

# Ortho-ambivalence des groupes finis

Obed NTABUHASHE ZAHINDA

Mai 2008

Thèse présentée en vue de l'obtention  
du grade de docteur en sciences  
Promoteur: Jean-Pierre TIGNOL

Faculté des Sciences  
Ecole doctorale en mathématiques

Université Catholique de Louvain

# Ortho-ambivalence des groupes finis

## Membres du jury:

-Jean-Pierre TIGNOL: **Promoteur**

(Professeur à l'Université Catholique de Louvain, Belgique)

- Jean MAWHIN: **Président du jury**

(Professeur à l'Université Catholique de Louvain, Belgique)

- Francis BORCEUX

(Professeur à l'Université Catholique de Louvain, Belgique)

- Yves FELIX

(Professeur à l'Université Catholique de Louvain, Belgique)

- Pasquale MAMMONE

(Professeur à l'Université d'Artois Lens, France)

**Pré-défense:** le 09 avril 2008

**Défense publique:** le 16 mai 2008

*”Jésus lui dit : Je suis le chemin, la  
vérité, et la vie. Nul ne vient au Père  
que par moi.”*  
*(Jean 14 : 6).*



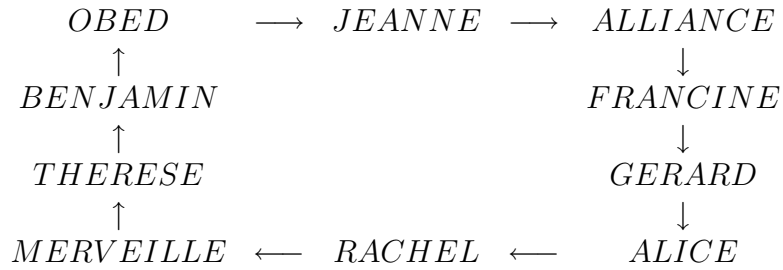
**Dédié à**

Baderha Ntakwindja Jeanne,  
Ntabuhashe Amani Alliance,  
Ntabuhashe Mugoli Francine,  
Ntabuhashe Cizige Gérard,  
Ntabuhashe Bindja Alice,  
Ntabuhashe Biluge Rachel,  
Ntabuhashe Namulisa Merveille,  
Ntabuhashe Bibentyo Thérèse  
et  
Ntabuhashe Zahinda Benjamin.

\*

\*\*

Vous faites partie de la belle suite décagonale suivante :





# Remerciements

Si longue soit la nuit, elle finit par laisser place au jour. Cette thèse est le fruit du concours de plusieurs personnes, par la grâce de notre Seigneur Jésus Christ.

Notre gratitude s'adresse particulièrement au Professeur Jean-Pierre TIGNOL qui a accepté de diriger cette thèse. Son savoir-faire, sa disponibilité, sa gentillesse, sa persévérance,... nous ont beaucoup marqué et continueront à nous émerveiller.

Nous remercions tous les professeurs de l'Institut de Mathématique pure et appliquée de l'Université Catholique de Louvain pour l'accueil et l'encadrement dont nous avons été bénéficiaires. Nous pensons spécialement aux membres de notre comité d'encadrement et/ou du jury, les professeurs Francis BORCEUX, Yves FELIX, Jean MAWHIN et Pasquale MAMMONE.

A tous ceux qui nous ont soutenu moralement, spirituellement ou matériellement, nous disons de tout notre coeur : "merci et que Dieu vous bénisse".





# Table des matières

|                                                 |             |
|-------------------------------------------------|-------------|
| <b>Remerciements</b>                            | <b>vii</b>  |
| <b>Introduction</b>                             | <b>xi</b>   |
| <b>Notations</b>                                | <b>xvii</b> |
| <b>1 Notions préliminaires</b>                  | <b>1</b>    |
| 1.1 Représentations des groupes finis . . . . . | 1           |
| 1.2 Algèbres et involutions . . . . .           | 3           |
| 1.3 Algèbre de groupe . . . . .                 | 11          |
| <b>2 Involution canonique</b>                   | <b>15</b>   |
| 2.1 Cas d'un corps algébriquement clos. . . . . | 16          |
| 2.2 Changement de caractéristique . . . . .     | 28          |
| 2.3 Extension des scalaires . . . . .           | 36          |
| 2.4 Quelques résultats. . . . .                 | 48          |
| <b>3 Quelques groupes particuliers</b>          | <b>53</b>   |
| 3.1 Quelques résultats préliminaires . . . . .  | 53          |
| 3.2 Des p-groupes. . . . .                      | 61          |
| 3.3 Des 2-groupes extra-spéciaux. . . . .       | 66          |
| 3.4 Des 2-groupes spéciaux . . . . .            | 75          |
| <b>4 Groupes de Witt</b>                        | <b>145</b>  |
| 4.1 Groupe de Witt usuel . . . . .              | 146         |
| 4.2 Groupe de Witt dérivé . . . . .             | 149         |

|                      |                                                   |            |
|----------------------|---------------------------------------------------|------------|
| 4.3                  | Groupes de Witt tordus et<br>dodécagone . . . . . | 155        |
| 4.4                  | Application à une algèbre de groupe . . . . .     | 169        |
| <b>Conclusion</b>    |                                                   | <b>177</b> |
| <b>Bibliographie</b> |                                                   | <b>181</b> |

# Introduction

La théorie des caractères fournit un outil précieux pour démontrer des résultats sur les groupes finis. Isaacs stipule qu'il y a des théorèmes sur les groupes finis qu'on ne sait démontrer actuellement qu'en utilisant les caractères. C'est le cas par exemple pour le théorème de Frobenius : "*Si  $G$  est un groupe de Frobenius de complément  $H$  (voir définition 2.4.4), alors il existe un sous-groupe normal  $N$  de  $G$  tel que  $HN = G$  et  $H \cap N = 1$  (voir [25, théorème 7.2, page 100])*" et pour le théorème de Burnside suivant : "*Si  $G$  est un groupe d'ordre  $p^a q^b$ ,  $p, q, a, b$  étant des entiers naturels tels que  $p$  et  $q$  soient premiers, alors  $G$  est résoluble (voir [25, théorème 3.10, page 37])*".

Un caractère (complexe) d'un groupe fini  $G$  est dit orthogonal s'il est le caractère d'une  $\mathbb{C}$ -représentation de  $G$  réalisable sur  $\mathbb{R}$ . Un tel caractère est réel. C'est possible qu'un caractère d'un groupe fini  $G$  soit réel sans qu'il soit caractère d'une  $\mathbb{C}$ -représentation réalisable sur  $\mathbb{R}$  (il est dit réel non orthogonal). Un groupe fini est dit totalement orthogonal si tous ses caractères irréductibles sont orthogonaux. Si  $\chi$  est un caractère irréductible d'un groupe fini  $G$ , on appelle indicateur de Schur-Frobenius de  $\chi$  et on note  $\nu(\chi)$  le nombre  $\nu(\chi) = \frac{1}{|G|} \sum_{g \in G} \chi(g^2)$ . Les caractères irréductibles d'un groupe fini se caractérisent de la manière suivante : "*Pour qu'un caractère irréductible  $\chi$  d'un groupe fini  $G$  soit orthogonal, réel non orthogonal ou non réel, il faut et il suffit que son indicateur de Schur-Frobenius soit respectivement égal à 1,  $-1$  ou 0 (voir proposition 2.1.13)*". Dans la suite, le type d'un caractère irréductible

$\chi$  se définit comme étant son indicateur  $\nu(\chi)$  de Schur-Frobenius (voir remarque 2.1.15).

Depuis longtemps, il est connu que pour que tout caractère irréductible d'un groupe fini soit réel, il faut et il suffit que ce groupe soit ambivalent c'est-à-dire que tout élément de ce groupe soit conjugué à son inverse. En 1988, Wang et Grove révèlent dans [42] qu'en 1963, Brauer cite le problème de recherche du nombre de caractères irréductibles orthogonaux d'un groupe fini  $G$  comme étant une question très ancienne. Ce problème dit "de Brauer" reste ouvert jusqu'à ce jour. Toutefois, on peut noter quelques progrès dans la recherche des solutions à ce problème.

- En 1976, Gow trouve la solution à ce problème pour les groupes dont les 2-sous-groupes de Sylow sont cycliques (voir [18, théorème 4, page 268]).

- En 1979, Gow établit un résultat, solution au problème de Brauer, pour les groupes nilpotents de classe 2 avec un 2-sous-groupe de Sylow abélien (voir [19, théorème 7.6, page 412]).

- En 1988, Wang et Grove donnent une solution pour les groupes de Frobenius [42, théorème 5.3, page 306] ; ils étudient le cas extrême du problème de Brauer, les groupes totalement orthogonaux (voir propositions allant de 2.4.5 à 2.4.11).

- En 2003, Quinlan donne une solution partielle au problème de Brauer pour les 2-groupes  $G$  d'ordre  $2^{n+\binom{n}{2}}$  tels que  $G' = Z(G)$  est un groupe abélien élémentaire d'ordre  $2^{\binom{n}{2}}$  et  $\frac{G}{G'}$  est un groupe abélien élémentaire d'ordre  $2^n$  (de tels groupes sont appelés des recouvrements de Schur d'un groupe abélien élémentaire d'ordre  $2^n$ ) : cette solution est donnée en terme de relations de récurrence donnant le nombre  $a(n, r, 1)$  de caractères linéaires  $\theta$  de  $G'$  pour

lesquels les caractères irréductibles de  $G$  induits par  $\theta$  sont de degré  $2^r$  et de type 1 (voir [35, théorème 4.1, page 205]).

Soit  $G$  un groupe fini et  $k$  un corps dont la caractéristique ne divise pas l'ordre de  $G$ . D'après le théorème de Maschke, l'algèbre de groupe  $kG$  est semi-simple. L'application  $g \mapsto g^{-1}$  de  $G$  dans  $G$  se prolonge de façon naturelle en une involution  $k$ -linéaire sur  $kG$ , appelée involution canonique sur  $kG$ . En utilisant la théorie des caractères, Boulagouaz et Oukhtite démontrent dans [9] que pour que la restriction de l'involution canonique à chaque composante simple de  $kG$  soit une involution de première espèce, il faut et il suffit que le groupe  $G$  soit ambivalent. En vertu du 3-ième paragraphe, il est équivalent de dire que tous les caractères complexes de  $G$  sont réels. C'est curieux car, de tous les travaux auxquels nous avons eu accès, aucun ne parle des liens qui existent entre le comportement de l'involution canonique sur les composantes simples de l'algèbre de groupe  $kG$  et les types des caractères complexes irréductibles de  $G$ .

On dit qu'un groupe fini  $G$  est ortho-ambivalent par rapport à un corps  $k$  dont la caractéristique ne divise pas l'ordre de  $G$ , si la restriction de l'involution canonique à chaque composante simple de l'algèbre de groupe  $kG$  est une involution de première espèce de type orthogonal. Nous nous proposons de *chercher à trouver des conditions nécessaires et suffisantes pour qu'un groupe fini  $G$  soit ortho-ambivalent par rapport à un corps  $k$  dont la caractéristique ne divise pas l'ordre de  $G$ .*

Nous arrivons à établir (voir corollaire 4.4.4) que les propositions suivantes sont équivalentes :

- (1)  $G$  est ortho-ambivalent par rapport à  $k$  ;
- (2)  $G$  est ortho-ambivalent par rapport à  $\mathbb{C}$  ;
- (3)  $G$  est ambivalent et pour tout caractère irréductible  $\chi$  de  $G$ ,  
 $\nu(\chi) = 1$  ;

- (4)  $G$  est ambivalent et  $t(1) = \sum_{\chi \in \text{Irr}(G)} \chi(1)$ ,  $t(1)$  étant le nombre d'éléments  $g$  de  $G$  tels que  $g^2 = 1$  et  $\text{Irr}(G)$ , l'ensemble des caractères irréductibles complexes de  $G$ ;
- (5)  $G$  est totalement orthogonal.

Et si  $\text{car } k \neq 2$ , les cinq premières propositions sont équivalentes à la proposition suivante :

- (6)  $G$  est ambivalent et le premier groupe de Witt tordu de la catégorie des  $kG$ -modules libres finiment engendrés munie de la dualité  $(*, \varpi)$  définie dans la section 4.1 par (4.1), (4.2) et (4.3) (dépendant de l'involution canonique sur  $kG$ ), est trivial.

Dans le premier chapitre, nous rappelons quelques résultats sur les représentations et les caractères des groupes finis, sur les algèbres et involutions et sur les algèbres de groupe.

Dans le second, nous établissons des liens entre le type de la restriction de l'involution canonique à chaque composante simple d'une algèbre de groupe semi-simple et le type des caractères irréductibles complexes de ce groupe. Cela nous amène à établir que pour qu'un groupe fini  $G$  soit ortho-ambivalent par rapport à un corps  $k$  dont la caractéristique ne divise pas l'ordre de  $G$ , il faut et il suffit que  $G$  soit totalement orthogonal. Nous clôturons ce chapitre par des résultats déductibles directement de ceux donnés par Wang et Grove dans [42] sur les groupes totalement orthogonaux ; parmi ces résultats figure une condition nécessaire et suffisante pour qu'un 2-groupe soit ortho-ambivalent par rapport à un corps de caractéristique différente de 2 (voir théorème 2.4.18).

Le troisième chapitre est consacré à l'étude des algèbres de groupes pour des  $p$ -groupes, des 2-groupes extra-spéciaux et des 2-groupes spéciaux. Nous démontrons que si  $p$  est un entier premier  $> 2$ , tout  $p$ -groupe fini non trivial possède un unique caractère irréductible de type 1, tous les autres étant de type 0 (voir corollaire 3.2.2) ; pour

un tel groupe, on ne peut donc parler ni d'ambivalence, ni d'ortho-ambivalence par rapport à un corps. Un critère d'ortho-ambivalence étant déjà donné dans le chapitre 2 pour les 2-groupes, nous donnons quelques particularités de ceux-ci (voir proposition 3.2.3). Nous démontrons qu'à chaque 2-groupe extra-spécial correspond une forme quadratique régulière sur le quotient de ce groupe par son centre (qui est un 2-groupe abélien élémentaire) vu comme un espace vectoriel sur le corps  $\mathbb{F}_2$  à deux éléments : l'invariant d'Arf de cette forme quadratique est appelé l'invariant d'Arf de ce 2-groupe extra-spécial. Nous établissons qu'un 2-groupe extra-spécial est ortho-ambivalent par rapport à un corps de caractéristique différente de 2 si et seulement si son invariant d'Arf est nul (voir corollaire 3.4.27). Nous démontrons qu'à chaque 2-groupe spécial correspond une application quadratique régulière du groupe quotient de ce groupe par son centre dans le centre de ce groupe (ces deux derniers groupes sont en fait abéliens élémentaires et regardés comme des espaces vectoriels sur le corps  $\mathbb{F}_2$ ). Etant donnés deux groupes abéliens élémentaires  $A$  et  $B$ , nous prouvons que le deuxième groupe de cohomologie  $H^2(A, B)$  de  $A$  à coefficients dans  $B$  est isomorphe au groupe  $Quad(A, B)$  des applications quadratiques de  $A$  dans  $B$  ; ainsi comme  $H^2(A, B)$  classe les extensions centrales de  $B$  par  $A$ , il en est de même pour  $Quad(A, B)$  ; en particulier, nous démontrons que pour toute application quadratique régulière  $q$  de  $A$  dans  $B$  telle que  $B$  soit engendré par l'image de l'application polaire, il existe un unique 2-groupe spécial  $G$  (à isomorphisme près) de centre  $B$ , de quotient par le centre isomorphe à  $A$  et d'application quadratique  $q$  (voir théorème 3.4.23). Nous obtenons ainsi une construction de l'extension centrale de  $B$  par  $A$  correspondant à  $q$  et donc à la classe de cohomologie du 2-cocycle (normalisé de  $A$  à coefficients dans  $B$ ) correspondant à  $q$  par l'isomorphisme entre  $H^2(A, B)$  et  $Quad(A, B)$ . Nous démontrons que si  $G$  est un 2-groupe spécial ambivalent, alors pour toute représentation irréductible  $\rho$  de  $G$  de degré  $> 1$ ,  $\rho(G)$  est un 2-groupe extra-spécial et que  $G$  est ortho-ambivalent par rapport à un corps de caractéristique différente de 2 si et seulement si pour toute représentation irréducti-

ble  $\rho$  de  $G$  de degré  $> 1$ , l'invariant d'Arf de  $\rho(G)$  est nul (voir corollaire 3.4.31). Nous démontrons enfin qu'un 2-groupe spécial ambivalent  $G$  d'application quadratique  $q$  est ortho-ambivalent par rapport à un corps de caractéristique différente de 2 si et seulement si pour toute  $\mathbb{F}_2$ -forme linéaire  $s$  sur  $Z(G)$ , l'invariant d'Arf de la forme quadratique induite par le transfert de  $q$  par  $s$  est nul.

Dans le quatrième chapitre, après avoir défini les groupes de Witt des catégories avec dualité  $R_\sigma - proj$  et  $R_\sigma - lib$  (voir ( 4.4) pour la définition de ces catégories),  $R$  étant une algèbre semi-simple sur un corps  $k$  et  $\sigma$  une involution sur  $R$ , nous arrivons à trouver des conditions nécessaires et suffisantes pour qu'un groupe fini  $G$  soit ortho-ambivalent par rapport à un corps  $k$  dont la caractéristique ne divise pas l'ordre de  $G$ , ceci, en termes de groupe de Witt.

Dans toute la suite, tous les corps sont supposés commutatifs et tous les anneaux, unitaires.



# Notations

|                  |                                                                                                             |
|------------------|-------------------------------------------------------------------------------------------------------------|
| $(G : H)$        | : Indice de $H$ dans $G$ , 2                                                                                |
| $(\#, \pi)$      | : Dualité, (voir remarque 4.2.2), 152                                                                       |
| $(*, \varpi)$    | : Dualité, (voir remarque 4.1.2), 146                                                                       |
| $(\chi, \chi')$  | : $= \frac{1}{ G } \sum_{g \in G} \chi(g) \chi'(g^{-1})$ , pour des caractères $\chi$ et $\chi'$ de $G$ , 3 |
| $(a, b)_k$       | : Algèbre des quaternions en caractéristique différente de 2, 8                                             |
| $2_+^{1+2n}$     | : Produit central de $n$ groupes égaux à $D_4$ , 67                                                         |
| $2_-^{1+2n}$     | : Produit central de $Q_2$ et $2_+^{-1+2n}$ , 67                                                            |
| $A^\times$       | : Groupe des éléments inversibles d'une algèbre $A$ , 3                                                     |
| $A^{op}$         | : Algèbre opposée d'une algèbre $A$ , 4                                                                     |
| $A_K$            | : $= A \otimes_k K$ , pour une extension de corps $K/k$ et une $k$ -algèbre $A$ , 4                         |
| $A_n$            | : Groupe alterné (d'ordre $\frac{n!}{2}$ si $n \neq 1$ ), 50                                                |
| $Alt(A, \sigma)$ | : $= \{a - \sigma(a)   a \in A\}$ , 7                                                                       |
| $Arf(G)$         | : Invariant d'Arf d'un 2-groupe extra spécial $G$ , 102                                                     |
| $Arf(q)$         | : Invariant d'Arf d'une forme quadratique régulière $q$ , 81                                                |
| $Bil(k)$         | : Ensemble des espaces bilinéaires symétriques sur $k$ , 129                                                |
| $B^2(A, B)$      | : Groupe des 2-cobords de $A$ à coefficients dans $B$ , 84                                                  |
| $C(u_\bullet)$   | : $= Cone(u_\bullet)$ : Cône de $u_\bullet$ , 150                                                           |

|                                                    |                                                                                                             |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| $\mathcal{C}$                                      | : $= R_\sigma - lib$ ou $R_\sigma - proj$ , 147                                                             |
| $D^b(\mathcal{C})$                                 | : Catégorie dérivée de $\mathcal{C}$ , 154                                                                  |
| $D^{n \times m}$                                   | : Ensemble des matrices $n \times m$ à entrées dans $D$ , 166                                               |
| $D_n$                                              | : Groupe diédral d'ordre $2n$ , 20                                                                          |
| $End_k(V)$                                         | : Algèbre des $k$ -endomorphismes de $V$ , 5, 17                                                            |
| $G_1 \circ \dots \circ G_n$                        | : Produit central des groupes $G_1, \dots$ et $G_n$ , 67                                                    |
| $Gal(K/k)$                                         | : Groupe de Galois de l'extension de corps $K/k$ , 28                                                       |
| $G' = [G, G]$                                      | : Sous-groupe dérivé d'un groupe $G$ , 61                                                                   |
| $GL(V)$                                            | : Groupe linéaire de $V$ , 1                                                                                |
| $GL_n(k)$                                          | : Groupe des matrices carrées inversibles d'ordre $n$ à entrées dans $k$ , 1                                |
| $H^2(A, B)$                                        | : 2-ième groupe de cohomologie de $A$ à coefficients dans $B$ , 85                                          |
| $H_r(M)$                                           | : Espace hyperbolique associé à $M$ , 164                                                                   |
| $\mathbb{H}(V)$                                    | : Espace (quadratique) hyperbolique associé à $V$ , 128                                                     |
| $Hom_k(V, W)$                                      | : Ensemble des $k$ -morphisms de $V$ dans $W$                                                               |
| $\widehat{H}^i(\frac{\mathbb{Z}}{2\mathbb{Z}}, A)$ | : $i$ -ième groupe de cohomologie de Tate de $\frac{\mathbb{Z}}{2\mathbb{Z}}$ à coefficients dans $A$ , 161 |
| $I_n$                                              | : Matrice unité d'ordre $n$ , 10                                                                            |
| $Id_{\mathcal{C}}$                                 | : Foncteur identité sur $\mathcal{C}$ , 146                                                                 |
| $Im f$                                             | : Image de $f$                                                                                              |
| $Int(u)$                                           | : Automorphisme intérieur de... associé à $u$ , 8                                                           |
| $Irr(G)$                                           | : Ensemble des caractères irréductibles de $G$ , 23                                                         |
| $K/k$                                              | : Extension de corps $k \subset K$ , 5                                                                      |
| $K^b(\mathcal{C})$                                 | : Catégorie homotopique de $\mathcal{C}$ , 149                                                              |
| $K_0 R$                                            | : 0-ième groupe de $K$ -théorie de $R$ , 162                                                                |
| $\widetilde{K}_0 R$                                | : 0-ième groupe réduit de $K$ -théorie de $R$ , 162                                                         |
| $K_p$                                              | : Clôture algébrique de $\mathbb{F}_p$ , 31                                                                 |
| $Ker f$                                            | : Noyau de $f$                                                                                              |

|                                |                                                                                                         |
|--------------------------------|---------------------------------------------------------------------------------------------------------|
| $\mathbb{M}(V)$                | : Espace métabolique associé à $V$ , 129                                                                |
| $MW^\varepsilon(\mathcal{C})$  | : Monoïde de Witt- $(\varepsilon)$ de $\mathcal{C}$ , 148                                               |
| $MW^-(\mathcal{C})$            | : $= MW^{-1}(\mathcal{C})$ , 149                                                                        |
| $MW(\mathcal{C})$              | : $= MW^{+1}(\mathcal{C})$ , 149                                                                        |
| $M_n(k)$                       | : Algèbre des matrices carrées d'ordre $n$<br>à entrées dans $k$ , 4                                    |
| $(M, \varphi) \perp (N, \psi)$ | : Somme orthogonale de $(M, \varphi)$ et<br>$(N, \psi)$ , 148                                           |
| $NW(\mathcal{C})$              | : $= NW^{+1}(\mathcal{C})$ , 149                                                                        |
| $NW^-(\mathcal{C})$            | : $= NW^{-1}(\mathcal{C})$ , 149                                                                        |
| $NW^\varepsilon(\mathcal{C})$  | : Ensemble des classes des espaces $(\varepsilon)$ -<br>symétriques métaboliques de $\mathcal{C}$ , 148 |
| $Q_n$                          | : Groupe quaternionique d'ordre $4n$ , 20                                                               |
| $Quad(A, B)$                   | : Groupe des applications quadratiques de<br>$A$ dans $B$ , 84                                          |
| $Quad(k)$                      | : Ensemble des espaces quadratiques sur<br>$k$ , 128                                                    |
| $Q^{-1}K^b(\mathcal{C})$       | : Localisation de $K^b(\mathcal{C})$ par $Q$ , 153                                                      |
| $R - lib$                      | : Catégorie des $R$ -modules libres (à gauche)<br>finiment engendrés, 145                               |
| $R - proj$                     | : Catégorie des $R$ -modules projectifs<br>(à gauche) finiment engendrés, 145                           |
| $R_\sigma - lib$               | : $= (R - lib, *, \varpi)$ , 147                                                                        |
| $R_\sigma - proj$              | : $= (R - proj, *, \varpi)$ , 147                                                                       |
| $S_n$                          | : Groupe symétrique d'ordre $n!$ , 20                                                                   |
| $Sh(\mathcal{C})$              | : Catégorie des complexes courts de $\mathcal{C}$ , 156                                                 |
| $Skew(A, \sigma)$              | : $= \{a \in A \mid \sigma(a) = -a\}$ , 7                                                               |
| $Sym(A, \sigma)$               | : $= \{a \in A \mid \sigma(a) = a\}$ , 7                                                                |
| $Symd(A, \sigma)$              | : $= \{a + \sigma(a) \mid a \in A\}$ , 7                                                                |
| $T(A_\bullet)$                 | : $= A_\bullet[-1]$ , 150                                                                               |
| $Tr_{k/F}$                     | : Forme trace de l'extension $k/F$ , 131                                                                |
| $V^*$                          | : $= Hom_k(V, k)$ , pour un $k$ -espace<br>vectoriel $V$ , 3                                            |
| $W(k)$                         | : Anneau de Witt des espaces bilinéaires<br>symétriques sur $k$ , 130                                   |

|                                   |                                                                                           |
|-----------------------------------|-------------------------------------------------------------------------------------------|
| $\widehat{W}(k)$                  | : Anneau de Witt de Grothendieck des espaces bilinéaires symétriques sur $k$ , 130        |
| $W_q(k)$                          | : Groupe de Witt des espaces quadratiques sur $k$ , 130                                   |
| $\widehat{W}_q(k)$                | : Groupe de Witt de Grothendieck des espaces quadratiques sur $k$ , 130                   |
| $W_{der}(\mathcal{C})$            | : Groupe de Witt dérivé de $\mathcal{C}$ , 155                                            |
| $W_{sh}^+(\mathcal{C})$           | : $= W_{sh}^{+1}(\mathcal{C})$ , 159                                                      |
| $W_{sh}^-(\mathcal{C})$           | : $= W_{sh}^{-1}(\mathcal{C})$ , 159                                                      |
| $W_{us}^-(\mathcal{C})$           | : $= W^{-1}(\mathcal{C})$ , 149                                                           |
| $W^\varepsilon(\mathcal{C})$      | : Groupe de Witt $\varepsilon$ de $\mathcal{C}$ , 149                                     |
| $W_{sh}^\varepsilon(\mathcal{C})$ | : Groupe de Witt des complexes courts $\varepsilon$ -symétriques de $\mathcal{C}$ , 159   |
| $W^n(\mathcal{C})$                | : $n$ -ième groupe de Witt de $\mathcal{C}$ , 156                                         |
| $W_{us}(\mathcal{C})$             | : $= W^{+1}(\mathcal{C}) := W(\mathcal{C})$ , groupe de Witt usuel de $\mathcal{C}$ , 149 |
| $Z(A)$                            | : Centre d'une algèbre $A$ , 4                                                            |
| $Z(G)$                            | : Centre d'un groupe $G$ , 2                                                              |
| $Z^2(A, B)$                       | : Groupe des 2-cocycles de $A$ à coefficients dans $B$ , 84                               |
| $[K : k]$                         | : Degré d'une extension de corps $K/k$ , 5                                                |
| $[M, \varphi]$                    | : Classe d'isométrie d'un espace symétrique $(M, \varphi)$ , 149                          |
| $[a, b]_k$                        | : Algèbre des quaternions en caractéristique 2, 8                                         |
| $[a, b]$                          | : Forme quadratique $\cong ax^2 + xy + by^2$ , en caractéristique 2, 121                  |
| $p \times [a, b]$                 | : Somme orthogonale de $p$ formes quadratiques isométriques à $[a, b]$ , 121              |
| $[m]$                             | : Classe de $m$ , 149                                                                     |
| $[x, y]$                          | : Commutateur $x^{-1}y^{-1}xy$ , 61                                                       |
| $< \alpha_1, \dots, \alpha_r >$   | : Espace bilinéaire symétrique diagonalisable, 131                                        |
| $\Omega(G)$                       | : $= sgr < x \in G/x^2 = 1 >$ , pour un groupe $G$ , 76                                   |
| $\wedge^2 A$                      | : 2-ième puissance extérieure de $A$ , 116                                                |

|                                  |                                                                             |
|----------------------------------|-----------------------------------------------------------------------------|
| $\Phi(G)$                        | : Sous-groupe de Frattini d'un groupe $G$ , 75                              |
| $\chi^\vee$                      | : Caractère contragrédient de $\chi$ , 3                                    |
| $\delta_{ij}$                    | : Symbole de Kronecker, 3                                                   |
| $\frac{\mathbb{Z}}{p\mathbb{Z}}$ | : Anneau des entiers modulo $p$                                             |
| $\mathbb{C}$                     | : Corps des nombres complexes                                               |
| $\mathbb{F}_p$                   | : Corps fini à $p$ éléments                                                 |
| $\mathbb{H}$                     | : $= (-1, -1)_{\mathbb{R}}$ , 18                                            |
| $\mathbb{N}$                     | : Ensemble des nombres entiers naturels                                     |
| $\mathbb{N}_0$                   | : $= \mathbb{N} - \{0\}$                                                    |
| $\mathbb{R}$                     | : Corps des nombres réels                                                   |
| $\mathbb{Z}$                     | : Anneau des nombres entiers                                                |
| $\mathcal{P}(n)$                 | : Nombre de partitions d'un entier naturel $n$ , 172                        |
| $ G $                            | : Ordre, cardinal de $G$ , 2                                                |
| $\mu_n$                          | : Groupe des racines $n$ -ièmes de l'unité                                  |
| $\nu(\chi)$                      | : Indicateur de Schur-Frobenius de $\chi$ , 22                              |
| $\bar{k}$                        | : Clôture algébrique de $k$                                                 |
| $\bar{x}$                        | : Classe de $x$ modulo un sous-groupe normal d'un groupe                    |
| $\rho^\vee$                      | : Représentation contragrédiente de $\rho$ , 3                              |
| $\wp(k)$                         | : $= \{x^2 + x \mid x \in k\}$ , pour un corps $k$ de caractéristique 2, 81 |
| $a^t$                            | : Transposée de $a$                                                         |
| $ad_b$                           | : Involution adjointe de $b$ , 6                                            |
| $b_q$                            | : Application polaire de $q$ , 78                                           |
| $car k$                          | : Caractéristique de $k$                                                    |
| $\deg A$                         | : Degré d'une algèbre simple $A$ , 5                                        |
| $\deg \chi$                      | : Degré d'un caractère $\chi$ , 3                                           |
| $\deg \rho$                      | : Degré d'une représentation $\rho$ , 1                                     |
| $\dim_k M$                       | : Dimension de $M$ sur $k$ , 5                                              |
| $gf := g \circ f$                | : Fonction composée de $f$ et $g$                                           |
| $id_A$ ou $id$                   | : Application identique sur $A$                                             |
| $ind A$                          | : Indice de Schur de $A$ , 5                                                |
| $inf(c)$                         | : Inflation de $c$ , 108                                                    |

|                    |                                                                                                                     |
|--------------------|---------------------------------------------------------------------------------------------------------------------|
| $kG$               | : Algèbre du groupe $G$ sur $k$ , 11                                                                                |
| $o(R)$             | : Nombre de composantes simples de $R$ sur lesquelles la restriction d'une involution sur $R$ est orthogonale, 169  |
| $ord(x)$           | : Ordre de $x$                                                                                                      |
| $q_s$              | : forme quadratique induite par $s_*(q)$ , 110                                                                      |
| $q \perp q'$       | : Somme orthogonale de $q$ et $q'$ , 82                                                                             |
| $radb_q$           | : Radical de $b_q$ , 78                                                                                             |
| $radq$             | : Radical de $q$ , 78                                                                                               |
| $s(R)$             | : Nombre de composantes simples de $R$ sur lesquelles la restriction d'une involution sur $R$ est symplectique, 169 |
| $s_*(q)$           | : Transfert de $q$ par $s$ , 105, 108                                                                               |
| $sev < A >$        | : Sous-espace vectoriel engendré par $A$ , 110                                                                      |
| $sgr < A >$        | : Sous-groupe engendré par $A$ , 60                                                                                 |
| $t(x)$ ou $t_G(x)$ | : Nombre d'éléments $g$ d'un groupe $G$ tels que $g^2 = x$ , 23                                                     |
| $x^y$              | : $= y^{-1}xy$ , 79                                                                                                 |
| resp.              | : respectivement                                                                                                    |

# Chapitre 1

## Notions préliminaires

Dans ce chapitre, nous rappelons certains résultats qui constituent la base de nos investigations.

### 1.1 Représentations des groupes finis

La plupart des résultats de cette section sont tirés de [17] ou [38]. Soient  $G$  un groupe fini,  $k$  un corps et  $V$  et  $V'$  des espaces vectoriels sur  $k$  de dimensions finies respectives  $n$  et  $n'$ . Soient  $GL(V)$  le groupe des  $k$ -automorphismes de  $V$  (appelé le groupe linéaire de  $V$ ) et  $GL_n(k)$  le groupe des matrices carrées inversibles d'ordre  $n$ , à éléments dans  $k$  (ces deux groupes sont isomorphes).

**Définition 1.1.1.** *On appelle représentation linéaire de  $G$  dans  $V$  (ou représentation de  $G$ ), un morphisme de groupes de  $G$  dans  $GL(V)$ . Si  $\rho$  est une représentation de  $G$  dans  $V$ , la dimension de  $V$  sur  $k$  est appelée degré de  $\rho$  et se note  $\deg \rho$ . On dit aussi que  $\rho$  est une  $k$ -représentation de  $G$  ou une représentation de  $G$  sur  $k$ .*

**Définition 1.1.2.** *Soient  $\rho : G \rightarrow GL(V)$  et  $\rho' : G \rightarrow GL(V')$  deux représentations respectives de  $G$  dans  $V$  et de  $G$  dans  $V'$ . On dit que  $\rho$  et  $\rho'$  sont semblables ou isomorphes s'il existe un isomorphisme d'espaces vectoriels,  $\alpha$  de  $V$  sur  $V'$  tel que pour tout  $g \in G$ ,  $\alpha \rho(g) = \rho'(g) \alpha$  c'est-à-dire  $\rho'(g) = \alpha \rho(g) \alpha^{-1}$ .*

**Définition 1.1.3.** Soient  $\rho : G \rightarrow GL(V)$  une représentation de  $G$  dans  $V$  et  $W$  un sous-espace vectoriel de  $V$ . On dit que  $W$  est stable (ou invariant) par  $G$  si pour tout  $g \in G$ ,  $\rho(g)(W) = W$ . On dit que  $\rho$  est irréductible si  $V \neq 0$  et aucun sous-espace vectoriel propre de  $V$  n'est stable par  $G$ .

**Proposition 1.1.4.** On suppose que  $k$  est un corps algébriquement clos et que la caractéristique de  $k$  ne divise pas l'ordre de  $G$ . Alors :

- (1) le nombre de représentations irréductibles de  $G$  (à isomorphisme près) est égal au nombre de classes de conjugaison de  $G$  ([38, théorème 7, page 19] et [14, théorème 4.5, page 236]) ;
- (2) le degré d'une représentation irréductible de  $G$  divise  $(G : Z(G))$  et donc  $|G|$ , où  $Z(G)$  désigne le centre de  $G$  ([38, corollaire 2 et proposition 17, pages 52-53] et [14, théorème 4.6, page 237]) ;
- (3) si  $(n_i)_{1 \leq i \leq r}$  est la famille des degrés respectifs des représentations irréductibles de  $G$  (à isomorphisme près), deux à deux non isomorphes, alors  $\sum_{i=1}^r n_i^2 = |G|$  ([38, corollaire 2, page 18]). ■

Soient  $K$  un corps algébriquement clos contenant  $k$  et  $\rho : G \rightarrow GL(V)$  une représentation de  $G$  dans un  $k$ -espace vectoriel  $V$ . Soit  $V_K$  le  $K$ -espace vectoriel défini par  $V_K := K \otimes_k V$ .  $\rho$  permet de définir une représentation  $\rho_K$  de  $G$  dans  $V_K$  par :

$$\rho_K : G \rightarrow GL(V_K) : g \mapsto \rho_K(g) = id_K \otimes \rho(g).$$

**Définition 1.1.5.** Une représentation de  $G$  sur  $K$  est dite réalisable sur  $k$  (ou rationnelle sur  $k$ ) si elle est isomorphe à une représentation de la forme  $\rho_K$ , où  $\rho$  est une représentation de  $G$  sur  $k$ . Cela signifie qu'il est possible de la réaliser par des matrices à éléments dans  $k$ .

