \leq j \leq n$. C'est une application K-linéaire bijective.

Soit $g \in G$ et $v \in V$. Soit $1 \leq i \leq s$ et $h \in H$ tels que $g = g_ih$. Soit $\lambda_1, \ldots, \lambda_n \in K$ tels que $hN \cdot v = \sum_{j=1}^n \lambda_j v_j$. Alors

$$\begin{aligned}\alpha(g \otimes v) &= \alpha(g_ih \otimes v) = \alpha(g_i \otimes hN \cdot v) \\ &= \alpha(\sum_{j=1}^{n} \lambda_j g_i \otimes v_j) = \sum_{j=1}^{n} \lambda_j \alpha(g_i \otimes v_j) \\ &= \sum_{j=1}^{n} \lambda_j g_iN \otimes v_j = g_iN \otimes \sum_{j=1}^{n} \lambda_j v_j \\ &= g_iN \otimes hN \cdot v = g_iNhN \otimes v = gN \otimes v.\end{aligned}$$

Cela va permettre de montrer que α est un homomorphisme de KG-modules. Soit $g, h \in G$ et $v \in V$. Alors

$$\begin{aligned}\alpha(h \cdot g \otimes v) =& \alpha(hg \otimes v) = hgN \otimes v \\ =& h \cdot gN \otimes v = h \cdot \alpha(g \otimes v).\end{aligned}$$

Ainsi α est un isomorphisme de KG-modules entre $\operatorname{Ind}_H^G \operatorname{Inf}_{H/N}^H V$ et $\operatorname{Inf}_{G/N}^G \operatorname{Ind}_{H/N}^{G/N} V$ □

Proposition B.41 *Soit K un corps, G un groupe fini et N un sous-groupe normal de G. Alors l'inflation de G/N à G préserve les suites exactes, c'est-à-dire que si*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

est une suite exacte de $K(G/N)$-modules (de dimension finie), alors l'inflation induit une suite exacte de KG-modules

$$0 \longrightarrow \operatorname{Inf}_{G/N}^G A \longrightarrow \operatorname{Inf}_{G/N}^G B \longrightarrow \operatorname{Inf}_{G/N}^G C \longrightarrow 0.$$

Preuve: Soit A, B, C des $K(G/N)$-modules (de dimension finie) et $f : A \to B$ et $g : B \to C$ des homomorphismes de $K(G/N)$-modules tels que

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

soit une suite exacte. Alors comme K-espaces vectoriel, $\operatorname{Inf}_{G/N}^G A = A$, $\operatorname{Inf}_{G/N}^G B = B$ et $\operatorname{Inf}_{G/N}^G C = C$, et l'action de g sur $a \in A$, $b \in B$, $c \in C$ respectivement est défini comme l'action de gN sur a, b, c respectivement, pour tout $g \in G$. De plus, f induit un homomorphisme de KG-modules $\operatorname{Inf}_{G/N}^G f : \operatorname{Inf}_{G/N}^G A \to \operatorname{Inf}_{G/N}^G B$ par $\operatorname{Inf}_{G/N}^G f(a) = f(a)$ pour tout $a \in \operatorname{Inf}_{G/N}^G A$. De la même manière, g induit un homomorphisme de KG-modules $\operatorname{Inf}_{G/N}^G g : \operatorname{Inf}_{G/N}^G B \to \operatorname{Inf}_{G/N}^G C$ par $\operatorname{Inf}_{G/N}^G g(b) = g(b)$ pour tout $b \in \operatorname{Inf}_{G/N}^G B$. Il faut montrer que

$$0 \longrightarrow \operatorname{Inf}_{G/N}^G A \overset{\operatorname{Inf}_{G/N}^G f}{\longrightarrow} \operatorname{Inf}_{G/N}^G B \overset{\operatorname{Inf}_{G/N}^G g}{\longrightarrow} \operatorname{Inf}_{G/N}^G C \longrightarrow 0$$

est une suite exacte, c'est-à-dire que $\operatorname{Inf}_{G/N}^G f$ est injective, $\operatorname{Im} \operatorname{Inf}_{G/N}^G f = \operatorname{Ker} \operatorname{Inf}_{G/N}^G g$ et $\operatorname{Inf}_{G/N}^G g$ est surjective. Or cela découle du fait que

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

est une suite exacte, c'est-à-dire que f est injective, $\operatorname{Im} f = \operatorname{Ker} g$ et g est surjective. □

Proposition B.42 *Soit K un corps, G un groupe fini et H un sous-groupe de G. Alors l'induction de H à G préserve les suites exactes, c'est-à-dire que si*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

est une suite exacte de KH-modules (de dimension finie), alors l'induction induit une suite exacte de KG-modules

$$0 \longrightarrow \mathrm{Ind}_H^G A \longrightarrow \mathrm{Ind}_H^G B \longrightarrow \mathrm{Ind}_H^G C \longrightarrow 0.$$

Preuve: Soit A, B, C des KH-modules (de dimension finie) et $f : A \to B$ et $g : B \to C$ des homomorphismes de KH-modules tels que