**Définition 1.1.6.** Soit  $\rho$  une représentation de  $G$  sur  $k$  et  $\chi : G \rightarrow k$  l'application qui est telle que pour tout  $g \in G$ ,  $\chi(g)$  est la trace de



$\rho(g)$ .  $\chi$  est appelée le caractère de  $\rho$  ; on dit simplement que  $\chi$  est un caractère de  $G$ . Le degré de  $\rho$  est aussi appelé le degré de  $\chi$  et se note  $\deg \chi$ . Si  $\rho$  est irréductible, on dit que  $\chi$  est un caractère irréductible de  $G$ .

Si  $\chi$  et  $\chi'$  sont deux caractères d'un groupe  $G$ , on pose

$$(\chi, \chi') = \frac{1}{|G|} \sum_{g \in G} \chi(g) \chi'(g^{-1}). \quad (1.1)$$

Quelques propriétés remarquables des caractères d'un groupe fini sont données dans la proposition suivante :

**Proposition 1.1.7.** *Soit  $\chi$  un caractère de  $G$  et  $(\chi_i)_{1 \leq i \leq r}$  la famille des caractères irréductibles de  $G$ . Alors*

- (1)  $\chi(1) = \deg \chi$  et pour tous  $g, h \in G$ ,  $\chi(hgh^{-1}) = \chi(g)$  ([17, (2.1), (2.2), pages 10-11]).
- (2) Deux  $k$ -représentations isomorphes de  $G$  ont même caractère ([17, (2.2), page 11]).
- (3) Pour tous  $i, j$ ,  $(\chi_i, \chi_j) = \delta_{ij}$ , où  $\delta_{ij}$  désigne le symbole de Kronecker ([17, (2.9), page 15]). ■

**Définition 1.1.8.** [17, page 3] Soit  $\rho : G \rightarrow GL(V)$  une représentation irréductible de  $G$  sur  $k$  de caractère  $\chi$ . On appelle représentation contragrédiente de  $\rho$  et on note  $\rho^\vee$ , la représentation irréductible  $\rho^\vee : G \rightarrow GL(V^*)$ , avec  $V^* = \text{Hom}_k(V, k)$ , définie par  $\rho^\vee(g) = (\rho(g^{-1}))^t$ , pour tout  $g \in G$  ; son caractère noté  $\chi^\vee$  est défini par  $\chi^\vee(g) = \chi(g^{-1})$ , pour tout  $g \in G$ .  $\chi^\vee$  est appelé le caractère contragrédient de  $\chi$ .

## 1.2 Algèbres et involutions

Tous les résultats de cette section sont tirés de [30]. Soient  $k$  un corps et  $A$  une algèbre sur  $k$  (supposée toujours unitaire). On note par  $A^\times$  le groupe des éléments inversibles de  $A$ . Si  $A \neq 0$ ,  $k$

s'identifie à la sous-algèbre  $k.1$  de  $A$ . On dit que  $A$  est une *algèbre à division* si  $A \neq 0$  et tout élément non nul de  $A$  est inversible. On appelle *centre de  $A$*  et on note  $Z(A)$  l'ensemble des éléments  $a$  de  $A$  tels que pour tout  $x \in A$ ,  $ax = xa$ ; c'est une sous-algèbre de  $A$ . Si  $Z(A) = k$ , on dit que  $A$  est une  *$k$ -algèbre centrale*. On dit que  $A$  est *simple* si  $A \neq 0$  et les seuls idéaux bilatères de  $A$  sont  $0$  et  $A$ . On dit que  $A$  est *semi-simple* si  $A$  est somme directe d'un nombre fini de sous-algèbres simples de  $A$  (qu'on appelle les *composantes simples* de  $A$ ).

Soit maintenant  $K$  une extension du corps  $k$ . On note par  $A_K$  la  $K$ -algèbre obtenue à partir de  $A$ , en étendant les scalaires à  $K$  et définie par

$$A_K := A \otimes_k K.$$

On appelle algèbre opposée de  $A$  et on note  $A^{op}$  la  $k$ -algèbre définie par

$$A^{op} = \{a^{op} | a \in A\},$$

où les opérations sont définies par : pour tous  $a, b \in A$ , pour tout  $\alpha \in k$ ,

$$a^{op} + b^{op} = (a + b)^{op}, \quad a^{op}.b^{op} = (ba)^{op}, \quad \alpha.a^{op} = (\alpha.a)^{op}.$$

Une caractérisation des algèbres simples centrales est donnée par le théorème de Wedderburn suivant :

**Théorème 1.2.1.** (Wedderburn) [30, théorème 1.1, page 3] *Soit  $A$  une algèbre sur un corps  $k$ . Les conditions suivantes sont équivalentes :*

- (1)  *$A$  est centrale simple.*
- (2) *L'application  $A \otimes_k A^{op} \rightarrow \text{End}_k(A)$  qui à  $a \otimes b^{op}$  associe l'application linéaire  $x \mapsto axb$ , est un isomorphisme d'algèbres.*
- (3) *Il existe une extension  $K$  du corps  $k$  telle que  $A_K$  soit isomorphe à l'algèbre  $M_n(K)$  des matrices carrées d'ordre  $n$ , à éléments dans  $K$ , pour un certain entier naturel non nul  $n$ .*

- (4) Si  $L$  est un corps algébriquement clos contenant  $k$ ,  $A_L$  est isomorphe à  $M_n(L)$ , pour un certain entier naturel non nul  $n$ .
- (5) Il existe une algèbre centrale à division  $D$  de dimension finie sur  $k$  et un entier naturel non nul  $r$  tel que  $A$  soit isomorphe à  $M_r(D)$ .

De plus, si ces conditions sont réalisées, tous les  $A$ -modules simples à gauche (à droite) sont isomorphes et l'algèbre à division  $D$  est déterminée de façon unique (à isomorphisme d'algèbres près) par  $D = \text{End}_A(M)$ , pour un certain  $A$ -module simple à gauche  $M$ . ■

Tout corps  $K$  vérifiant la condition (3) de ce théorème, est appelé *corps déployant de  $A$*  et on dit que  $A_K$  est une algèbre déployée sur  $K$ . De plus, l'entier  $n$  donné par la condition (3) est tel que  $\dim_k A = \dim_K A_K = n^2$  : il est appelé *le degré de  $A$*  et se note par  $\deg A$ . Dans la condition (5), le degré de l'algèbre à division  $D$  est appelé l'indice de  $A$  (ou l'indice de Schur de  $A$ ) et se note  $\text{ind} A$  et on a :

$$\dim_k M = (\deg A)(\text{ind} A).$$

Soit  $A$  une algèbre sur un corps  $k$ . Une *involution sur  $A$*  est une application  $\sigma : A \rightarrow A$  telle que pour tous  $a, b \in A$ ,  $\sigma(a + b) = \sigma(a) + \sigma(b)$ ,  $\sigma(ab) = \sigma(b)\sigma(a)$  et  $\sigma^2(a) = a$ . Supposons maintenant que  $A$  est une  $k$ -algèbre simple centrale. Soit  $\sigma$  une involution sur  $A$  et  $k^\sigma$  l'ensemble des éléments  $a$  de  $k$  tels que  $\sigma(a) = a$ .  $k^\sigma$  est un sous-corps de  $k$  et le degré de l'extension  $k/k^\sigma$  est inférieur ou égal à 2. Si  $[k : k^\sigma] = 1$ , on dit que  $\sigma$  est une *involution de première espèce* : dans ce cas  $\sigma$  est  $k$ -linéaire. Si  $[k : k^\sigma] = 2$ , on dit que  $\sigma$  est une *involution de deuxième espèce* ou une *involution unitaire*.

Soient  $A$  et  $A'$  des algèbres simples centrales sur un corps  $k$ ,  $\sigma$  et  $\sigma'$  des involutions respectivement sur  $A$  et  $A'$ . On dit que les algèbres à involution  $(A, \sigma)$  et  $(A', \sigma')$  sont *isomorphes* s'il existe un isomorphisme de  $k$ -algèbres  $f$  de  $A$  sur  $A'$  tel que  $f\sigma = \sigma'f$ .

Soit  $(A, \sigma)$  une  $k$ -algèbre simple centrale à involution, où  $\sigma$  est une involution de première espèce. Soit  $L \supset k$  un corps déployant de  $A$ . Alors  $A_L = A \otimes_k L \cong M_n(L)$ , où  $n = \deg A$ .  $\sigma$  se prolonge en l'involution de première espèce  $\sigma_L : A_L \rightarrow A_L$  telle que  $\sigma_L = \sigma \otimes id_L$ . Il existe un  $L$ -espace vectoriel  $V$  de dimension finie  $n$  tel que  $A_L \cong M_n(L) \cong \text{End}_L(V)$ . Soit  $b : V \times V \rightarrow L$  une forme bilinéaire non dégénérée sur  $V$ . L'application  $\widehat{b} : V \rightarrow V^* = \text{Hom}_L(V, L)$ , avec  $\widehat{b}(x)(y) = b(x, y)$ , pour tous  $x, y \in V$ , est un isomorphisme de  $L$ -espaces vectoriels. Soit  $\sigma_b : \text{End}_L(V) \rightarrow \text{End}_L(V)$  telle que  $\sigma_b(f) = \widehat{b}^{-1} f^t \widehat{b}$ , pour tout  $f \in \text{End}_L(V)$ .  $\sigma_b$  est une involution de première espèce sur  $\text{End}_L(V)$ , telle que pour tous  $x, y \in V$ , pour tout  $f \in \text{End}_L(V)$ ,

$$b(x, f(y)) = b(\sigma_b(f)(x), y).$$

$\sigma_b$  est appelée l'involution adjointe de  $b$  et se note  $ad_b$ . L'involution  $\sigma_L$  sur  $A_L$  s'identifie à l'involution  $\sigma_g$  définie sur  $M_n(L)$  par  $\sigma_g(m) = g^{-1}mg$ , pour tout  $m \in M_n(L)$ , où  $g$  désigne la matrice de Gram de  $b$ , dans la base qui sert à identifier  $\text{End}_L(V)$  à  $M_n(L)$  de telle sorte que  $g^t = g$  si  $b$  est symétrique et  $g^t = -g$  si  $b$  est antisymétrique.

**Proposition 1.2.2.** [30, proposition 2.1, page 14] *Soient  $(A, \sigma)$  une  $k$ -algèbre simple centrale de degré  $n$  avec involution de première espèce  $\sigma$ ,  $L$  un corps déployant de  $A$  et  $V$  un  $L$ -espace vectoriel de dimension finie  $n$ . Il existe une forme bilinéaire non dégénérée (symétrique ou antisymétrique)  $b$  sur  $V$  et une matrice inversible  $g \in GL_n(L)$  telle que  $g^t = g$  si  $b$  est symétrique et  $g^t = -g$  si  $b$  est antisymétrique, telles que les  $L$ -algèbres à involutions  $(A_L, \sigma_L)$ ,  $(\text{End}_L(V), \sigma_b)$  et  $(M_n(L), \sigma_g)$  sont isomorphes. ■*

**Définition 1.2.3.** *Avec les hypothèses et notations de la proposition 1.2.2, l'involution de première espèce  $\sigma$  sur  $A$  est dite symplectique (resp. orthogonale) si pour tout isomorphisme  $(A_L, \sigma_L) \cong (\text{End}_L(V), \sigma_b)$ , la forme bilinéaire  $b$  est alternée (resp. symétrique et non alternée).*

Soit  $(A, \sigma)$  une  $k$ -algèbre simple centrale avec involution de

première espèce  $\sigma$ . On pose :

$$\text{Sym}(A, \sigma) = \{a \in A \mid \sigma(a) = a\},$$

$$\text{Skew}(A, \sigma) = \{a \in A \mid \sigma(a) = -a\},$$

$$\text{Symd}(A, \sigma) = \{a + \sigma(a) \mid a \in A\},$$

$$\text{Alt}(A, \sigma) = \{a - \sigma(a) \mid a \in A\}.$$

Si  $\text{car } k \neq 2$ , alors  $\text{Sym}(A, \sigma) = \text{Symd}(A, \sigma)$ ,  $\text{Skew}(A, \sigma) = \text{Alt}(A, \sigma)$  et  $A = \text{Sym}(A, \sigma) \oplus \text{Skew}(A, \sigma)$ .

**Proposition 1.2.4.** [30, proposition 2.6, page 16] *Soient  $(A, \sigma)$  une  $k$ -algèbre simple centrale de degré  $n$  avec involution de première espèce  $\sigma$ .*

- (1) *On suppose que la caractéristique de  $k$  est différente de 2.*  
 – *Si  $\sigma$  est de type orthogonal, alors*

$$\dim_k \text{Sym}(A, \sigma) = \frac{n(n+1)}{2} \text{ et } \dim_k \text{Skew}(A, \sigma) = \frac{n(n-1)}{2}.$$

- *Si  $\sigma$  est de type symplectique, alors*

$$\dim_k \text{Sym}(A, \sigma) = \frac{n(n-1)}{2} \text{ et } \dim_k \text{Skew}(A, \sigma) = \frac{n(n+1)}{2}.$$

*De plus, dans ce cas,  $n$  est nécessairement pair.*

- (2) *Si  $\text{car } k = 2$ , alors  $\text{Sym}(A, \sigma) = \text{Skew}(A, \sigma)$  et  $\text{Symd}(A, \sigma) = \text{Alt}(A, \sigma)$  ; de plus,*

$$\dim_k \text{Sym}(A, \sigma) = \frac{n(n+1)}{2} \text{ et } \dim_k \text{Alt}(A, \sigma) = \frac{n(n-1)}{2}.$$

*L'involution  $\sigma$  est de type symplectique si et seulement si  $1 \in \text{Alt}(A, \sigma)$ . Dans ce cas,  $n$  est nécessairement pair. ■*

**Exemple 1.2.5.** *Pour tout corps  $k$ , pour tout entier naturel non nul  $n$ , l'algèbre  $M_n(k)$  des matrices carrées d'ordre  $n$  est une  $k$ -algèbre simple centrale de degré  $n$ . La transposition  $^t$  est une involution de première espèce de type orthogonal. Toute involution de première espèce  $\sigma$  sur  $M_n(k)$  est de la forme  $\sigma = \text{Int}(u) \circ ^t$ , pour une certaine matrice inversible  $u \in GL_n(k)$ , déterminée de façon unique à un facteur près dans  $k^\times$ , telle que  $u^t = \pm u$ , où  $\text{Int}(u)$  désigne l'automorphisme intérieur de  $M_n(k)$  définie par  $\text{Int}(u)(m) = umu^{-1}$ , pour tout  $m \in M_n(k)$ . De plus, l'involution  $\sigma$  est orthogonale si  $u^t = u$  et  $u \notin \text{Alt}(M_n(k), ^t)$  et elle est symplectique si  $u \in \text{Alt}(M_n(k), ^t)$  [30, proposition 2.19, page 24].*

**Exemple 1.2.6.** *Soient  $k$  un corps et  $a, b \in k^\times$ .*

*Si  $\text{car } k \neq 2$ , on note  $Q = (a, b)_k$  la  $k$ -algèbre des quaternions ayant pour base  $\{1, i, j, ij\}$  telle que  $i^2 = a$ ,  $j^2 = b$  et  $ij = -ji$ ; c'est une  $k$ -algèbre simple centrale de degré 2. La conjugaison  $-$  définie sur  $Q$  par*

$$\overline{\alpha + \beta i + \gamma j + \delta ij} = \alpha - \beta i - \gamma j - \delta ij,$$

*pour tous  $\alpha, \beta, \gamma, \delta \in F$ , est une involution symplectique (appelée involution canonique sur  $Q$ ).*

*Si  $\text{car } k = 2$ , on note  $Q = [a, b]_k$  la  $k$ -algèbre des quaternions ayant pour base  $\{1, i, j, ij\}$  telle que  $i^2 + i = a$ ,  $j^2 = b$  et  $ij = ji + j$ ; c'est une  $k$ -algèbre simple centrale de degré 2. La conjugaison  $-$  définie sur  $Q$  par*

$$\overline{\alpha + \beta i + \gamma j + \delta ij} = \alpha + \beta(i + 1) + \gamma j + \delta ij,$$

*pour tous  $\alpha, \beta, \gamma, \delta \in k$ , est une involution symplectique (appelée involution canonique sur  $Q$ ).*

*Quelle que soit la caractéristique du corps  $k$ , l'involution canonique sur la  $k$ -algèbre des quaternions  $Q$  est l'unique involution symplectique sur  $Q$ . De plus, toute involution orthogonale  $\sigma$  sur  $Q$  est de la forme  $\sigma = \text{Int}(u) \circ ^-$ , où  $u$  est un quaternion inversible de  $\text{Skew}(Q, ^-) = k$  déterminé de façon unique par  $\sigma$  à un facteur de  $k^\times$  près [30, proposition 2.21, page 26].*

**Exemple 1.2.7.** [30, page 26] Soit  $k$  un corps. L'application  $J$  définie sur l'algèbre  $M_2(k)$  des matrices carrées d'ordre 2 par

$$J\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix},$$

est une involution de première espèce de type symplectique.

Soit  $k$  un corps. D'après [39, corollaire 2.4, page 287],

$$M_r(M_2(k)) \cong M_{2r}(k).$$

On a le résultat suivant :

**Proposition 1.2.8.** Soit  $\tau$  l'application définie sur  $M_{2r}(k)$  telle que pour tout  $\alpha \in M_{2r}(k)$ , si  $\alpha = (\alpha_{ij})_{1 \leq i, j \leq r}$ , avec  $\alpha_{ij} \in M_2(k)$ ,

$$\tau(\alpha) = (J(\alpha_{ij}))_{1 \leq i, j \leq r}^t,$$

$J$  étant l'involution définie dans l'exemple 1.2.7 et  $^t$ , la transposition matricielle.  $\tau$  est une involution de première espèce de type symplectique.

*Preuve :*  $M_{2r}(k)$  est une  $k$ -algèbre simple centrale de degré  $2r$ . On vérifie aisément que  $\tau$  est une involution de première espèce (en utilisant le fait que  $J$  et  $^t$  sont des involutions de première espèce).

Si  $\text{car } k \neq 2$ , soit  $\alpha \in \text{Sym}(M_{2r}(k), \tau)$  tel que  $\alpha = (\alpha_{ij})_{1 \leq i, j \leq r}$ , avec  $\alpha_{ij} = \begin{pmatrix} a_{ij} & b_{ij} \\ c_{ij} & d_{ij} \end{pmatrix} \in M_2(k)$ . Alors  $\tau(\alpha) = \alpha$ . Donc pour tout  $i, j$ ,  $J(\alpha_{ij}) = \alpha_{ji}$ , c'est-à-dire

$$\begin{pmatrix} d_{ij} & -b_{ij} \\ -c_{ij} & a_{ij} \end{pmatrix} = \begin{pmatrix} a_{ji} & b_{ji} \\ c_{ji} & d_{ji} \end{pmatrix}.$$

Pour  $i = j$ ,  $d_{ii} = a_{ii}$  et  $b_{ii} = c_{ii} = 0$  et donc

$$\alpha = \begin{pmatrix} a_{11} & 0 & a_{12} & b_{12} & \cdots & \cdots & a_{1r} & b_{1r} \\ 0 & a_{11} & c_{12} & d_{12} & \cdots & \cdots & c_{1r} & d_{1r} \\ d_{12} & -b_{12} & a_{22} & 0 & \cdots & \cdots & a_{2r} & b_{2r} \\ -c_{12} & a_{12} & 0 & a_{22} & \cdots & \cdots & c_{2r} & d_{2r} \\ \vdots & \vdots & \vdots & \vdots & \ddots & & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & & \ddots & \vdots & \vdots \\ d_{1r} & -b_{1r} & d_{2r} & -b_{2r} & \cdots & \cdots & a_{rr} & 0 \\ -c_{1r} & a_{1r} & -c_{2r} & a_{2r} & \cdots & \cdots & 0 & a_{rr} \end{pmatrix}.$$

Il en résulte que

$$\dim_k \text{Sym}(M_{2r}(k), \tau) = r + 4\left(\frac{r^2 - r}{2}\right) = 2r^2 - r = \frac{2r(2r - 1)}{2}.$$

De façon analogue, on vérifie que

$$\dim_k \text{Skew}(M_{2r}(k), \tau) = \frac{2r(2r + 1)}{2}.$$

D'où d'après la proposition 1.2.4,  $\tau$  est une involution symplectique.

Si  $\text{cark} = 2$ , soit  $(U_{ij})_{1 \leq i, j \leq 2}$  la base canonique de  $M_2(k)$ .  $U_{ij}$  est la matrice  $2 \times 2$  dont toutes les entrées sont nulles sauf celle située en  $(i, j)$  qui est égale à 1. Dans  $M_{2r}(k)$ , pour

$$\alpha = \begin{pmatrix} U_{11} & 0 & \cdots & 0 \\ 0 & U_{11} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & U_{11} \end{pmatrix},$$

on a :

$$\tau(\alpha) = \begin{pmatrix} U_{22} & 0 & \cdots & 0 \\ 0 & U_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & U_{22} \end{pmatrix},$$

et donc  $\alpha + \tau(\alpha) = I_{2r}$ ; par suite  $I_{2r} \in \text{Alt}(M_{2r}(k), \tau)$  et d'après la proposition 1.2.4,  $\tau$  est de type symplectique. ■



## 1.3 Algèbre de groupe

Soient  $G$  un groupe fini et  $k$  un corps dont la caractéristique ne divise pas l'ordre de  $G$ . Notons par  $kG$  l'algèbre du groupe  $G$  sur  $k$  ; cette algèbre possède une base qu'on peut identifier à  $G$ . Chaque élément  $x$  de  $kG$  s'écrit de façon unique sous la forme

$$x = \sum_{g \in G} \alpha_g g,$$

avec  $\alpha_g \in k$ , et la multiplication dans  $kG$  est un prolongement de celle du groupe  $G$ . D'après le théorème de Maschke ([34, théorème 4.2, page 55]),  $kG$  est une  $k$ -algèbre semi-simple. Soit  $\sigma : kG \rightarrow kG$  telle que pour tout  $x \in kG$ , avec  $x = \sum_{g \in G} \alpha_g g$  et  $\alpha_g \in k$ ,

$$\sigma(x) = \sum_{g \in G} \alpha_g g^{-1}.$$

$\sigma$  est une involution sur  $kG$ , appelée involution canonique sur  $kG$ . De plus,  $\sigma$  est  $k$ -linéaire.

**Proposition 1.3.1.** [33, proposition 1.4.1, page 9] *Si  $k$  est un corps algébriquement clos de caractéristique 0, alors le nombre de composantes simples de  $kG$  égale le nombre de  $k$ -représentations irréductibles de  $G$ .*

**Définition 1.3.2.** [14, page 252] *Un groupe  $G$  est dit ambivalent si pour tout  $x \in G$ ,  $x$  et  $x^{-1}$  sont conjugués c'est-à-dire il existe  $y \in G$  tel que  $x^{-1} = yxy^{-1}$ .*

Soit  $\bar{k}$  une clôture algébrique de  $k$ . Soit  $\rho : G \rightarrow GL(V)$  une  $\bar{k}$ -représentation irréductible de  $G$  dans un  $\bar{k}$ -espace vectoriel  $V$  de dimension finie  $n$ . Une forme bilinéaire  $b : V \times V \rightarrow \bar{k}$  est dite  $G$ -invariante si pour tous  $x, y \in V$ , pour tout  $g \in G$ ,

$$b(\rho(g)(x), \rho(g)(y)) = b(x, y).$$

La proposition suivante donne des conditions nécessaires et suffisantes pour que la restriction de l'involution canonique à chaque composante simple de  $kG$  soit une involution de première espèce.

**Proposition 1.3.3.** [9, théorème 3, page 14] *Soient  $k$  un corps dont la caractéristique ne divise pas l'ordre de  $G$  et  $\sigma$  l'involution canonique de  $kG$ . Les conditions suivantes sont équivalentes :*

- (1) *Pour toute représentation irréductible  $\rho : G \rightarrow GL(V)$  de  $G$  sur  $\bar{k}$ , il existe une forme bilinéaire non nulle  $b : V \times V \rightarrow \bar{k}$  qui est  $G$ -invariante*
- (2)  *$G$  est un groupe ambivalent.*
- (3) *La restriction de  $\sigma$  à chaque composante simple  $A$  de  $kG$ , est une involution de première espèce.*

**Remarque 1.3.4.** *Si les conditions de la proposition 1.3.3 sont réalisées, la forme bilinéaire  $b$  est non dégénérée et si  $\text{car } k \neq 2$ ,  $b$  est symétrique ou antisymétrique [9, proposition 10, page 12]. De plus, avec les notations de la proposition 1.2.2, on a :*

*pour toute composante simple  $A$  de  $kG$ , de degré  $n$ , il existe une  $\bar{k}$ -représentation irréductible  $\rho : G \rightarrow GL(V)$  de  $G$  de degré  $n$  et une forme bilinéaire non dégénérée  $b : V \times V \rightarrow \bar{k}$  qui est  $G$ -invariante, telle que les algèbres à involutions*

$$(A_{\bar{k}}, \alpha_{\bar{k}}), (End_{\bar{k}}(V), \sigma_b) \text{ et } (M_n(\bar{k}), \sigma_g)$$

*sont isomorphes, où  $\alpha$  est la restriction de  $\sigma$  à  $A$ ,  $A_{\bar{k}} = A \otimes_{Z(A)} \bar{k}$  et  $\alpha_{\bar{k}} = \alpha \otimes id_{\bar{k}}$ . Par suite, la restriction de  $\sigma$  à  $A$  est orthogonale (resp. symplectique) si et seulement si  $b$  est symétrique (resp. antisymétrique) si et seulement si  $\sigma_b$  et  $\sigma_g$  sont orthogonales (resp. symplectiques). Il est aussi à noter que  $A_{\bar{k}} \cong End_{\bar{k}}(V) \cong M_n(\bar{k})$  est isomorphe à une composante simple de  $\bar{k}G$  [38, corollaire de proposition 9, page 48] et  $A \cong A \otimes_k k \subset A_{\bar{k}}$ .*

**Définition 1.3.5.** *Soit  $R$  une algèbre semi-simple sur un corps  $k$ . Un élément  $x$  de  $R$  est dit idempotent si  $x^2 = x$  ; il est dit central s'il appartient à  $Z(R)$ . Deux éléments centraux idempotents sont dits orthogonaux si leur produit est nul. Un élément idempotent central non nul de  $R$  est dit centralement primitif s'il ne peut pas s'écrire comme somme de deux éléments idempotents orthogonaux centraux non nuls de  $R$ . Donc si  $e$  est un élément idempotent centralement*

*primitif de  $R$ , alors pour tout idempotent central  $f$  de  $R$ ,  $ef = 0$  ou  $ef = e$ . De plus, pour tout élément idempotent  $e$  de  $R$ ,  $e$  est centralement primitif si et seulement si  $eR$  est une composante simple de  $R$  ([32, page 336] et [16, page 55]).*

**Remarque 1.3.6.** *Soit  $G$  un groupe et  $k$  un corps dont la caractéristique ne divise pas l'ordre de  $G$ . Pour toute composante simple  $A$  de  $\bar{k}G$ , de degré  $n$ , il existe une  $\bar{k}$ -représentation irréductible  $\rho : G \rightarrow GL(V)$  de  $G$ , de degré  $n$ , de caractère  $\chi$  tel que  $A$  soit l'idéal de  $\bar{k}G$  engendré par  $e$  c'est-à-dire  $A = e\bar{k}G$ ,  $e$  étant l'élément idempotent centralement primitif de  $\bar{k}G$ , donné par :*

$$e = \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(g^{-1})g.$$

*Le degré de  $\chi$  est aussi appelé le degré de  $e$  et se note  $\text{dege}$ .*



# Chapitre 2

## Involution canonique

Soit  $G$  un groupe fini,  $k$  un corps dont la caractéristique ne divise pas l'ordre de  $G$  et  $\sigma$  l'involution canonique de  $kG$ . La  $k$ -algèbre  $kG$  étant semi-simple, elle se décompose de façon unique sous la forme

$$kG = A_1 \times A_2 \times \cdots \times A_m, \quad (2.1)$$

comme somme directe de ses composantes simples  $A_i$ , avec  $1 \leq i \leq m$ . D'où, pour tout  $i = 1, 2, \dots, m$ ,  $\sigma(A_i) = A_j$ , pour un certain  $j$  et  $A_i$  est une algèbre simple centrale sur  $Z(A_i)$ . Si  $\sigma(A_i) = A_j$ , avec  $i \neq j$ , il est possible de considérer la restriction de  $\sigma$  à  $A_i \times \sigma(A_i) = A_i \times A_j$  : cette restriction ne présente pas d'intérêt particulier. Si  $\sigma(A_i) = A_i$ , la restriction de  $\sigma$  à  $A_i$  est une involution de première espèce (de type orthogonal ou symplectique) ou une involution de deuxième espèce. De plus, il existe des éléments idempotents centralement primitifs orthogonaux uniques  $e_1, e_2, \dots, e_m$  de  $kG$  tels que  $A_i = e_i kG$ , pour tout  $i$  et  $1 = e_1 + e_2 + \cdots + e_m$ .

Si  $\bar{k}$  est une clôture algébrique de  $k$ , il y a correspondance biunivoque entre l'ensemble des composantes simples de  $\bar{k}G$ , l'ensemble des idempotents centralement primitifs de  $\bar{k}G$  et l'ensemble des  $\bar{k}$ -caractères irréductibles de  $G$ , de telle sorte qu'à tout  $\bar{k}$ -caractère irréductible  $\chi$  de  $G$  correspond l'élément idempotent centralement

primitif  $e$  défini par

$$e = \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(g^{-1})g$$

et à  $e$  correspond la composante simple  $A = e\bar{k}G$  de  $\bar{k}G$ .

De plus, pour tout élément idempotent centralement primitif  $f$  de  $kG$ , il existe des éléments idempotents centralement primitifs  $f_1, f_2, \dots, f_s$  de  $\bar{k}G$  tels que  $f = f_1 + f_2 + \dots + f_s$  (conséquence directe de [32, proposition (2.2.1), page 336]).

Dans ce chapitre, nous donnons les conditions pour que la restriction de l'involution canonique à une composante simple de  $\mathbb{C}G$  soit une involution orthogonale ou symplectique, en utilisant l'indicateur de Schur-Frobenius. Nous établissons des résultats qui permettent de trouver le type de la restriction de l'involution canonique à chaque composante simple de  $kG$  lorsque nous connaissons le type de la restriction de l'involution canonique à chaque composante simple de  $\mathbb{C}G$ , que ce soit par changement de caractéristique ou par extension des scalaires. Nous présentons enfin, quelques résultats déductibles de ceux existant dans la littérature.

## 2.1 Cas d'un corps algébriquement clos.

Soit  $G$  un groupe fini,  $k$  un corps algébriquement clos dont la caractéristique ne divise pas l'ordre de  $G$  et  $\sigma$  l'involution canonique de  $kG$ . Supposons que  $kG$  s'écrit comme somme directe de ses composantes simples sous la forme donnée par (2.1). Pour tout  $i$ , soit  $\rho_i : G \rightarrow GL(V_i)$  la  $k$ -représentation irréductible (à isomorphisme près) de  $G$  correspondant à  $A_i$  et  $\chi_i$  son caractère ; soit  $e_i$  l'élément idempotent centralement primitif de  $kG$  correspondant à  $A_i$ . On rappelle que

$$e_i = \frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i(g^{-1})g \quad \text{et} \quad A_i = e_i kG.$$

$k$  étant algébriquement clos, toutes les composantes simples de  $kG$  sont déployées sur  $k$  et alors la restriction de  $\sigma$  à chaque composante simple (fixée par  $\sigma$ ) est une involution de première espèce. Plus précisément, pour tout  $i$ ,  $A_i$  est isomorphe à la  $k$ -algèbre simple centrale  $\text{End}_k(V_i)$  des  $k$ -endomorphismes du  $k$ -espace vectoriel  $V_i$ . On a :

**Lemme 2.1.1.** *Avec les hypothèses ci-dessus, pour tout  $i$ ,  $\sigma(e_i)$  correspond à la  $k$ -représentation contragrédiente  $\rho_i^\vee$ .*

**Preuve :** Par hypothèse,  $e_i = \frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i(g^{-1})g$ . Donc

$$\begin{aligned} \sigma(e_i) &= \frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i(g^{-1})g^{-1} \\ &= \frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i^\vee(g)g^{-1} \\ &= \frac{\chi_i^\vee(1)}{|G|} \sum_{g \in G} \chi_i^\vee(g^{-1})g, \end{aligned}$$

l'application  $G \rightarrow G : g \mapsto g^{-1}$  étant bijective. Donc  $\sigma(e_i)$  correspond au caractère  $\chi_i^\vee$  et donc à la représentation  $\rho_i^\vee$ . ■

**Proposition 2.1.2.** *Avec les hypothèses ci-dessus, pour tous  $i, j$ , les conditions suivantes sont équivalentes :*

- (1)  $\sigma(A_i) = A_j$
- (2)  $\sigma(e_i) = e_j$
- (3)  $\rho_i^\vee$  est isomorphe à  $\rho_j$
- (4)  $\chi_i^\vee = \chi_j$

**Preuve :**

(1)  $\Rightarrow$  (2), en effet supposons que  $\sigma(A_i) = A_j$ ; alors  $\sigma(e_i) \in A_j$ . Donc  $e_j \sigma(e_i) = \sigma(e_i)$  (car  $A_j = e_j kG$ ). Par suite,  $e_i \sigma(e_j) = \sigma(e_j \sigma(e_i)) = e_i$  et comme  $\sigma(e_j) \in A_i$ , alors  $e_i \sigma(e_j) = \sigma(e_j)$ . Il en résulte que  $\sigma(e_j) = e_i$  et donc  $\sigma(e_i) = e_j$ .

(2)  $\Rightarrow$  (3) : cela découle du lemme 2.1.1.

(3)  $\Rightarrow$  (4) : c'est évident car deux représentations isomorphes ont même caractère.

(4)  $\Rightarrow$  (1), en effet, si  $\chi_i^\vee = \chi_j$ , d'après le lemme 2.1.1,  $\sigma(e_i) = e_j$ . Par suite,

$$\sigma(A_i) = \sigma(e_i kG) = \sigma(e_i)kG = e_j kG = A_j. \blacksquare$$

On en déduit alors que :

**Corollaire 2.1.3.** *Pour tout  $i$ , on a :*

$$\sigma(A_i) = A_i \Leftrightarrow \sigma(e_i) = e_i \Leftrightarrow \rho_i^\vee \text{ est isomorphe à } \rho_i \Leftrightarrow \chi_i^\vee = \chi_i \blacksquare$$

Dans la suite de cette section, nous allons nous intéresser au cas où  $k$  est isomorphe au corps  $\mathbb{C}$  des nombres complexes.

Soit  $\mathbb{R}$  un corps réel clos. Notons par  $\mathbb{H}$  la  $\mathbb{R}$ -algèbre à division des quaternions de Hamilton  $(-1, -1)_{\mathbb{R}}$  et par  $\mathbb{C}$  la clôture algébrique  $\mathbb{R}(\sqrt{-1})$  de  $\mathbb{R}$ . Soient  $G$  un groupe fini,  $\sigma$  l'involution canonique de  $\mathbb{R}G$  et  $A$  une composante simple de  $\mathbb{R}G$ . D'après Scharlau [39, théorème 13.3, page 323],  $\sigma(A) = A$  et

$$(A, \sigma) \cong (M_r(D), {}^{-t}), \tag{2.2}$$

pour un entier naturel non nul  $r$ , où  $D = \mathbb{R}, \mathbb{C}$  ou  $\mathbb{H}$ ,  $t$  est la transposition matricielle et  $^{-}$  l'identité sur  $\mathbb{R}$ , la conjugaison complexe sur  $\mathbb{C}$  ou l'involution canonique sur  $\mathbb{H}$ . On a le résultat suivant, qui est bien énoncé par Scharlau [39, remarque 13.4, page 324] :

**Proposition 2.1.4.** *La restriction de  $\sigma$  à  $A$  est une involution orthogonale, symplectique ou unitaire si  $D = \mathbb{R}, \mathbb{H}$  ou  $\mathbb{C}$  respectivement.*

**Preuve :** Soit  $V$  un  $\mathbb{R}G$ -module irréductible correspondant à  $A$ . Comme  $(A, \sigma) \cong (M_r(D), {}^{-t})$ , alors  $A$  est isomorphe à  $\text{End}_D(V)$



et donc  $\dim_D V = r$ . Soit  $\Omega = (\omega_i)_{1 \leq i \leq r}$  une base de  $V$  sur  $D$ . Soit  $b : V \times V \rightarrow D$  l'application définie par

$$b(x, y) = \sum_i \overline{x_i} y_i$$

pour tous éléments  $x$  et  $y$  de  $V$  tels que  $x = \sum_i \omega_i x_i$  et  $y = \sum_i \omega_i y_i$ , avec  $x_i, y_i \in D$ .

$b$  est une forme hermitienne définie positive, en effet, pour tous  $x, y, x', y' \in V$  tels que  $x = \sum_i \omega_i x_i$ ,  $y = \sum_i \omega_i y_i$ ,  $x' = \sum_i \omega_i x'_i$  et  $y' = \sum_i \omega_i y'_i$ , pour tous  $\alpha, \beta \in D$ , on a :

$$b(x+x', y) = \sum_i (\overline{x_i + x'_i}) y_i = \sum_i \overline{x_i} y_i + \sum_i \overline{x'_i} y_i = b(x, y) + b(x', y),$$

$$b(x, y+y') = \sum_i \overline{x_i} (y_i + y'_i) = \sum_i \overline{x_i} y_i + \sum_i \overline{x_i} y'_i = b(x, y) + b(x, y'),$$

$$b(x\alpha, y\beta) = \sum_i \overline{x_i \alpha} y_i \beta = \sum_i \overline{\alpha} \overline{x_i} y_i \beta = \overline{\alpha} (\sum_i \overline{x_i} y_i) \beta = \overline{\alpha} b(x, y) \beta,$$

$$b(x, y) = \sum_i \overline{x_i} y_i = \sum_i \overline{y_i x_i} = \overline{\sum_i y_i x_i} = \overline{b(y, x)}$$

et

$$b(x, x) = \sum_i \overline{x_i} x_i > 0 \text{ (pour } x \neq 0 \text{)}.$$

Soit  $B : V \times V \rightarrow D$  l'application définie par

$$B(x, y) = \sum_{g \in G} b(gx, gy).$$

$B$  est une forme hermitienne définie positive (et donc non dégénérée) car  $b$  l'est. De plus, pour tout  $g \in G$ , pour tous  $x, y \in V$ , on a :

$$B(gx, gy) = \sum_h b(hgx, hgy) = \sum_h b(hx, hy) = B(x, y)$$

et donc  $B$  est  $G$ -invariante.

- Si  $D = \mathbb{R}$ , alors  $B$  est une forme bilinéaire symétrique (car  $-$  désigne l'identité sur  $\mathbb{R}$ ). Donc la restriction de  $\sigma$  à  $A$  est orthogonale.
- Si  $D = \mathbb{H}$ , la conjugaison étant symplectique sur  $\mathbb{H}$ , il en est de même de l'involution adjointe à  $B$  (d'après [30, théorème 4.2, page 43]). D'où la restriction de  $\sigma$  à  $A$  est symplectique.
- Si  $D = \mathbb{C}$ , la conjugaison étant une involution de seconde espèce sur la  $\mathbb{R}$ -algèbre  $\mathbb{C}$ , il en est de même de l'involution adjointe à  $B$  (d'après [30, théorème 4.2, page 43]). Donc la restriction de  $\sigma$  à  $A$  est unitaire. ■

**Définition 2.1.5.** Soient  $G$  un groupe fini et  $k$  un corps dont la caractéristique ne divise pas l'ordre de  $G$ . On dit que  $G$  est ortho-ambivalent par rapport à  $k$  si la restriction de l'involution canonique à chaque composante simple de  $kG$  est une involution de première espèce de type orthogonal. Un tel groupe est évidemment ambivalent (en vertu de la proposition 1.3.3).

**Corollaire 2.1.6.** Soit  $G$  un groupe fini. Si toutes les composantes simples de  $\mathbb{R}G$  sont déployées sur  $\mathbb{R}$ , alors  $G$  est ortho-ambivalent par rapport à  $\mathbb{R}$ .

**Preuve :** C'est une conséquence directe de la proposition 2.1.4. ■

Avant de continuer, rappelons quelques résultats sur les groupes diédraux, quaternioniques et symétriques.

**Définition 2.1.7.** Soit  $n$  un entier naturel non nul. On appelle groupe diédral d'ordre  $2n$  et on note  $D_n$ , un groupe engendré par deux éléments  $a$  et  $b$  d'ordres respectifs  $n$  et  $2$  et tels que  $bab^{-1} = a^{-1}$ . On appelle groupe quaternionique d'ordre  $4n$  et on note  $Q_n$ , un groupe engendré par deux éléments  $a$  et  $b$  tels que  $a$  soit d'ordre  $2n$ ,  $b^2 = a^n$  et  $bab^{-1} = a^{-1}$ . On appelle groupe symétrique d'ordre  $n!$  et on note  $S_n$ , le groupe des permutations d'un ensemble à  $n$  éléments.

**Proposition 2.1.8.** [33, proposition 1.1.9, page 2] *Avec les notations de la définition 2.1.7,  $S_n$  et  $D_n$  sont des groupes ambivalents et pour que  $Q_n$  soit ambivalent, il faut et il suffit que  $n$  soit pair.*

*Preuve :*  $S_n$  est ambivalent d'après [27, 1.2.8, page 11].

- Supposons que  $D_n$  est le groupe d'ordre  $2n$  engendré par deux éléments  $a$  et  $b$  d'ordres respectifs  $n$  et  $2$  et tels que  $bab^{-1} = a^{-1}$ . Alors

$$D_n = \{a^r, a^r b \mid 0 \leq r \leq n-1\}.$$

Pour tout entier  $r$  tel que  $0 \leq r \leq n-1$ , on a :  $ba^r b^{-1} = a^{-r}$  et  $(a^r b)^2 = a^r b a^r b^{-1} = 1$ , donc  $(a^r b)^{-1} = a^r b$ ; il en résulte que  $D_n$  est ambivalent.

- Soit  $Q_n$  le groupe d'ordre  $4n$  engendré par deux éléments  $a$  et  $b$  tels que  $a$  soit d'ordre  $2n$ ,  $b^2 = a^n$  et  $bab^{-1} = a^{-1}$ . Alors

$$Q_n = \{a^r, a^r b \mid 0 \leq r \leq 2n-1\}.$$

Pour tout entier  $r$  tel que  $0 \leq r \leq 2n-1$ , on a :  $ba^r b^{-1} = a^{-r}$  et

a) si  $n = 2p$  pour un entier naturel non nul  $p$ , alors  $a^p b a^{-p} = a^p b^2 a^p b^{-1} = b^{-1}$  et donc  $a^p a^r b a^{-p} = a^r a^p b a^{-p} = a^r b^{-1} = b^{-1} a^{-r} = (a^r b)^{-1}$ .

b) Si  $n = 2p+1$  pour un entier naturel  $p$ , alors  $b^{-1} = a^n b = a^{2p+1} b$  et donc

$$a^r b a^{-r} = a^r b^2 a^r b^{-1} = a^{2r} a^n b^{-1} = a^{2r} b \neq a^{2p+1} b = b^{-1}$$

et

$$a^r b b (a^r b)^{-1} = a^r b a^{-r} \neq b^{-1};$$

d'où  $b$  et  $b^{-1}$  ne sont pas conjugués.

On en déduit que  $Q_n$  est ambivalent si  $n$  est pair et non ambivalent si  $n$  est impair. ■

Le corollaire 2.1.6 nous permet de retrouver le résultat suivant, donné dans [33, proposition 3.3.7, page 49] pour un sous-corps quelconque de  $\mathbb{C}$  :

**Corollaire 2.1.9.** *Soit  $S_n$  le groupe symétrique, avec  $n \in \mathbb{N}_0$ .  $S_n$  est ortho-ambivalent par rapport à  $\mathbb{R}$ .*

**Preuve :** D'après Jacobson [26, théorème 5.9, page 268], toutes les composantes simples de  $\mathbb{R}S_n$  sont déployées sur  $\mathbb{R}$ ; le résultat découle alors du corollaire 2.1.6. ■

**Définition 2.1.10.** [17, (3.5), page 21] *Soient  $G$  un groupe fini et  $\chi$  un caractère irréductible de  $G$ . On appelle indicateur de Schur-Frobenius de  $\chi$  et on note  $\nu(\chi)$ , le nombre*

$$\nu(\chi) = \frac{1}{|G|} \sum_{g \in G} \chi(g^2).$$

**Définition 2.1.11.** [17, page 20] *Soient  $G$  un groupe fini et  $\rho : G \rightarrow GL(V)$  une  $\mathbb{C}$ -représentation irréductible de  $G$ , de caractère  $\chi$ . Soit  $A$  la composante simple de  $\mathbb{R}G$  correspondant à  $\rho$ .*

- *On dit que  $\rho$  est de première espèce si  $\rho$  est réalisable sur  $\mathbb{R}$ ; d'après [38, page 108], c'est équivalent de dire que  $A$  est isomorphe à  $M_r(\mathbb{R})$ , pour un certain entier naturel  $r$ .*
- *On dit que  $\rho$  est de deuxième espèce si  $\rho$  est isomorphe à la représentation conjuguée  $\bar{\rho}$  sans être réalisable sur  $\mathbb{R}$ ; d'après [38, page 108], c'est équivalent de dire que  $A$  est isomorphe à  $M_r(\mathbb{H})$ , avec  $\mathbb{H} = (-1, -1)_{\mathbb{R}}$ , pour un certain entier naturel  $r$ . Rappelons que si  $\deg \rho = n$  et  $\rho : G \rightarrow GL_n(\mathbb{C})$ , la représentation conjuguée  $\bar{\rho}$  est définie par*

$$\bar{\rho}(g) = \overline{\rho(g)} \quad \text{pour } g \in G,$$

- *étant la conjugaison matricielle.*
- *On dit que  $\rho$  est de troisième espèce si  $\rho$  n'est pas isomorphe à la représentation conjuguée  $\bar{\rho}$  c'est-à-dire il existe  $g \in G$  tel que  $\chi(g)$  n'est pas réel; d'après [38, page 108], c'est équivalent de dire que  $A$  est isomorphe à  $M_r(\mathbb{C})$ , pour un certain entier naturel  $r$ .*

**Remarque 2.1.12.** Les  $\mathbb{C}$ -représentations de première, deuxième et troisième espèces sont celles que Serre appelle dans [38, page 108] représentations respectivement de deuxième, troisième et premier type.

**Proposition 2.1.13.** Soient  $G$  un groupe fini,  $\chi$  un caractère irréductible de  $G$ . On a :

- (1)  $\nu(\chi) = 1 \iff \chi$  est de première espèce ;
- (2)  $\nu(\chi) = -1 \iff \chi$  est de deuxième espèce ;
- (3)  $\nu(\chi) = 0 \iff \chi$  est de troisième espèce.

*Preuve :* voir [38, proposition 39, page 109] ou [17, (3.5), page 21].

**Proposition 2.1.14.** Soient  $G$  un groupe fini,  $\sigma$  l'involution canonique de  $\mathbb{R}G$ ,  $A$  une composante simple de  $\mathbb{R}G$  et  $\chi$  le caractère irréductible de  $G$  correspondant à  $A$ . Pour que la restriction de  $\sigma$  à  $A$  soit orthogonale, symplectique ou unitaire, il faut et il suffit que l'indicateur de Schur-Frobenius  $\nu(\chi)$  de  $\chi$  soit respectivement égal à 1, -1 ou 0.

*Preuve :* Cela découle de la définition 2.1.11 et des propositions 2.1.4 et 2.1.13. ■

**Remarque 2.1.15.** Dans toute la suite, si  $\chi$  est un caractère irréductible d'un groupe fini  $G$ , on dira que  $\chi$  est de type 1, 0, ou -1 lorsque l'indicateur de Schur-Frobenius  $\nu(\chi)$  de  $\chi$  est égal à 1, 0, ou -1 respectivement. C'est cette définition qui est utilisée par R. Quinlan dans [35, page 194].

**Proposition 2.1.16.** [17, (3.6), page 22] Soient  $G$  un groupe fini et  $x \in G$ . Notons par  $t(x)$  ou  $t_G(x)$  le nombre d'éléments  $g$  de  $G$  tels que  $g^2 = x$ . Soit  $\text{Irr}(G)$  l'ensemble des caractères irréductibles de  $G$ . On a :

$$t(x) = \sum_{\chi \in \text{Irr}(G)} \nu(\chi) \chi(x). \quad \blacksquare$$

**Proposition 2.1.17.** *Soit  $G$  un groupe fini. Les assertions suivantes sont équivalentes :*

- (1)  $G$  est ortho-ambivalent par rapport à  $\mathbb{R}$ .
- (2)  $G$  est ambivalent et pour tout caractère irréductible  $\chi$  de  $G$ ,  $\nu(\chi) = 1$ .
- (3)  $G$  est ambivalent et  $t(1) = \sum_{\chi \in \text{Irr}(G)} \chi(1)$ .

*Preuve :* Soit  $\sigma$  l'involution canonique de  $\mathbb{R}G$ .

Si (1) est vérifiée, pour toute composante simple  $A$  de  $\mathbb{R}G$ , la restriction de  $\sigma$  à  $A$  est orthogonale ; d'après la définition 2.1.5,  $G$  est ambivalent et d'après la proposition 2.1.14, pour tout caractère irréductible  $\chi$  de  $G$ ,  $\nu(\chi) = 1$ . Donc (1)  $\Rightarrow$  (2).

Si (2) est vérifiée, d'après la proposition 2.1.16,

$$t(1) = \sum_{\chi \in \text{Irr}(G)} \nu(\chi)\chi(1) = \sum_{\chi \in \text{Irr}(G)} \chi(1).$$

Donc (2)  $\Rightarrow$  (3).

Si (3) est vérifiée, d'après [17, (3.7), page 23], tout caractère de  $G$  est de type 1 et alors d'après les propositions 2.1.13 et 2.1.14, pour toute composante simple  $A$  de  $\mathbb{R}G$ , la restriction de  $\sigma$  à  $A$  est orthogonale. Donc (3)  $\Rightarrow$  (1). ■

En remplaçant  $\mathbb{R}$  par  $\mathbb{C}$ , nous allons maintenant établir un résultat semblable à celui énoncé respectivement dans la proposition 2.1.14 et dans la proposition 2.1.17. Pour y arriver, nous aurons besoin des lemmes suivants :

**Lemme 2.1.18.** *Pour tout corps  $k$ , soit  $\nu$  l'application définie sur  $M_r(k) \times M_r(k)$  par*

$$\nu(a, b) = (b^t, a^t), \quad \forall a, b \in M_r(\mathbb{C}),$$

*où  $^t$  désigne la transposition matricielle.  $\nu$  est une involution sur  $M_r(k) \times M_r(k)$  envoyant  $M_r(k) \times 0$  sur  $0 \times M_r(k)$ .*

*Preuve* : Calculs simples. ■

**Lemme 2.1.19.** *Les  $\mathbb{C}$ -algèbres à involution  $(M_r(\mathbb{C}) \otimes_{\mathbb{R}} \mathbb{C}, {}^{-t} \otimes id_{\mathbb{C}})$  et  $(M_r(\mathbb{C}) \times M_r(\mathbb{C}), \nu)$  sont isomorphes, où  ${}^{-}$  désigne la conjugaison sur  $\mathbb{C}$ ,  ${}^t$ , la transposition matricielle et  $\nu$ , l'involution sur  $M_r(\mathbb{C}) \times M_r(\mathbb{C})$  définie dans le lemme 2.1.18.*

*Preuve* : Soit  $\psi$  l'application de  $M_r(\mathbb{C}) \otimes_{\mathbb{R}} \mathbb{C}$  dans  $M_r(\mathbb{C}) \times M_r(\mathbb{C})$  définie par

$$\psi(a \otimes \lambda) = (a\lambda, \bar{a}\lambda), \quad \forall a \in M_r(\mathbb{C}), \quad \forall \lambda \in \mathbb{C}.$$

On vérifie que  $\psi$  est un isomorphisme de  $\mathbb{C}$ -algèbres. De plus, pour tout  $a \in M_r(\mathbb{C})$ , on a :

$$\psi({}^{-t} \otimes id_{\mathbb{C}})(a \otimes 1) = \psi(\bar{a}^t \otimes 1) = (\bar{a}^t, a^t) = \nu(a, \bar{a}) = \nu\psi(a \otimes 1).$$

Donc  $\psi({}^{-t} \otimes id_{\mathbb{C}}) = \nu\psi$ , et le résultat s'ensuit. ■

Le résultat suivant utilise l'indicateur de Schur-Frobenius pour traduire le commentaire fait en quelques lignes par Scharlau dans [39, page 324], par rapport au comportement de l'involution canonique sur chaque composante simple de  $\mathbb{C}G$ .

**Théorème 2.1.20.** *Soit  $G$  un groupe fini,  $\chi$  un  $\mathbb{C}$ -caractère irréductible de  $G$  et  $\chi^\vee$  le caractère contragrédient de  $\chi$ . Soient  $A$  la composante simple de  $\mathbb{C}G$  correspondant à  $\chi$ ,  $A^\vee$ , celle correspondant à  $\chi^\vee$  et  $\sigma$  l'involution canonique de  $\mathbb{C}G$ . Alors  $\sigma(A) = A^\vee$  et on a :*

- (1)  $\nu(\chi) = 1$  si et seulement si  $\sigma(A) = A$  et la restriction de  $\sigma$  à  $A$  est une involution orthogonale.
- (2)  $\nu(\chi) = -1$  si et seulement si  $\sigma(A) = A$  et la restriction de  $\sigma$  à  $A$  est une involution symplectique.
- (3)  $\nu(\chi) = 0$  si et seulement si  $\sigma(A) \neq A$ .

*Preuve* : D'après la proposition 2.1.2,  $\sigma(A) = A^\vee$ . D'après [34, lemme 3.6, page 26],  $\mathbb{C}G \cong \mathbb{R}G \otimes_{\mathbb{R}} \mathbb{C}$ . De plus, par cet isomorphisme,  $\sigma$  s'identifie à l'involution  $\sigma_{\mathbb{R}} \otimes id_{\mathbb{C}}$ , où  $\sigma_{\mathbb{R}}$  désigne l'involution canonique sur  $\mathbb{R}G$  et  $id_{\mathbb{C}}$ , l'identité sur  $\mathbb{C}$ . Il existe une composante simple  $B$  de  $\mathbb{R}G$  telle que  $A$  soit une composante simple

de la  $\mathbb{C}$ -algèbre  $B \otimes_{\mathbb{R}} \mathbb{C}$ . Comme chaque composante simple de  $\mathbb{R}G$  est fixée par  $\sigma_{\mathbb{R}}$ , alors  $B \otimes_{\mathbb{R}} \mathbb{C}$  est fixée par  $\sigma_{\mathbb{R}} \otimes id_{\mathbb{C}}$ . D'après ( 2.2),  $(B, \sigma_{\mathbb{R}}) \cong (M_r(D), {}^{-t})$ , pour un certain entier naturel non nul  $r$ , où  $D = \mathbb{R}, \mathbb{C}$  ou  $\mathbb{H}$ ,  $t$  est la transposition matricielle et  $-$  l'identité sur  $\mathbb{R}$ , la conjugaison complexe sur  $\mathbb{C}$  ou l'involution canonique sur  $\mathbb{H}$ . Par suite,

$$(B \otimes_{\mathbb{R}} \mathbb{C}, \sigma_{\mathbb{R}} \otimes id_{\mathbb{C}}) \cong (M_r(D) \otimes_{\mathbb{R}} \mathbb{C}, {}^{-t} \otimes id_{\mathbb{C}}).$$

D'après [34, lemme 3.2, page 191],

$$M_r(D) \otimes_{\mathbb{R}} \mathbb{C} \cong M_r(D \otimes_{\mathbb{R}} \mathbb{C}).$$

- Si  $D = \mathbb{R}$ , alors  $M_r(D) \otimes_{\mathbb{R}} \mathbb{C} \cong M_r(\mathbb{R} \otimes_{\mathbb{R}} \mathbb{C}) \cong M_r(\mathbb{C})$  est une  $\mathbb{C}$ -algèbre simple centrale de degré  $r$  fixée par  $\sigma$ . Donc  $A = M_r(\mathbb{C})$  et comme la restriction de  $\sigma_{\mathbb{R}}$  à  $B \cong M_r(\mathbb{R})$  est orthogonale (proposition 2.1.4), alors la restriction de  $\sigma \equiv \sigma_{\mathbb{R}} \otimes id_{\mathbb{C}}$  à  $A$  est une involution orthogonale.
- Si  $D = \mathbb{H}$ , alors  $M_r(D) \otimes_{\mathbb{R}} \mathbb{C} \cong M_r(\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C}) \cong M_r(M_2(\mathbb{C}))$ . D'après [39, corollaire 2.4, page 287],  $M_r(M_2(\mathbb{C})) \cong M_{2r}(\mathbb{C})$ . Donc  $M_r(D) \otimes_{\mathbb{R}} \mathbb{C} \cong M_{2r}(\mathbb{C})$  est une  $\mathbb{C}$ -algèbre simple centrale de degré  $2r$  fixée par  $\sigma$ . Il en résulte que  $A = M_{2r}(\mathbb{C})$  et comme la restriction de  $\sigma_{\mathbb{R}}$  à  $B \cong M_r(\mathbb{H})$  est symplectique (proposition 2.1.4), alors la restriction de  $\sigma \equiv \sigma_{\mathbb{R}} \otimes id_{\mathbb{C}}$  à  $A$  est une involution symplectique.
- Si  $D = \mathbb{C}$ , alors  $M_r(D) \otimes_{\mathbb{R}} \mathbb{C} \cong M_r(\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}) \cong M_r(\mathbb{C}) \times M_r(\mathbb{C})$  est produit direct de deux  $\mathbb{C}$ -algèbres simples centrales de degré  $r$ . Donc  $A = M_r(\mathbb{C}) \times 0$  ou  $A = 0 \times M_r(\mathbb{C})$ . D'après le lemme 2.1.19, l'involution canonique restreinte à  $M_r(\mathbb{C}) \otimes_{\mathbb{R}} \mathbb{C}$  se transforme en l'involution  $\nu$  sur  $M_r(\mathbb{C}) \times M_r(\mathbb{C})$  définie dans le lemme 2.1.18, laquelle, d'après ce lemme, envoie  $M_r(\mathbb{C}) \times 0$  sur  $0 \times M_r(\mathbb{C})$ . Donc  $\sigma(A) \neq A$ .

Le résultat découle alors de la proposition 2.1.14. ■

On en déduit alors immédiatement que :

**Corollaire 2.1.21.** *Soit  $G$  un groupe fini. Les assertions suivantes sont équivalentes :*



- (1)  $G$  est ortho-ambivalent par rapport à  $\mathbb{C}$ .
- (2)  $G$  est ambivalent et pour tout caractère irréductible  $\chi$  de  $G$ ,  $\nu(\chi) = 1$ .
- (3)  $G$  est ambivalent et  $t(1) = \sum_{\chi \in \text{Irr}(G)} \chi(1)$ . ■

Avant de clôturer cette section, il est utile de préciser comment la restriction de l'involution canonique à une composante simple de  $\mathbb{C}G$  ( $G$  étant un groupe fini) se transforme par isomorphisme en une involution sur une  $\mathbb{C}$ -algèbre des matrices. Cela constitue un outil dont nous aurons besoin dans la section suivante.

**Proposition 2.1.22.** *Les  $\mathbb{C}$ -algèbres à involution*

$$(M_r(\mathbb{R}) \otimes_{\mathbb{R}} \mathbb{C}, {}^{-t} \otimes id_{\mathbb{C}}) \text{ et } (M_r(\mathbb{C}), {}^t)$$

sont isomorphes, où  $-$  désigne l'identité sur  $\mathbb{R}$  et  ${}^t$ , la transposition matricielle.

*Preuve :* On vérifie aisément que l'application  $g : M_r(\mathbb{R}) \otimes_{\mathbb{R}} \mathbb{C} \rightarrow M_r(\mathbb{C})$  définie par  $g(a \otimes 1) = a$ , pour tout  $a \in M_r(\mathbb{R})$ , est un isomorphisme de  $\mathbb{C}$ -algèbres qui transforme l'involution  ${}^{-t} \otimes id_{\mathbb{C}}$  en l'involution  ${}^t$ . ■

**Proposition 2.1.23.** *Les  $\mathbb{C}$ -algèbres à involution*

$$(M_r(\mathbb{H}) \otimes_{\mathbb{R}} \mathbb{C}, {}^{-t} \otimes id_{\mathbb{C}}) \text{ et } (M_{2r}(\mathbb{C}), \tau)$$

sont isomorphes, où  $-$  désigne la conjugaison sur  $\mathbb{H}$ ,  ${}^t$ , la transposition matricielle et  $\tau$ , l'involution sur  $M_{2r}(\mathbb{C})$  définie dans la proposition 1.2.8.

*Preuve :* Soit  $\{1, i, j, ij\}$  la base de  $\mathbb{H} = (-1, -1)_{\mathbb{R}}$  telle que  $i^2 = j^2 = -1$  et  $ij = -ji$ . D'après [33, page 18], l'application

$$f : (\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C}, {}^{-t} \otimes id_{\mathbb{C}}) \rightarrow (M_2(\mathbb{C}), J)$$

définie par

$$f((a + bj) \otimes 1) = \begin{pmatrix} a & \bar{b} \\ -b & \bar{a} \end{pmatrix},$$

pour tous  $a, b \in \mathbb{C}$ , est un isomorphisme de  $\mathbb{C}$ -algèbres à involutions, où  $J$  désigne l'involution sur  $M_2(\mathbb{C})$  définie à l'exemple 1.2.7 par

$$J \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Donc  $f(-\otimes id_{\mathbb{C}}) = Jf$ . Soit maintenant

$$\varphi : M_r(\mathbb{H}) \otimes_{\mathbb{R}} \mathbb{C} \rightarrow M_{2r}(\mathbb{C})$$

l'application telle que pour tout  $\alpha = (\alpha_{pq})_{1 \leq p, q \leq r} \in M_r(\mathbb{H})$ ,

$$\varphi(\alpha \otimes 1) = (f(\alpha_{pq} \otimes 1))_{1 \leq p, q \leq r}.$$

On vérifie que  $\varphi$  est un isomorphisme de  $\mathbb{C}$ -algèbres. De plus, pour tout  $\alpha = (\alpha_{pq})_{1 \leq p, q \leq r} \in M_r(\mathbb{H})$ , on a :

$$\begin{aligned} \varphi(-^t \otimes id_{\mathbb{C}})(\alpha \otimes 1) &= \varphi(((-\otimes id_{\mathbb{C}})(\alpha_{pq} \otimes 1))_{1 \leq p, q \leq r}^t) \\ &= (f(-\otimes id_{\mathbb{C}})(\alpha_{pq} \otimes 1))_{1 \leq p, q \leq r}^t \\ &= (Jf(\alpha_{pq} \otimes 1))_{1 \leq p, q \leq r}^t \\ &= \tau((f(\alpha_{pq} \otimes 1))_{1 \leq p, q \leq r}) \\ &= \tau\varphi(\alpha \otimes 1). \end{aligned}$$

Donc  $\varphi(-^t \otimes id_{\mathbb{C}}) = \tau\varphi$  et le résultat est ainsi démontré. ■

## 2.2 Changement de caractéristique

Soit  $G$  un groupe fini,  $K_0$  un corps premier dont la caractéristique ne divise pas l'ordre de  $G$  et  $K = \overline{K_0}$  la clôture algébrique de  $K_0$ . Soit  $\mathcal{G} = Gal(K/K_0)$  le groupe de Galois de l'extension  $K/K_0$ .  $\mathcal{G}$  agit naturellement sur  $KG$  par l'action définie par :

$$\gamma \cdot \left( \sum_{g \in G} \alpha_g g \right) = \sum_{g \in G} \gamma(\alpha_g) g, \quad \forall \gamma \in \mathcal{G}, \quad \forall \alpha_g \in K$$

La sous-algèbre de  $KG$  fixe sous  $\mathcal{G}$  est  $(KG)^{\mathcal{G}} = K_0G$ . Rappelons que la  $\mathcal{G}$ -orbite  $a^{\mathcal{G}}$  d'un élément  $a$  de  $KG$ , est définie par :

$$a^{\mathcal{G}} = \{x \in KG \mid \exists \gamma \in \mathcal{G}, \gamma.x = a\}$$

On a le résultat suivant :

**Lemme 2.2.1.** [34, lemme 1.3, page 647] *Il existe une correspondance biunivoque entre les éléments idempotents centralement primitifs de  $K_0G$  et les  $\mathcal{G}$ -orbites  $e^{\mathcal{G}}$  des éléments idempotents centralement primitifs  $e$  de  $KG$ . Plus précisément,*

*$f \leftrightarrow e^{\mathcal{G}} = \{e = e_1, e_2, \dots, e_s\}$  si et seulement si  $f = e_1 + e_2 + \dots + e_s$ ,  $e_1, e_2, \dots, e_s$  (resp.  $f$ ) étant des éléments idempotents centralement primitifs de  $KG$  (resp. de  $K_0G$ ). De plus,*

$$\dim_{K_0} f K_0G = |e^{\mathcal{G}}| \cdot \dim_K e KG,$$

$$\dim_{K_0} Z(f K_0G) = |e^{\mathcal{G}}|$$

*et donc*

$$\dim_{Z(f K_0G)} f K_0G = \dim_K e KG. \blacksquare$$

De ce lemme, il ressort que l'étude des composantes simples de  $K_0G$  peut se faire en étudiant celles de  $KG$  (qui sont en fait les moins compliquées,  $K$  étant algébriquement clos).

**Lemme 2.2.2.** [34, lemme 1.4, page 649] *Soit  $\chi : G \rightarrow K$  un  $K$ -caractère irréductible de  $G$  de degré  $d$ . Supposons que  $G$  est d'exposant  $m$ . Soit  $\varepsilon$  une racine primitive  $m$ -ième de l'unité dans  $K$ . Pour tout  $g \in G$ , il existe des entiers  $a_1, a_2, \dots, a_d$  tels que*

$$\chi(g) = \sum_{i=1}^d \varepsilon^{a_i} \in K_0[\varepsilon]. \blacksquare$$

Soient  $r$  le nombre de classes de conjugaison de  $G$  et  $e_1, e_2, \dots, e_r$  les éléments idempotents centralement primitifs (orthogonaux) de  $KG$ , correspondant aux  $K$ -caractères irréductibles respectifs  $\chi_1, \chi_2, \dots, \chi_r$  de  $G$ . Alors  $\{e_1, e_2, \dots, e_r\}$  est une base de  $Z(KG)$  sur  $K$ . Soient  $\gamma_1, \gamma_2, \dots, \gamma_r$  les classes de conjugaison de  $G$ . Pour tout  $i$ , on pose

$$\widehat{\gamma}_i := \sum_{g \in \gamma_i} g.$$

D'après [34, lemme 1.1, page 113],  $\{\widehat{\gamma}_1, \widehat{\gamma}_2, \dots, \widehat{\gamma}_r\}$  est une base de  $Z(KG)$  sur  $K$ . Le résultat suivant donne le passage de l'une à l'autre de ces deux bases.

**Lemme 2.2.3.** [34, lemme 1.5, page 650] *La caractéristique de  $K$  ne divise pas l'ordre de  $G$  (avec les hypothèses qui précèdent le lemme 2.2.1) et on a :*

$$e_i = \frac{\chi_i(1)}{|G|} \sum_{j=1}^r \chi_i(g_j^{-1}) \widehat{\gamma}_j, \quad \text{avec } g_j \in \gamma_j, \forall j$$

et

$$\widehat{\gamma}_i = |\gamma_i| \sum_{j=1}^r \frac{\chi_j(g_i)}{\chi_j(1)} e_j, \quad \text{avec } g_i \in \gamma_i$$

(dans chaque classe  $\gamma_i$  on choisit un élément  $g_i$ ). ■

Soient  $e$  un élément idempotent centralement primitif de  $KG$  et  $\chi$  le  $K$ -caractère irréductible de  $G$  correspondant à  $e$ . Soit  $K_0(e)$  (resp.  $K_0(\chi)$ ) le sous-corps de  $K = \overline{K_0}$  engendré sur  $K_0$  par les coefficients de  $e$  (resp. par les éléments  $\chi(g)$ , avec  $g \in G$ ). On a alors :

**Lemme 2.2.4.** [34, lemme 1.7, page 652] *Soit  $f$  un élément idempotent centralement primitif de  $K_0G$ . Supposons que  $f \leftrightarrow e^{\mathcal{G}}$  par la correspondance biunivoque définie dans le lemme 2.2.1. Alors*

$$K_0(e) = K_0(\chi) = Z(fK_0G).$$

*Si  $G$  a pour exposant  $m$  et  $\varepsilon$  est une racine primitive  $m$ -ième de l'unité dans  $K$ , alors  $K_0(e) \subset K_0[\varepsilon]$  et l'extension  $K_0(e)/K_0$  est galoisienne finie de groupe de Galois abélien.* ■

Soit maintenant  $k$  un corps algébriquement clos dont la caractéristique ne divise pas l'ordre de  $G$ ,  $K_0$  le sous-corps premier de  $k$  et  $K$  une clôture algébrique de  $K_0$ . On a les extensions de corps suivantes :

$$K_0 \subset K \subset k.$$

On a le résultat suivant qui est semblable à celui donné par le lemme 2.2.2 :

**Proposition 2.2.5.** [15, proposition 6.4.1, page 233] *Soit  $\chi$  un  $k$ -caractère de  $G$ . Pour tout  $g \in G$ , si  $g$  est d'ordre  $s$ ,  $\chi(g)$  est somme des racines  $s$ -ièmes de l'unité dans  $k$ . ■*

On en déduit alors que :

**Corollaire 2.2.6.** *Avec les hypothèses ci-dessus, soit  $\varepsilon$  une racine primitive  $|G|$ -ième de l'unité dans  $k$  et  $\chi : G \rightarrow k$  un  $k$ -caractère irréductible de  $G$ . Pour tout  $g \in G$ , il existe des entiers  $a_{g1}, a_{g2}, \dots, a_{gm}$  tels que*

$$\chi(g) = \sum_{j=1}^m \varepsilon^{a_{gj}} \in K_0[\varepsilon]. \quad \blacksquare$$

**Remarque 2.2.7.** *Du corollaire 2.2.6, il résulte que les  $k$ -caractères irréductibles de  $G$  sont des  $K$ -caractères irréductibles de  $G$ .  $k$  et  $K$  étant algébriquement clos, les nombres des  $k$ -caractères irréductibles et des  $K$ -caractères irréductibles de  $G$  sont égaux au nombre de classes de conjugaison de  $G$ . Donc les  $k$ -caractères irréductibles et les  $K$ -caractères irréductibles de  $G$  coïncident. Le lemme 2.2.3 reste donc valable lorsqu'on remplace  $K$  par  $k$ . Notons aussi que les éléments idempotents centralement primitifs de  $kG$  appartiennent alors à l'algèbre de groupe  $K_0[\varepsilon]G$ .*

Soit  $G$  un groupe fini. Dans la section 2.1, nous avons donné une description complète de la restriction de l'involution canonique à chaque composante simple de  $\mathbb{C}G$ . La remarque 2.2.7 nous permet alors d'en déduire le comportement de l'involution canonique sur chaque composante simple de  $\overline{\mathbb{Q}}G$ . Dans cette section, notre objectif est de décrire le type de la restriction de l'involution canonique à chaque composante simple de  $K_pG$ , pour tout entier naturel premier  $p$  ne divisant pas l'ordre de  $G$ ,  $K_p$  étant la clôture algébrique du sous-corps premier  $\mathbb{F}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$  d'un corps de caractéristique  $p$ . Pour y arriver, nous nous servirons d'une place de  $\overline{\mathbb{Q}}$  dans  $K_p$ .

**Définition 2.2.8.** [34, page 39], [39, page 139] *Un sous-anneau  $R$  d'un corps  $K$  est dit anneau de valuation si pour tout  $x \in K - R$ ,  $x^{-1} \in R$ .*

**Proposition 2.2.9.** *Si  $R$  est un anneau de valuation dans un corps  $K$ , alors  $R$  est un anneau local (c'est-à-dire un anneau dans lequel l'ensemble des éléments non inversibles est l'unique idéal maximal).*

**Preuve :** cela découle directement de [34, lemme 2.2, page 39].

■

**Définition 2.2.10.** [34, page 39], [39, page 140] *Soient  $K$  et  $F$  deux corps. On appelle place de  $K$  dans  $F$  une application  $\varphi : K \rightarrow F^\infty = F \cup \{\infty\}$  telle que  $R := \varphi^{-1}(F)$  est un sous-anneau de  $K$ , la restriction de  $\varphi$  à  $R$  est un morphisme d'anneaux de  $R$  dans  $F$  et  $\varphi(x) = \infty \Leftrightarrow \varphi(x^{-1}) = 0$ , pour tout  $x \in K$ .*

**Proposition 2.2.11.** [34, lemme 2.3, page 40] *Si  $\varphi$  est une place d'un corps  $K$  dans un corps  $F$ , alors  $R := \varphi^{-1}(F)$  est un anneau de valuation dans  $K$ , d'unique idéal maximal le noyau  $M$  de la restriction de  $\varphi$  à  $R$ . De plus, si  $\varphi$  est non trivial (et surjective), alors  $F$  est isomorphe au corps résiduel  $\frac{R}{M}$  de  $R$ . ■*

**Remarque 2.2.12.** [34, lemme 2.3, page 40], [39, page 140] *Soient  $R$  un anneau de valuation dans un corps  $K$ ,  $M$  l'unique idéal maximal de  $R$  et  $F = \frac{R}{M}$  le corps résiduel de  $R$ . L'application  $\varphi : K \rightarrow F^\infty = F \cup \{\infty\}$  définie par*

$$\varphi(x) = \begin{cases} x + M & \text{si } x \in R \\ \infty & \text{si } x \in K - R \end{cases} ,$$

*est une place de  $K$  dans  $F$ .*

Le résultat suivant donne une description des composantes simples de l'algèbre d'un groupe sur le corps  $K_p$  lorsqu'on connaît les composantes simples de l'algèbre de ce groupe sur le corps  $\overline{\mathbb{Q}}$  par l'intermédiaire d'une place de  $\overline{\mathbb{Q}}$  dans  $K_p$ .