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

soit une suite exacte. Alors on a $\mathrm{Ind}_H^G A = KG \otimes_{KH} A$, $\mathrm{Ind}_H^G B = KG \otimes_{KH} B$ et $\mathrm{Ind}_H^G C = KG \otimes_{KH} C$. De plus, f induit un homomorphisme de KG-modules $\mathrm{Ind}_H^G f : KG \otimes_{KH} A \to KG \otimes_{KH} B$ par

$$\mathrm{Ind}_H^G f(x \otimes a) = x \otimes f(a)$$

pour tout $x \in KG$ et $a \in A$. De la même manière, g induit un homomorphisme de KG-modules $\mathrm{Ind}_H^G g : KG \otimes_{KH} B \to KG \otimes_{KH} C$ par

$$\mathrm{Ind}_H^G g(x \otimes b) = x \otimes g(b)$$

pour tout $x \in KG$ et $b \in B$. Il faut montrer que

$$0 \longrightarrow KG \otimes_{KH} A \xrightarrow{\mathrm{Ind}_H^G f} KG \otimes_{KH} B \xrightarrow{\mathrm{Ind}_H^G g} KG \otimes_{KH} C \longrightarrow 0$$

est une suite exacte, c'est-à-dire que $\mathrm{Ind}_H^G f$ est injective, $\mathrm{Im}\,\mathrm{Ind}_H^G f = \mathrm{Ker}\,\mathrm{Ind}_H^G g$ et $\mathrm{Ind}_H^G g$ est surjective. On sait que

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

est une suite exacte, c'est-à-dire que f est injective, $\mathrm{Im}\, f = \mathrm{Ker}\, g$ et g est surjective.

Soit $\{a_1, \ldots, a_n\}$ une K-base de A et $\{x_1, \ldots x_r\}$ un ensemble de représentants des classes à gauche modulo H dans G. Alors $\{x_i \otimes a_j \,\big|\, 1 \leq i \leq r, 1 \leq j \leq n\}$ est une base de $KG \otimes_{KH} A$. On pose $b_i = f(a_i)$, pour tout $1 \leq i \leq n$. Comme f est injective, $\{b_1, \ldots, b_n\}$ est un ensemble linéairement indépendant de B. On complète cette ensemble pour obtenir une base $\{b_1, \ldots, b_m\}$ de B (on a $m \geq n$). Alors $\{x_i \otimes b_j \,\big|\, 1 \leq i \leq r, 1 \leq j \leq m\}$ est une base de $KG \otimes_{KH} B$.

- L'application $\mathrm{Ind}_H^G f$ est injective :
  Soit $x \in KG \otimes_{KH} A$ tel que $\mathrm{Ind}_H^G f(x) = 0$. Alors il existe

$\{q_{ij} \in K \,\big|\, 1 \leq i \leq r, 1 \leq j \leq n\}$ tels que $x = \sum_{i=1}^{r} \sum_{j=1}^{n} q_{ij}(x_i \otimes a_j)$. Alors

$$\begin{aligned} 0 &= \operatorname{Ind}_H^G f(x) \\ &= \operatorname{Ind}_H^G f\Big(\sum_{i=1}^{r}\sum_{j=1}^{n} q_{ij}(x_i \otimes a_j)\Big) \\ &= \sum_{i=1}^{r}\sum_{j=1}^{n} q_{ij} \operatorname{Ind}_H^G f(x_i \otimes a_j) \\ &= \sum_{i=1}^{r}\sum_{j=1}^{n} q_{ij}\big(x_i \otimes f(a_j)\big) \\ &= \sum_{i=1}^{r}\sum_{j=1}^{n} q_{ij}(x_i \otimes b_j) \end{aligned}$$

Or $\{x_i \otimes b_j \,\big|\, 1 \leq i \leq r, 1 \leq j \leq m\}$ est une base de $KG \otimes_{KH} B$, donc $q_{ij} = 0$ pour tout $1 \leq i \leq r$ et $1 \leq j \leq n$, c'est-à-dire que $x = 0$.

- L'application $\operatorname{Ind}_H^G g$ est surjective :
  Comme $\{x \otimes c \,\big|\, x \in KG, c \in C\}$ est un ensemble de générateurs de $KG \otimes_{KH} C$, il suffit de voir que $x \otimes c \in \operatorname{Im} \operatorname{Ind}_H^G g$, pour tout $x \in KG$ et $c \in C$. Soit $x \in KG$ et $c \in C$. Alors comme g est surjective, il existe $b \in B$ tel que $g(b) = c$. Ainsi $\operatorname{Ind}_H^G g(x \otimes b) = x \otimes g(b) = x \otimes c$, donc $x \otimes c \in \operatorname{Im} \operatorname{Ind}_H^G g$.
- On a $\operatorname{Im} \operatorname{Ind}_H^G f = \operatorname{Ker} \operatorname{Ind}_H^G g$:
  Soit $x \in \operatorname{Im} \operatorname{Ind}_H^G f$. Alors il existe $y \in KG \otimes_{KH} A$ tel que $\operatorname{Ind}_H^G f(y) = x$. Il existe $\{q_{ij} \in K \,\big|\, 1 \leq i \leq r, 1 \leq j \leq n\}$ tels que

$$y = \sum_{i=1}^{r}\sum_{j=1}^{n} q_{ij}(x_i \otimes a_j).$$

  Alors

$$x = \sum_{i=1}^{r}\sum_{j=1}^{n} q_{ij}\big(x_i \otimes f(a_j)\big),$$

  donc on a

$$\begin{aligned} \operatorname{Ind}_H^G g(x) &= \operatorname{Ind}_H^G g\Big(\sum_{i=1}^{r}\sum_{j=1}^{n} q_{ij}x_i \otimes f(a_j)\Big) \\ &= \sum_{i=1}^{r}\sum_{j=1}^{n} q_{ij} \operatorname{Ind}_H^G g\big(x_i \otimes f(a_j)\big) \\ &= \sum_{i=1}^{r}\sum_{j=1}^{n} q_{ij}x_i \otimes \underbrace{g\big(f(a_j)\big)}_{=\,0} = 0 \end{aligned}$$

et donc $x \in \operatorname{Ker} \operatorname{Ind}_H^G g$. Ainsi on a montré que $\operatorname{Im} \operatorname{Ind}_H^G f \subset \operatorname{Ker} \operatorname{Ind}_H^G g$. Or on a