**Proposition 2.2.13.** [34, lemme 1.8, page 653] *Soient  $G$  un groupe fini,  $p$  un entier naturel premier ne divisant pas l'ordre de  $G$ ,  $\overline{\mathbb{Q}}$  la clôture algébrique du corps  $\mathbb{Q}$  des nombres rationnels et  $K_p$  la clôture algébrique du corps  $\mathbb{F}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$ . Soit  $\varphi : \overline{\mathbb{Q}} \rightarrow K_p \cup \{\infty\}$  une*

place d'anneau de valuation  $R = \varphi^{-1}(K_p)$ . Soient  $M$  l'unique idéal maximal de  $R$ . Alors  $\mathbb{Z} \subset R$  et  $p\mathbb{Z} \subset M$ . Le morphisme d'anneaux  $\varphi : R \rightarrow K_p$  se prolonge de façon naturelle en un morphisme d'anneaux de groupe noté aussi  $\varphi$  et défini de  $RG$  dans  $K_p G$  par

$$\varphi\left(\sum_{g \in G} a_g g\right) = \sum_{g \in G} \varphi(a_g) g,$$

avec  $a_g \in R$ , pour tout  $g \in G$ . Soient  $e_1, e_2, \dots, e_m$  les éléments idempotents centralement primitifs de  $\overline{\mathbb{Q}}G$ . Alors  $e_i \in RG$ , pour tout  $i = 1, 2, \dots, m$  et  $\varphi(e_1), \varphi(e_2), \dots, \varphi(e_m)$  sont exactement les éléments idempotents centralement primitifs de  $K_p G$ . De plus,

$$\deg(\varphi(e_i)) = \deg(e_i) \quad \text{et} \quad \mathbb{F}_p(\varphi(e_i)) = \varphi(\text{int}(\mathbb{Q}(e_i))),$$

où  $\text{int}(\mathbb{Q}(e_i))$  désigne l'ensemble des entiers algébriques de  $\mathbb{Q}(e_i)$ . ■

Jusqu'à la fin de cette section, nous utiliserons les notations et les hypothèses de la proposition 2.2.13. Soient  $\sigma$  l'involution canonique sur  $\overline{\mathbb{Q}}G$  et  $\bar{\sigma}$  l'involution canonique sur  $K_p G$ . Notons aussi par  $\sigma$  l'involution canonique sur  $\mathbb{C}G$  et même sur  $RG$ .

**Lemme 2.2.14.**  *$\varphi$  est un morphisme d'anneaux à involutions de  $(RG, \sigma)$  sur  $(K_p G, \bar{\sigma})$ .*

*Preuve :* Comme  $\varphi$  est un morphisme d'anneaux, il suffit de démontrer que  $\varphi\sigma = \bar{\sigma}\varphi$ . Soit  $x = \sum_{g \in G} a_g g$  un élément de  $RG$ .

$$\varphi\sigma(x) = \varphi\left(\sum_{g \in G} a_g g^{-1}\right) = \sum_{g \in G} \varphi(a_g) g^{-1} = \bar{\sigma}\left(\sum_{g \in G} \varphi(a_g) g\right) = \bar{\sigma}\varphi(x).$$

D'où le résultat. ■

Soit maintenant  $A$  une composante simple de  $\overline{\mathbb{Q}}G$  de degré  $d$ . Soient  $\chi$  le  $\mathbb{C}$ -caractère irréductible et  $e$  l'élément idempotent centralement primitif de  $\overline{\mathbb{Q}}G$  correspondant à  $A$ . Alors

$$e = \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(g^{-1}) g, \quad A = e\overline{\mathbb{Q}}G \quad \text{et} \quad A_{\mathbb{C}} := A \otimes_{\overline{\mathbb{Q}}} \mathbb{C} = e\mathbb{C}G$$

est la composante simple de  $\mathbb{C}G$  correspondant à  $\chi$ . D'après la proposition 2.2.13,  $e \in RG$ ,  $\varphi(e)$  est un élément idempotent centralement primitif de  $K_p G$  et  $\deg \varphi(e) = \deg e = \deg A = d$ . Soit  $A^\varphi$  la composante simple de  $K_p G$  correspondant à  $\varphi(e)$ . C'est clair que

$$A^\varphi = \varphi(e)K_p G = \varphi(eRG).$$

Comme  $\overline{\mathbb{Q}}$  et  $K_p$  sont algébriquement clos, alors  $A \cong M_d(\overline{\mathbb{Q}})$  et  $A^\varphi \cong M_d(K_p)$ . C'est clair que  $eRG \cong M_d(R)$ , la restriction de l'isomorphisme  $A \xrightarrow{\sim} M_d(\overline{\mathbb{Q}})$  à  $eRG$  étant un isomorphisme de  $eRG$  sur  $M_d(R)$ . Comme par définition, le morphisme d'anneaux  $\varphi : eRG \rightarrow A^\varphi$  agit uniquement sur les éléments de  $R$ ,  $eRG \cong M_d(R)$  et  $A^\varphi \cong M_d(K_p)$ , alors ce morphisme  $\varphi$  peut être regardé comme le morphisme d'anneaux  $\overline{\varphi} : M_d(R) \rightarrow M_d(K_p)$  défini par : pour tout  $a = (a_{ij})_{1 \leq i, j \leq d} \in M_d(R)$ ,

$$\overline{\varphi}(a) = (\varphi(a_{ij}))_{1 \leq i, j \leq d}.$$

On a alors le résultat suivant :

**Théorème 2.2.15. (1)** *Si  $\sigma(A_{\mathbb{C}}) = A_{\mathbb{C}}$  et la restriction de  $\sigma$  à  $A_{\mathbb{C}}$  est orthogonale, alors  $\overline{\sigma}(A^\varphi) = A^\varphi$  et la restriction de  $\overline{\sigma}$  à  $A^\varphi$  est orthogonale.*

**(2)** *Si  $\sigma(A_{\mathbb{C}}) = A_{\mathbb{C}}$  et la restriction de  $\sigma$  à  $A_{\mathbb{C}}$  est symplectique, alors  $\overline{\sigma}(A^\varphi) = A^\varphi$  et la restriction de  $\overline{\sigma}$  à  $A^\varphi$  est symplectique.*

**(3)** *Si  $\sigma(A_{\mathbb{C}}) \neq A_{\mathbb{C}}$ , alors  $\overline{\sigma}(A^\varphi) \neq A^\varphi$ .*

*Preuve :* Du lemme 2.2.14, il suit que la restriction de  $\varphi$  à  $eRG$ , notée aussi  $\varphi$ , est un morphisme d'anneaux à involutions de  $(eRG, \sigma)$  sur  $(A^\varphi, \overline{\sigma})$ .

**1.** Si  $\sigma(A_{\mathbb{C}}) = A_{\mathbb{C}}$  et la restriction de  $\sigma$  à  $A_{\mathbb{C}}$  est orthogonale, alors d'après la démonstration du théorème 2.1.20 et la proposition 2.1.22,  $(A_{\mathbb{C}}, \sigma) \cong (M_d(\mathbb{C}), {}^t)$ ,  ${}^t$  étant la transposition matricielle. Par ailleurs  $\overline{\varphi}$  transforme  $(M_d(R), {}^t)$  en  $(M_d(K_p), {}^t)$ , en effet, pour tout  $a = (a_{ij})_{1 \leq i, j \leq d} \in M_d(R)$ , on a :

$$\overline{\varphi}(a^t) = (\varphi(a_{ij}))_{1 \leq i, j \leq d}^t = (\overline{\varphi}(a))^t.$$



Et comme la transposition matricielle est une involution orthogonale sur  $M_d(K_p)$  (exemple 1.2.5), on en déduit que  $\bar{\sigma}(A^\varphi) = A^\varphi$  et la restriction de  $\bar{\sigma}$  à  $A^\varphi$  est orthogonale.

**2.** Si  $\sigma(A_{\mathbb{C}}) = A_{\mathbb{C}}$  et la restriction de  $\sigma$  à  $A_{\mathbb{C}}$  est symplectique, alors d'après la démonstration du théorème 2.1.20 et la proposition 2.1.23,  $(A_{\mathbb{C}}, \sigma) \cong (M_d(\mathbb{C}), \tau)$ , avec  $d = 2r$  pour un certain entier naturel non nul  $r$ ,  $\tau$  étant l'involution définie sur  $M_{2r}(\mathbb{C})$  dans la proposition 1.2.8 par : pour tout  $\alpha \in M_{2r}(\mathbb{C})$ , si  $\alpha = (\alpha_{ij})_{1 \leq i, j \leq r}$ , avec  $\alpha_{ij} \in M_2(\mathbb{C})$ ,

$$\tau(\alpha) = (J(\alpha_{ij}))_{1 \leq i, j \leq r}^t,$$

$J$  étant l'involution définie sur  $M_2(\mathbb{C})$  dans l'exemple 1.2.7 par

$$J \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Montrons que  $\bar{\varphi}$  transforme  $(M_{2r}(R), \tau)$  en  $(M_{2r}(K_p), \tau_p)$ ,  $\tau_p$  étant l'involution définie sur  $M_{2r}(K_p)$  dans la proposition 1.2.8 de la même façon que  $\tau$ . Pour tout  $\alpha = (\alpha_{ij})_{1 \leq i, j \leq r} \in M_{2r}(R)$ , avec  $\alpha_{ij} \in M_2(R)$ , on a :

$$\begin{aligned} \bar{\varphi}\tau(\alpha) &= \bar{\varphi}((J(\alpha_{ij}))_{1 \leq i, j \leq r}^t) \\ &= (J_p(\varphi(\alpha_{ij})))_{1 \leq i, j \leq r}^t \\ &= \tau_p((\varphi(\alpha_{ij}))_{1 \leq i, j \leq r}) \\ &= \tau_p(\bar{\varphi}(\alpha)), \end{aligned}$$

$J_p$  étant l'involution définie sur  $M_2(K_p)$  dans l'exemple 1.2.7 de la même façon que  $J$ . Donc  $\bar{\varphi}\tau = \tau_p\bar{\varphi}$ . D'après la proposition 1.2.8,  $\tau_p$  est une involution symplectique. Donc  $\bar{\sigma}(A^\varphi) = A^\varphi$  et la restriction de  $\bar{\sigma}$  à  $A^\varphi$  est symplectique.

**3.** Si  $\sigma(A_{\mathbb{C}}) \neq A_{\mathbb{C}}$ , alors  $\sigma(e) \neq e$ . D'après la proposition 2.2.13, les éléments idempotents centralement primitifs de  $\bar{\mathbb{Q}}G$  (et donc de

$\mathbb{C}G$ ) sont en correspondance biunivoque avec les éléments idempotents centralement primitifs de  $K_p G$  via le morphisme  $\varphi : RG \rightarrow K_p G$ . Donc  $\varphi(\sigma(e)) \neq \varphi(e)$  et alors  $\bar{\sigma}(\varphi(e)) \neq \varphi(e)$ . Il en résulte que  $\bar{\sigma}(A^\varphi) \neq A^\varphi$ . ■

**Proposition 2.2.16.** *Avec les notations et hypothèses du théorème 2.2.15, on a :*

- (1)  $\nu(\chi) = 1$  si et seulement si  $\sigma(A^\varphi) = A^\varphi$  et la restriction de  $\bar{\sigma}$  à  $A^\varphi$  est une involution orthogonale.
- (2)  $\nu(\chi) = -1$  si et seulement si  $\sigma(A^\varphi) = A^\varphi$  et la restriction de  $\bar{\sigma}$  à  $A^\varphi$  est une involution symplectique.
- (3)  $\nu(\chi) = 0$  si et seulement si  $\bar{\sigma}(A^\varphi) \neq A^\varphi$ .

*Preuve :* Cela découle des théorèmes 2.2.15 et 2.1.20. ■

On en déduit alors que :

**Corollaire 2.2.17.** *Les assertions suivantes sont équivalentes :*

- (1)  $G$  est ortho-ambivalent par rapport à  $\mathbb{C}$  ;
- (2)  $G$  est ortho-ambivalent par rapport à  $K_p$ .

**Preuve :** Cela découle de la proposition 2.2.16 et du corollaire 2.1.21. ■

## 2.3 Extension des scalaires

Soient  $G$  un groupe fini,  $p$  un entier naturel premier ne divisant pas l'ordre de  $G$  et  $K_p$  la clôture algébrique du corps  $\mathbb{F}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$ . Dans les sections 2.1 et 2.2 nous nous sommes intéressés au type de la restriction de l'involution canonique à chaque composante simple de  $\mathbb{C}G$  et  $K_p G$  respectivement.

Soit  $k$  un corps dont la caractéristique ne divise pas l'ordre de  $G$ . Dans cette section, nous déterminons le type de la restriction de l'involution canonique à chaque composante simple de  $kG$  fixée par l'involution canonique et sur laquelle cette restriction est une involution de première espèce. Nous le faisons par extension des scalaires en passant par les corps  $\mathbb{C}$  ou  $K_p$  (et leurs sous-corps premiers) suivant que  $k$  est de caractéristique nulle ou  $p$ . Pour y arriver, nous avons besoin de certains résultats préliminaires.

**Lemme 2.3.1.** *Soient  $L/k$  et  $K/k$  des extensions de corps telles que  $L/k$  soit finie. Soit  $V$  un espace vectoriel de dimension finie sur  $L$ .  $V \otimes_k K$  est un module libre sur  $L \otimes_k K$  et les modules  $End_L(V) \otimes_k K$  et  $End_{L \otimes_k K}(V \otimes_k K)$  sont  $L \otimes_k K$ -isomorphes.*

**Preuve :** Soit  $(e_i)_{1 \leq i \leq n}$  une base de  $V$  sur  $L$ . On vérifie aisément que  $(e_i \otimes 1)_{1 \leq i \leq n}$  est une base de  $V \otimes_k K$  sur  $L \otimes_k K$ . Par suite

$$V \otimes_k K = \bigoplus_{i=1}^n (L \otimes_k K)(e_i \otimes 1)$$

est isomorphe à  $(L \otimes_k K)^n$  et donc  $V \otimes_k K$  est un module libre sur  $L \otimes_k K$ .

Soit

$$\psi : End_L(V) \otimes_k K \rightarrow End_{L \otimes_k K}(V \otimes_k K)$$

l'application telle que pour tous éléments  $\varepsilon$  de  $End_L(V) \otimes_k K$  et  $w$  de  $V \otimes_k K$  tels que  $\varepsilon = \sum_i f_i \otimes \alpha_i$  et  $w = \sum_i v_i \otimes \gamma_i$ , avec  $f_i \in End_L(V)$ ,  $v_i \in V$  et  $\alpha_i, \gamma_i \in K$ , pour tout  $i$ ,

$$\psi(\varepsilon)(w) = \sum_{i,j} f_i(v_j) \otimes \alpha_i \gamma_j$$

Par de simples calculs, on vérifie que  $\psi$  est un morphisme de groupes additifs. Montrons que  $\psi$  est  $L \otimes_k K$ -linéaire. Soient

$\varepsilon \in End_L(V) \otimes_k K$ ,  $w \in V \otimes_k K$  et  $l \in L \otimes_k K$  tels que  $\varepsilon = \sum_i f_i \otimes \alpha_i$ ,  $w = \sum_i v_i \otimes \gamma_i$  et  $l = \sum_i l_i \otimes k_i$ , avec  $f_i \in End_L(V)$ ,

$v_i \in V$ ,  $\alpha_i, \gamma_i, k_i \in K$  et  $l_i \in L$ , pour tout  $i$ .

$$\begin{aligned}
\psi(l\varepsilon)(w) &= \psi\left(\left(\sum_i l_i \otimes k_i\right)\left(\sum_i f_i \otimes \alpha_i\right)\right)\left(\sum_i v_i \otimes \gamma_i\right) \\
&= \psi\left(\sum_{i,j} l_i f_j \otimes k_i \alpha_j\right)\left(\sum_i v_i \otimes \gamma_i\right) \\
&= \sum_{i,j,t} l_i f_j(v_t) \otimes k_i \alpha_j \gamma_t \\
&= \left(\sum_i l_i \otimes k_i\right) \sum_{j,t} f_j(v_t) \otimes \alpha_j \gamma_t \\
&= l\psi\left(\sum_j f_j \otimes \alpha_j\right)\left(\sum_t v_t \otimes \gamma_t\right) \\
&= l\psi(\varepsilon)(w).
\end{aligned}$$

Donc  $\psi$  est un morphisme de  $L \otimes_k K$ -modules.

Montrons que  $\psi$  est surjectif. Soient  $f \in \text{End}_{L \otimes_k K}(V \otimes_k K)$  et  $g$  la restriction de  $f$  à  $V = V \otimes 1$ .  $g$  est bien un  $L$ -endomorphisme de  $V$  car pour tout  $l \in L$ , pour tout  $v \in V$ ,

$$g(lv) = f((l \otimes 1)(v \otimes 1)) = (l \otimes 1)f(v \otimes 1) = lg(v).$$

De plus, pour tout  $\beta \in K$ , pour tout  $v \in V$ , on a :

$$\begin{aligned}
\psi(g \otimes 1)(v \otimes \beta) &= g(v) \otimes \beta \\
&= (1 \otimes \beta)(g(v) \otimes 1) \\
&= (1 \otimes \beta)f(v \otimes 1) \\
&= f(v \otimes \beta).
\end{aligned}$$

Donc  $\psi(g \otimes 1) = f$  et alors  $\psi$  est surjectif.

Par ailleurs, comme  $\dim_{L \otimes_k K}(V \otimes_k K) = \dim_L V$ , alors  $\text{End}_L(V) \otimes_k K$  et  $\text{End}_{L \otimes_k K}(V \otimes_k K)$  sont des  $L \otimes_k K$ -modules libres de même dimension  $\dim_L \text{End}_L(V)$ . On en déduit que  $\psi$  est un isomorphisme de  $L \otimes_k K$ -modules. ■

**Lemme 2.3.2.** *Soient  $L/k$ ,  $M/L$  et  $K/k$  des extensions de corps telles que  $L/k$  et  $M/L$  soient finies. Soit  $B$  une algèbre simple centrale sur  $L$ . Les modules  $(B \otimes_L M) \otimes_k K$  et  $(B \otimes_k K) \otimes_{L \otimes_k K} (M \otimes_k K)$  sont  $L \otimes_k K$ -isomorphes.*

**Preuve :** Soient

$$\psi : (B \otimes_L M) \otimes_k K \rightarrow (B \otimes_k K) \otimes_{L \otimes_k K} (M \otimes_k K)$$

et

$$\varphi : (B \otimes_k K) \otimes_{L \otimes_k K} (M \otimes_k K) \rightarrow (B \otimes_L M) \otimes_k K$$

les applications telles que pour tous éléments  $w$  de  $(B \otimes_L M) \otimes_k K$  et  $v$  de  $(B \otimes_k K) \otimes_{L \otimes_k K} (M \otimes_k K)$  donnés par  $w = \sum_{i,j} (b_{ij} \otimes m_{ij}) \otimes \alpha_i$  et  $v = \sum_{i,j,t} (b_{ij} \otimes \alpha_{ij}) \otimes (m_{it} \otimes \beta_{it})$ , avec  $b_{ij} \in B$ ,  $m_{ij} \in M$ ,  $\alpha_i, \alpha_{ij}, \beta_{ij} \in K$  pour tous  $i, j$ ,

$$\psi(w) = \sum_{i,j} (b_{ij} \otimes 1) \otimes (m_{ij} \otimes \alpha_i)$$

et

$$\varphi(v) = \sum_{i,j,t} (b_{ij} \otimes m_{it}) \otimes (\alpha_{ij} \beta_{it}).$$

On vérifie aisément que  $\psi$  et  $\varphi$  sont des morphismes de groupes additifs. Montrons que  $\psi$  et  $\varphi$  sont  $L \otimes_k K$ -linéaires. Pour tout  $l \in L \otimes_k K$  tel que  $l = \sum_i l_i \otimes k_i$ , avec  $l_i \in L$  et  $k_i \in K$ , pour tout  $i$ , on a :

$$\begin{aligned} \psi(lw) &= \psi\left(\sum_{i,j,t} (l_i b_{jt} \otimes m_{jt}) \otimes k_i \alpha_j\right) \\ &= \sum_{i,j,t} (l_i b_{jt} \otimes 1) \otimes (m_{jt} \otimes k_i \alpha_j) \\ &= \sum_i \left[ \sum_{j,t} ((l_i \otimes 1)(b_{jt} \otimes 1)) \otimes ((1 \otimes k_i)(m_{jt} \otimes \alpha_j)) \right] \\ &= \sum_i (l_i \otimes 1)(1 \otimes k_i) \sum_{j,t} (b_{jt} \otimes 1) \otimes (m_{jt} \otimes \alpha_j) \\ &= \sum_i (l_i \otimes k_i) \sum_{j,t} (b_{jt} \otimes 1) \otimes (m_{jt} \otimes \alpha_j) \\ &= l\psi(w) \end{aligned}$$

et

$$\begin{aligned}
\varphi(lv) &= \varphi\left(\sum_{i,j,t,r} (l_i b_{jt} \otimes \alpha_{jt}) \otimes (m_{jr} \otimes k_i \beta_{jr})\right) \\
&= \sum_{i,j,t,r} (l_i b_{jt} \otimes m_{jr}) \otimes (\alpha_{jt} k_i \beta_{jr}) \\
&= \sum_i (l_i \otimes k_i) \sum_{j,t,r} (b_{jt} \otimes m_{jr}) \otimes \alpha_{jt} \beta_{jr} \\
&= l\varphi(v).
\end{aligned}$$

Donc  $\psi$  et  $\varphi$  sont des morphismes de  $L \otimes_k K$ -modules.  
Soient  $b \in B$ ,  $m \in M$  et  $\alpha, \beta \in K$  ;

$$\begin{aligned}
\psi(\varphi((b \otimes \alpha) \otimes (m \otimes \beta))) &= \psi((b \otimes m) \otimes \alpha\beta) \\
&= (1 \otimes \alpha)\psi((b \otimes m) \otimes \beta) \\
&= (1 \otimes \alpha \otimes 1)[(b \otimes 1) \otimes (m \otimes \beta)] \\
&= [(1 \otimes \alpha)(b \otimes 1)] \otimes (m \otimes \beta) \\
&= (b \otimes \alpha) \otimes (m \otimes \beta)
\end{aligned}$$

et

$$\begin{aligned}
\varphi(\psi((b \otimes m) \otimes \beta)) &= \varphi((b \otimes 1) \otimes (m \otimes \beta)) \\
&= (b \otimes m) \otimes \beta.
\end{aligned}$$

On en déduit que  $\psi\varphi$  et  $\varphi\psi$  sont respectivement l'identité sur  $(B \otimes_k K) \otimes_{L \otimes_k K} (M \otimes_k K)$  et l'identité sur  $(B \otimes_L M) \otimes_k K$ . D'où  $\psi$  et  $\varphi$  sont des bijections et alors  $\psi$  est un isomorphisme de  $L \otimes_k K$ -modules. ■

**Lemme 2.3.3.** Soient  $L_1/k$  et  $L_2/k$  des extensions finies de corps et  $V_i$  un espace vectoriel de dimension finie sur  $L_i$ , pour  $i = 1, 2$ .  $V_1 \times V_2$  est un module sur  $L_1 \times L_2$  et les modules  $\text{End}_{L_1 \times L_2}(V_1 \times V_2)$  et  $\text{End}_{L_1}(V_1) \times \text{End}_{L_2}(V_2)$  sont  $L_1 \times L_2$ -isomorphes.

**Preuve :** Soit

$$\psi : \text{End}_{L_1}(V_1) \times \text{End}_{L_2}(V_2) \rightarrow \text{End}_{L_1 \times L_2}(V_1 \times V_2)$$

l'application définie par

$$\psi(f, g)(v, w) = (f(v), g(w))$$

pour tous  $(f, g) \in \text{End}_{L_1}(V_1) \times \text{End}_{L_2}(V_2)$  et  $(v, w) \in V_1 \times V_2$ . On vérifie aisément que  $\psi$  est un morphisme de  $L_1 \times L_2$ -modules.

Soit  $(f, g) \in \text{Ker}\psi$ ; alors pour tout  $(v, w) \in V_1 \times V_2$ ,  $(f(v), g(w)) = (0, 0)$  et donc  $(f, g) = 0$ . Il en résulte que  $\psi$  est injective.

Soient  $h \in \text{End}_{L_1 \times L_2}(V_1 \times V_2)$ ,  $f$  la restriction de  $h$  à  $V_1 = V_1 \times 0$  et  $g$  la restriction de  $h$  à  $V_2 = 0 \times V_2$ . Par l'intermédiaire de l'identification  $L_1 = L_1 \times 0$  et  $L_2 = 0 \times L_2$ , il est clair que  $f \in \text{End}_{L_1}(V_1)$  et  $g \in \text{End}_{L_2}(V_2)$ . De plus, pour tout  $(v, w) \in V_1 \times V_2$ , on a :

$$\psi(f, g)(v, w) = (f(v), g(w)) = h(v, 0) + h(0, w) = h(v, w)$$

Donc  $\psi(f, g) = h$  et alors  $\psi$  est surjective. D'où  $\psi$  est un isomorphisme de  $L_1 \times L_2$ -modules. ■

**Lemme 2.3.4.** *Soient  $L_1/k$  et  $L_2/k$  des extensions de corps,  $B_i$  et  $M_i$  des algèbres sur  $L_i$ , pour  $i = 1, 2$ . Les modules  $(B_1 \times B_2) \otimes_{L_1 \times L_2} (M_1 \times M_2)$  et  $(B_1 \otimes_{L_1} M_1) \times (B_2 \otimes_{L_2} M_2)$  sont  $L_1 \times L_2$ -isomorphes.*

**Preuve :** Soient

$$\psi : (B_1 \times B_2) \otimes_{L_1 \times L_2} (M_1 \times M_2) \rightarrow (B_1 \otimes_{L_1} M_1) \times (B_2 \otimes_{L_2} M_2)$$

et

$$\varphi : (B_1 \otimes_{L_1} M_1) \times (B_2 \otimes_{L_2} M_2) \rightarrow (B_1 \times B_2) \otimes_{L_1 \times L_2} (M_1 \times M_2)$$

les applications telles que pour tous éléments  $\alpha$  de  $(B_1 \times B_2) \otimes_{L_1 \times L_2} (M_1 \times M_2)$  et  $x$  de  $(B_1 \otimes_{L_1} M_1) \times (B_2 \otimes_{L_2} M_2)$ , donnés par  $\alpha = \sum_i (b_{1i}, b_{2i}) \otimes (m_{1i}, m_{2i})$  et  $x = (\sum_i b_{1i} \otimes m_{1i}, \sum_i b_{2i} \otimes m_{2i})$ , avec  $b_{ji} \in B_j$  et  $m_{ji} \in M_j$ , pour tout  $j = 1, 2$ , pour tout  $i$ ,

$$\psi(\alpha) = \left( \sum_i b_{1i} \otimes m_{1i}, \sum_i b_{2i} \otimes m_{2i} \right)$$

et

$$\varphi(x) = \sum_i (b_{1i}, b_{2i}) \otimes (m_{1i}, m_{2i}).$$

Par des simples calculs, on vérifie aisément que  $\psi$  et  $\varphi$  sont des morphismes de groupes additifs. Montrons qu'ils sont  $L_1 \times L_2$ -linéaires. Pour tout  $l = (l_1, l_2) \in L_1 \times L_2$ , on a :

$$\begin{aligned} \psi(l\alpha) &= \psi\left(\sum_i (l_1 b_{1i}, l_2 b_{2i}) \otimes (m_{1i}, m_{2i})\right) \\ &= \left(\sum_i l_1 b_{1i} \otimes m_{1i}, \sum_i l_2 b_{2i} \otimes m_{2i}\right) \\ &= (l_1, l_2) \left(\sum_i b_{1i} \otimes m_{1i}, \sum_i b_{2i} \otimes m_{2i}\right) \\ &= l\psi(\alpha) \end{aligned}$$

et

$$\begin{aligned} \varphi(lx) &= \varphi\left(\sum_i l_1 b_{1i} \otimes m_{1i}, \sum_i l_2 b_{2i} \otimes m_{2i}\right) \\ &= \sum_i (l_1 b_{1i}, l_2 b_{2i}) \otimes (m_{1i}, m_{2i}) \\ &= (l_1, l_2) \sum_i (b_{1i}, b_{2i}) \otimes (m_{1i}, m_{2i}) \\ &= l\varphi(x). \end{aligned}$$

Donc  $\psi$  et  $\varphi$  sont des morphismes de  $L_1 \times L_2$ -modules. De plus, par définition,

$$\psi(\varphi(x)) = \psi(\alpha) = x$$

et

$$\varphi(\psi(\alpha)) = \varphi(x) = \alpha$$

Donc  $\psi\varphi$  et  $\varphi\psi$  sont respectivement l'identité sur  $(B_1 \otimes_{L_1} M_1) \times (B_2 \otimes_{L_2} M_2)$  et l'identité sur  $(B_1 \times B_2) \otimes_{L_1 \times L_2} (M_1 \times M_2)$ . Donc  $\psi$  et  $\varphi$  sont des isomorphismes de  $L_1 \times L_2$ -modules. ■



**Lemme 2.3.5.** *Soient  $B$  une algèbre simple sur un corps  $k$  et  $K/k$  une extension de corps. Si  $B$  est déployée sur son centre, alors toutes les composantes simples de  $B_K = B \otimes_k K$  sont déployées sur leurs centres respectifs.*

**Preuve :** Soient  $B_1, B_2, \dots, B_s$  les composantes simples de  $B_K$ ,  $L$  le centre de  $B$  et  $L_i$  celui de  $B_i$ , pour tout  $i$ . Le centre de  $B_K$  est  $L \otimes_k K$  et est isomorphe à  $L_1 \times L_2 \times \dots \times L_s$ .  $B$  étant déployée sur  $L$ , elle est isomorphe à  $\text{End}_L(V)$ ,  $V$  étant un espace vectoriel sur  $L$  de dimension finie. D'une part, d'après le lemme 2.3.1,

$$\begin{aligned} B_K &\cong \text{End}_L(V) \otimes_k K \\ &\cong \text{End}_{L \otimes_k K}(V \otimes_k K) \\ &\cong \text{End}_{L_1 \times L_2 \times \dots \times L_s}(V \otimes_k K). \end{aligned}$$

Pour tout  $i$ , posons

$$V_i = \underbrace{(0 \times \dots \times 0 \times L_i \times 0 \times \dots \times 0)}_{s \text{ facteurs}} \cdot (V \otimes_k K),$$

de telle sorte que dans le produit

$$\underbrace{0 \times \dots \times 0 \times L_i \times 0 \times \dots \times 0}_{s \text{ facteurs}},$$

$L_i$  occupe la  $i$ -ème position. Il est clair que  $V_i$  est un espace vectoriel de dimension finie sur  $L_i$  et le  $L_1 \times L_2 \times \dots \times L_s$ -module  $(V \otimes_k K)$  est isomorphe à  $V_1 \times V_2 \times \dots \times V_s$ . Donc

$$\begin{aligned} B_K &\cong \text{End}_{L_1 \times L_2 \times \dots \times L_s}(V_1 \times V_2 \times \dots \times V_s) \\ &\cong \text{End}_{L_1}(V_1) \times \text{End}_{L_2}(V_2) \times \dots \times \text{End}_{L_s}(V_s) \quad (\text{lemme 2.3.3}). \end{aligned}$$

On en déduit que pour tout  $i$ ,  $B_i$  est isomorphe à  $\text{End}_{L_i}(V_i)$  et le résultat s'ensuit.

**Proposition 2.3.6.** *Soient  $B$  une algèbre simple sur un corps  $k$  et  $\sigma$  une involution de première espèce sur  $B$ . Soient  $K/k$  une*

extension de corps et  $B_1, B_2, \dots, B_s$  les composantes simples de  $B_K = B \otimes_k K$ . Soient  $\sigma_K =: \sigma \otimes \text{id}_K$  et  $\sigma_i$  la restriction de  $\sigma_K$  à  $B_i$ , pour tout  $i = 1, 2, \dots, s$ . Le type de  $\sigma$  est celui de  $\sigma_i$ , pour tout  $i$ .

**Preuve :** Soient  $L$  le centre de  $B$  et  $L_i$  celui de  $B_i$ , pour tout  $i$ . Le centre de  $B_K$  est  $L \otimes_k K$  et est isomorphe à  $L_1 \times L_2 \times \dots \times L_s$ . Deux cas peuvent être envisagés :

*Premier cas :* Si  $B$  est déployée sur  $L$ . D'après le lemme 2.3.5, pour tout  $i$ ,  $B_i$  est une  $L_i$ -algèbre simple centrale déployée et est donc isomorphe à  $\text{End}_{L_i}(V_i)$ , pour un certain  $L_i$ -espace vectoriel de dimension finie  $V_i$ . D'où

$$B_K \cong \text{End}_{L_1}(V_1) \times \text{End}_{L_2}(V_2) \times \dots \times \text{End}_{L_s}(V_s)$$

et

$$V_K = V \otimes_k K \cong V_1 \times V_2 \times \dots \times V_s.$$

Comme  $\sigma$  est une involution de première espèce, il en est de même pour  $\sigma_i$ , pour tout  $i$  et donc ces involutions sont adjointes à des formes bilinéaires non dégénérées. Soient alors  $b : V \times V \rightarrow L$  et  $b_i : V_i \times V_i \rightarrow L_i$  des formes bilinéaires non dégénérées telles que  $\sigma = \text{ad}_b$  et  $\sigma_i = \text{ad}_{b_i}$ , pour tout  $i$ . Soit

$$b_K : V_K \times V_K \rightarrow L_K = L \otimes_k K$$

la forme bilinéaire définie par  $b_K = b \otimes b'$  (où  $b'$  désigne la forme bilinéaire canonique sur  $K$  définie par  $b'(x, y) = xy$ , pour  $(x, y) \in K^2$ ), telle que  $\sigma_K$  soit l'involution adjointe à  $b_K$ . Pour tout  $i = 1, 2, \dots, s$ ,  $b_i$  est la restriction de  $b_K$  à

$$V_i = \underbrace{0 \times \dots \times 0 \times V_i \times 0 \times \dots \times 0}_{s \text{ facteurs}},$$

(de telle sorte que dans ce produit,  $V_i$  occupe la  $i$ -ème position) et  $b_K = b_1 \times b_2 \times \dots \times b_s$ .

Supposons  $\sigma$  orthogonale (resp. symplectique). Alors  $b$  est symétri-

que non alternée (resp. alternée); donc  $b_K = b \otimes b'$  est symétrique non alternée (resp. alternée), car  $b'$  est symétrique. Pour tout  $i$ , comme  $b_i$  est la restriction de  $b_K$  à  $V_i$ , on en déduit que  $b_i$  est symétrique non alternée (resp. alternée) et donc  $\sigma_i$  est orthogonale (resp. symplectique).

Réciproquement, supposons  $\sigma_i$  orthogonale (resp. symplectique), pour tout  $i$ ; alors  $b_i$  est symétrique non alternée (resp. alternée); par suite,  $b_K = b_1 \times b_2 \times \cdots \times b_s$  est symétrique non alternée (resp. alternée). Par ailleurs,  $b$  est la restriction de  $b_K$  à  $V = V \otimes 1$ . Donc  $b$  est symétrique non alternée (resp. alternée) et alors  $\sigma$  est orthogonale (resp. symplectique).