$$\begin{aligned}
\dim_K \operatorname{Ker} \operatorname{Ind}_H^G g &\overset{(1)}{=} \dim_K KG \otimes_{KH} B - \dim_K \operatorname{Im} \operatorname{Ind}_H^G g \\
&\overset{(2)}{=} \dim_K KG \otimes_{KH} B - \dim_K KG \otimes_{KH} C \\
&\overset{(3)}{=} |G:H| \dim_K B - |G:H| \dim_K C \\
&= |G:H|(\dim_K B - \dim_K C) \\
&\overset{(4)}{=} |G:H|(\dim_K B - \dim_K \operatorname{Im} g) \\
&\overset{(5)}{=} |G:H| \dim_K \operatorname{Ker} g \\
&\overset{(6)}{=} |G:H| \dim_K \operatorname{Im} f \\
&\overset{(7)}{=} |G:H| \dim_K A \\
&\overset{(8)}{=} \dim_K KG \otimes_{KH} A \\
&\overset{(9)}{=} \dim_K \operatorname{Im} \operatorname{Ind}_H^G f,
\end{aligned}$$

où les égalités (1) et (5) découlent du fait que si on a une application K-linéaire $\alpha : V \to W$, où V et W sont des K-espaces vectoriels de dimension finie, alors $\dim_K V = \dim_K \operatorname{Ker} \alpha + \dim_K \operatorname{Im} \alpha$, l'égalité (2) du fait que $\operatorname{Ind}_H^G g$ est surjective, les égalités (3) et (8) du corollaire B.29, l'égalité (4) du fait que g et surjective, l'égalité (6) du fait que $\operatorname{Im} f = \operatorname{Ker} g$, l'égalité (7) du fait que f est injective et l'égalité (9) du fait que $\operatorname{Ind}_H^G f$ est injective. Ainsi $\dim_K \operatorname{Ker} \operatorname{Ind}_H^G g = \dim_K \operatorname{Im} \operatorname{Ind}_H^G f$ et donc $\operatorname{Ker} \operatorname{Ind}_H^G g = \operatorname{Im} \operatorname{Ind}_H^G f$.

□

Proposition B.43 *Soit K un corps, G un groupe fini et (T, S) une section de G. Alors $\operatorname{Ind}_T^G \operatorname{Inf}_{T/S}^T K(T/S) \cong K(G/S)$, où $K(G/S)$ est le KG-module associé à l'action de G sur G/S.*

Preuve: On a que $\operatorname{Inf}_{T/S}^T K(T/S)$ est égal à $K(T/S)$ comme K-espace vectoriel. Alors $\operatorname{Ind}_T^G \operatorname{Inf}_{T/S}^T K(T/S) = KG \otimes_{KT} K(T/S)$. Soit $g_1, \dots g_n$ un ensemble de représentants des classes à gauche modulo T dans G et $t_1, \dots, t_m$ un ensemble de représentants des classes à gauche modulo S dans T. Alors $\{g_i \otimes t_j S \,\big|\, 1 \leq i \leq n, 1 \leq j \leq m\}$ est une base de $KG \otimes_{KT} K(T/S)$. De plus

$$G = \bigsqcup_{i=1}^{n} g_i T = \bigsqcup_{i=1}^{n} \bigsqcup_{j=1}^{m} g_i t_j S$$

donc $\{g_i t_j \,\big|\, 1 \leq i \leq n, 1 \leq j \leq m\}$ est un ensemble de représentants des classes à gauche modulo S dans G et donc $\{g_i t_j S \,\big|\, 1 \leq i \leq n, 1 \leq j \leq m\}$ est une base de $K(G/S)$. On définit l'application

$$\alpha : KG \otimes_{KT} K(T/S) \to K(G/S)$$

par $\alpha(g_i \otimes t_j S) = g_i t_j S$, pour tout $1 \leq i \leq n$ et pour tout $1 \leq j \leq m$, que l'on prolonge par linéarité à $KG \otimes_{KT} K(T/S)$. Ainsi on obtient une application K-linéaire bijective (car α envoie une base de $KG \otimes_{KT} K(T/S)$ sur une base de $K(G/S)$). On va montrer que c'est un homomorphisme de KG-modules. Il suffit de le vérifier pour une base de $KG \otimes_{KT} K(T/S)$. Soit $1 \leq i \leq n$, $1 \leq j \leq m$ et $g \in G$. Alors, si $1 \leq k \leq n$, $t \in T$ et $1 \leq l \leq m$ tels que $gg_i = g_k t$ et $tt_j S = t_l S$,

$$\begin{aligned}
\alpha(g \cdot g_i \otimes t_j S) &= \alpha(gg_i \otimes t_j S) \\
&= \alpha(g_k t \otimes t_j S) \\
&= \alpha(g_k \otimes tt_j S) \\
&= \alpha(g_k \otimes t_l S) \\
&= g_k t_l S \\
&= g_k tt_j S \\
&= gg_i t_j S \\
&= g\alpha(g_i \otimes t_j S).
\end{aligned}$$

Ainsi α est un isomorphisme de KG-modules et donc

$$\mathrm{Ind}_T^G \mathrm{Inf}_{T/S}^T K(T/S) \cong K(G/S).$$

□

B.2.1 Le théorème de Clifford

Définition B.44 *Soit G un groupe fini, H un sous-groupe de G et V un KH-module (de dimension finie). Soit $g \in G$ fixé. On définit le $K({}^gH)$-module ${}^gV$ par ${}^gV = V$ comme espace vectoriel et on le munit de l'action $ghg^{-1} \star v = hv$, pour tout $h \in H$. On appelle ${}^gV$ un* ***conjugué de*** *V.*

Remarque B.45 Soit G un groupe fini et N un sous-groupe normal de G. Alors pour tout KN-module V (de dimension finie) et pour tout $g \in G$, ${}^gV$ est un KN-module muni de l'action $h \star v = g^{-1}hgv$ pour tout $h \in N$.