*Deuxième cas : Si  $B$  n'est pas déployée sur  $L$ . Soit  $M/L$  une extension finie de corps telle que  $B \otimes_L M$  soit déployée.*

$$\begin{aligned} M_K = M \otimes_k K &= M \otimes_L (L \otimes_k K) \\ &= M \otimes_L (L_1 \times L_2 \times \cdots \times L_s) \\ &= (M \otimes_L L_1) \times (M \otimes_L L_2) \times \cdots \times (M \otimes_L L_s) \\ &= M_1 \times M_2 \times \cdots \times M_s \end{aligned}$$

avec  $M_i = M \otimes_L L_i$ , pour tout  $i$ .  $M_i$  est une  $L_i$ -algèbre de dimension finie  $\dim_L M$ . D'une part, d'après le lemme 2.3.4,

$$\begin{aligned} B_K \otimes_{L_K} M_K &= (B_1 \times B_2 \times \cdots \times B_s) \otimes_{L_1 \times L_2 \times \cdots \times L_s} (M_1 \times M_2 \times \cdots \times M_s) \\ &= (B_1 \otimes_{L_1} M_1) \times (B_2 \otimes_{L_2} M_2) \times \cdots \times (B_s \otimes_{L_s} M_s) \end{aligned}$$

D'autre part, d'après le lemme 2.3.2,

$$B_K \otimes_{L_K} M_K = (B \otimes_k K) \otimes_{L \otimes_k K} (M \otimes_k K) = (B \otimes_L M) \otimes_k K.$$

Donc

$$(B \otimes_L M) \otimes_k K = (B_1 \otimes_{L_1} M_1) \times (B_2 \otimes_{L_2} M_2) \times \cdots \times (B_s \otimes_{L_s} M_s);$$

Pour tout  $i$ ,

$$B_i \otimes_{L_i} M_i = B_i \otimes_{L_i} (M \otimes_L L_i) \cong B_i \otimes_{L_i} (L_i \otimes_L M) \cong B_i \otimes_L M.$$

Soient  $B_{i1}, B_{i2}, \dots, B_{il_i}$  les composantes simples de  $B_i \otimes_{L_i} M_i = B_i \otimes_L M$ . Alors

$$(B \otimes_L M) \otimes_k K = \prod_{i,j} B_{ij}.$$

Posons  $\sigma_M = \sigma \otimes id_M$ ,  $(\sigma_M)_K = \sigma_M \otimes id_K$  et  $(\sigma_i)_{M_i} = \sigma_i \otimes id_{M_i}$ . Soit  $\sigma_{ij}$  la restriction de  $(\sigma_M)_K$  à  $B_{ij}$ .  $\sigma_{ij}$  est bien la restriction de  $(\sigma_i)_{M_i}$  et de  $(\sigma_i)_M$  à  $B_{ij}$ .  $B \otimes_L M$  étant déployée, d'après le lemme 2.3.5,  $B_{ij}$  est déployée pour tous  $i = 1, 2, \dots, s$  et  $j = 1, 2, \dots, l_i$ .

Supposons  $\sigma$  orthogonale (resp. symplectique). Alors  $\sigma_M$  est orthogonale (resp. symplectique) sur  $B \otimes_L M$ . D'où d'après le premier cas, pour tous  $i$  et  $j$ ,  $\sigma_{ij}$  est orthogonale (resp. symplectique) sur  $B_{ij}$  et donc  $\sigma_i$  est orthogonale (resp. symplectique).

Réciproquement, supposons  $\sigma_i$  orthogonale (resp. symplectique), pour tout  $i$ . Alors pour tout  $j$ ,  $\sigma_{ij}$  est orthogonale (resp. symplectique). Par suite, d'après le premier cas,  $\sigma_M$  est orthogonale (resp. symplectique). Il en résulte que  $\sigma$  est orthogonale (resp. symplectique). ■

**Théorème 2.3.7.** *Soient  $G$  un groupe fini,  $K/k$  une extension de corps telle que la caractéristique de  $k$  ne divise pas l'ordre de  $G$ . Les assertions suivantes sont équivalentes :*

- (1)  $G$  est ortho-ambivalent par rapport à  $k$  ;
- (2)  $G$  est ortho-ambivalent par rapport à  $K$ .

**Preuve :** Soit  $\sigma$  l'involution canonique de  $kG$  ;  $\sigma_K =: \sigma \otimes id_K$  est l'involution canonique de  $KG = kG \otimes_k K$ .

(1)  $\Rightarrow$  (2). Supposons (1) vérifiée. Soit  $B$  une composante simple de  $KG = kG \otimes_k K$ . Il existe alors une composante simple  $A$  de  $kG$  telle que  $B \subset A \otimes_k K$ . D'où  $B$  est une composante simple

de  $A \otimes_k K$ . Comme par hypothèse, la restriction de  $\sigma$  à  $A$  est orthogonale, alors d'après la proposition 2.3.6, la restriction de  $\sigma_K$  à  $B$  est orthogonale. Donc  $G$  est ortho-ambivalent par rapport à  $K$ .

(2)  $\Rightarrow$  (1). Supposons (2) vérifiée. Soit  $A$  une composante simple de  $kG$ . soient  $B_1, B_2, \dots, B_s$  les composantes simples de  $A \otimes_k K$ . Par hypothèse, la restriction de  $\sigma_K$  à  $B_i$  est orthogonale pour tout  $i$ . Donc d'après la proposition 2.3.6, la restriction de  $\sigma$  à  $A$  est orthogonale et alors  $G$  est ortho-ambivalent par rapport à  $k$ . ■

**Corollaire 2.3.8.** *Soient  $G$  un groupe fini et  $k$  un corps dont la caractéristique ne divise pas l'ordre de  $G$ . Les conditions suivantes sont équivalentes :*

- (1)  $G$  est ortho-ambivalent par rapport à  $k$  ;
- (2)  $G$  est ortho-ambivalent par rapport à  $\mathbb{C}$ .

**Preuve :**

Supposons (1) vérifiée. Si  $k$  est de caractéristique 0, alors, à isomorphisme près,  $\mathbb{Q}$  est son sous-corps premier. On utilise alors le théorème 2.3.7 en passant respectivement par les extensions  $k/\mathbb{Q}$  et  $\mathbb{C}/\mathbb{Q}$ , pour obtenir que  $G$  est ortho-ambivalent par rapport à  $\mathbb{C}$ . Si  $k$  est de caractéristique  $p$  premier, alors, à isomorphisme près,  $\mathbb{F}_p$  est son sous-corps premier. On utilise le théorème 2.3.7 en passant respectivement par les extensions  $k/\mathbb{F}_p$  et  $K_p/\mathbb{F}_p$ , pour obtenir que  $G$  est ortho-ambivalent par rapport à la clôture algébrique  $K_p$  de  $\mathbb{F}_p$ . On utilise enfin le corollaire 2.2.17 pour avoir que  $G$  est ortho-ambivalent par rapport à  $\mathbb{C}$ . Donc (1)  $\Rightarrow$  (2).

Supposons (2) vérifiée. Si  $k$  est de caractéristique 0, on utilise le théorème 2.3.7 en passant respectivement par les extensions  $\mathbb{C}/\mathbb{Q}$  et  $k/\mathbb{Q}$ , pour obtenir que  $G$  est ortho-ambivalent par rapport à  $k$ . Si  $k$  est de caractéristique  $p$  premier, le corollaire 2.2.17 donne que  $G$  est ortho-ambivalent par rapport à  $K_p$ . On utilise enfin le

théorème 2.3.7 en passant respectivement par les extensions  $K_p/\mathbb{F}_p$  et  $k/\mathbb{F}_p$ , pour obtenir que  $G$  est ortho-ambivalent par rapport  $k$ . D'où (2)  $\Rightarrow$  (1). ■

Le corollaire 2.3.8 nous permet de généraliser les résultats obtenus dans [33, proposition 3.3.7, page 49 et corollaire 2.1.4, page 14], pour un sous-corps de  $\mathbb{C}$  de la manière suivante :

**Corollaire 2.3.9.** *Soient  $n$  un entier naturel non nul et  $k$  un corps dont la caractéristique est nulle ou strictement supérieure à  $n$ .  $S_n$  est ortho-ambivalent par rapport à  $k$ .*

**Preuve :** Cela découle des corollaires 2.1.9 et 2.3.8. ■

**Corollaire 2.3.10.** *Soient  $n$  un entier naturel non nul et  $k$  un corps dont la caractéristique ne divise pas l'ordre du groupe diédral  $D_n$  d'ordre  $2n$ .  $D_n$  est ortho-ambivalent par rapport à  $k$ .*

**Preuve :** Cela découle de [33, corollaire 2.1.4, page 14] et du corollaire 2.3.8. ■

## 2.4 Quelques résultats.

Dans cette section, nous constituons un répertoire des résultats déduits immédiatement de ceux existant dans la littérature par l'intermédiaire des résultats obtenus ci-dessus. Pour y arriver il nous est indispensable de préciser certaines notions.

**Définition 2.4.1.** [42, page 300] *Un groupe fini  $G$  est dit totalement orthogonal si tous ses caractères irréductibles sont de type 1.*

**Proposition 2.4.2.** *Soient  $G$  un groupe fini et  $k$  un corps dont la caractéristique ne divise pas l'ordre de  $G$ . Les assertions suivantes sont équivalentes :*

(1)  $G$  est totalement orthogonal ;

(2)  $G$  ortho-ambivalent par rapport à  $\mathbb{C}$  ;

(3)  $G$  ortho-ambivalent par rapport à  $k$ .

*Preuve* : Cela découle des corollaires 2.1.21 et 2.3.8. ■

**Définition 2.4.3.** *Dans un groupe fini  $G$ , on appelle involution de  $G$  un élément de  $G$  d'ordre 2.*

**Définition 2.4.4.** [25, définition (7.1), page 99] *Un groupe  $G$  est dit groupe de Frobenius s'il existe un sous-groupe propre  $H$  de  $G$  tel que pour tout  $x \in G - H$ ,  $H \cap (x^{-1}Hx) = 1$  ; dans ce cas, on dit que  $G$  est un groupe de Frobenius de complément  $H$ .*

Dans [42], Wang et Grove trouvent les résultats suivants sur les groupes totalement orthogonaux :

**Proposition 2.4.5.** [42, théorème 3.3, page 301] *Si un groupe est totalement orthogonal, il est engendré par des involutions.* ■

**Proposition 2.4.6.** [42, proposition 3.6, page 302] *Si  $H$  est un sous-groupe d'indice 2 d'un groupe fini totalement orthogonal  $G$ , alors  $H$  ne possède aucun caractère irréductible de type  $-1$ .* ■

**Proposition 2.4.7.** [42, corollaire 3.8, page 302] *Si  $H$  est un sous-groupe d'indice 2 d'un groupe fini totalement orthogonal  $G$ , alors  $H$  est totalement orthogonal si et seulement si  $H$  est ambivalent.* ■

**Proposition 2.4.8.** [42, théorème 3.11, page 302] *Un 2-groupe  $G$  est totalement orthogonal si et seulement si  $G$  est ambivalent, engendré par des involutions et aucun sous-groupe de  $G$  d'indice 2, ne possède un caractère irréductible de type  $-1$ .* ■

**Proposition 2.4.9.** [42, corollaire 5.6, page 307] *Si  $G$  est un groupe de Frobenius, alors  $G$  est totalement orthogonal si et seulement si  $G$  est 2-uniforme (c'est-à-dire  $\{1, 2\}$  est l'ensemble des degrés des caractères irréductibles de  $G$ ).* ■

**Proposition 2.4.10.** [42, théorème 6.2, page 307] et [42, théorème 6.5, page 308] *Pour tout entier naturel non nul  $n$ , tout 2-sous-groupe de Sylow du groupe symétrique  $S_n$  (resp. du groupe alterné  $A_n$ ) est totalement orthogonal. ■*

**Proposition 2.4.11.** [42, page 307] *Pour tout  $n \in \{1, 2, 5, 6, 10, 14\}$ , le groupe alterné  $A_n$  est totalement orthogonal.*

Il est possible d'en déduire immédiatement des résultats sur l'ortho-ambivalence d'un groupe fini par rapport à un corps, en se servant de la proposition 2.4.2.

Soient alors  $G$  un groupe fini et  $k$  un corps dont la caractéristique ne divise pas l'ordre de  $G$ . On a les résultats suivants :

**Théorème 2.4.12.** *Si  $G$  est ortho-ambivalent par rapport à  $k$ , alors  $G$  est engendré par des involutions.*

*Preuve :* cela découle des propositions 2.4.2 et 2.4.5. ■

**Proposition 2.4.13.** *On suppose que  $G$  est ortho-ambivalent par rapport à  $k$ . Soit  $H$  un sous-groupe de  $G$  d'indice 2. Alors  $H$  ne possède aucun caractère irréductible de type  $-1$ .*

*Preuve :* cela découle des propositions 2.4.2 et 2.4.6. ■

De la proposition 2.4.13 et du corollaire 2.3.9, il résulte que pour tout entier naturel non nul  $n$ , si  $A_n$  désigne le groupe alterné (d'ordre  $\frac{n!}{2}$ , si  $n > 1$ ), il n'existe aucune composante simple de  $\mathbb{C}A_n$  sur laquelle l'involution canonique est symplectique.

**Proposition 2.4.14.** [42, Corollaire 3.8, page 302] *On suppose que  $G$  est ortho-ambivalent par rapport à  $k$ . Soit  $H$  un sous-groupe de  $G$  d'indice 2. Alors  $H$  est ortho-ambivalent par rapport à  $k$  si et seulement si  $H$  est ambivalent.*

*Preuve :* Conséquence de la proposition 2.4.13. ■



**Remarque 2.4.15.** *J. Berggren [8, théorème 1.2, page 290] montre que pour que le groupe alterné  $A_n$  soit ambivalent, il faut et il suffit que  $n \in \{1, 2, 5, 6, 10, 14\} =: \mathcal{A}$  [42, page 307]. Donc d'après la proposition 2.4.14 et le corollaire 2.3.8, pour tout  $n \in \mathcal{A}$ ,  $A_n$  est ortho-ambivalent par rapport à tout corps dont la caractéristique ne divise pas l'ordre de  $A_n$ .*

**Proposition 2.4.16.** *Pour tout entier naturel non nul  $n$ , tout 2-sous-groupe de Sylow du groupe symétrique  $S_n$  (resp. du groupe alterné  $A_n$ ) est ortho-ambivalent par rapport à tout corps de caractéristique différente de 2.*

*Preuve :* cela découle des propositions 2.4.2 et 2.4.10. ■

**Proposition 2.4.17.** *Si  $G$  est un groupe de Frobenius, alors  $G$  est ortho-ambivalent par rapport à  $k$  si et seulement si  $G$  est 2-uniforme.*

*Preuve :* cela découle des propositions 2.4.2 et 2.4.10. ■

Le résultat suivant donne une condition nécessaire et suffisante pour qu'un 2-groupe fini soit ortho-ambivalent par rapport à  $k$ .

**Théorème 2.4.18.** *Soit  $G$  un 2-groupe et  $k$  un corps dont la caractéristique est différente de 2. Les conditions suivantes sont équivalentes :*

- (1)  *$G$  est ortho-ambivalent par rapport à  $k$ .*
- (2)  *$G$  est ambivalent, engendré par des involutions et aucun sous-groupe de  $G$  d'indice 2, ne possède un caractère irréductible de type  $-1$ .*

*Preuve :* cela découle des propositions 2.4.2 et 2.4.8. ■



# Chapitre 3

## Quelques groupes particuliers

Soit  $G$  un groupe fini et  $k$  un corps dont la caractéristique ne divise pas l'ordre de  $G$ . Dans le chapitre 2, il est établi que lorsque la restriction de l'involution canonique à chaque composante simple de  $\mathbb{C}G$  est une involution de première espèce, on peut en déduire le type de la restriction de l'involution canonique à chaque composante simple de  $kG$ . Dans ce chapitre, nous nous préoccupons de déterminer le type de la restriction de l'involution canonique à chaque composante simple de  $\mathbb{C}G$ . Nous dégageons quelques particularités des  $p$ -groupes ( $p$  entier naturel premier). Si  $G$  est un 2-groupe, le théorème 2.4.18 donne des conditions nécessaires et suffisantes pour que  $G$  soit ortho-ambivalent ; nous nous intéressons plus particulièrement aux 2-groupes extra-spéciaux et aux 2-groupes spéciaux.

### 3.1 Quelques résultats préliminaires

Dans cette section, nous établissons des résultats généraux qui nous sont utiles pour démontrer certains de ceux obtenus dans les sections suivantes.

**Proposition 3.1.1.** *Soient  $G$  un groupe fini,  $\sigma$  l'involution canonique de  $\mathbb{C}G$ ,  $\rho$  une  $\mathbb{C}$ -représentation irréductible de  $G$  de degré  $n$  et  $A$  la composante simple de  $\mathbb{C}G$  correspondant à  $\rho$ . Si  $\sigma(A) = A$ , alors  $\rho(Z(G)) \subset \mu_2$  et on a :*

- (1) *Si  $\rho(Z(G)) = 1$ , alors il existe un unique morphisme de groupes  $\rho' : \frac{G}{Z(G)} \rightarrow GL_n(\mathbb{C})$  tel que  $\rho = \rho'\varphi$ ,  $\varphi$  étant l'épimorphisme canonique de  $G$  sur  $\frac{G}{Z(G)}$ .*
- (2) *Si  $\rho(Z(G)) = \mu_2$ , alors il existe un morphisme de groupes  $\rho'' : \frac{G}{Z(G)} \rightarrow \frac{\rho(G)}{\mu_2}$  tel que  $\rho''\varphi = \varphi'\rho$ ,  $\varphi'$  étant l'épimorphisme canonique de  $\rho(G)$  sur  $\frac{\rho(G)}{\mu_2}$ .*

**Preuve :** Soit  $e$  l'élément idempotent centralement primitif tel que  $A = \mathbb{C}Ge$  et  $\chi$  le caractère de  $\rho$ . Comme  $\sigma(A) = A$ , alors  $\sigma(e) = e$ . Or

$$e = \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(g^{-1})g$$

et

$$\sigma(e) = \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(g^{-1})g^{-1} = \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(g)g.$$

Donc pour tout  $g \in G$ ,  $\chi(g) = \chi(g^{-1})$ . Par ailleurs  $\rho(G)$  contient une base de  $M_n(\mathbb{C})$  car  $\rho$  est irréductible, donc

$$\rho(Z(G)) \subset Z(GL_n(\mathbb{C})) = \mathbb{C}^\times.$$

Il en résulte que pour tout  $g \in Z(G)$ ,  $\rho(g) = \lambda = \lambda I_n$  ( $I_n$  étant la matrice unité d'ordre  $n$ ), avec  $\lambda \in \mathbb{C}^\times$ ; d'où

$$\chi(g) = \text{Tr}(\rho(g)) = n\lambda = n\rho(g)$$

et  $\chi(g^{-1}) = n\rho(g^{-1})$ ; donc  $\rho(g) = \rho(g^{-1})$ ; par suite  $(\rho(g))^2 = 1$  et donc  $\rho(g) \in \mu_2$ . D'où  $\rho(Z(G)) \subset \mu_2$ .

- 1. Si  $\rho(Z(G)) = 1$ , alors  $Z(G) \subset \ker \rho$  et donc il existe un unique morphisme de groupes  $\rho' : \frac{G}{Z(G)} \rightarrow GL_n(\mathbb{C})$  tel que  $\rho = \rho'\varphi$ .

**2.** Si  $\rho(Z(G)) = \mu_2$ , soit  $\bar{\rho} : \frac{G}{Z(G)} \rightarrow \frac{\rho(G)}{\mu_2}$  tel que  $gZ(G) \mapsto \rho(g)\mu_2$ .  $\bar{\rho}$  est bien définie, en effet, pour tous  $g, h \in G$ ,

$$gZ(G) = hZ(G) \Rightarrow g^{-1}h \in Z(G) \Rightarrow \rho(g^{-1}h) \in \mu_2$$

$$\Rightarrow \rho(g)\mu_2 = \rho(h)\mu_2 \Rightarrow \bar{\rho}(gZ(G)) = \bar{\rho}(hZ(G)).$$

Comme  $\rho$  est un morphisme de groupes, il en est de même pour  $\bar{\rho}$ . De plus, pour tout  $g \in G$ ,

$$(\bar{\rho}\varphi)(g) = \bar{\rho}(gZ(G)) = \rho(g)\mu_2 = \varphi'(\rho(g)) = (\varphi'\rho)(g). \blacksquare$$

**Proposition 3.1.2.** *Soit  $G$  un groupe fini,  $H$  un sous-groupe normal de  $G$ ,  $\rho : G \rightarrow GL(V)$  et  $\psi : \frac{G}{H} \rightarrow GL(V)$  deux représentations de groupes telles que  $\rho = \psi\varphi$ , de caractères respectifs  $\chi$  et  $\chi'$ , où  $\varphi : G \rightarrow \frac{G}{H}$  désigne la surjection canonique. Soient  $\sigma$  (resp.  $\sigma'$ ) l'involution canonique de  $\mathbb{C}G$  (resp.  $\mathbb{C}\frac{G}{H}$ ) et  $\varphi_{\mathbb{C}G}$  le prolongement naturel de  $\varphi$  à  $\mathbb{C}G$  défini par :*

$$\varphi_{\mathbb{C}G}\left(\sum_{g \in G} a_g g\right) = \sum_{g \in G} a_g \varphi(g).$$

- (1)  $\rho$  est irréductible si et seulement si  $\psi$  l'est.
- (2)  $\varphi_{\mathbb{C}G}\sigma = \sigma'\varphi_{\mathbb{C}G}$ .
- (3) On suppose que  $\rho$  est irréductible ; soient  $A$  (resp.  $B$ ) la composante simple de  $\mathbb{C}G$  (resp.  $\mathbb{C}\frac{G}{H}$ ) et  $e$  (resp.  $e'$ ) l'élément idempotent centralement primitif de  $\mathbb{C}G$  (resp.  $\mathbb{C}\frac{G}{H}$ ) correspondant à  $\rho$  (resp.  $\psi$ ).
  - (a)  $\varphi_{\mathbb{C}G}(e) = e'$
  - (b) Si  $\sigma(A) = A$ , alors  $\sigma'(B) = B$  et les restrictions respectives de  $\sigma$  à  $A$  et de  $\sigma'$  à  $B$  sont des involutions de même type.

*Preuve :*

1. Si  $\rho$  est irréductible, alors  $\psi$  est irréductible, sinon il existe un sous-espace vectoriel non trivial  $W$  de  $V$  tel que pour tout  $g \in G$ ,  $\psi(gH)(W) = W$  c'est-à-dire

$$\rho(g)(W) = \psi(\rho(g))(W) = \psi(gH)(W) = W$$

et donc  $\rho$  est réductible, ce qui est absurde. Réciproquement, Si  $\psi$  est irréductible, alors  $\rho$  est irréductible, sinon il existe un sous-espace vectoriel non trivial  $W$  de  $V$  tel que pour tout  $g \in G$ ,  $\rho(g)(W) = W$  c'est-à-dire  $\psi(gH)(W) = \rho(g)(W) = W$  et donc  $\psi$  est réductible, ce qui est contradictoire.

2. Soit  $\alpha = \sum_{g \in G} a_g g$  un élément de  $\mathbb{C}G$ .

$$\begin{aligned} (\varphi_{\mathbb{C}G}\sigma)(\alpha) &= \varphi_{\mathbb{C}G}\left(\sum_{g \in G} a_g g^{-1}\right) \\ &= \sum_{g \in G} a_g (\varphi(g))^{-1} \\ &= \sigma'\left(\sum_{g \in G} a_g \varphi(g)\right) \\ &= \sigma'(\varphi_{\mathbb{C}G}(\alpha)) \\ &= (\sigma' \varphi_{\mathbb{C}G})(\alpha) \end{aligned}$$

**3.** Supposons l'hypothèse vérifiée.

a) Pour tout  $g \in G$ ,  $\chi(g) = \text{Tr}(\rho'(\varphi(g))) = \chi'(\varphi(g))$  et donc

$$\begin{aligned}
 \varphi_{\mathbb{C}G}(e) &= \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(g^{-1}) \varphi(g) \\
 &= \frac{\chi'(\varphi(1))}{|G|} \sum_{\varepsilon \in \frac{G}{H}} \sum_{g \in \varepsilon} \chi'(\varphi(g^{-1})) \varphi(g) \\
 &= \frac{\chi'(1)}{|G|} \sum_{\varepsilon \in \frac{G}{H}} \sum_{g \in \varepsilon} \chi'(\varepsilon^{-1}) \varepsilon \\
 &= \frac{\chi'(1)}{|G|} \sum_{\varepsilon \in \frac{G}{H}} |\varepsilon| \chi'(\varepsilon^{-1}) \varepsilon \\
 &= \frac{\chi'(1)|H|}{|G|} \sum_{\varepsilon \in \frac{G}{H}} \chi'(\varepsilon^{-1}) \varepsilon \\
 &= e'.
 \end{aligned}$$

b) Si  $\sigma(A) = A$ , alors  $\sigma(e) = e$  (corollaire 2.1.3) et de (2) et (3a), il résulte que  $\sigma'(e') = e'$ ; donc  $\sigma'(B) = B$ . De plus,

- Si la restriction de  $\sigma$  à  $A$  est orthogonale (resp. symplectique), il existe une forme bilinéaire non dégénérée symétrique non alternée (resp. alternée)  $b : V \times V \rightarrow \mathbb{C}$  qui est  $G$ -invariante.  $b$  est  $\frac{G}{H}$ -invariante, en effet, pour tout  $g \in G$ , pour tous  $x, y \in V$ , on a :

$$\begin{aligned}
 b(\psi(gH)(x), \psi(gH)(y)) &= b(\rho(g)(x), \rho(g)(y)) \\
 &= b(x, y),
 \end{aligned}$$

$b$  étant  $G$ -invariante. Donc la restriction de  $\sigma'$  à  $B$  est orthogonale (resp. symplectique).

- Réciproquement, si la restriction de  $\sigma'$  à  $B$  est orthogonale (resp. symplectique), il existe une forme bilinéaire non dégénérée symétrique non alternée (resp. alternée)  $b : V \times V \rightarrow \mathbb{C}$  qui est  $\frac{G}{H}$ -invariante.  $b$  est  $G$ -invariante, en effet, pour tout  $g \in G$ , pour tous  $x, y \in V$ ,

on a :

$$\begin{aligned} b(\rho(g)(x), \rho(g)(y)) &= b(\psi(gH)(x), \psi(gH)(y)) \\ &= b(x, y), \end{aligned}$$

$b$  étant  $\frac{G}{H}$ -invariante. Donc la restriction de  $\sigma$  à  $A$  est orthogonale (resp. symplectique). ■

La première partie de la proposition 3.1.2 traduit le résultat donné dans [25, lemme 2.22 (c), page 24].

Si  $G_1$  et  $G_2$  sont des groupes finis, alors  $\mathbb{C}(G_1 \times G_2) \cong (\mathbb{C}G_1 \otimes_{\mathbb{C}} \mathbb{C}G_2)$  (voir [34, lemme 3.4, page 25]) et ses composantes simples sont de la forme  $A = A_1 \otimes_{\mathbb{C}} A_2$ , où  $A_i$  est une composante simple de  $\mathbb{C}G_i$ , pour tout  $i = 1, 2$ . On a le résultat suivant :

**Lemme 3.1.3.** *Soient  $G_1$  et  $G_2$  des groupes finis,  $\sigma_i$  l'involution canonique de  $\mathbb{C}G_i$  ( $i = 1, 2$ ),  $A_i$  une composante simple de  $\mathbb{C}G_i$  telle que  $\sigma_i(A_i) = A_i$ ,  $\sigma = \sigma_1 \otimes \sigma_2$  l'involution canonique de  $\mathbb{C}(G_1 \times G_2) \cong (\mathbb{C}G_1 \otimes_{\mathbb{C}} \mathbb{C}G_2)$  et  $A = A_1 \otimes_{\mathbb{C}} A_2$ .*

- (1) *Si la restriction de  $\sigma_i$  à  $A_i$  est orthogonale (resp. symplectique) pour tout  $i = 1, 2$ , alors la restriction de  $\sigma$  à  $A$  est orthogonale.*
- (2) *Si l'une des restrictions de  $\sigma_i$  à  $A_i$  est orthogonale, l'autre symplectique, alors la restriction de  $\sigma$  à  $A$  est symplectique.*

*Preuve :* Soit  $\rho_i : G_i \rightarrow GL(V_i)$  la représentation irréductible correspondant à  $A_i$ , pour  $i = 1, 2$ . Alors  $\rho = \rho_1 \otimes \rho_2 : G_1 \times G_2 \rightarrow GL(V_1 \otimes V_2)$  est la représentation irréductible correspondant à  $A = A_1 \otimes_{\mathbb{C}} A_2$ . Rappelons que  $\rho$  est définie par

$$\rho(g_1, g_2)(v_1 \otimes v_2) = \rho_1(g_1)(v_1) \otimes \rho_2(g_2)(v_2),$$

pour tout  $(g_1, g_2) \in G_1 \times G_2$ , pour tout  $(v_1, v_2) \in V_1 \times V_2$  et est irréductible d'après [38, théorème 10, page 27].



1. Supposons que la restriction de  $\sigma_i$  à  $A_i$  est orthogonale (resp. symplectique) pour tout  $i = 1, 2$ . Alors il existe une forme bilinéaire symétrique (resp. antisymétrique) non dégénérée  $b_i : V_i \times V_i \rightarrow \mathbb{C}$  qui est  $G_i$ -invariante. Soit  $b = b_1 \otimes b_2 : (V_1 \otimes V_2) \times (V_1 \otimes V_2) \rightarrow \mathbb{C}$  définie par

$$b(v_1 \otimes v_2, w_1 \otimes w_2) = b_1(v_1, w_1)b_2(v_2, w_2).$$

On vérifie que  $b$  est une forme bilinéaire symétrique non dégénérée. Pour tous  $(g_1, g_2) \in G_1 \times G_2$ ,  $v_1, w_1 \in V_1$  et  $v_2, w_2 \in V_2$ , on a :

$$\begin{aligned} & b(\rho(g_1, g_2)(v_1 \otimes v_2), \rho(g_1, g_2)(w_1 \otimes w_2)) \\ &= (b_1 \otimes b_2)(\rho_1(g_1)(v_1) \otimes \rho_2(g_2)(v_2), \rho_1(g_1)(w_1) \otimes \rho_2(g_2)(w_2)) \\ &= b_1(\rho_1(g_1)(v_1), \rho_1(g_1)(w_1))b_2(\rho_2(g_2)(v_2), \rho_2(g_2)(w_2)) \\ &= b_1(v_1, w_1)b_2(v_2, w_2) \\ &= b(v_1 \otimes v_2, w_1 \otimes w_2). \end{aligned}$$

Donc  $b$  est  $G_1 \times G_2$ -invariante et alors la restriction de  $\sigma$  à  $A$  est une involution orthogonale.

2. Supposons par exemple que la restriction de  $\sigma_1$  à  $A_1$  est orthogonale et la restriction de  $\sigma_2$  à  $A_2$  est symplectique. Alors il existe une forme bilinéaire symétrique non dégénérée  $b_1 : V_1 \times V_1 \rightarrow \mathbb{C}$  qui est  $G_1$ -invariante et une forme bilinéaire antisymétrique non dégénérée  $b_2 : V_2 \times V_2 \rightarrow \mathbb{C}$  qui est  $G_2$ -invariante. Soit  $b = b_1 \otimes b_2 : (V_1 \otimes V_2) \times (V_1 \otimes V_2) \rightarrow \mathbb{C}$  définie par

$$b(v_1 \otimes v_2, w_1 \otimes w_2) = b_1(v_1, w_1)b_2(v_2, w_2).$$

On vérifie de même que  $b$  est une forme bilinéaire antisymétrique non dégénérée qui est  $G_1 \times G_2$ -invariante et alors la restriction de  $\sigma$  à  $A$  est une involution symplectique. ■

Le lemme 3.1.3 se généralise par induction de la manière suivante :

**Proposition 3.1.4.** *Soient  $G_1, G_2, \dots, G_s$  des groupes finis,  $\sigma_i$  l'involution canonique de  $\mathbb{C}G_i$  ( $i = 1, 2, \dots, s$ ),  $A_i$  une composante simple de  $\mathbb{C}G_i$  telle que  $\sigma_i(A_i) = A_i$ ,  $\sigma = \sigma_1 \otimes \sigma_2 \otimes \dots \otimes \sigma_s$  l'involution canonique de  $\mathbb{C}(G_1 \times G_2 \times \dots \times G_s) \cong (\mathbb{C}G_1 \otimes_{\mathbb{C}} \mathbb{C}G_2 \otimes_{\mathbb{C}} \dots \otimes_{\mathbb{C}} \mathbb{C}G_s)$  et  $A = A_1 \otimes_{\mathbb{C}} A_2 \otimes_{\mathbb{C}} \dots \otimes_{\mathbb{C}} A_s$ .*

- (1) *Si un nombre pair des restrictions de  $\sigma_i$  à  $A_i$  ( $i = 1, 2, \dots, s$ ) sont symplectiques, alors la restriction de  $\sigma$  à  $A$  est orthogonale.*
- (2) *Si un nombre impair des restrictions de  $\sigma_i$  à  $A_i$  ( $i = 1, 2, \dots, s$ ) sont symplectiques, alors la restriction de  $\sigma$  à  $A$  est symplectique. ■*

**Proposition 3.1.5.** *Si  $G$  est un groupe cyclique d'ordre  $n$ ,  $n$  entier naturel,  $G = \langle x \rangle$  et  $\omega$  est une racine primitive  $n$ -ième de l'unité, alors la famille des  $n$  caractères irréductibles de  $G$  est  $(\chi_k)_{0 \leq k \leq n-1}$ , avec  $\chi_k(x) = \omega^k$ . Soient  $e_k$  l'élément idempotent centralement primitif de  $\mathbb{C}G$  correspondant à  $\chi_k$  et  $\sigma$  l'involution canonique sur  $\mathbb{C}G$ . Alors  $\sigma(e_k) = e_{n-k}$ .*

**Preuve :** La première partie de la proposition est triviale. D'autre part, comme

$$e_k = \frac{1}{n} \sum_{j=0}^{n-1} \chi_k(x^{-j}) x^j = \frac{1}{n} \sum_{j=0}^{n-1} \omega^{-kj} x^j,$$

alors

$$\begin{aligned}
\sigma(e_k) &= \frac{1}{n} \sum_{j=0}^{n-1} \omega^{-kj} x^{-j} \\
&= \frac{1}{n} \sum_{j=0}^{n-1} \omega^{-n^2+nj+nk-kj} x^{n-j} \\
&= \frac{1}{n} \sum_{j=0}^{n-1} \omega^{-(n-k)(n-j)} x^{n-j} \\
&= \frac{1}{n} \sum_{j=0}^{n-1} \chi_{n-k}(x^{-(n-j)}) x^{n-j} \\
&= e_{n-k}.
\end{aligned}$$

D'où le résultat. ■

Rappelons que si  $G$  est un groupe, on appelle sous-groupe dérivé de  $G$  et on note  $G'$  ou  $[G, G]$  le sous-groupe de  $G$  engendré par les commutateurs  $[x, y] := x^{-1}y^{-1}xy$ , avec  $x, y \in G$ . Le résultat suivant donne le nombre de caractères irréductibles de degré 1 d'un groupe fini.

**Proposition 3.1.6.** *Soit  $G$  un groupe fini. Le nombre de caractères linéaires de  $G$  égale l'indice  $(G : G')$  du sous-groupe dérivé de  $G$  dans  $G$ .*

*Preuve :* voir [25, corollaire 2.23(b), page 25] ou [15, proposition 6.4.2, page 234]. ■

## 3.2 Des p-groupes.

Dans cette section, nous démontrons que si  $G$  est un  $p$ -groupe fini ( $p$  entier naturel premier  $> 2$ ), l'unique composante simple de  $\mathbb{C}G$  fixée par l'involution canonique est celle correspondant au caractère trivial : ce cas ne nous intéresse pas. Nous établissons que

si  $G$  est un 2-groupe non trivial, alors au moins deux composantes simples de  $\mathbb{C}G$  sont fixées par l'involution canonique et les sous-groupes de  $G$  d'indice deux sont en correspondance biunivoque avec les composantes simples de  $\mathbb{C}G$  de degré un, non triviales stables par l'involution canonique.

**Théorème 3.2.1.** *Soient  $p$  un entier premier  $> 2$  et  $G$  un  $p$ -groupe d'ordre  $p^r$  ( $r$  entier positif) et  $\sigma$  l'involution canonique de  $\mathbb{C}G$ . La seule composante simple de  $\mathbb{C}G$  fixée par  $\sigma$  est celle correspondant au caractère trivial de  $G$ .*

**Preuve :** Nous allons raisonner par induction sur  $r$ .

Pour  $r = 0$ , le résultat est trivial.

Pour  $r = 1$ ,  $G$  est d'ordre  $p$  et donc  $G$  est cyclique. Supposons que

$$G = \langle x \mid \text{ord}(x) = p \rangle.$$

D'après la proposition 3.1.5, si  $\omega$  est une racine primitive  $p$ -ième de l'unité, la famille des  $p$  caractères irréductibles de  $G$  est  $(\chi_k)_{0 \leq k \leq p-1}$ , avec  $\chi_k(x) = \omega^k$ ; de plus si  $e_k$  est l'élément idempotent centralement primitif correspondant à  $\chi_k$ , alors  $\sigma(e_k) = e_{p-k}$ . Pour  $A_k = \mathbb{C}Ge_k$ ,  $\sigma(A_k) = A_{p-k} \neq A_k$  si  $k \neq 0$ ,  $p$  étant premier  $> 2$ .