Proposition B.46 *Soit K un corps, G un groupe fini, H un sous-groupe de G, N un sous-groupe normal de H et $g \in G$. Alors*

$$\mathrm{Ind}_{{}^xH}^G \mathrm{Inf}_{({}^xH)/({}^xN)}^{{}^xH} {}^xV \cong \mathrm{Ind}_H^G \mathrm{Inf}_{H/N}^H V,$$

pour tout $K(H/N)$-module V (de dimension finie).

Preuve: On peut voir $\mathrm{Ind}_H^G \mathrm{Inf}_{H/N}^H V$ comme le KG-module $KG \otimes_{KH} V$, où V est le KH-module $\mathrm{Inf}_{H/N}^H V$. De même, on peut voir $\mathrm{Ind}_{{}^xH}^G \mathrm{Inf}_{({}^xH)/({}^xN)}^{{}^xH} {}^xV$ comme le KG-module $KG \otimes_{K({}^xH)} {}^xV$.

Soit $g_1, \dots, g_s$ un ensemble de représentant des classes à droites modulo H de G et $v_1, \dots, v_n$ une base de V. Alors $g_1x^{-1}, \dots, g_sx^{-1}$ est un ensemble de représentant des classes à droites modulo ${}^xH$ de G. L'ensemble $\{g_i \otimes v_j \,\big|\, 1 \leq i \leq s, 1 \leq j \leq n\}$ est une base de $KG \otimes_{KH} V$ et l'ensemble $\{g_ix^{-1} \otimes v_j \,\big|\, 1 \leq i \leq s, 1 \leq j \leq n\}$ est une base de $KG \otimes_{K({}^xH)} {}^xV$.

On définit l'application K-linéaire $\alpha : KG \otimes_{KH} V \to KG \otimes_{K({}^xH)} {}^xV$ par

$$\alpha(g_i \otimes v_j) = g_ix^{-1} \otimes v_j,$$

pour tout $1 \leq i \leq s$ et $1 \leq j \leq n$. C'est une application K-linéaire bijective.

Soit $g \in G$ et $v \in V$. Soit $1 \leq i \leq s$ et $h \in H$ tels que $g = g_ih$. Soit $\lambda_1, \dots, \lambda_n \in K$ tels que $hN \cdot v = \sum_{j=1}^n \lambda_j v_j$. Alors

$$\begin{aligned}
\alpha(g \otimes v) = \alpha(g_ih \otimes v) &= \alpha(g_i \otimes hN \cdot v) \\
&= \alpha(\sum_{j=1}^n \lambda_j g_i \otimes v_j) = \sum_{j=1}^n \lambda_j \alpha(g_i \otimes v_j) \\
&= \sum_{j=1}^n \lambda_j g_ix^{-1} \otimes v_j = g_ix^{-1} \otimes \sum_{j=1}^n \lambda_j v_j \\
&= g_ix^{-1} \otimes hN \cdot v = g_ix^{-1} \otimes {}^xh\,{}^xN \star v \\
&= g_ix^{-1}\,{}^xh \otimes v = g_ihx^{-1} \otimes v = gx^{-1} \otimes v.
\end{aligned}$$

Cela va permettre de montrer que α est un homomorphisme de KG-modules. Soit $g, h \in G$ et $v \in V$. Alors

$$\begin{aligned}
\alpha(h \cdot g \otimes v) =& \alpha(hg \otimes v) = hgx^{-1} \otimes v \\
=& h \cdot gx^{-1} \otimes v = h \cdot \alpha(g \otimes v).
\end{aligned}$$

Ainsi α est un isomorphisme de KG-modules entre $\operatorname{Ind}_H^G \operatorname{Inf}_{H/N}^H V$ et $\operatorname{Ind}_{{}^xH}^G \operatorname{Ind}_{{}^xH/{}^xN}^{{}^xH} {}^xV$ □

Théorème B.47 ([CR66], théorème 49.2, page 343) *Soit K un corps, G un groupe fini, N un sous-groupe normal et V un KG-module irréductible (de dimension finie). Alors $\operatorname{Res}_N^G V$ se décompose en une somme directe de KN-modules irréductibles (de dimension finie) qui sont tous conjugués entre eux.*

Une conséquence du théorème de Clifford est que si V est un KG-module irréductible et W est un KN-module qui est un facteur de composition de $\operatorname{Res}_N^G V$, alors il existe $g_1, \dots, g_s \in G$ tels que

$$\operatorname{Res}_N^G V = \bigoplus_{i=1}^s {}^{g_i}W. \tag{B.1}$$

Soit $\{{}^{g_1}W, \dots, {}^{g_r}W\}$ un sous-ensemble maximal de KN-module non-isomorphes de $\{{}^{g_i}W \,\big|\, 1 \leq i \leq s\}$ (en renumérotant si nécessaire). Pour

tout $1 \leq i \leq r$, on pose V_i comme la somme de tous les conjugués ${}^{g_j}W$, $1 \leq j \leq s$ tels que ${}^{g_j}W \cong {}^{g_i}W$. Alors

$$\mathrm{Res}_N^G V = \bigoplus_{i=1}^{r} V_i \tag{B.2}$$

et on peut montrer que les V_i ne dépendent pas du choix de la décomposition obtenu en B.1.

Définition B.48 *Les KN-sous-modules V_i de $\mathrm{Res}_N^G V$ uniquement déterminé défini ci-dessus sont appelés les* ***composantes homogènes*** *de $\mathrm{Res}_N^G V$. Chacune est une somme directe de conjugués de KN-modules isomorphes.*

Théorème B.49 ([CR66], page 348, corollaire 50.6) *Soit K un corps, G un groupe fini et N un sous-groupe normal de G. Soit V un KG-module irréductible (de dimension finie). On définit le sous-groupe I de G comme l'ensemble des éléments $h \in G$ tels que ${}^hW \cong W$, où W est une des composantes homogènes de $\mathrm{Res}_N^G V$. Alors W est un KI-module irréductible (de dimension finie) et $V \cong \mathrm{Ind}_I^G W$.*

B.3 Quelques tables de caractères sur $\mathbb{C}$

Voici quelques tables de caractères.

Exemple B.50: Les groupes abéliens ([JL06], pages 81-82)
Soit G un groupe abélien. Alors il existe des nombres premiers $p_1, p_2, \ldots, p_n$ (pas forcément distincts) et des entiers strictement positifs $\alpha_1, \alpha_2, \ldots, \alpha_n$ tels que

$$G \cong C_{p_1^{\alpha_1}} \times C_{p_2^{\alpha_2}} \times \ldots \times C_{p_n^{\alpha_n}}.$$

Pour tout $i \in \{1, \ldots, n\}$, soit ξ_i une racine $p_1^{\alpha_1}$ ième primitive de l'unité, x_i un générateur de $C_{p_i^{\alpha_i}}$ et $g_i = (1, \ldots, 1, x_i, 1, \ldots, 1)$. On définit l'ensemble I par

$$I = \{(r_1, r_2, \ldots, r_n) \in \mathbb{N} \,\big|\, 0 \leq r_i \leq \alpha_i, \text{ pour tout } i \in \{1, \ldots, n\}\}.$$

Alors, pour tout $r = (r_1, r_2, \ldots, r_n) \in I$, on définit le caractère ψ_r par

$$\psi_r(g_1^{\gamma_1}, g_2^{\gamma_2}, \ldots, g_n^{\gamma_n}) = \prod_{i=1}^{n} (\xi^{r_i})^{\gamma_i}.$$

Alors, $\{\psi_i \,\big|\, i \in I\}$ est l'ensemble des caractères irréductibles sur $\mathbb{C}$ de G.

Exemple B.51: Le groupe cyclique C_{p^n} ([JL06], exemple 9.9 (1), page 82)
Soit $n \in \mathbb{N}^*$, p un nombre premier et $G = C_{p^n}$. Alors, la table de caractère de G est :

	1	a	$\cdots$	a^k	$\cdots$	a^{p^n-1}
$\psi_0 = \mathbf{1}_G$	1	1	$\cdots$	1	$\cdots$	1
ψ_j	1	ξ^j	$\cdots$	$(\xi^j)^k$	$\cdots$	$(\xi^j)^{p^n-1}$

$0 \leq j \leq p^n - 1$, ξ est une racine p^n-ième primitive de l'unité (par exemple $\xi = \exp(\frac{2\pi\imath}{p^n})$).

Exemple B.52: Le groupe symétrique S_3 ([JL06], exemple 14.18, page 142)
Voici la table de caractère de S_3 :

	1	$(1\ 2)$	$(1\ 2\ 3)$
$\mathbf{1}_G$	1	1	1
ψ_2	1	-1	1
ψ_3	2	0	-1

Exemple B.53: Le groupe D_8 ([JL06], exemple 16.3 (3), pages 160-161)
Voici la table de caractère de $D_8 = \langle x, y \,|\, x^4 = y^2 = 1, yxy = x^{-1} \rangle$:

	1	x^2	x	y	xy
ψ_1	1	1	1	1	1
ψ_2	1	1	1	-1	-1
ψ_3	1	1	-1	-1	1
ψ_4	1	1	-1	1	-1
ψ_5	2	-2	$\omega + \omega^{-1}$	0	0

où ω est une racine 2^{n-1}-ième primitive de l'unité.

Exemple B.54: Le groupe D_{2^n}, $n \geq 3$ ([JL06], pages 182-183)
Voici la table de caractère de $D_{2^n} = \langle x, y \,|\, x^{2^{n-1}} = y^2 = 1, yxy = x^{-1} \rangle$:

	1	$x^{2^{n-2}}$	x^k $1 \leq k \leq 2^{n-2} - 1$	y	xy
η_1	1	1	1	1	1
η_2	1	1	1	-1	-1
η_3	1	1	$(-1)^k$	-1	1
η_4	1	1	$(-1)^k$	1	-1
ψ_j	2	$(-1)^j 2$	$\omega^{jk} + \omega^{-jk}$	0	0

$1 \leq j \leq 2^{n-2} - 1$, ω est une racine 2^{n-1}-ième primitive de l'unité.

Exemple B.55: Le groupe SD_{2^n}, $n \geq 4$
On veut trouver les caractères du goupe

$$SD_{2^n} = \langle x, y \,\big|\, x^{2^{n-1}} = y^2 = 1, yxy = x^{2^{n-2}-1} \rangle.$$

On a que $[SD_{2^n}, SD_{2^n}] = \langle x^2 \rangle$ et $SD_{2^n}/[SD_{2^n}, SD_{2^n}] \cong C_2 \times C_2$. Ainsi, par inflation, on obtient les quatre caractères linéaires de SD_{2^n}. Il reste à trouver les caractères non-linéaires. On définit, pour $i \in \mathbb{Z}$ l'homomorphisme $\rho_i : SD_{2^n} \to GL_2(\mathbb{C})$ par

$$\rho_i(x) = \begin{pmatrix} \omega^i & 0 \\ 0 & (-\omega)^{-i} \end{pmatrix}, \quad \rho_i(y) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

où ω est une racine 2^{n-1}-ième primitive de l'unité. Alors, pour tout $i \in \mathbb{Z}$, ρ_i est une représentation irréductible car $\operatorname{Im} \rho_i$ est non abélien. On pose :

$$I = \{i \in 2\mathbb{N} \,\big|\, 1 \leq i \leq 2^{n-2} - 1\} \cup \{i \in 2\mathbb{N} + 1 \,\big|\, -2^{n-3} < i < 2^{n-3}\}.$$