Soit maintenant  $G$  un  $p$ -groupe d'ordre  $p^r$  ( $r$  entier  $> 0$ ). Soit  $A$  une composante simple de  $\mathbb{C}G$  de degré  $n$  telle que  $\sigma(A) = A$ ; soit  $\rho : G \rightarrow GL_n(\mathbb{C})$  la représentation irréductible correspondant à  $A$ , de caractère associé  $\chi$ ,  $e$  l'élément idempotent centralement primitif correspondant à  $\rho$ . Soient  $\sigma'$  l'involution canonique de  $\mathbb{C}\frac{G}{Z(G)}$ ,  $\varphi : G \rightarrow \frac{G}{Z(G)}$  l'épimorphisme canonique de groupes et  $\varphi_{\mathbb{C}G} : \mathbb{C}G \rightarrow \mathbb{C}\frac{G}{Z(G)}$  le prolongement naturel de  $\varphi$ . D'après la proposition 3.1.1,  $\rho(Z(G)) \subset \mu_2$ . Comme  $G$  est un  $p$ -groupe non trivial, alors  $|Z(G)| \geq p$  et donc  $|Z(G)| = p^s$ ,  $s$  étant un entier tel que  $1 \leq s \leq r$ . D'où pour tout  $g \in Z(G)$ ,  $(\rho(g))^{p^s} = 1$  et donc  $\rho(Z(G)) \subset \mu_{p^s}$ . Par suite,  $\rho(Z(G)) \subset \mu_2 \cap \mu_{p^s} = 1$  ( $p^s$  étant impair). Donc  $Z(G) \subset \ker \rho$ . Il existe alors un unique morphisme de groupes  $\rho' : \frac{G}{Z(G)} \rightarrow GL_n(\mathbb{C})$  tel que  $\rho = \rho' \varphi$ ;  $\rho'$  est une représentation irréductible de  $\frac{G}{Z(G)}$ ,  $\rho$  étant irréductible (proposi-

tion 3.1.2). Soient  $\chi'$  le caractère associé à  $\rho'$ ,  $e'$  l'élément idempotent centralement primitif correspondant à  $\rho'$  et  $A' = \mathbb{C} \frac{G}{Z(G)} e'$ . D'après la proposition 3.1.2,  $\varphi_{\mathbb{C}G} \sigma = \sigma' \varphi_{\mathbb{C}G}$  et  $\varphi_{\mathbb{C}G}(e) = e'$ . Donc

$$\sigma'(e') = \sigma'(\varphi_{\mathbb{C}G}(e)) = \varphi_{\mathbb{C}G}(\sigma(e)) = \varphi_{\mathbb{C}G}(e) = e'$$

et alors  $\sigma'(A') = A'$  (corollaire 2.1.3). Comme  $|Z(G)| \geq p$ , alors  $|\frac{G}{Z(G)}| < |G|$ ; d'où d'après l'hypothèse d'induction,  $\rho' = 1$ . Il en résulte que

$$\rho = \rho' \varphi = 1. \blacksquare$$

On en déduit alors que :

**Corollaire 3.2.2.** *Soient  $p$  un entier premier  $> 2$  et  $G$  un  $p$ -groupe non trivial. Alors  $G$  possède un unique caractère irréductible de type 1, tous les autres étant de type 0.*

*Preuve :* Cela découle des théorèmes 3.2.1 et 2.1.20, et étant donné que la restriction de l'involution canonique à la composante simple de  $\mathbb{C}G$  correspondant au caractère trivial est orthogonale.

Du corollaire 3.2.2, il résulte qu'on ne peut envisager ni l'ambivalence, ni l'ortho-ambivalence d'un  $p$ -groupe non trivial pour  $p$  entier premier  $> 2$ . On a le résultat suivant pour les 2-groupes.

**Proposition 3.2.3.** *Soit  $G$  un 2-groupe non trivial.*

- (1) *Au moins deux composantes simples de  $\mathbb{C}G$  sont fixées par l'involution canonique.*
- (2) *Soit  $\Omega_G$  l'ensemble des sous-groupes de  $G$  d'indice deux. Le nombre de composantes simples de  $\mathbb{C}G$ , de degré un, stables par l'involution canonique, égale  $1 + |\Omega_G|$ .*
- (3) *Il y a une correspondance biunivoque entre les composantes simples de degré un, non triviales stables par l'involution canonique de  $\mathbb{C}G$  et les sous-groupes de  $G$  d'indice deux.*

**Preuve :**

1. Si  $|G| = 2$ , le résultat est immédiat car  $G$  est ambivalent commutatif. Si  $|G| = 2^r$ , où  $r$  est un entier  $> 1$ , d'après un théorème de Sylow,  $G$  possède un sous-groupe  $H$  d'ordre  $2^{r-1}$ . D'où  $(G : H) = 2$  et donc  $H$  est normal dans  $G$ .  $\frac{G}{H}$  est donc un 2-groupe d'ordre 2 ; il possède alors exactement deux caractères irréductibles  $\chi_1$  et  $\chi_2$  de degré un, définis par  $\chi_i(G - H) = (-1)^{i-1}$ , avec  $1 \leq i \leq 2$ . Soient  $\varphi : G \rightarrow \frac{G}{H}$  l'épimorphisme canonique de groupes et  $\sigma$  l'involution canonique de  $\mathbb{C}G$ . Pour tout  $i$ ,  $\psi_i = \chi_i \varphi$  est bien un caractère irréductible de  $G$  de degré un. Soit  $e_i$  l'élément idempotent centralement primitif correspondant à  $\psi_i$ . Nous avons :

$$\begin{aligned}
 e_i &= \frac{1}{2^r} \sum_{g \in G} \chi_i(\varphi(g^{-1}))g \\
 &= \frac{1}{2^r} \left[ \sum_{g \in H} \chi_i(g^{-1}H)g + \sum_{g \in G-H} \chi_i(g^{-1}H)g \right] \\
 &= \frac{1}{2^r} \left[ \sum_{g \in H} \chi_i(H)g + \sum_{g \in G-H} \chi_i(G-H)g \right] \\
 &= \frac{1}{2^r} \left[ \sum_{g \in H} g + (-1)^{i-1} \sum_{g \in G-H} g \right]
 \end{aligned}$$

et

$$\begin{aligned}
 \sigma(e_i) &= \frac{1}{2^r} \left[ \sum_{g \in H} g^{-1} + (-1)^{i-1} \sum_{g \in G-H} g^{-1} \right] \\
 &= \frac{1}{2^r} \left[ \sum_{g \in H} g + (-1)^{i-1} \sum_{g \in G-H} g \right] \\
 &= e_i,
 \end{aligned}$$

car  $H$  étant un sous-groupe de  $G$  d'indice deux, les applications  $H \rightarrow H : g \mapsto g^{-1}$  et  $G - H \rightarrow G - H : g \mapsto g^{-1}$  sont toutes deux bijectives. Il en résulte que  $A_i = \mathbb{C}Ge_i$  est une composante simple de  $\mathbb{C}G$  telle que  $\sigma(A_i) = A_i$ , pour tout  $1 \leq i \leq 2$ .

2. D'après la démonstration de (1),  $\Omega_G$  est non vide. Soit  $\Lambda_G$  l'ensemble des composantes simples de  $\mathbb{C}G$ , non triviales, de degré un,

stables par  $\sigma$ . D'après (1),  $\Lambda_G$  est non vide. Soient  $H \in \Omega_G$ ,  $\chi$  le caractère irréductible de  $\frac{G}{H}$  tel que  $\chi(G - H) = -1$ ,  $\psi = \chi\varphi$  ( $\varphi$  étant le morphisme canonique de  $G$  sur  $\frac{G}{H}$ ),  $e$  l'élément idempotent centralement primitif de  $\mathbb{C}G$  correspondant à  $\psi$  et  $A = \mathbb{C}Ge$ . D'après la démonstration de (1),  $\sigma(A) = A$  et donc  $A \in \Lambda_G$ . Considérons l'application  $\Delta : \Omega_G \rightarrow \Lambda_G$  telle que  $\Delta(H) = A$ .

Soient  $H, H' \in \Omega_G$  tels que  $\Delta(H) = \Delta(H')$ . Soient  $\chi$  et  $\chi'$  les caractères irréductibles respectifs de  $\frac{G}{H}$  et  $\frac{G}{H'}$  tels que  $\chi(G - H) = -1$  et  $\chi'(G - H') = -1$ . Soient  $\psi = \chi\varphi$  et  $\psi' = \chi'\varphi'$  les caractères irréductibles correspondant respectivement à  $\Delta(H)$  et  $\Delta(H')$ ,  $\varphi : G \rightarrow \frac{G}{H}$  et  $\varphi' : G \rightarrow \frac{G}{H'}$  étant les épimorphismes canoniques de groupes. Alors

$$\psi(g) = \begin{cases} 1 & \text{si } g \in H \\ -1 & \text{si } g \in G - H \end{cases}$$

et

$$\psi'(g) = \begin{cases} 1 & \text{si } g \in H' \\ -1 & \text{si } g \in G - H' \end{cases}$$

Donc  $\text{Ker}\psi = H$  et  $\text{Ker}\psi' = H'$ . Comme les composantes simples de  $\mathbb{C}G$  sont en correspondance biunivoque avec les  $\mathbb{C}$ -caractères irréductibles de  $G$  et  $\Delta(H) = \Delta(H')$ , alors  $\psi = \psi'$ . D'où  $H = \text{Ker}\psi = \text{Ker}\psi' = H'$  et donc  $\Delta$  est injective.

Soit  $A \in \Lambda_G$  et  $\rho : G \rightarrow \mathbb{C}^\times$  la représentation correspondant à  $A$ . Comme  $\sigma(A) = A$  et  $A$  est de degré un, alors pour tout  $g \in G$ ,  $\rho(g) = \rho(g^{-1})$  et donc  $(\rho(g))^2 = 1$ . D'où  $\rho(G) \subset \mu_2$ .  $A$  étant non triviale,  $\rho \neq 1$  et donc  $\rho(G) = \mu_2$ . Par suite, il existe un unique isomorphisme de groupes  $\rho' : \frac{G}{\text{Ker}\rho} \rightarrow \mu_2$  tel que  $\rho = \rho'\varphi''$ ,  $\varphi''$  étant l'épimorphisme canonique de  $G$  sur  $\frac{G}{\text{Ker}\rho}$ .  $\text{Ker}\rho$  est donc un sous-groupe de  $G$  d'indice deux et par définition de  $\Delta$ ,  $\Delta(\text{Ker}\rho) = A$ .  $\Delta$  est donc surjective.

$\Delta$  est alors bijective et donc  $|\Omega_G| = |\Lambda_G|$ , d'où le résultat, étant donné que l'unique composante simple triviale de  $\mathbb{C}G$  est stable par  $\Delta$ .

**3.** Cela découle de (1) et (2). ■

### 3.3 Des 2-groupes extra-spéciaux.

Nous servant de la classification des 2-groupes extra-spéciaux (qui est bien connue), nous démontrons que tout 2-groupe extra-spécial est ambivalent et précisons les 2-groupes extra-spéciaux qui sont ortho-ambivalents par rapport à un corps de caractéristique différente de 2. Il est important de noter que si la caractéristique d'un corps ne divise pas l'ordre d'un 2-groupe, elle est différente de 2.

**Définition 3.3.1.** [13, page 5], [22, page 30] *Un 2-groupe fini  $G$  est dit extra-spécial si  $G' = Z(G)$  est d'ordre 2 et  $\frac{G}{G'}$  est un 2-groupe commutatif élémentaire (c'est à dire isomorphe à  $(\frac{\mathbb{Z}}{2\mathbb{Z}})^s$  pour un certain entier naturel non nul  $s$ ).*

**Lemme 3.3.2.** [31, (1.6.2.a,b), page 29] *Soient  $G_1, G_2, \dots, G_s$  des groupes finis.*

- (1)  $Z(G_1 \times G_2 \times \dots \times G_s) = Z(G_1) \times Z(G_2) \times \dots \times Z(G_s)$
- (2) *Pour tout  $i = 1, 2, \dots, s$ , soit  $H_i$  un sous-groupe normal de  $G_i$ . Alors*

$$\frac{G_1 \times G_2 \times \dots \times G_s}{H_1 \times H_2 \times \dots \times H_s} \cong \frac{G_1}{H_1} \times \frac{G_2}{H_2} \times \dots \times \frac{G_s}{H_s} \blacksquare$$

**Définition 3.3.3.** *Soient  $G_1, G_2, \dots, G_n$  des groupes finis dont les centres sont isomorphes. Pour tout  $1 \leq i \leq n-1$ , soit  $f_i : Z(G_i) \rightarrow Z(G_n)$  un isomorphisme de groupes. Soit*

$$\varphi : \prod_{i=1}^n Z(G_i) \rightarrow Z(G_n)$$

*l'application définie par*

$$\varphi(x_1, \dots, x_{n-1}, x_n) = \left( \prod_{i=1}^{n-1} f_i(x_i) \right) x_n, \text{ pour } x_i \in Z(G_i).$$

*On vérifie que  $\varphi$  est un morphisme surjectif de groupes. Le groupe  $G := \frac{\prod_{i=1}^n G_i}{\text{Ker } \varphi}$  est appelé un produit central des groupes  $G_1, G_2, \dots$ ,*



$G_n$ , et se note simplement par  $G := G_1 \circ G_2 \circ \cdots \circ G_n$ ; il a pour centre

$$Z(G) = \frac{Z(\prod_{i=1}^n G_i)}{\text{Ker}\varphi} = \frac{\prod_{i=1}^n Z(G_i)}{\text{Ker}\varphi} \cong Z(G_n).$$

**Proposition 3.3.4.** *Avec les hypothèses et notations de la définition 3.3.3,*

$$\frac{G_1 \circ G_2 \circ \cdots \circ G_n}{Z(G_1 \circ G_2 \circ \cdots \circ G_n)} \cong \frac{G_1}{Z(G_1)} \times \frac{G_2}{Z(G_2)} \times \cdots \times \frac{G_n}{Z(G_n)}.$$

*Preuve :* Pour  $G := G_1 \circ G_2 \circ \cdots \circ G_n := \frac{\prod_{i=1}^n G_i}{\text{Ker}\varphi}$ , on a :

$$\frac{G}{Z(G)} \cong \frac{\frac{\prod_{i=1}^n G_i}{\text{Ker}\varphi}}{\frac{\prod_{i=1}^n Z(G_i)}{\text{Ker}\varphi}} \cong \frac{\prod_{i=1}^n G_i}{\prod_{i=1}^n Z(G_i)} \cong \prod_{i=1}^n \frac{G_i}{Z(G_i)},$$

après usage successif des résultats repris dans la définition 3.3.3, d'un théorème d'isomorphisme de groupes et du lemme 3.3.2. ■

Une caractérisation complète des 2-groupes extra-spéciaux existe déjà et est donnée en partie par la proposition suivante :

**Proposition 3.3.5.** [22, théorème 5.2] *Tout 2-groupe extra-spécial est d'ordre  $2^{1+2n}$ , pour un certain entier  $n \geq 1$ ; et pour chaque entier  $n \geq 1$ , il y a exactement (à isomorphisme près) deux 2-groupes extra-spéciaux d'ordre  $2^{1+2n}$ , notés respectivement  $2_+^{1+2n}$  et  $2_-^{1+2n}$  et définis par :*

$$2_+^{1+2n} = \underbrace{D_4 \circ D_4 \circ \cdots \circ D_4}_{n \text{ facteurs}}$$

et

$$2_-^{1+2n} = \underbrace{Q_2 \circ D_4 \circ \cdots \circ D_4}_{n \text{ facteurs}} = Q_2 \circ 2_+^{-1+2n},$$

où  $D_4$  est le groupe diédral d'ordre 8,  $Q_2$ , le groupe quaternionique d'ordre 8, et  $\circ$ , le produit central des groupes.

Pour étudier l'ambivalence d'un 2-groupe extra-spécial, nous avons besoin du résultat suivant :

**Lemme 3.3.6.** *Soient  $G, G_1, G_2, \dots, G_n$  des groupes finis ambivalents.*

- (1) *Si  $H$  est un sous-groupe normal de  $G$ , alors le groupe quotient  $\frac{G}{H}$  est ambivalent.*
- (2)  *$Z(G)$  est un 2-groupe abélien élémentaire.*
- (3) *Si  $G$  est commutatif, alors  $G$  est un groupe abélien élémentaire.*
- (4) *Le produit direct  $\prod_{i=1}^n G_i := G_1 \times G_2 \times \dots \times G_n$  est un groupe ambivalent.*
- (5) *Avec les notations de la définition 3.3.3, si les centres des groupes  $G_1, G_2, \dots, G_n$  sont isomorphes, alors le produit central  $G_1 \circ G_2 \circ \dots \circ G_n$  est un groupe ambivalent.*

*Preuve :*

1. Soit  $x \in G$ .  $G$  étant ambivalent, il existe  $y \in G$  tel que  $x^{-1} = yxy^{-1}$ . D'où  $(xH)^{-1} = yxy^{-1}H = yHxH(yH)^{-1}$  et donc  $\frac{G}{H}$  est ambivalent.
2. Soit  $x \in Z(G)$ .  $G$  étant ambivalent, il existe  $y \in G$  tel que  $x^{-1} = yxy^{-1}$  et donc  $x = x^{-1}$ , d'où le résultat.
3. Si  $G$  est commutatif, alors  $G = Z(G)$  et le résultat découle de (2).
4. Soit  $(x_1, x_2, \dots, x_n) \in \prod_{i=1}^n G_i$ . Pour tout  $1 \leq i \leq n$ ,  $G_i$  étant ambivalent, il existe  $y_i \in G_i$  tel que  $x_i^{-1} = y_i x_i y_i^{-1}$ . Par suite,

$$\begin{aligned}
 (x_1, x_2, \dots, x_n)^{-1} &= (x_1^{-1}, x_2^{-1}, \dots, x_n^{-1}) \\
 &= (y_1 x_1 y_1^{-1}, y_2 x_2 y_2^{-1}, \dots, y_n x_n y_n^{-1}) \\
 &= (y_1, y_2, \dots, y_n)(x_1, x_2, \dots, x_n)(y_1, y_2, \dots, y_n)^{-1},
 \end{aligned}$$

et donc  $\prod_{i=1}^n G_i$  est ambivalent.

5. Comme  $G_1 \circ G_2 \circ \dots \circ G_n = \frac{\prod_{i=1}^n G_i}{\text{Ker}\varphi}$ , le résultat découle alors de (4) et (1). ■

**Proposition 3.3.7.** *Tout 2-groupe extra-spécial est ambivalent.*

*Preuve :* Cela découle de la proposition 3.3.5, du lemme 3.3.6 et du fait que les groupes diédral  $D_4$  et quaternionique  $Q_2$  sont ambivalents (d'après la proposition 2.1.8). ■

**Proposition 3.3.8.** *Soient  $G$  un 2-groupe extra-spécial,  $\sigma$  l'involution canonique de  $\mathbb{C}G$  et  $A$  une composante simple de  $\mathbb{C}G$  de degré  $> 1$ . La restriction de  $\sigma$  à  $A$  est orthogonale (resp. symplectique) si et seulement si  $t(1) = \frac{|G|(1+\deg A)}{2\deg A}$  (resp.  $t(1) = \frac{|G|(-1+\deg A)}{2\deg A}$ ),  $t(1)$  étant le nombre d'éléments  $g$  de  $G$  tels que  $g^2 = 1$ .*

*Preuve :* Soient  $\chi$  le caractère et  $\rho : G \rightarrow GL(V)$  la représentation irréductibles de  $G$  correspondant à  $A$ . Soit  $g$  un élément de  $G$ . Par hypothèse,  $\frac{G}{Z(G)} = \frac{G}{Z(G)}$  est isomorphe à  $(\frac{\mathbb{Z}}{2\mathbb{Z}})^s$  pour un certain entier naturel non nul  $s$ . Donc  $g^2 Z(G) = Z(G)$  et alors  $g^2 \in Z(G)$ . Comme  $G$  est ambivalent (proposition 3.3.7), alors  $\sigma(A) = A$  et la restriction de  $\sigma$  à  $A$  est une involution de première espèce (proposition 1.3.3). D'où, d'après la proposition 3.1.1,  $\rho(Z(G)) \subset \mu_2$ . Si  $\rho(Z(G)) = 1$ , il existe alors un unique morphisme de groupes  $\rho' : \frac{G}{Z(G)} \rightarrow GL(V)$  tel que  $\rho = \rho'\varphi$ , où  $\varphi : G \rightarrow \frac{G}{Z(G)}$  désigne l'épimorphisme canonique.  $\rho'$  est irréductible car  $\rho$  l'est (d'après la proposition 3.1.2).  $\frac{G}{Z(G)}$  étant un groupe commutatif,  $\rho'$  est de degré 1 ; il en est donc de même pour  $\rho$ , ce qui est contradictoire. On en déduit que  $\rho(Z(G)) = \mu_2$  et donc la restriction de  $\rho$  à  $Z(G)$  est un isomorphisme de  $Z(G)$  sur  $\mu_2$  ( $Z(G)$  étant d'ordre 2). En supposant donc que  $Z(G) = \langle y \rangle$ , avec  $y^2 = 1$ ,  $\rho(y) = -1$ .

- Si  $g^2 = 1$ , alors  $\rho(g^2) = 1$  et donc  $\chi(g^2) = \deg A$ .
- Si  $g^2 \neq 1$ , alors  $g^2 = y$  et donc  $\rho(g^2) = -1$  ; d'où  $\chi(g^2) = -\deg A$ .

Par suite, si  $\nu$  désigne l'indicateur de Schur-Frobenius, on a :

$$\begin{aligned}
 \nu(\chi) &= \frac{1}{|G|} \sum_{g \in G} \chi(g^2) \\
 &= \frac{1}{|G|} \left( \sum_{g^2=1} \chi(g^2) + \sum_{g^2 \neq 1} \chi(g^2) \right) \\
 &= \frac{1}{|G|} (t(1) \deg A - (|G| - t(1)) \deg A) \\
 &= \frac{\deg A (2t(1) - |G|)}{|G|}.
 \end{aligned}$$

D'où

$$t(1) = \frac{|G|(\nu(\chi) + \deg A)}{2 \deg A}$$

et le résultat découle alors du théorème 2.1.20. ■

Nous nous proposons maintenant d'étudier l'ortho-ambivalence d'un 2-groupe extra-spécial par rapport à un corps de caractéristique différente de 2. Pour y arriver, nous allons d'abord établir un résultat analogue à celui énoncé dans le lemme 3.1.3 pour certains produits centraux de groupes.

Soient alors  $G_1$  et  $G_2$  des groupes finis tels que  $|Z(G_i)| = 2$ , pour tout  $i = 1, 2$  et supposons que  $Z(G_i) = \text{sgr} \langle w_i \rangle$ . Soit  $\rho_i : G_i \rightarrow GL(V_i)$  une représentation irréductible de  $G_i$  telle que  $\rho_i(Z(G_i)) = \mu_2$ . Alors  $\rho_i(w_i) = -1$ . D'après [38, théorème 10, page 27],  $\rho = \rho_1 \otimes \rho_2 : G_1 \times G_2 \rightarrow GL(V_1 \otimes V_2)$  est une représentation irréductible de  $G_1 \times G_2$ . De plus

$$\rho(w_1, w_2) = \rho_1(w_1) \otimes \rho_2(w_2) = -1 \otimes -1 = 1;$$

d'où  $\text{sgr} \langle (w_1, w_2) \rangle \subset \text{Ker} \rho$ . Il existe donc un unique morphisme de groupes  $\psi : \frac{G_1 \times G_2}{\text{sgr} \langle (w_1, w_2) \rangle} \rightarrow GL(V_1 \otimes V_2)$  tel que  $\rho = \psi \varphi$ , où  $\varphi : G_1 \times G_2 \rightarrow \frac{G_1 \times G_2}{\text{sgr} \langle (w_1, w_2) \rangle}$  est la surjection canonique. Par définition,

$\frac{G_1 \times G_2}{\text{sgr} \langle (w_1, w_2) \rangle}$  est bien le produit central  $G_1 \circ G_2$  (voir définition 3.3.3). D'après la proposition 3.1.2,  $\psi$  est une représentation irréductible de  $G_1 \circ G_2$  et donc  $\deg \psi = \deg \rho = (\deg \rho_1)(\deg \rho_2)$ .  $\psi$  est appelé le produit central de  $\rho_1$  et  $\rho_2$  et se note  $\rho_1 \circ \rho_2$ . Soit  $A$  la composante simple de  $\mathbb{C}(G_1 \circ G_2)$  correspondant à  $\psi = \rho_1 \circ \rho_2$  et  $A_i$  la composante simple de  $\mathbb{C}G_i$  correspondant à  $\rho_i$ , pour  $i = 1, 2$ . Soient  $\bar{\sigma}$  l'involution canonique de  $\mathbb{C}(G_1 \circ G_2)$ ,  $\sigma_i$  l'involution canonique de  $\mathbb{C}(G_i)$  et  $\sigma = \sigma_1 \otimes \sigma_2$  l'involution canonique de  $\mathbb{C}(G_1 \times G_2) \cong (\mathbb{C}G_1 \otimes_{\mathbb{C}} \mathbb{C}G_2)$ . Supposons que  $\sigma_i(A_i) = A_i$ , pour  $i = 1, 2$ . D'après la proposition 3.1.2, la restriction de  $\sigma$  à  $A_1 \otimes_{\mathbb{C}} A_2$  et la restriction de  $\bar{\sigma}$  à  $A$  sont des involutions de même type. D'où d'après le lemme 3.1.3, si les restrictions respectives de  $\sigma_i$  à  $A_i$  sont toutes orthogonales ou toutes symplectiques, alors la restriction de  $\bar{\sigma}$  à  $A$  est symplectique et si ces restrictions sont l'une orthogonale, l'autre symplectique, alors la restriction de  $\bar{\sigma}$  à  $A$  est symplectique. Nous avons ainsi démontré le résultat suivant :

**Proposition 3.3.9.** *Soient  $G_1$  et  $G_2$  des groupes finis tels que  $|Z(G_i)| = 2$ , pour tout  $i = 1, 2$ ,  $\sigma_i$  l'involution canonique de  $\mathbb{C}G_i$ ,  $A_i$  une composante simple de  $\mathbb{C}G_i$  telle que*

$$\sigma_i(A_i) = A_i \text{ et } \rho_i(Z(G_i)) = \mu_2,$$

$\rho_i : G_i \rightarrow GL(V_i)$  étant la représentation irréductible de  $G_i$  correspondant à  $A_i$ . Soient  $\bar{\sigma}$  l'involution canonique de  $\mathbb{C}(G_1 \circ G_2)$  et  $A$  la composante simple de  $\mathbb{C}(G_1 \circ G_2)$  correspondant à  $\rho_1 \circ \rho_2 : G_1 \circ G_2 \rightarrow GL(V_1 \otimes V_2)$ . Alors  $\deg A = (\deg A_1)(\deg A_2)$  et

- (1) *Si la restriction de  $\sigma_i$  à  $A_i$  est orthogonale (resp. symplectique) pour tout  $i = 1, 2$ , alors la restriction de  $\bar{\sigma}$  à  $A$  est orthogonale.*
- (2) *Si l'une des restrictions de  $\sigma_i$  à  $A_i$  est orthogonale, l'autre symplectique, alors la restriction de  $\bar{\sigma}$  à  $A$  est symplectique. ■*

La proposition 3.3.9 se généralise par induction de la manière suivante :

**Proposition 3.3.10.** *Soient  $G_1, G_2, \dots, G_s$  des groupes finis tels que  $|Z(G_i)| = 2$ , pour tout  $i = 1, 2, \dots, s$ ,  $\sigma_i$  l'involution canonique de  $\mathbb{C}G_i$ ,  $A_i$  une composante simple de  $\mathbb{C}G_i$  telle que*

$$\sigma_i(A_i) = A_i \text{ et } \rho_i(Z(G_i)) = \mu_2,$$

*$\rho_i : G_i \rightarrow GL(V_i)$  étant la représentation irréductible de  $G_i$  correspondant à  $A_i$ . Soient  $\bar{\sigma}$  l'involution canonique de  $\mathbb{C}(G_1 \circ G_2 \circ \dots \circ G_s)$  et  $A$  la composante simple de  $\mathbb{C}(G_1 \circ G_2 \circ \dots \circ G_s)$  correspondant à*

$$\rho_1 \circ \rho_2 \circ \dots \circ \rho_s : G_1 \circ G_2 \circ \dots \circ G_s \longrightarrow GL(V_1 \otimes V_2 \otimes \dots \otimes V_s).$$

*Alors  $\deg A = (\deg A_1)(\deg A_2) \dots (\deg A_s)$  et*

- (1) *Si un nombre pair des restrictions de  $\sigma_i$  à  $A_i$  ( $i = 1, 2, \dots, s$ ) sont symplectiques, alors la restriction de  $\bar{\sigma}$  à  $A$  est orthogonale.*
- (2) *Si un nombre impair des restrictions de  $\sigma_i$  à  $A_i$  ( $i = 1, 2, \dots, s$ ) sont symplectiques, alors la restriction de  $\bar{\sigma}$  à  $A$  est symplectique. ■*

Nous avons enfin, le résultat suivant :

**Théorème 3.3.11.** *Soient  $G$  un 2-groupe extra-spécial d'ordre  $2^{1+2n}$ , pour un certain entier naturel non nul  $n$  et  $k$  un corps dont la caractéristique est différente de 2.  $\mathbb{C}G$  possède une unique composante simple de degré  $> 1$ . Cette composante est de degré  $2^n$ . De plus, avec les notations de la proposition 3.3.5, pour tout entier naturel non nul  $n$ ,*

- (1) *Le 2-groupe extra-spécial  $2_+^{1+2n}$  est ortho-ambivalent par rapport à  $k$ .*
- (2) *Le 2-groupe extra-spécial  $2_-^{1+2n}$  n'est pas ortho-ambivalent par rapport à  $k$ .*

*Preuve :* Soit  $\sigma$  l'involution canonique de  $\mathbb{C}G$ .  $G$  étant ambivalent (proposition 3.3.7), toutes les composantes simples de  $\mathbb{C}G$  sont

fixées par  $\sigma$  et la restriction de  $\sigma$  à chaque composante simple de degré 1 est orthogonale. D'après la proposition 3.3.5,

$$G = 2_+^{1+2n} = \underbrace{D_4 \circ D_4 \circ \cdots \circ D_4}_{n \text{ facteurs}}$$

ou

$$G = 2_-^{1+2n} = \underbrace{Q_2 \circ D_4 \circ \cdots \circ D_4}_{n \text{ facteurs}},$$

où  $D_4$  est le groupe diédral d'ordre 8,  $Q_2$ , le groupe quaternionique d'ordre 8, et  $\circ$ , le produit central des groupes. D'après [33, (2.1.1), page 12 et (2.2.1), page 16],  $D_4$  (resp.  $Q_2$ ) possède une unique représentation irréductible  $\rho$  (resp.  $\rho'$ ) de degré deux.  $D_4$  et  $Q_2$  étant des 2-groupes extra-spéciaux, leurs centres sont d'ordre deux et d'après la démonstration de la proposition 3.3.8,  $\rho(Z(D_4)) = \rho'(Z(Q_2)) = \mu_2$ . Donc d'après la proposition 3.3.10,

$$\rho_1 := \underbrace{\rho \circ \rho \circ \cdots \circ \rho}_{n \text{ facteurs}}$$

et

$$\rho_2 := \underbrace{\rho' \circ \rho \circ \cdots \circ \rho}_{n \text{ facteurs}}$$

sont des représentations irréductibles respectives de  $2_+^{1+2n}$  et  $2_-^{1+2n}$  et  $\deg \rho_1 = \deg \rho_2 = 2^n$ . Soit  $A$  la composante simple de  $\mathbb{C}G$  correspondant à  $\rho_1$  (resp.  $\rho_2$ );  $\deg A = 2^n$ . De plus, d'après la proposition 3.3.10, si  $G = 2_+^{1+2n}$ , la restriction de  $\sigma$  à  $A$  est orthogonale et si  $G = 2_-^{1+2n}$ , la restriction de  $\sigma$  à  $A$  est symplectique.

Soit  $B$  une autre composante simple de  $\mathbb{C}G$ , de degré  $> 1$ . D'après la proposition 3.3.8,

- Si les restrictions respectives de  $\sigma$  à  $A$  et à  $B$  sont toutes orthogonales ou symplectiques, alors

$$t(1) = \frac{|G|(\varepsilon + \deg A)}{2\deg A} = \frac{|G|(\varepsilon + \deg B)}{2\deg B},$$

avec  $\varepsilon = \pm 1$  et donc  $\deg A = \deg B$ .

- Si les restrictions respectives de  $\sigma$  à  $A$  et à  $B$  sont l'une orthogonale, l'autre symplectique, alors

$$t(1) = \frac{|G|(\varepsilon + \deg A)}{2\deg A} = \frac{|G|(-\varepsilon + \deg B)}{2\deg B},$$

avec  $\varepsilon = \pm 1$  et donc  $\deg A = -\deg B$ , ce qui est impossible. Soit alors  $r$  (resp.  $l$ ) le nombre de composantes simples de  $\mathbb{C}G$  de degré un (resp.  $2^n = \deg A > 1$ ). D'après la proposition 3.1.6,

$$r = (G : G') = \frac{1}{2}|G| = 2^{2n}. \quad (3.1)$$

D'après la proposition 1.1.4,

$$2^{1+2n} = |G| = r + l(\deg A)^2 = 2^{2n} + 2^{2n}.l. \quad (3.2)$$

De (3.2), il résulte alors que  $l = 1$  et l'unicité de  $A$  est ainsi établie. On conclut enfin que  $2_+^{1+2n}$  (resp.  $2_-^{1+2n}$ ) est ortho-ambivalent (resp. n'est pas ortho-ambivalent) par rapport à  $\mathbb{C}$  et donc le résultat découle du corollaire 2.3.8. ■

On en déduit le résultat suivant :

**Corollaire 3.3.12.** *Soit  $G$  un 2-groupe extra-spécial et  $A$  l'unique composante simple de  $\mathbb{C}G$  de degré  $> 1$  dont le caractère correspondant est  $\chi$ . Alors  $t(1) = (\deg A)^2 + \nu(\chi)\deg A$ . De plus le nombre de composantes simples de  $\mathbb{C}G$  est  $1 + \frac{1}{2}|G|$  et  $|G| = 2(\deg A)^2$ .*

*Preuve :* Supposons que  $G$  est d'ordre  $2^{1+2n}$  ; d'après la proposition 3.3.11,  $\deg A = 2^n$ . La proposition 3.3.8 donne alors

$$\begin{aligned} t(1) &= \frac{|G|(\nu(\chi) + \deg A)}{2\deg A} \\ &= \frac{2^{1+2n}(\nu(\chi) + 2^n)}{2^{1+n}} \\ &= 2^{2n} + \nu(\chi)2^n \\ &= (\deg A)^2 + \nu(\chi)\deg A. \end{aligned}$$



Le deuxième résultat découle de ( 3.1) et de l'unicité de la composante simple de degré  $> 1$ . Enfin,

$$|G| = 2^{1+2n} = 2.(2^n)^2 = 2(deg A)^2. \blacksquare$$

## 3.4 Des 2-groupes spéciaux

Les 2-groupes extra-spéciaux sont des cas particuliers des 2-groupes spéciaux. Dans cette section, nous associons à tout 2-groupe spécial (resp. 2-groupe extra-spécial) une application (resp. forme) quadratique. Nous utilisons alors l'invariant d'Arf pour étudier l'ortho-ambivalence d'un 2-groupe spécial ambivalent par rapport à un corps de caractéristique différente de 2.

Nous sommes loin de donner une classification des 2-groupes spéciaux, mais nous arrivons à établir qu'il est possible de construire par des générateurs et relations, des 2-groupes spéciaux à partir des applications quadratiques régulières (vérifiant certaines conditions) entre des 2-groupes abéliens élémentaires (voir théorème 3.4.23)

**Définition 3.4.1.** [31, page 105] *Soit  $G$  un groupe fini. L'intersection des sous-groupes maximaux de  $G$  est appelée **sous-groupe de Frattini de  $G$**  et se note  $\Phi(G)$ . Si  $G = 1$ , on pose  $\Phi(G) = 1$ . En particulier, si  $G$  est un 2-groupe,  $\Phi(G)$  est l'intersection des sous-groupes de  $G$  d'indice deux.*

**Proposition 3.4.2.** *Soit  $G$  un 2-groupe. Alors*

- (1)  $\Phi(G)$  est un sous-groupe normal de  $G$  et  $\frac{G}{\Phi(G)}$  est un 2-groupe abélien élémentaire.
- (2)  $\Phi(G)$  est le plus petit sous-groupe normal de  $G$  tel que  $\frac{G}{\Phi(G)}$  soit un 2-groupe abélien élémentaire.
- (3)  $\Phi(G) = \text{sgr} \langle x^2 | x \in G \rangle$ .

*Preuve :* Pour (1) voir [31, (5.2.7), page 106], pour (2), voir [31, (5.2.8), page 106] et pour (3), voir [31, exercice 9, page 107].