Alors, les représentations ρ_i, où $i \in I$, sont distinctes (car si $i, j \in I$, $i \neq j$, alors $\rho_i(x)$ et $\rho_j(x)$ n'ont pas les mêmes valeurs propres). Alors le nombre de caractères irréductibles non-linéaires distincts obtenus est :

$$\frac{2^{n-2}}{2} - 1 + 2^{n-3} = 2^{n-2} - 1.$$

Il reste à voir qu'il n'y en a pas d'autres. Pour cela, on va calculer les classes de conjugaison car on sait que le nombre de caractères irréductibles distincts sur $\mathbb{C}$ est égal au nombre de classes de conjugaison. Or il y a $2^{n-2} + 3$ classes de conjugaison :

- $Cl_G(1) = \{1\}$;
- $Cl_G(x^{2^{n-2}}) = \{x^{2^{n-2}}\}$;
- $Cl_G(x^i) = \{x^i, x^{-i}\}$, pour tout $1 \leq i \leq 2^{n-2} - 1$, i pair ;
- $Cl_G(x^i) = \{x^i, x^{2^{n-2}-i}\}$, pour tout $-2^{n-3} + 1 \leq i \leq 2^{n-3} - 1$, i impair ;
- $Cl_G(y) = \left\{x^{2j} y \,\big|\, j \in \{0, \dots 2^{n-2} - 1\}\right\}$;
- $Cl_G(xy) = \left\{x^{2j+1} y \,\big|\, j \in \{0, \dots 2^{n-2} - 1\}\right\}$.

Ainsi on voit que l'on a trouvé tous les caractères irréductibles. Voici la table de caractères de SD_{2^n} :

	1	$x^{2^{n-2}}$	x^{2k} $1 \leq k \leq 2^{n-3} - 1$	x^{2k+1} $-2^{n-4} \leq k \leq 2^{n-4} - 1$	y	xy
$\widetilde{\psi_1}$	1	1	1	1	1	1
$\widetilde{\psi_2}$	1	1	1	1	-1	-1
$\widetilde{\psi_3}$	1	1	1	-1	1	-1
$\widetilde{\psi_4}$	1	1	1	-1	-1	1
ψ_j	2	$(-1)^j 2$	$\omega^{jk} + \omega^{-jk}$	$\omega^{jk} - \omega^{-jk}$	0	0

$1 \leq j \leq 2^{n-2} - 1$, ω est une racine 2^{n-1}-ième primitive de l'unité.

Remarque B.56 L'exemple précédent se base sur la partie § 47. Applications : Representations of Metacyclic Groups du livre *Representation theory of finite groups and associative algebras* de Charles W. Crutis et Irving Reiner, [CR66], pages 333-340.

Exemple B.57: Le groupe Q_8 ([JL06], exercice 17.1, page 177, corrigé page 416)
Voici la table de caractère de $Q_8 = \langle x, y \,|\, x^4 = 1, y^2 = x^2, yxy = x^{-1} \rangle$:

	1	x^2	x	y	xy
ψ_1	1	1	1	1	1
ψ_2	1	1	1	-1	-1
ψ_3	1	1	-1	-1	1
ψ_4	1	1	-1	1	-1
ψ_5	2	-2	$\omega + \omega^{-1}$	0	0

ω est une racine 2^{n-1}-ième primitive de l'unité.
On peut remarquer que D_8 et Q_8 ont la même table de caractères sur $\mathbb{C}$ bien que ce soit des groupes non-isomorphes.

Exemple B.58: Le groupe Q_{2^n}, $n \geq 3$
On voit trouver les caractères du groupe

$$Q_{2^n} = \langle x, y \,|\, x^{2^{n-1}} = 1, y^2 = x^{2^{n-2}}, yxy = x^{-1} \rangle.$$

On a que $[Q_{2^n}, Q_{2^n}] = \langle x^2 \rangle$ et $Q_{2^n}/[Q_{2^n}, Q_{2^n}] \cong C_2 \times C_2$. Ainsi, par inflation, on obtient les quatre caractères linéaires de Q_{2^n}. Il reste à trouver les caractères non-linéaires. On définit, pour $i = 1, \ldots, 2^{n-2} - 1$ l'homomorphisme $\rho_i : Q_{2^n} \to GL_2\mathbb{C}$ par

$$\rho_i(x) = \begin{pmatrix} \omega^i & 0 \\ 0 & \omega^{-i} \end{pmatrix}, \quad \rho_i(y) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

où ω est une racine 2^{n-1}-ième primitive de l'unité. Alors pour tout $i = 1, \ldots, 2^{n-2} - 1$, ρ_i est une représentation irréductible car $\operatorname{Im} \rho_i$ est non abélien. De plus, ce sont des représentations distinctes (car si $i \neq j$, alors $\rho_i(x)$ et $\rho_j(x)$ n'ont pas les mêmes valeurs propres). Cela donne $2^{n-2} - 1$ caractères distincts non-linéaires. Il reste à voir qu'il n'y en a pas d'autres. Pour cela, on va calculer les classes de conjugaison car on sait que le nombre de caractères irréductibles distincts sur $\mathbb{C}$ est égal au nombre de classes de conjugaison. Or il y a $2^{n-2} + 3$ classes de conjugaison :

- $Cl_G(1) = \{1\}$;
- $Cl_G(x^{2^{n-2}}) = \{x^{2^{n-2}}\}$;
- $Cl_G(x^i) = \{x^i, x^{-i}\}$, pour tout $i = 1, \ldots, 2^{n-2} - 1$;
- $Cl_G(y) = \left\{x^{2j} y \,\middle|\, j \in \{0, \ldots 2^{n-2} - 1\}\right\}$;

- $Cl_G(xy) = \left\{x^{2j+1}y \,\middle|\, j \in \{0, \dots 2^{n-2}-1\}\right\}$.