■

**Définition 3.4.3. *Notation* :** [31, page 47] Soit  $G$  un 2-groupe. On pose

$$\Omega(G) := \text{sgr} \langle x \in G \mid x^2 = 1 \rangle.$$

Si  $G$  est commutatif, alors

$$\Omega(G) := \{x \in G \mid x^2 = 1\}.$$

**Définition 3.4.4.** [31, page 107] Un 2-groupe  $G$  est dit *spécial* si  $G$  est non commutatif et  $G' = \Phi(G) = Z(G) = \Omega(Z(G))$ . En particulier, si  $G$  est un 2-groupe spécial tel que  $|Z(G)| = 2$ , alors  $G$  est un 2-groupe *extra-spécial* (d'après la proposition 3.4.2(1)). Réciproquement, si  $G$  est un 2-groupe extra-spécial, alors  $G$  est un 2-groupe spécial dont le centre est d'ordre 2 (d'après la proposition 3.4.2(2)).

**Lemme 3.4.5.** Soient  $G, G_1, G_2, \dots, G_s$  des groupes finis.

- (1)  $(G_1 \times G_2 \times \dots \times G_s)' = G_1' \times G_2' \times \dots \times G_s'$ .
- (2) Si  $H$  est un sous-groupe normal de  $G$ , alors  $(\frac{G}{H})' = \frac{G'H}{H}$ .
- (3)  $\Omega(G_1 \times G_2 \times \dots \times G_s) = \Omega(G_1) \times \Omega(G_2) \times \dots \times \Omega(G_s)$ .
- (4) Si  $G_1, G_2, \dots, G_s$  sont des 2-groupes, alors

$$\Phi(G_1 \times G_2 \times \dots \times G_s) = \Phi(G_1) \times \Phi(G_2) \times \dots \times \Phi(G_s).$$

*Preuve :*

- 1. Voir [31, (1.6.2.b), page 29].
- 2. Cela découle de [31, (1.5.1), page 24] et [31, (1.5.3), démonstration, page 25].
- 3. Cela découle du fait que pour tout  $(g_1, g_2, \dots, g_s) \in G_1 \times G_2 \times \dots \times G_s$ ,

$$(g_1, g_2, \dots, g_s)^2 = 1 \iff g_1^2 = g_2^2 = \dots = g_s^2 = 1.$$

**3.** Cela est une conséquence de la proposition 3.4.2.(3) et du fait que pour tout  $(g_1, g_2, \dots, g_s) \in G_1 \times G_2 \times \dots \times G_s$ ,

$$(g_1, g_2, \dots, g_s)^2 = (g_1^2, g_2^2, \dots, g_s^2). \blacksquare$$

**Proposition 3.4.6.** *Soient  $G_1, G_2, \dots, G_s$  des 2-groupes spéciaux. Le produit direct  $G_1 \times G_2 \times \dots \times G_s$  est un 2-groupe spécial.*

*Preuve :* On applique directement les lemmes 3.4.5 et 3.3.2.  $\blacksquare$

**Remarque 3.4.7.** *Soit  $G$  un 2-groupe spécial. Si  $G$  est le produit direct d'un nombre fini de 2-groupes extra-spéciaux, le type de la restriction de l'involution canonique à chaque composante simple de  $\mathbb{C}G$  s'obtient en utilisant la proposition 3.1.4. Par exemple, avec les notations de la proposition 3.3.5, si  $G_1 = 2_+^{1+2n}$ ,  $G_2 = 2_-^{1+2m}$  et  $G = G_1 \times G_2$ , avec  $n, m \in \mathbb{N}_0$ , on a :*

$\mathbb{C}G_1$  possède  $2^{2n}$  composantes simples de degré 1 et une seule de degré  $2^n$  (sur lesquelles l'involution canonique est orthogonale);  $\mathbb{C}G_2$  possède  $2^{2m}$  composantes simples de degré 1 (sur lesquelles l'involution canonique est orthogonale) et une seule de degré  $2^m$  (sur laquelle l'involution canonique est symplectique); donc  $\mathbb{C}G$  possède  $2^{2(n+m)}$  composantes simples de degré 1,  $2^{2m}$  composantes simples de degré  $2^n$  (sur lesquelles l'involution canonique est orthogonale),  $2^{2n}$  composantes simples de degré  $2^m$  (sur lesquelles l'involution canonique est symplectique) et une composante simple de degré  $2^{n+m}$  (sur laquelle l'involution canonique est symplectique).

Soit  $G$  un 2-groupe spécial. Comme  $Z(G)$  et  $\frac{G}{Z(G)}$  sont des 2-groupes abéliens élémentaires, ils peuvent être regardés comme des espaces vectoriels sur le corps  $\mathbb{F}_2$  à deux éléments. Par ailleurs la suite

$$1 \rightarrow Z(G) \hookrightarrow G \twoheadrightarrow \frac{G}{Z(G)} \rightarrow 1$$

est exacte. On dit simplement que  $G$  est une extension centrale de  $Z(G)$  par  $\frac{G}{Z(G)}$ . Toutes les extensions centrales de  $Z(G)$  par  $\frac{G}{Z(G)}$  ( $Z(G)$  et  $\frac{G}{Z(G)}$  vus comme des  $\mathbb{F}_2$ -espaces vectoriels) se classifient

par le deuxième groupe de cohomologie de  $\frac{G}{Z(G)}$  à coefficients dans  $Z(G)$ . Nous allons établir qu'elles peuvent aussi être classifiées par le groupe des applications quadratiques de  $\frac{G}{Z(G)}$  dans  $Z(G)$ .

**Définition 3.4.8.** Soient  $A$  et  $B$  des 2-groupes abéliens élémentaires : ils peuvent être regardés comme des espaces vectoriels sur le corps  $\mathbb{F}_2$  à deux éléments. Une application  $q : A \rightarrow B$  est dite quadratique si pour tout  $x \in A$ , l'application  $b_q : A \times A \rightarrow B$  définie par

$$b_q(x, y) = q(xy)q(x^{-1})q(y^{-1}) = q(xy)q(x)q(y),$$

est bi-multiplicative c'est-à-dire pour tous  $x, y, z \in A$ ,

$$b_q(xz, y) = b_q(x, y)b_q(z, y) \quad \text{et} \quad b_q(x, yz) = b_q(x, y)b_q(x, z).$$

$b_q$  est appelée l'application polaire de  $q$  ; elle est alternée et symétrique.

**Remarque 3.4.9.** En notation additive, si  $A$  et  $B$  sont des espaces vectoriels sur le corps  $\mathbb{F}_2$ , une application  $q : A \rightarrow B$  est dite quadratique si l'application  $b_q : A \times A \rightarrow B$  définie par

$$b_q(x, y) = q(x + y) - q(x) - q(y),$$

est bilinéaire.

**Définition 3.4.10.** Soient  $A$  et  $B$  des 2-groupes abéliens élémentaires et  $q : A \rightarrow B$  une application quadratique d'application polaire  $b_q : A \times A \rightarrow B$ . On appelle radical de  $b_q$  (resp. radical de  $q$ ) et on note  $\text{rad}b_q$  (resp.  $\text{rad}q$ ), le sous-ensemble de  $A$  défini par :

$$\text{rad}b_q = \{a \in A \mid b_q(a, x) = 1, \forall x \in A\}$$

$$(\text{resp. } \text{rad}q = \{x \in \text{rad}b_q \mid q(x) = 1\}).$$

On dit que  $q$  est régulière si  $\text{rad}b_q = 1$ , singulière si  $\text{rad}b_q \neq 1$  et totalement singulière si  $\text{rad}b_q = A$ .

Si  $G$  est un 2-groupe spécial, alors  $\frac{G}{Z(G)}$  et  $Z(G)$  sont des 2-groupes commutatifs élémentaires. Nous allons définir une application quadratique de  $\frac{G}{Z(G)}$  dans  $Z(G)$ . Pour y arriver, nous avons besoin du lemme suivant :

**Lemme 3.4.11.** [31, (1.5.4), page 25] *Soient  $G$  un groupe et  $x, y, z \in G$ . On pose  $x^y := y^{-1}xy$ ,  $x^{-y} := (x^{-1})^y$  et  $[x, y] = x^{-1}y^{-1}xy = x^{-1}x^y = y^{-x}y$ . On a :*

$$(1) \quad [x, yz] = [x, z][x, y]^z$$

$$(2) \quad [xz, y] = [x, y]^z[z, y]$$

*Preuve :* Pour tous  $x, y, z \in G$ , on a :

$$\begin{aligned} [x, yz] &= x^{-1}z^{-1}y^{-1}xyz &= (x^{-1}z^{-1}xz)z^{-1}(x^{-1}y^{-1}xy)z \\ &= [x, z][x, y]^z \end{aligned}$$

et

$$\begin{aligned} [xz, y] &= z^{-1}x^{-1}y^{-1}xzy &= z^{-1}(x^{-1}y^{-1}xy)z(z^{-1}y^{-1}zy) \\ &= [x, y]^z[z, y]. \quad \blacksquare \end{aligned}$$

**Proposition 3.4.12.** *Soient  $G$  un 2-groupe spécial et*

$$\phi : \frac{G}{Z(G)} \longrightarrow Z(G) : xZ(G) := \bar{x} \longmapsto x^2.$$

*$\phi$  est une application quadratique et son application polaire  $b_\phi$  est définie par*

$$b_\phi(\bar{x}, \bar{y}) = [x, y].$$

*Preuve :* Soient  $x, y \in G$  tels que  $\bar{x} = \bar{y}$ . Alors  $x^{-1}y \in Z(G)$ ; d'où  $x^{-1}y = xx^{-1}(x^{-1}y) = x(x^{-1}y)x^{-1} = yx^{-1}$  et donc  $x^{-2}y^2 = (x^{-1}y)^2 = 1$  ( $Z(G)$  étant élémentaire). Par suite  $x^2 = y^2$  et alors  $\phi$  est bien définie.

Soit  $b_\phi : \frac{G}{Z(G)} \times \frac{G}{Z(G)} \longrightarrow Z(G)$  l'application définie par

$$b_\phi(\bar{x}, \bar{y}) = \phi(\overline{xy})\phi(\overline{x^{-1}})\phi(\overline{y^{-1}}).$$

$G$  étant spécial, pour tous  $x, y \in G$ ,  $x^2 \in Z(G)$  et donc

$$b_\phi(\bar{x}, \bar{y}) = (xy)^2 x^{-2} y^{-2} = x^{-2} x y y^{-2} x y = x^{-1} y^{-1} x y;$$

d'où

$$b_\phi(\bar{x}, \bar{y}) = [x, y]. \quad (3.3)$$

Remarquons d'abord que  $b_\phi$  est alternée car  $b_\phi(\bar{x}, \bar{x}) = [x, x] = 1$ , pour tout  $x \in G$ . Et comme  $Z(G)$  est abélien élémentaire, alors pour tous  $x, y \in G$ ,

$$b_\phi(\bar{x}, \bar{y}) = [x, y] = [x, y]^{-1} = [y, x] = b_\phi(\bar{y}, \bar{x}).$$

D'une part,

$$\begin{aligned} b_\phi(\bar{x}\bar{z}, \bar{y}) &= [xz, y] \text{ (d'après (3.3))} \\ &= [x, y]^z [z, y] \text{ (lemme 3.4.11)} \\ &= z^{-1} [x, y] z [z, y] \\ &= [x, y] [z, y] \text{ (car } G' = Z(G)) \\ &= b_\phi(\bar{x}, \bar{y}) b_\phi(\bar{z}, \bar{y}); \end{aligned}$$

D'autre part,  $b_\phi$  étant symétrique, d'après ce qui précède,

$$\begin{aligned} b_\phi(\bar{x}, \bar{y}\bar{z}) &= b_\phi(\bar{y}\bar{z}, \bar{x}) \\ &= b_\phi(\bar{y}, \bar{x}) b_\phi(\bar{z}, \bar{x}) \\ &= b_\phi(\bar{x}, \bar{y}) b_\phi(\bar{x}, \bar{z}). \end{aligned}$$

Il en résulte que  $\phi$  est une application quadratique. ■

**Définition 3.4.13.** *L'application quadratique  $\phi : \frac{G}{Z(G)} \longrightarrow Z(G)$  définie dans la proposition 3.4.12, est appelée application quadratique du 2-groupe spécial  $G$ .*

**Remarque 3.4.14.** Avec les notations et hypothèses de la proposition 3.4.12, l'application quadratique  $\phi : \frac{G}{Z(G)} \longrightarrow Z(G)$  est régulière car pour tout  $x \in G$ , on a :

$$x \in Z(G) \iff [x, y] = 1, \forall y \in G.$$

**Remarque 3.4.15.** Soit  $G$  un 2-groupe extra-spécial. Comme  $Z(G)$  est d'ordre 2, il peut être regardé comme un corps à deux éléments, l'élément neutre étant l'élément nul et l'élément générateur, l'élément unité. Avec les notations et hypothèses de la proposition 3.4.12, l'application quadratique  $\phi : \frac{G}{Z(G)} \longrightarrow Z(G)$  est donc une forme quadratique régulière. Il est possible de calculer l'invariant d'Arf de  $\phi$ . Pour le faire, rappelons d'abord la définition de cet invariant.

**Définition 3.4.16.** Soient  $k$  un corps de caractéristique 2 et  $V$  un espace vectoriel sur  $k$  de dimension finie. Soit  $q : V \rightarrow k$  une forme quadratique régulière de forme polaire  $b_q : V \times V \rightarrow k$  (c'est-à-dire pour tout  $\alpha \in k$ , pour tout  $x \in V$ ,  $q(\alpha x) = \alpha^2 q(x)$  et  $q$  est une application quadratique régulière). Comme  $b_q$  est alternée, d'après [39, page 265], l'espace  $(V, b_q)$  possède une base  $(e_i, f_i)_{i=1}^n$  vérifiant les conditions suivantes :

$$b_q(e_i, e_i) = b_q(f_i, f_i) = 0, \quad \forall i \quad (3.4)$$

$$b_q(e_i, f_i) = b_q(f_i, e_i) = 1, \quad \forall i \quad (3.5)$$

$$b_q(e_i, e_j) = b_q(e_i, f_j) = b_q(f_i, e_j) = b_q(f_i, f_j) = 0, \quad \forall i \neq j. \quad (3.6)$$

Une telle base est dite symplectique. On pose

$$\wp(k) := \{x^2 + x \mid x \in k\}.$$

Dans  $\frac{k}{\wp(k)}$ , la classe de l'élément  $\sum_{i=1}^n q(e_i)q(f_i)$  est indépendante de la base symplectique considérée [39, théorème 9.4.2, page 340] et est appelée l'invariant d'Arf de  $q$ ; on le notera par  $\text{Arf}(q)$ .

$$\text{Arf}(q) := \sum_{i=1}^n q(e_i)q(f_i) + \wp(k).$$

Notons que  $\wp(\mathbb{F}_2) = 0$ ,  $\mathbb{F}_2$  étant le corps à deux éléments.

**Proposition 3.4.17.** [39, 9.4.3, page 340] Soient  $k$  un corps de caractéristique 2,  $V$  et  $V'$  des espaces vectoriels sur  $k$  de dimensions finies et  $q : V \rightarrow k$  et  $q' : V' \rightarrow k$  des formes quadratiques régulières.

Soit  $q \perp q' : V \times V' \rightarrow k$  la somme orthogonale de  $q$  et  $q'$ , définie par  $(q \perp q')(x, y) = q(x) + q'(y)$ . Alors

$$\text{Arf}(q \perp q') = \text{Arf}(q) + \text{Arf}(q'). \blacksquare$$

**Proposition 3.4.18.** Soit  $G$  un 2-groupe extra-spécial d'ordre  $2^{1+2n}$  et

$$\phi_n : \frac{G}{Z(G)} \longrightarrow Z(G) : xZ(G) := \bar{x} \longmapsto x^2$$

la forme quadratique régulière définie dans la proposition 3.4.12. Avec les notations de la proposition 3.3.5, l'invariant d'Arf de  $\phi_n$  est 0 (resp. 1) si  $G = 2_+^{1+2n}$  (resp. si  $G = 2_-^{1+2n}$ ).

*Preuve :* Pour  $n = 1$ ,  $G = D_4$  ou  $G = Q_2$ , où  $D_4$  désigne le groupe diédral d'ordre 8 et  $Q_2$ , le groupe quaternionique d'ordre 8. Soient

$$\phi_1 : \frac{D_4}{Z(D_4)} \longrightarrow Z(D_4) : xZ(D_4) := \bar{x} \longmapsto x^2$$

et

$$\phi'_1 : \frac{Q_2}{Z(Q_2)} \longrightarrow Z(Q_2) : xZ(Q_2) := \bar{x} \longmapsto x^2.$$

Supposons que

$$D_4 = \text{sgr} \langle a, b \mid \text{ord}(a) = 4, \text{ord}(b) = 2, bab^{-1} = a^{-1} \rangle$$

et

$$Q_2 = \text{sgr} \langle c, d \mid \text{ord}(c) = 4, d^2 = c^2, dcd^{-1} = c^{-1} \rangle.$$

D'une part,  $Z(D_4) = \text{sgr} \langle a^2 \rangle$  et l'espace  $(\frac{D_4}{Z(D_4)}, \phi_1)$  a pour base symplectique  $(\bar{b}, \overline{ab})$ , car  $b_{\phi_1}(\bar{b}, \bar{b}) = [b, b] = 1$ ,  $b_{\phi_1}(\overline{ab}, \overline{ab}) = [ab, ab] = 1$  et  $b_{\phi_1}(\bar{b}, \overline{ab}) = [b, ab] = a^2$ . Donc

$$\text{Arf}(\phi_1) = \phi_1(\bar{b}).\phi_1(\overline{ab}) = b^2.(ab)^2 = 1.1 = 1$$

est l'élément nul du corps  $Z(D_4)$ .

D'autre part,  $Z(Q_2) = \text{sgr} \langle c^2 \rangle$  et l'espace  $(\frac{Q_2}{Z(Q_2)}, \phi'_1)$  a pour base



symplectique  $(\bar{c}, \bar{d})$ , car  $b_{\phi'_1}(\bar{c}, \bar{c}) = [c, c] = 1$ ,  $b_{\phi'_1}(\bar{d}, \bar{d}) = [d, d] = 1$  et  $b_{\phi'_1}(\bar{c}, \bar{d}) = [c, d] = c^2$ . Donc

$$\text{Arf}(\phi'_1) = \phi'_1(\bar{c}).\phi'_1(\bar{d}) = c^2.d^2 = c^2.c^2 = c^2$$

est l'élément unité du corps  $Z(Q_2)$ .

Pour un entier  $n \geq 2$ , d'après la proposition 3.3.5,

$$G = \underbrace{G_1 \circ D_4 \circ \cdots \circ D_4}_{n \text{ facteurs}},$$

avec

$$G_1 = \begin{cases} D_4 & \text{si } G = 2_+^{1+2n} \\ Q_2 & \text{si } G = 2_-^{1+2n}. \end{cases}$$

D'après la proposition 3.3.4,

$$\frac{G}{Z(G)} \cong \underbrace{\frac{G_1}{Z(G_1)} \times \frac{D_4}{Z(D_4)} \times \cdots \times \frac{D_4}{Z(D_4)}}_{n \text{ facteurs}}.$$

D'où, en vertu du lemme 3.3.2.(2), pour tout  $x \in G$ , il existe  $(x_1, x_2, \dots, x_n) \in G_1 \times D_4 \times \cdots \times D_4$  tel que  $\bar{x} = (\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n)$ . Pour tout  $i = 1, 2, \dots, n$ , le produit

$$\underbrace{0 \times \cdots \times 0 \times \mathbb{F}_2 \times 0 \times \cdots \times 0}_{n \text{ facteurs}}$$

où  $\mathbb{F}_2$  se trouve à la  $i$ -ième position, s'identifie au corps à deux éléments  $\mathbb{F}_2$  qui, en vertu de la remarque 3.4.15, s'identifie respectivement à  $Z(G)$ , à  $Z(D_4)$  et à  $Z(Q_2)$ . On a alors :

$$\begin{aligned} \phi_n(\bar{x}) = (x_1^2, x_2^2, \dots, x_n^2) &= x_1^2 + x_2^2 + \cdots + x_n^2 \\ &= \phi(\bar{x}_1) + \phi_1(\bar{x}_2) + \cdots + \phi_1(\bar{x}_n), \end{aligned}$$

avec

$$\phi = \begin{cases} \phi_1 & \text{si } G = 2_+^{1+2n} \\ \phi'_1 & \text{si } G = 2_-^{1+2n} \end{cases},$$

Donc

$$\phi_n = \underbrace{\phi \perp \phi_1 \perp \cdots \perp \phi_1}_{n \text{ facteurs}}$$

et d'après la proposition 3.4.17,

$$\begin{aligned} \text{Arf}(\phi_n) &= \underbrace{\text{Arf}(\phi) + \text{Arf}(\phi_1) + \cdots + \text{Arf}(\phi_1)}_{n \text{ termes}} \\ &= \begin{cases} 0 & \text{si } G = 2_+^{1+2n} \\ 1 & \text{si } G = 2_-^{1+2n}. \blacksquare \end{cases} \end{aligned}$$

Il convient maintenant d'étudier la réciproque de la proposition 3.4.12. Autrement dit, étant donnés deux 2-groupes abéliens élémentaires  $A$  et  $B$  (vus comme des espaces vectoriels sur  $\mathbb{F}_2$ ) et une application quadratique  $q : A \rightarrow B$ , existe-t-il un 2-groupe spécial  $G$  tel que  $\frac{G}{Z(G)}$  et  $Z(G)$  soient respectivement isomorphes à  $A$  et  $B$  ?

Pour y arriver, il nous est indispensable de donner d'abord une classification des extensions centrales d'un espace vectoriel par un autre sur le corps  $\mathbb{F}_2$  à deux éléments.

Soient  $A$  et  $B$  deux espaces vectoriels sur le corps  $\mathbb{F}_2$ . On note

- $\text{Quad}(A, B)$  le groupe des applications quadratiques de  $A$  vers  $B$  ;
- $Z^2(A, B)$  le groupe des 2-cocycles normalisés de  $A$  à coefficients dans  $B$ , pour l'action triviale de  $A$  sur  $B$ , c'est-à-dire des applications  $c : A \times A \rightarrow B$  telles que pour  $x, y, z \in A$ ,

$$c(y, z) - c(x + y, z) + c(x, y + z) - c(x, y) = 0$$

et

$$c(x, 0) = c(0, x) = 0;$$

- $B^2(A, B)$  le sous-groupe de  $Z^2(A, B)$  constitué des cocycles de la forme

$$c(x, y) = \lambda(y) - \lambda(x + y) + \lambda(x)$$

- pour une application  $\lambda : A \rightarrow B$  telle que  $\lambda(0) = 0$  ;  
 –  $H^2(A, B) = \frac{Z^2(A, B)}{B^2(A, B)}$ , le deuxième groupe de cohomologie de  $A$  à coefficients dans  $B$ .

Le groupe  $H^2(A, B)$  classe les extensions centrales de  $B$  par  $A$ , c'est-à-dire les suites exactes

$$0 \rightarrow B \rightarrow G \rightarrow A \rightarrow 0$$

où  $G$  est un groupe contenant (l'image de)  $B$  dans son centre, voir [23, théorème 15.8.1] ou [20, exemple 3.2.6].

**Remarque 3.4.19.** *Il est important de préciser que pour tout  $c \in Z^2(A, B)$ , l'extension centrale de  $B$  par  $A$  correspondant à  $[c] \in H^2(A, B)$  est isomorphe au groupe*

$$G = \{(a.b) \mid a \in A, b \in B\}$$

dans lequel la multiplication est définie par :

$$(a, b).(a', b') = (a+a', c(a, a')+b+b'), \text{ pour } a, a' \in A \text{ et } b, b' \in B.$$

De plus dans la suite exacte

$$0 \longrightarrow B \xrightarrow{\alpha} G \xrightarrow{\pi} A \longrightarrow 0,$$

les morphismes  $\alpha$  et  $\pi$  sont définis par

$$\alpha(b) = (0, b) \text{ et } \pi(a, b) = a, \text{ pour } a \in A, b \in B.$$

Le résultat suivant est inspiré de [20, lemme 6.7.2] :

**Proposition 3.4.20.** *Pour tout cocycle  $c \in Z^2(A, B)$ , l'application  $q_c : A \rightarrow B$  définie par  $q_c(x) = c(x, x)$  est quadratique et  $b_{q_c}(x, y) = c(x, y) - c(y, x)$  pour  $x, y \in A$ . L'application*

$$\varphi : Z^2(A, B) \rightarrow \text{Quad}(A, B) : c \mapsto q_c$$

*induit un homomorphisme*

$$\overline{\varphi} : H^2(A, B) \rightarrow \text{Quad}(A, B).$$

*Si  $\dim A$  est finie, alors  $\overline{\varphi}$  est un isomorphisme.*

*Preuve :* Pour  $x, y \in A$ , la relation de cocycle donne

$$\begin{aligned} c(x+y, x+y) &= c(x, y+x+y) + c(x, y) + c(y, x+y) \\ &= c(x, x) + c(x, y) + c(y, x+y) \end{aligned}$$

et

$$\begin{aligned} c(y, y+x) &= c(y+y, x) + c(y, x) + c(y, y) \\ &= c(y, x) + c(y, y). \end{aligned}$$

En combinant ces égalités, on obtient

$$c(x+y, x+y) = c(x, x) + c(x, y) + c(y, x) + c(y, y),$$

donc

$$c(x+y, x+y) - c(x, x) - c(y, y) = c(x, y) - c(y, x)$$

et alors

$$q_c(x+y) - q_c(x) - q_c(y) = b_{q_c}(x, y).$$

Il reste à voir que l'application  $b_{q_c}$  est bilinéaire. Comme elle est clairement symétrique, il suffit de voir que pour  $x, y, z \in A$ ,

$$c(x+y, z) - c(z, x+y) = c(x, z) - c(z, x) + c(y, z) - c(z, y). \quad (3.7)$$

La relation de cocycle donne

$$c(y, z) - c(x+y, z) + c(x, y+z) - c(x, y) = 0,$$

$$c(z, y) - c(x+z, y) + c(x, z+y) - c(x, z) = 0,$$

$$c(x, y) - c(z+x, y) + c(z, x+y) - c(z, x) = 0.$$

En sommant ces égalités, on obtient (3.7).

Si  $c \in B^2(A, B)$  il est facile de voir que  $\varphi(c) = q_c = 0$ . Dès lors, l'application  $\varphi$  induit une application  $\bar{\varphi}$  bien définie sur les classes de cohomologie. On vérifie aisément que  $\bar{\varphi}$  est un morphisme de groupes.

Supposons que  $\dim A$  est finie.

- Prouvons d'abord que  $\bar{\varphi}$  est surjectif. On raisonne par induction sur  $\dim A$ . Si  $\dim A = 1$ , alors  $A = \{0, a\}$ . A toute application quadratique  $q : A \rightarrow B$  on associe l'application  $c : A \times A \rightarrow B$  définie par

$$c(0, 0) = c(a, 0) = c(0, a) = 0, \quad c(a, a) = q(a).$$

Il est facile de vérifier que  $c$  est un cocycle normalisé tel que  $q_c = q$ , ce qui établit la propriété lorsque  $\dim A = 1$ . Supposons ensuite que la propriété vaut pour les dimensions  $< n$ , et soit  $\dim A = n$ . Soit  $A_0 \subseteq A$  un sous-espace de dimension  $n - 1$  et soit  $e \in A \setminus A_0$ , de sorte que  $A = A_0 \cup (e + A_0)$ . Soit  $q \in \text{Quad}(A, B)$ . Par hypothèse d'induction, il existe un cocycle normalisé  $c_0 \in Z^2(A_0, B)$  tel que

$$c_0(x, x) = q(x) \quad \text{pour } x \in A_0.$$

On définit  $c : A \times A \rightarrow B$  comme suit : pour  $x, y \in A_0$ ,

$$c(x, e + y) = c(x, y) = c_0(x, y),$$

$$c(e + x, y) = c_0(x, y) + b_q(e, y),$$

$$c(e + x, e + y) = c_0(x, y) + b_q(e, y) + q(e).$$

Des vérifications sans difficulté montrent que  $c$  est un 2-cocycle normalisé tel que  $q_c = q$ .

- Montrons finalement que  $\bar{\varphi}$  est injectif. Soit  $c \in \text{Ker } \varphi$ , alors pour tout  $x \in A$ ,  $c(x, x) = 0$ . Donc  $q_c = 0$  et  $b_{q_c} = 0$  et alors  $c(x, y) = c(y, x)$  pour tous  $x, y \in A$ . Il suffit de prouver que  $c \in B^2(A, B)$  c'est-à-dire qu'il existe une application  $\lambda : A \rightarrow B$  telle que  $\lambda(0) = 0$  et  $c(x, y) = \lambda(x) + \lambda(y) - \lambda(x + y)$ . Raisonnons par induction sur  $\dim A$ . Si  $\dim A = 1$ , alors  $A = \{0, a\}$  et donc  $c(0, 0) = c(a, 0) = c(0, a) = 0$  ( $c$  étant normalisé) et  $c(a, a) = 0$  (par hypothèse). On peut donc prendre  $\lambda = 0$ . Supposons le résultat vérifié pour les dimensions  $< n$  et que  $\dim A = n$ . Soit  $A_0$  un sous-espace vectoriel de  $A$  de dimension  $n - 1$  et soit  $e \in A \setminus A_0$ , de sorte

que  $A = A_0 \cup (e + A_0)$ . D'après l'hypothèse d'induction, il existe une application  $\lambda_0 : A_0 \rightarrow B$  telle que  $\lambda_0(0) = 0$  et

$$c(x, y) = \lambda_0(x) + \lambda_0(y) - \lambda_0(x + y), \quad \text{pour tous } x, y \in A_0 \quad (3.8)$$

Soit  $\lambda : A \rightarrow B$  l'application définie par

$$\lambda(x) = \lambda_0(x) \quad \text{et} \quad \lambda(e + x) = c(e, x) + \lambda_0(x) \quad \text{pour tout } x \in A_0$$

Soient  $x, y \in A_0$ . La relation de cocycle donne

$$c(x, y) - c(e + x, y) + c(e, x + y) - c(e, x) = 0,$$

donc

$$c(e + x, y) = c(x, y) + c(e, x + y) - c(e, x). \quad (3.9)$$

Par définition de  $\lambda$ , on a :

$$c(e, x + y) = \lambda(e + x + y) - \lambda_0(x + y) \quad \text{et} \quad c(e, x) = \lambda(e + x) - \lambda_0(x). \quad (3.10)$$

De ( 3.8), ( 3.9) et ( 3.10) il résulte que

$$c(e + x, y) = \lambda(e + x) + \lambda(y) - \lambda(e + x + y) \quad (3.11)$$

et par symétrie,

$$c(x, e + y) = \lambda(x) + \lambda(e + y) - \lambda(e + x + y). \quad (3.12)$$

La relation de cocycle donne

$$c(x, y) - c(x + x, y) + c(x, x + y) - c(x, x) = 0,$$

donc

$$c(x, y) = c(x, x + y). \quad (3.13)$$

La relation ( 3.13) vaut pour tous  $x, y \in A$  et donc

$$c(e + x, e + y) = c(e + x, e + x + e + y) = c(e + x, x + y).$$

D'après ( 3.11),

$$\begin{aligned} c(e+x, x+y) &= \lambda(e+x) + \lambda(x+y) - \lambda(e+x+x+y) \\ &= \lambda(e+x) + \lambda(x+y) - \lambda(e+y). \end{aligned}$$

On en déduit que

$$\begin{aligned} c(e+x, e+y) &= \lambda(e+x) + \lambda(x+y) - \lambda(e+y) \\ &= \lambda(e+x) + \lambda(e+y) - \lambda(e+x+e+y). \end{aligned} \quad (3.14)$$

De ( 3.8), ( 3.11), ( 3.12) et ( 3.14), il résulte que  $c \in B^2(A, B)$ , donc  $\bar{\varphi}$  est injectif. ■

**Remarque 3.4.21.** Avec les notations de la proposition 3.4.20, si  $\dim A$  est finie,  $H^2(A, B) \cong \text{Quad}(A, B)$  classifie les extensions centrales de  $B$  par  $A$ . En particulier, si  $G$  est un 2-groupe spécial, le groupe  $\text{Quad}(\frac{G}{Z(G)}, Z(G))$  classifie les extensions centrales de  $Z(G)$  par  $\frac{G}{Z(G)}$ .

Pour trouver la réciproque de la proposition 3.4.12, nous aurons aussi besoin du lemme suivant :

**Lemme 3.4.22.** Soient  $G$  un groupe fini et  $(x_i)_{1 \leq i \leq n}$  et  $(y_j)_{1 \leq j \leq m}$  des familles d'éléments de  $G$  tels que  $[x_i, y_j] \in Z(G)$ , pour tous  $i, j$ . Alors

$$[x_1 x_2 \cdots x_n, y_1 y_2 \cdots y_m] = \prod_{i,j} [x_i, y_j].$$

*Preuve :* Raisonnons par induction sur  $n$  et  $m$ .

1. D'après le lemme 3.4.11,

$$[x_1 x_2, y_1] = [x_1, y_1]^{x_2} [x_2, y_1] = [x_1, y_1] [x_2, y_1].$$

Soit  $n$  un entier  $> 2$ . D'après le lemme 3.4.11,

$$[x_1 x_2 \cdots x_n, y_1] = [x_1 x_2 \cdots x_{n-1}, y_1]^{x_n} [x_n, y_1]; \quad (3.15)$$

d'après l'hypothèse d'induction,

$$[x_1 x_2 \cdots x_{n-1}, y_1] = \prod_{i=1}^{n-1} [x_i, y_1] \in Z(G). \quad (3.16)$$

( 3.15) et ( 3.16) donnent alors :

$$[x_1 x_2 \cdots x_n, y_1] = \left( \prod_{i=1}^{n-1} [x_i, y_1] \right) [x_n, y_1] = \prod_{i=1}^n [x_i, y_1]. \quad (3.17)$$

2. Par un raisonnement analogue, on établit que

$$[x_1, y_1 y_2 \cdots y_m] = \prod_{j=1}^m [x_1, y_j]. \quad (3.18)$$

3. Soient maintenant  $n$  et  $m$  des entiers  $\geq 2$ . D'après le lemme 3.4.11,

$$\begin{aligned} & [x_1 x_2 \cdots x_n, y_1 y_2 \cdots y_m] \\ &= [x_1 x_2 \cdots x_{n-1}, y_1 y_2 \cdots y_m]^{x_n} [x_n, y_1 y_2 \cdots y_m] \\ &= ([x_1 x_2 \cdots x_{n-1}, y_m] [x_1 x_2 \cdots x_{n-1}, y_1 y_2 \cdots y_{m-1}]^{y_m})^{x_n} [x_n, y_1 y_2 \cdots y_m]. \end{aligned}$$

D'après l'hypothèse d'induction,

$$[x_1 x_2 \cdots x_{n-1}, y_1 y_2 \cdots y_{m-1}] = \prod_{\substack{1 \leq i \leq n-1 \\ 1 \leq j \leq m-1}} [x_i, y_j] \in Z(G).$$

et en utilisant ( 3.18) et ( 3.17), on obtient alors

$$[x_1 x_2 \cdots x_n, y_1 y_2 \cdots y_m] = \prod_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} [x_i, y_j]. \quad \blacksquare$$



On a alors le résultat suivant :

**Théorème 3.4.23.** *Soient  $A$  et  $B$  des 2-groupes abéliens élémentaires,  $q : A \rightarrow B$  une application quadratique régulière d'application polaire  $b_q : A \times A \rightarrow B$ . On suppose que  $B = \text{sgr} \langle b_q(A \times A) \rangle$ . A isomorphisme près, il existe alors un unique 2-groupe spécial  $G$  d'application quadratique  $q$ , tel que  $B = Z(G)$  et  $A = \frac{G}{Z(G)}$ .*

*Preuve :*

**Construction de  $G$ .** Soit  $(e_i)_{1 \leq i \leq n}$  une base de  $A$  sur le corps  $\mathbb{F}_2$ . Soit  $(\delta_i)_{1 \leq i \leq n}$  une famille de  $n$  symboles. Soit  $L$  le groupe libre engendré par  $(\delta_i)_{1 \leq i \leq n}$ . Soit  $P = B \times L := BL$  le produit direct de  $B$  et  $L$ . Tout élément  $p$  de  $P$  s'écrit donc de façon unique sous la forme  $p = bl = lb$ , avec  $b \in B$  et  $l \in L$ . Soit  $\gamma : P \rightarrow A$  l'homomorphisme de groupes tel que

$$\gamma(\delta_i) = e_i, \forall i \text{ et } \gamma(u) = 1, \forall u \in B.$$

C'est clair que  $\gamma$  est un morphisme surjectif de groupes. Soit

$$R = \text{sgr} \langle x^2 q(\gamma(x)) \mid x \in L \rangle$$

Pour tout  $i = 1, 2, \dots, n$ , pour tout  $x \in L$ , pour tout  $u \in B$ , on a :

$$\delta_i x^2 q(\gamma(x)) \delta_i^{-1} = (\delta_i x \delta_i^{-1})^2 q(\gamma(\delta_i x \delta_i^{-1})) \in R;$$

donc  $\delta_i R \delta_i^{-1} \subset R$ ; de plus, comme  $u$  commute avec tout élément de  $L$  et  $B$  est commutatif, alors  $u$  commute avec tout élément de  $R$  et donc  $u R u^{-1} \subset R$ . Il en résulte que  $R$  est un sous-groupe normal de  $P$ . Posons maintenant  $G = \frac{P}{R}$  et pour tout  $i = 1, 2, \dots, n$ ,  $g_i = \delta_i R$ . Pour tout  $x \in L$ ,

$$\gamma(x^2 q(\gamma(x))) = \gamma(x^2) \gamma(q(\gamma(x))) = (\gamma(x))^2 = 1.$$

Donc  $\gamma(R) = 1$  et alors  $R \subset \text{Ker} \gamma$ . Il existe alors un unique morphisme de groupes  $\bar{\gamma} : \frac{P}{R} = G \rightarrow A$  tel que  $\bar{\gamma} \tau = \gamma$ , où  $\tau : P \rightarrow G$  est la surjection canonique. De plus, on a :

$$\text{Ker} \bar{\gamma} = \tau(\text{Ker} \gamma) = \tau(B).$$

Plus précisément,  $\bar{\gamma}$  est défini par :

$$\bar{\gamma}(uR) = 1, \forall u \in B \text{ et } \bar{\gamma}(g_i) = e_i, \forall i. \quad (3.19)$$

Soit  $\lambda : B \rightarrow G = \frac{P}{R}$  l'application définie par

$$\lambda(u) = uR \text{ pour } u \in B. \quad (3.20)$$

$\lambda$  est clairement un morphisme de groupes : c'est la restriction de la surjection canonique  $\tau : P \rightarrow G$  à  $B$ . D'une part, pour tout  $u \in B$ ,

$$\bar{\gamma}\lambda(u) = \bar{\gamma}(uR) = \gamma(u) = 1;$$

donc  $\bar{\gamma}\lambda = 1$ . D'autre part

$$Im\lambda = \lambda(B) = \tau(B) = Ker\bar{\gamma}.$$

Et comme  $\bar{\gamma}$  est surjective, alors la suite

$$B \xrightarrow{\lambda} G \xrightarrow{\bar{\gamma}} A \rightarrow 1$$

est exacte. Nous voulons démontrer que  $\lambda$  est injectif pour identifier  $B$  à son image dans  $G$ .