Ainsi on voit que l'on a trouvé tous les caractères irréductibles. Voici la table de caractère de Q_{2^n} :

	1	$x^{2^{n-2}}$	x^k $1 \leq k \leq 2^{n-2}-1$	y	xy
η_1	1	1	1	1	1
η_2	1	1	1	-1	-1
η_3	1	1	$(-1)^k$	-1	1
η_4	1	1	$(-1)^k$	1	-1
ψ_j	2	$(-1)^j 2$	$\omega^{jk} + \omega^{-jk}$	0	0

$1 \leq j \leq 2^{n-2}-1$, ω est une racine 2^{n-1}-ième primitive de l'unité.
On peut remarquer que D_{2^n} et Q_{2^n} ont la même table de caractère sur $\mathbb{C}$ bien que ce soit des groupes non-isomorphes.

Remarque B.59 L'exemple précédent se base sur la partie § 47. Applications : Representations of Metacyclic Groups du livre *Representation theory of finite groups and associative algebras* de Charles W. Crutis et Irving Reiner, [CR66], pages 333-340.

Annexe C

Rappels sur les formes bilinéaires

Définition C.1 *Soit K un corps et V un K-espace vectoriel de dimension finie. Alors une* ***forme bilinéaire sur*** *V est une application $\beta : V \times V \to K$ qui satisfait aux propriétés suivantes :*

i) Pour tout $u, v, w \in V$, pour tout $\lambda, \mu \in K$, on a

$$\beta(\lambda u + \mu v, w) = \lambda\beta(u, w) + \mu\beta(v, w).$$

ii) Pour tout $u, v, w \in V$, pour tout $\lambda, \mu \in K$, on a

$$\beta(u, \lambda v + \mu w) = \lambda\beta(u, v) + \mu\beta(u, w).$$

Définition C.2 *Soit K un corps, V un K-espace vectoriel de dimension finie et β une forme bilinéaire sur V. Alors β est une forme bilinéaire* ***non-dégénérée*** *si $\beta(u, v) = 0$ pour tout $u \in V$ implique que $v = 0$.*

Définition C.3 *Soit K un corps, V un K-espace vectoriel de dimension finie et β une forme bilinéaire sur V.*

i) La forme bilinéaire β est dite ***symétrique*** *si $\beta(u, v) = \beta(v, u)$, pour tout $u, v \in V$*

ii) La forme bilinéaire β est dite ***antisymétrique*** *si $\beta(u, v) = -\beta(v, u)$, pour tout $u, v \in V$.*

iii) La forme bilinéaire β est dite ***symplectique*** *si $\beta(v, v) = 0$, pour tout $v \in V$.*

Définition C.4 *Soit K un corps, V un K-espace vectoriel de dimension finie, β une forme bilinéaire sur V et X un sous-ensemble de V. Alors le* ***complément orthogonal*** *de X est*

$$X^{\perp} = \{u \in V \mid \beta(u, v) = 0 \text{ pour tout } v \in X\}.$$

Proposition C.5 ([Tay92], page 52) *Soit K un corps, V un K-espace vectoriel de dimension finie, β une forme bilinéaire sur V et X, Y des sous-espaces vectoriels de V. Alors on a*

$$dim_K X + dim_K X^\perp = dim_K V$$

et si $X \subset Y$, alors $Y^\perp \subset X^\perp$.

Définition C.6 *Soit K un corps, V un K-espace vectoriel de dimension finie et β une forme biliénaire sur V.*

*i) Un vecteur non-nul $v \in V$ est **isotrope** si $\beta(v, v) = 0$.*

*ii) Un sous-espace W de V est **totalement isotrope** si $W \subset W^\perp$.*

*iii) Une paire de vecteur (u, v) de V tels que u et v sont isotropes et $\beta(u, v) = 1$ est appelé une **paire hyperbolique**.*

*iv) Un sous-espace W est **non-dégénéré** si $W \cap W^\perp = \{0\}$.*

*v) Si $V = U \oplus W$ et que $\beta(u, w) = 0$ pour tout $u \in U$ et pour tout $w \in W$, alors on écrit $V = U \perp W$ et on dit que V est la **somme directe orthogonale** de U et W.*

Proposition C.7 *Soit K un corps, V un K-espace vectoriel de dimension finie, β une forme biliénaire symétrique, antisymétrique ou symplectique sur V et W un sous-espace non-dégénéré. Alors*

$$V = W \perp W^\perp.$$

Preuve: On a que, par la proposition C.5,

$$\dim_K W + W^\perp = \underbrace{\dim_K W + \dim_K W^\perp}_{= \dim_K V} - \underbrace{\dim_K (W \cap W^\perp)}_{= 0} = \dim_K V.$$

Ainsi $W + W^\perp = V$ et $W \cap W^\perp = \{0\}$, donc $V = W \oplus W^\perp$. Mais, par définition de $W^\perp$, on a $\beta(u, w) = 0$, pour tout $u \in W$ et pour tout $w \in W^\perp$, donc $V = W \perp W^\perp$. □

Définition C.8 *Soit K un corps, V un K-espace vectoriel de dimension finie et β une forme bilinéaire. Alors **l'indice de Witt** de la forme β est égal à la dimension d'un sous-espace totalement isotrope maximal de V.*

Remarque C.9 On peut montrer que si W et W' sont deux sous-espaces vectoriels totalement isotropes maximaux de V, alors leur dimension sont égales. Ainsi la définition précédent à bien un sens.

Proposition C.10 ([Tay92], page 69) *Soit K un corps, V un K-espace vectoriel de dimension finie et β une forme bilinéaire symplectique et non-dégénérée. Alors il existe une base $e_1, f_1, e_2, f_2, \ldots, e_m, f_m$ de V tel que $\beta(e_i, e_j) = \beta(f_i, f_j) = 0$ et $\beta(e_i, f_j) = \delta_{ij}$ pour tout $1 \leq i, j \leq m$. En particulier, la dimension de V est pair et l'indice de Witt est égal à m.*

Définition C.11 *Soit K un corps, V un K-espace vectoriel de dimension finie et β une forme bilinéaire symplectique et non-dégénérée. Alors une base $e_1, f_1, e_2, f_2, \ldots, e_m, f_m$ de V tel que $\beta(e_i, e_j) = \beta(f_i, f_j) = 0$ et $\beta(e_i, f_j) = \delta_{ij}$ pour tout $1 \leq i, j \leq m$ s'appelle une* ***base symplectique de*** *V.*

Définition C.12 *Soit K un corps et V un K-espace vectoriel de dimension finie. Une* ***forme quadratique sur*** *V est une application $Q : V \to K$ qui satisfait aux deux propriétés suivantes :*

i) $Q(av) = aQ(v)$ pour tout $a \in K$ et pour tout $v \in V$,

ii) L'application $\beta : V \times V \to K$ définie par

$$\beta(v, w) = Q(v + w) - Q(v) - Q(w)$$

pour tout $v, w \in V$ est une forme bilinéaire.

On appelle β la ***forme polaire associée à*** *Q.*

Théorème C.13: ([Die63], page 34)
Soit $K = \mathbb{F}_q$, où $q = 2^s$ et V un K-espace vectoriel de dimension finie. Si $Q : V \to K$ est une forme quadratique non-dégénérée sur K, alors il existe une base $\{b_1, b_2, \ldots, b_n\}$ de V tel que :

- *Si $n = 2m + 1$ pour un certain $m \in \mathbb{N}$,*

$$Q\Big(\sum_{i=1}^{n} \xi_i b_i\Big) = \sum_{i=1}^{m} \xi_i \xi_{m+i} + \xi_n^2.$$

- *Si $n = 2m$ pour un certain $m \in \mathbb{N}$,*

$$Q\Big(\sum_{i=1}^{n} \xi_i b_i\Big) = \sum_{i=1}^{m-1} \xi_i \xi_{m+i} + (\delta \xi_m^2 + \xi_m \xi_{2m} + \delta \xi_{2m}^2),$$

où $\delta = 0$ ou δ est tel que $\delta X^2 + X + \delta$ est un polynôme irréductible sur K.

Bibliographie

[Bou] Serge Bouc. *Biset functors for finite groups*. preprint 2007.

[Bou96] Serge Bouc. Foncteurs d'ensembles munis d'une double action. *J. Algebra*, (183) : pages 664–736, 1996.

[Bou00] Serge Bouc. Burnside rings. In *Handbook of Algebra*, volume 2, chapter 6E, pages 739–804. Amsterdam : Elsevier, 2000.

[Bou01] Serge Bouc. A remark on a theorem of Ritter and Segal. *J. Group Theory*, (4) : pages 11–18, 2001.

[BT] Serge Bouc and Jacques Thévenaz. Gluing torsion endo-permutation modules. preprint 2007.

[CR66] Charles W. Crutis and Irving Reiner. *Representation theory of finite groups and associative algebras*. New YorK [etc.] : Interscience Publishers, 1966.

[Die63] Jean Dieudonné. *La géométrie des groupes classiques*. Berlin [etc.] : Springer, 1963.

[Gor68] Daniel Gorenstein. *Finite groups*. New York [etc.] : Harper & Row, 1968.

[JL06] Gordon James and Martin Liebeck. *Representations and characters of groups*. Cambridge : Cambridge University Press, 2006.

[Kar92] Gregory Karpilovsky. *Introduction to group representations and characters*. Group Representations : vol. 1, part B. Amsterdam [etc.] : North-Holland, 1992.

[Laz07] Vincent Lazano. *Tout ce que vous avez toujours voulu savoir sur LaTeX sans jamais avoir osé le demander*. http ://cours.enise.fr/info/latex/, 24 octobre 2007, consulté le 21 novembre 2007.

[NT89] Hirosi Nagao and Yukio Tsushima. *Representations of finite groups*. Boston [etc.] : Academic Press, cop., 1989.

[Rob82] Derek John Scott Robinson. *A Course in the theory of groups*. New York a.o. : Springer, 1982.

[Rot95] Joseph Jonah Rotman. *An introduction to the theory of groups*. New York [etc.] : Springer-Verlag. cop., 1995.

[Ré89] László Rédei. *Endliche p-Gruppen.* Budapest : Akadémiai Kiadó, 1989.

[Ser78] Jean-Pierre Serre. *Représentations linéaires des groupes finis.* Paris : Hermann, 1978.

[Sta86] Richard P. Stanley. *Enumerative Combinatorics*, volume I. Monterey California : Wadsworth & Brooks/Cole, 1986.

[Tay92] Donald E. Taylor. *The Geometry of the Classical Groups.* Berlin : heldermann, cop., 1992.

[Tsu82] T. Tsuzuku. *Finite groups and finite geometries.* Cambridge a.o. : Cambridge University Press, 1982.

Index