Avec les notations de la proposition 3.4.20 (les espaces vectoriels  $A$  et  $B$  sont considérés en notation multiplicative), le morphisme  $\bar{\varphi}$  étant surjectif, il existe un 2-cocycle  $c \in Z^2(A, B)$  tel que  $\varphi(c) = q_c = q$ . Soit

$$1 \rightarrow B \xrightarrow{\omega} E \xrightarrow{\pi} A \rightarrow 1 \quad (3.21)$$

l'extension centrale de  $B$  par  $A$  associée au 2-cocycle  $c$ . Pour  $i = 1, 2, \dots, n$ , on choisit  $l_i \in E$  tel que  $\pi(l_i) = e_i$  et on définit un homomorphisme  $\psi : P \rightarrow E$  par

$$\psi(u) = u \text{ et } \psi(q(e_i)\delta_i) = l_i \text{ pour } u \in B \text{ et } i = 1, 2, \dots, n.$$

Alors

$$\psi(\delta_i) = \psi(q(e_i)\delta_i q(e_i)) = l_i q(e_i) \text{ pour } i = 1, 2, \dots, n.$$

La suite ( 3.21) étant exacte,  $\pi$  est surjectif,  $\omega$  est injectif et  $\text{Ker}\pi = \text{Im}\omega \cong B$ ; comme cette extension est centrale, alors  $B \subset Z(E)$ . Donc  $\frac{E}{\text{Ker}\pi}$  est isomorphe à  $A$  et l'isomorphisme  $\frac{E}{\text{Ker}\pi} \xrightarrow{\cong} A$  est tel que  $x\text{Ker}\pi \mapsto \pi(x)$  pour  $x \in E$ .  $q = q_c$  étant l'application quadratique associée à la suite ( 3.21), alors

$$x^2 = q(\pi(x)), \quad \text{pour } x \in E. \quad (3.22)$$

Montrons maintenant que  $\psi(R) = 1$ . Soit alors  $x \in L$  tel que l'écriture réduite de  $x$  soit

$$x = \delta_{i_1}^{\varepsilon_{i_1}} \delta_{i_2}^{\varepsilon_{i_2}} \cdots \delta_{i_t}^{\varepsilon_{i_t}},$$

avec  $1 \leq i_j \leq n$ ,  $\varepsilon_{i_j} = \pm 1$  et  $\varepsilon_{i_j} = \varepsilon_{i_{j+1}}$  si  $\delta_{i_j} = \delta_{i_{j+1}}$ , pour  $j = 1, 2, \dots, t$ . On a :

$$\begin{aligned} & \psi(x^2 q(\gamma(x))) \\ &= (\psi(x))^2 q(\gamma(x)) \\ &= q(\pi(\psi(x))) q(\gamma(x)) \quad (\text{d'après } 3.22) \\ &= q(\pi(\psi(\delta_{i_1}^{\varepsilon_{i_1}} \delta_{i_2}^{\varepsilon_{i_2}} \cdots \delta_{i_t}^{\varepsilon_{i_t}}))) q(\gamma(\delta_{i_1}^{\varepsilon_{i_1}} \delta_{i_2}^{\varepsilon_{i_2}} \cdots \delta_{i_t}^{\varepsilon_{i_t}})) \\ &= q(\pi(l_{i_1}^{\varepsilon_{i_1}} l_{i_2}^{\varepsilon_{i_2}} \cdots l_{i_t}^{\varepsilon_{i_t}}) q(e_{i_1}^{\varepsilon_{i_1}}) q(e_{i_2}^{\varepsilon_{i_2}}) \cdots q(e_{i_t}^{\varepsilon_{i_t}}))) q(e_{i_1}^{\varepsilon_{i_1}} e_{i_2}^{\varepsilon_{i_2}} \cdots e_{i_t}^{\varepsilon_{i_t}}) \\ &= q(e_{i_1}^{\varepsilon_{i_1}} e_{i_2}^{\varepsilon_{i_2}} \cdots e_{i_t}^{\varepsilon_{i_t}}) q(e_{i_1}^{\varepsilon_{i_1}} e_{i_2}^{\varepsilon_{i_2}} \cdots e_{i_t}^{\varepsilon_{i_t}}) \\ &= 1 \end{aligned}$$

Donc  $\psi(R) = 1$  et alors  $R \subset \text{Ker}\psi$ ; il en résulte que  $\psi$  induit un morphisme de groupes  $\bar{\psi} : G = \frac{P}{R} \rightarrow E$ . Par identification de tout élément de  $B$  à son image par  $\omega$  dans  $E$ , observons que d'une part,

$$\pi \bar{\psi}(g_i) = \pi(\bar{\psi}(\delta_i R)) = \pi(l_i q(e_i)) = e_i = \bar{\gamma}(g_i)$$

et

$$\pi \bar{\psi}(uR) = \pi(u) = \pi(\omega(u)) = 1 = \bar{\gamma}(uR);$$

donc  $\pi \bar{\psi} = \bar{\gamma}$ . D'autre part,

$$\bar{\psi} \lambda(u) = \bar{\psi}(uR) = u = \omega(u)$$

et alors  $\bar{\psi}\lambda = \omega$ . Dès lors le diagramme suivant où les lignes sont exactes, est commutatif :

$$\begin{array}{ccccccc} B & \xrightarrow{\lambda} & G & \xrightarrow{\bar{\gamma}} & A & \longrightarrow & 1 \\ \parallel & & \downarrow \bar{\psi} & & \parallel & & \\ 1 & \longrightarrow & B & \xrightarrow{\omega} & E & \xrightarrow{\pi} & A \longrightarrow 1 \end{array}$$

Cela prouve d'une part que  $\lambda$  est injectif, d'autre part que l'extension (3.21) est isomorphe à l'extension

$$1 \rightarrow B \xrightarrow{\lambda} G \xrightarrow{\bar{\gamma}} A \rightarrow 1.$$

On vérifie aisément que  $G$  est le groupe engendré par  $B$  et les éléments  $g_1, g_2, \dots, g_n$ . D'une part, observons que pour tous  $x, y \in L$ , pour tout  $u \in B$ ,

$$x^2 q(\gamma(x)) \in R, \quad [x, u] = 1 \in R$$

et

$$[x, y] b_q(\gamma(x), \gamma(y)) = x^{-2} q(\gamma(x^{-1})) (xy^{-1})^2 q(\gamma(xy^{-1})) y^2 q(\gamma(y)) \in R$$

Donc les éléments générateurs de  $G$  possèdent les propriétés suivantes :

$$g_i^2 = q(e_i), \forall i \tag{3.23}$$

$$[g_i, u] = 1, \forall i, \forall u \in B \tag{3.24}$$

$$[g_i, g_j] = b_q(e_i, e_j), \forall i, j. \tag{3.25}$$

Le lemme suivant donne une façon précise d'écrire tout élément du groupe  $G$ .

**Lemme 3.4.24.** *Tout élément  $g$  du groupe  $G$  donné ci-dessus s'écrit de façon unique sous la forme*

$$g = g_{i_1} g_{i_2} \cdots g_{i_s} u,$$

avec  $u \in B$  et  $0 \leq i_1 < i_2 < \cdots < i_s \leq n$ .

*Preuve :* Les relations qui définissent la multiplication dans le groupe  $G$ , impliquent respectivement que

$$g_i^{-1} = g_i q(e_i), \forall i \quad (3.26)$$

$$g_i u = u g_i, \quad \forall i, \forall u \in B \quad (3.27)$$

$$g_i g_j = g_j g_i b_q(e_i, e_j), \quad \forall i, j \quad (3.28)$$

et donc que tout élément du groupe  $G$  peut s'écrire comme annoncé dans le lemme. Il reste à prouver l'unicité de cette écriture. Soit  $g \in G$ . Supposons que  $g$  s'écrit de deux façons sous la forme

$$g = g_{i_1} g_{i_2} \cdots g_{i_s} u = g_{i'_1} g_{i'_2} \cdots g_{i'_{s'}} v, \quad (3.29)$$

avec  $u, v \in B$ ,  $0 \leq i_1 < i_2 < \cdots < i_s \leq n$  et  $0 \leq i'_1 < i'_2 < \cdots < i'_{s'} \leq n$ . Alors

$$\bar{\gamma}(g_{i_1} g_{i_2} \cdots g_{i_s} u) = \bar{\gamma}(g_{i'_1} g_{i'_2} \cdots g_{i'_{s'}} v).$$

D'où  $e_{i_1} e_{i_2} \cdots e_{i_s} = e_{i'_1} e_{i'_2} \cdots e_{i'_{s'}}$  et comme  $(e_i)_{1 \leq i \leq n}$  est une base de  $A$ , alors  $(i_1, i_2, \dots, i_s) = (i'_1, i'_2, \dots, i'_{s'})$ ; donc  $s = s'$  et  $i_j = i'_j$ , pour tout  $j$ . D'où  $u = v$ , ce qui prouve l'unicité de l'écriture. ■

Après cette phase de construction de  $G$ , nous allons établir la preuve du théorème en six étapes.

**Première étape :** Montrons que  $B = Z(G)$ . La condition (3.24) implique que  $B \subset Z(G)$ . Soit  $g \in Z(G)$ . Alors pour tout  $i = 1, 2, \dots, n$ ,

$$[g, g_i] = 1.$$

Supposons qu'il existe une partie non vide  $\Gamma_s = \{i_1, i_2, \dots, i_s / i_1 < i_2 < \cdots < i_s\}$  de  $\{1, 2, \dots, n\}$  telle que  $g = g_{i_1} g_{i_2} \cdots g_{i_s} u$ , avec  $u \in B$ . Pour tout  $j = 1, 2, \dots, s$ ,  $[g_{i_j}, g_i] = b_q(e_{i_j}, e_i) \in B \subset Z(G)$  (d'après (3.25)) et  $[u, g_i] = 1 \in Z(G)$ . Donc d'après le lemme 3.4.22,

$$1 = [g, g_i] = \prod_{j=1}^s [g_{i_j}, g_i] = \prod_{j=1}^s b_q(e_{i_j}, e_i) = b_q\left(\prod_{j=1}^s e_{i_j}, e_i\right).$$

Or  $(e_i)_{1 \leq i \leq n}$  est une base de  $A$  sur  $\mathbb{F}_2$ ; donc pour tout  $y \in A$ ,  $b_q(\prod_{j=1}^s e_{i_j}, y) = 1$ . Par suite  $\prod_{j=1}^s e_{i_j} \in \text{rad}b_q$  et  $q$  étant régulière, alors  $\prod_{j=1}^s e_{i_j} = 1$ , ce qui est absurde car le système  $(e_{i_j})_{j=1}^s$  est libre. On en déduit que  $g = u \in B$ . D'où  $Z(G) \subset B$ .

**Deuxième étape :** Comme  $Z(G) = B$  est un 2-groupe abélien élémentaire, alors  $\Omega(Z(G)) = Z(G)$ .

**Troisième étape :** Montrons que  $G' = B$ .

D'une part, soient  $g, h \in G$  tels que

$$g = g_{i_1} g_{i_2} \cdots g_{i_s} u \text{ et } h = g_{i'_1} g_{i'_2} \cdots g_{i'_{s'}} v$$

avec  $u, v \in B$ ,  $0 \leq i_1 < i_2 < \cdots < i_s \leq n$  et  $0 \leq i'_1 < i'_2 < \cdots < i'_{s'} \leq n$ . Pour tous  $j$  et  $l$ , on a :

$$[g_{i_j}, g_{i'_l}] = b_q(e_{i_j}, e_{i'_l}) \in Z(G)$$

et

$$[g_{i_j}, v] = [u, g_{i'_l}] = 1 \in Z(G).$$

Donc d'après le lemme 3.4.22,

$$[g, h] = \prod_{\substack{1 \leq j \leq s \\ 1 \leq l \leq s'}} [g_{i_j}, g_{i'_l}] \in B.$$

Il en résulte que  $G' \subset B$ .

D'autre part, soient  $x, y \in A$ . Si  $x = 1$  ou  $y = 1$ , alors  $b_q(x, y) = 1 \in G'$ . Si  $x \neq 1$  et  $y \neq 1$ , il existe des parties non vides  $\{i_1, i_2, \cdots, i_s / i_1 < i_2 < \cdots < i_s\}$  et  $\{i'_1, i'_2, \cdots, i'_{s'} / i'_1 < i'_2 < \cdots < i'_{s'}\}$  de  $\{1, 2, \cdots, n\}$  telles que

$$x = \prod_{j=1}^s e_{i_j} \text{ et } y = \prod_{l=1}^{s'} e_{i'_l}.$$

D'où

$$b_q(x, y) = \prod_{\substack{1 \leq j \leq s \\ 1 \leq l \leq s'}} b_q(e_{i_j}, e_{i'_l}) = \prod_{\substack{1 \leq j \leq s \\ 1 \leq l \leq s'}} [g_{i_j}, g_{i'_l}] \in G'.$$

On en déduit que  $B = \text{sgr} < b_q(A \times A) > \subset G'$ .

**Quatrième étape :** Montrons que  $\Phi(G) = G'$ . Pour y arriver, nous utiliserons le lemme suivant :

**Lemme 3.4.25.** *Avec les notations utilisées dans la démonstration ci-dessus, pour toute partie non vide  $\{i_1, i_2, \dots, i_s | i_1 < i_2 < \dots < i_s\}$  de  $\{1, 2, \dots, n\}$ , on a :*

$$q\left(\prod_{j=1}^s e_{i_j}\right) = (g_{i_1} g_{i_2} \cdots g_{i_s})^2 = \prod_{j=1}^s g_{i_j}^2 \prod_{1 \leq j < l \leq s} [g_{i_j}, g_{i_l}]$$

*Preuve :* Raisonnons par induction sur  $s$ . D'après ( 3.25),

$$[g_{i_1}, g_{i_2}] = b_q(e_{i_1}, e_{i_2}) = q(e_{i_1} e_{i_2}) q(e_{i_1}) q(e_{i_2}).$$

D'après ( 3.23),  $g_{i_j}^2 = q(e_{i_j}) \in B = Z(G)$ , pour tout  $j$ . Donc

$$q(e_{i_1} e_{i_2}) = g_{i_1}^2 g_{i_2}^2 [g_{i_1}, g_{i_2}] = (g_{i_1} g_{i_2})^2.$$

Soit  $s$  un entier  $> 2$ . Comme

$$b_q\left(\prod_{j=1}^{s-1} e_{i_j}, e_{i_s}\right) = q\left(\prod_{j=1}^s e_{i_j}\right) q\left(\prod_{j=1}^{s-1} e_{i_j}\right) q(e_{i_s}),$$

alors

$$\begin{aligned} q\left(\prod_{j=1}^s e_{i_j}\right) &= q\left(\prod_{j=1}^{s-1} e_{i_j}\right) q(e_{i_s}) b_q\left(\prod_{j=1}^{s-1} e_{i_j}, e_{i_s}\right) \\ &= q\left(\prod_{j=1}^{s-1} e_{i_j}\right) g_{i_s}^2 \prod_{j=1}^{s-1} b_q(e_{i_j}, e_{i_s}) \\ &= q\left(\prod_{j=1}^{s-1} e_{i_j}\right) g_{i_s}^2 \prod_{j=1}^{s-1} [g_{i_j}, g_{i_s}]. \end{aligned}$$

D'après l'hypothèse d'induction,

$$q\left(\prod_{j=1}^{s-1} e_{i_j}\right) = (g_{i_1}g_{i_2} \cdots g_{i_{s-1}})^2 = \prod_{j=1}^{s-1} g_{i_j}^2 \prod_{1 \leq j < l \leq s-1} [g_{i_j}, g_{i_l}].$$

On en déduit d'une part que

$$\begin{aligned} q\left(\prod_{j=1}^s e_{i_j}\right) &= (g_{i_1}g_{i_2} \cdots g_{i_{s-1}})^2 g_{i_s}^2 \prod_{j=1}^{s-1} [g_{i_j}, g_{i_s}] \\ &= (g_{i_1}g_{i_2} \cdots g_{i_{s-1}})^2 g_{i_s}^2 [g_{i_1}g_{i_2} \cdots g_{i_{s-1}}, g_{i_s}] \quad (\text{lemme 3.4.22}) \\ &= (g_{i_1}g_{i_2} \cdots g_{i_s})^2; \end{aligned}$$

et d'autre part que

$$\begin{aligned} q\left(\prod_{j=1}^s e_{i_j}\right) &= \prod_{j=1}^{s-1} g_{i_j}^2 \left( \prod_{1 \leq j < l \leq s-1} [g_{i_j}, g_{i_l}] \right) g_{i_s}^2 \prod_{j=1}^{s-1} [g_{i_j}, g_{i_s}] \\ &= \prod_{j=1}^s g_{i_j}^2 \prod_{1 \leq j < l \leq s} [g_{i_j}, g_{i_l}]. \end{aligned}$$

Le lemme est ainsi établi. ■

**Suite de la preuve du théorème 3.4.23 :** Montrons maintenant que  $\Phi(G) = G'$ . Soit  $g$  un élément de  $G$  tel que  $g = g_{i_1}g_{i_2} \cdots g_{i_s}u$ , avec  $u \in B$  et  $0 \leq i_1 < i_2 < \cdots < i_s \leq n$ . D'après le lemme 3.4.25,

$$g^2 = (g_{i_1}g_{i_2} \cdots g_{i_s})^2 u^2 = \prod_{j=1}^s g_{i_j}^2 \prod_{1 \leq j < l \leq s} [g_{i_j}, g_{i_l}].$$

Donc  $g^2 \in B = G'$  et comme  $B$  est un 2-groupe abélien élémentaire, alors l'ordre de  $g$  est au plus égal à 4. Donc  $G$  est un 2-groupe ; par suite, d'après la proposition 3.4.2,  $\Phi(G) = sgr < h^2/h \in G >$ . Il en résulte que  $\Phi(G) \subset G'$ . Réciproquement, d'après la troisième étape de la démonstration et l'hypothèse de départ,  $G' = B = sgr < b_q(A \times A) >$  ; par ailleurs,  $sgr < b_q(A \times A) > \subset sgr < q(A) >$ , en



effet, pour tous  $x, y \in A$ ,  $b_q(x, y) = q(xy)q(x)q(y) \in sgr < q(A) >$ . Donc  $G' \subset sgr < q(A) >$ . Soit alors  $x \in A$ . Si  $x \neq 1$ , alors étant donné que  $(e_i)_{1 \leq i \leq n}$  est une base de  $A$  sur  $\mathbb{F}_2$ , il existe une partie non vide  $\{i_1, i_2, \dots, i_s\}$  de  $\{1, 2, \dots, n\}$  telle que  $x = \prod_{j=1}^s e_{i_j}$ . D'après le lemme 3.4.25,  $q(x) = (g_{i_1} g_{i_2} \dots g_{i_s})^2 \in \Phi(G)$ ; on en déduit que  $G' \subset \Phi(G)$ .

Des 4 premières étapes, il résulte que  $G$  est un 2-groupe spécial.

**Cinquième étape :** Il reste à démontrer que  $A$  et  $\frac{G}{Z(G)}$  sont égaux à isomorphisme près. Le morphisme de groupes  $\bar{\gamma} : G \rightarrow A$  défini ci-dessus (voir ( 3.19)), est surjectif et a pour noyau  $B = Z(G)$ ; donc  $A$  et  $\frac{G}{Z(G)}$  sont isomorphes. Les lemmes 3.4.24 et 3.4.25 impliquent que pour tout  $g \in G$ ,

$$g^2 = q(\bar{\gamma}(g)). \quad (3.30)$$

Par ailleurs l'isomorphisme canonique  $\frac{G}{Z(G)} \rightarrow A$  induit par  $\bar{\gamma}$  est tel que pour tout  $g \in G$ ,  $\bar{g} = gZ(G) \mapsto \bar{\gamma}(g)$ . Donc l'application quadratique de  $G$  est  $q$ .

**Sixième étape :** Unicité de  $G$ . D'après ce qui précède, le 2-groupe spécial  $G$  est une extension de  $B$  par  $A$  via la suite exacte

$$1 \rightarrow B \xrightarrow{\lambda} G \xrightarrow{\bar{\gamma}} A \rightarrow 1,$$

d'application quadratique  $q$ ,  $\lambda$  et  $\bar{\gamma}$  étant les morphismes de groupes définis respectivement en ( 3.20) et en ( 3.19). Soit  $H$  un autre 2-groupe spécial tel que  $B = Z(H)$  et  $A = \frac{H}{Z(H)}$ , d'application quadratique  $q$ , qui est une extension de  $B$  par  $A$ , via une suite exacte

$$1 \rightarrow B \xrightarrow{\mu} H \xrightarrow{\beta} A \rightarrow 1.$$

Il faut prouver l'existence d'un isomorphisme de groupes  $\Delta : G \rightarrow H$  tel que le diagramme suivant soit commutatif :

$$\begin{array}{ccccccc}
 1 & \longrightarrow & B & \xrightarrow{\lambda} & G & \xrightarrow{\bar{\gamma}} & A \longrightarrow 1 \\
 & & \parallel & & \vdots & \Delta & \parallel \\
 1 & \longrightarrow & B & \xrightarrow{\mu} & H & \xrightarrow{\beta} & A \longrightarrow 1
 \end{array} \quad (3.31)$$

Posons  $\bar{H} := \frac{H}{Z(H)}$  et  $\bar{h} := hZ(H)$ , pour tout  $h \in H$ . La deuxième ligne de ce diagramme étant exacte,  $\beta$  est surjective et  $\text{Ker}\beta = \text{Im}\mu \cong B = Z(H)$ . D'où  $\frac{H}{\text{Ker}\beta} \cong A$  et donc l'isomorphisme  $\bar{H} \rightarrow A$  est tel que pour tout  $h \in H$ ,  $\bar{h} \mapsto \beta(h)$ . Or  $q$  est l'application quadratique de  $H$ . Donc pour tout  $h \in H$ ,

$$h^2 = q(\beta(h)). \quad (3.32)$$

$\beta$  étant surjective, pour tout  $i = 1, 2, \dots, n$ , il existe  $h_i \in G$  tel que  $\beta(h_i) = e_i$  et donc par l'isomorphisme  $\bar{H} \rightarrow A$ ,  $\bar{h}_i \mapsto \beta(h_i) = e_i$ . On en déduit que  $(\bar{h}_i)_{1 \leq i \leq n}$  est une base de  $\bar{H}$  sur le corps  $\mathbb{F}_2$ . Pour tout  $h \in H$ , il existe alors une partie  $\Gamma_s = \{i_1, i_2, \dots, i_s\}$  de  $\{1, 2, \dots, n\}$  à  $s$  éléments (qui est vide si  $h \in Z(H)$ ) telle que

$$\bar{h} = \bar{h}_{i_1} \bar{h}_{i_2} \cdots \bar{h}_{i_s} = \overline{(h_{i_1} h_{i_2} \cdots h_{i_s})}$$

et donc  $h^{-1}(h_{i_1} h_{i_2} \cdots h_{i_s}) \in Z(H)$ . D'où il existe  $u \in Z(H)$  tel que  $h = (h_{i_1} h_{i_2} \cdots h_{i_s})u$  et alors  $H$  est engendré par  $Z(H) = B$  et la famille  $(h_i)_{1 \leq i \leq n}$ . De (3.30) et (3.32), il résulte que pour tous  $g, g' \in G$ , pour tous  $h, h' \in H$ ,

$$[g, g'] = b_q(\bar{\gamma}(g), \bar{\gamma}(g')) \quad \text{et} \quad [h, h'] = b_q(\beta(h), \beta(h')).$$

On a alors :

$$h_i^2 = q(\beta(h_i)) = q(e_i) = q(\bar{\gamma}(g_i)) = g_i^2, \quad \forall i$$

$$[h_i, u] = 1 = [g_i, u], \quad \forall i, \forall u \in B$$

$$[h_i, h_j] = b_q(\beta(h_i), \beta(h_j)) = b_q(e_i, e_j) = b_q(\bar{\gamma}(g_i), \bar{\gamma}(g_j)) = [g_i, g_j],$$

pour tous  $i, j$ . Les générateurs de  $H$  possèdent alors les mêmes propriétés que ceux de  $G$ . D'où, d'après le lemme 3.4.24, tout élément  $h$  de  $H$  s'écrit de façon unique sous la forme

$$h = h_{i_1} h_{i_2} \cdots h_{i_s} u,$$

avec  $u \in B$  et  $0 \leq i_1 < i_2 < \cdots < i_s \leq n$ . Soit  $\Delta_0 : P \rightarrow H$  l'homomorphisme défini par

$$\Delta_0(u) = u \quad \text{et} \quad \Delta_0(\delta_i) = h_i \quad \text{pour} \quad u \in B \quad \text{et} \quad i = 1, 2, \dots, n.$$

Par un raisonnement analogue à celui utilisé dans la phase de construction de  $G$  pour démontrer que  $\lambda : B \rightarrow G$  est injectif (en passant par le morphisme  $\bar{\psi} : G \rightarrow E$ , juste avant le lemme 3.4.24), on vérifie que  $\Delta_0(R) = 1$  et donc que  $\Delta_0$  induit un morphisme de groupes  $\Delta : G \rightarrow H$  tel que  $\Delta(u) = u$  et  $\Delta(g_i) = h_i$  pour  $u \in B$  et  $i = 1, 2, \dots, n$ . L'unicité de l'écriture de tout élément de  $H$  sous la forme donnée par le lemme 3.4.24 implique que  $\Delta$  est injectif et donc bijectif. Donc  $\Delta$  est un isomorphisme de groupes. Il reste à vérifier que le diagramme (3.31) est commutatif. Notons d'abord que comme les lignes de ce diagramme sont exactes, les morphismes  $\lambda$  et  $\mu$  sont injectifs. Donc pour tout  $u \in B$ ,  $u$  s'identifie à  $\lambda(u)$  dans  $G$  et à  $\mu(u)$  dans  $H$  et alors  $\Delta(\lambda(u)) = \mu(u)$ . Donc  $\Delta\lambda = \mu$ . D'autre part, soit  $g \in G$  tel que  $g = g_{i_1} g_{i_2} \cdots g_{i_s} u$  avec  $u \in B$  et  $0 \leq i_1 < i_2 < \cdots < i_s \leq n$ . La deuxième ligne du diagramme étant exacte,  $\beta\mu = 1$ . On a donc :

$$\begin{aligned} \beta(\Delta(g)) &= \beta(h_{i_1} h_{i_2} \cdots h_{i_s} u) \\ &= e_{i_1} e_{i_2} \cdots e_{i_s} \beta(\mu(u)) \\ &= e_{i_1} e_{i_2} \cdots e_{i_s} \\ &= \bar{\gamma}(g). \end{aligned}$$

Par suite,  $\beta\Delta = \bar{\gamma}$  et ainsi s'achève la démonstration. ■

Il est possible de parler de "l'ortho-ambivalence" des 2-groupes spéciaux en utilisant l'invariant d'Arf. Pour y arriver, nous avons besoin de la définition suivante :

**Définition 3.4.26.** Soit  $G$  un 2-groupe extra-spécial. On appelle invariant d'Arf de  $G$  et on note  $Arf(G)$ , l'invariant d'Arf de la forme quadratique

$$q : \frac{G}{Z(G)} \longrightarrow Z(G) : xZ(G) := \bar{x} \longmapsto x^2.$$

On a alors le résultat suivant pour les 2-groupes extra-spéciaux :

**Corollaire 3.4.27.** Soit  $G$  un 2-groupe extra-spécial et  $k$  un corps dont la caractéristique est différente de 2. Alors :

- (1)  $G$  est ortho-ambivalent par rapport à  $k$  si et seulement si  $Arf(G) = 0$
- (2)  $G$  n'est pas ortho-ambivalent par rapport à  $k$  si et seulement si  $Arf(G) = 1$ .

*Preuve :*

Cela découle de la proposition 3.4.18 et du théorème 3.3.11. ■

Pour les 2-groupes spéciaux ambivalents, il est possible d'établir un résultat semblable à celui énoncé dans le corollaire 3.4.27. Afin d'y arriver, certains résultats nous sont indispensables.

**Théorème 3.4.28.** Soient  $G$  un 2-groupe spécial ambivalent et  $\rho : G \rightarrow GL(V)$  une représentation irréductible de  $G$  de degré  $> 1$ . Alors  $\rho(G)$  est un 2-groupe extra-spécial.

*Preuve :* Soit  $\chi$  le caractère de  $\rho$ . On sait que  $|Z(G)| \geq 2$ . Un raisonnement analogue à celui utilisé dans la démonstration du théorème 3.3.8 permet d'établir que  $\rho(Z(G)) = \mu_2$ . Donc la restriction  $\rho' : Z(G) \rightarrow \mu_2$  de  $\rho$  à  $Z(G)$  est surjective. D'où  $\frac{Z(G)}{Ker \rho'}$  est isomorphe à  $\mu_2$ . Par ailleurs  $Ker \rho' = Z(G) \cap Ker \rho$ . En posant

$H := Z(G) \cap \text{Ker} \rho$ ,  $\frac{Z(G)}{H}$  est alors isomorphe à  $\mu_2$ . D'après un théorème d'isomorphisme de groupes, il existe un unique isomorphisme de groupes  $\psi : \frac{G}{\text{Ker} \rho} \longrightarrow \rho(G) \subset GL(V)$  tel que  $\rho = \psi \varphi$ , où  $\varphi : G \longrightarrow \frac{G}{\text{Ker} \rho}$  est la surjection canonique. D'une part,

$$\begin{aligned}
 \left(\frac{G}{\text{Ker} \rho}\right)' &= \frac{G' \text{Ker} \rho}{\text{Ker} \rho} \text{ (lemme 3.4.5.(2))} \\
 &= \frac{Z(G) \text{Ker} \rho}{\text{Ker} \rho} \text{ (} G \text{ étant spécial)} \\
 &= \frac{Z(G)}{Z(G) \cap \text{Ker} \rho} \text{ (théorème d'isomorphisme de groupes)} \\
 &= \frac{Z(G)}{H} \\
 &= \mu_2.
 \end{aligned}$$

Soit  $h \in Z(\rho(G))$ . Il existe alors  $g \in G$  tel que  $h = \rho(g)$ .  $G$  étant ambivalent, il existe  $x \in G$  tel que  $g^{-1} = xgx^{-1}$ . Donc  $h^{-1} = \rho(x)h\rho(x^{-1})$  et alors  $h^2 = 1$ . Par ailleurs,  $Z(\rho(G)) \subset Z(GL(V)) = \mathbb{C}^\times$ ; il en résulte que  $h \in \mu_2 = \rho(Z(G))$  et donc  $Z(\rho(G)) \subset \rho(Z(G))$ . C'est clair que  $\rho(Z(G)) \subset Z(\rho(G))$ ; donc  $\rho(Z(G)) = Z(\rho(G))$  et alors

$$Z\left(\frac{G}{\text{Ker} \rho}\right) = Z(\rho(G)) = \rho(Z(G)) = \mu_2 = \left(\frac{G}{\text{Ker} \rho}\right)'.$$

D'autre part,

$$\frac{\frac{G}{\text{Ker} \rho}}{\left(\frac{G}{\text{Ker} \rho}\right)'} = \frac{\frac{G}{\text{Ker} \rho}}{\frac{Z(G) \text{Ker} \rho}{\text{Ker} \rho}} = \frac{G}{Z(G) \text{Ker} \rho}$$

est un sous-groupe de  $\frac{G}{Z(G)} = \frac{G}{\Phi(G)}$ , qui est un 2-groupe abélien élémentaire (proposition 3.4.2.(1)) : il est donc abélien élémentaire. On en déduit que  $\frac{G}{\text{Ker} \rho} \cong \rho(G)$  est un 2-groupe extra-spécial. ■

**Corollaire 3.4.29.** *Avec les notations et hypothèses du théorème 3.4.28, la restriction de  $\sigma$  à  $A$  est orthogonale (resp. symplectique) si et seulement si*

$$t_{\rho(G)}(1) = \frac{|\rho(G)|(\varepsilon + \deg A)}{2\deg A}$$

avec  $\varepsilon = 1$  (resp.  $\varepsilon = -1$ ).

*Preuve :* Utilisant les notations de la démonstration du théorème 3.4.28,  $\psi$  est une représentation irréductible de  $\frac{G}{\text{Ker } \rho}$  (proposition 3.1.2) et  $\rho$  et  $\psi$  sont de même degré. Soient  $A$  et  $B$  les composantes simples respectives de  $\mathbb{C}G$  et  $\mathbb{C}(\frac{G}{\text{Ker } \rho})$  correspondant respectivement à  $\rho$  et  $\psi$ . D'après la proposition 3.1.2, les restrictions des involutions canoniques respectivement à  $A$  et  $B$ , sont de même type et  $\deg A = \deg B$ . Le résultat découle enfin de la proposition 3.3.8,  $\rho(G)$  étant extra-spécial (théorème 3.4.28). ■

**Proposition 3.4.30.** *Soient  $G$  un 2-groupe spécial ambivalent et  $\rho$  une représentation irréductible de  $G$  de degré  $> 1$ , de caractère  $\chi$ . Alors*

- (1)  $\chi$  est de type 1 si et seulement si  $\text{Arf}(\rho(G)) = 0$  ;
- (2)  $\chi$  est de type  $-1$  si et seulement si  $\text{Arf}(\rho(G)) = 1$ .

*Preuve :* Soit  $\rho : G \rightarrow GL(V)$  une  $\mathbb{C}$ -représentation irréductible de  $G$  de degré  $> 1$  de caractère  $\chi$ . D'après le théorème 3.4.28,  $\rho(G) \cong \frac{G}{\text{Ker } \rho}$  est un 2-groupe extra-spécial. Soit  $\rho' : \frac{G}{\text{Ker } \rho} \rightarrow GL(V)$  l'unique morphisme de groupes tel que  $\rho = \rho' \varphi$ , où  $\varphi : G \rightarrow \frac{G}{\text{Ker } \rho}$  est la surjection canonique. D'après la proposition 3.1.2,  $\rho'$  est irréductible. Soient  $\chi'$  le caractère de  $\rho'$  et  $\sigma$  (resp.  $\sigma'$ ) l'involution canonique sur  $\mathbb{C}G$  (resp. sur  $\mathbb{C}(\frac{G}{\text{Ker } \rho}) \cong \mathbb{C}\rho(G)$ ). Soit  $A$  (resp.  $A'$ ) la composante simple de  $\mathbb{C}G$  (resp. de  $\mathbb{C}(\frac{G}{\text{Ker } \rho}) \cong \mathbb{C}\rho(G)$ ) correspondant à  $\chi$  (resp.  $\chi'$ ). C'est clair que  $A$  et  $A'$  sont de même degré.  $G$  étant ambivalent,  $\sigma(A) = A$ . D'où d'après la proposition 3.1.2,  $\sigma'(A') = A'$  et les restrictions respectives de  $\sigma$  à  $A$  et de  $\sigma'$  à  $A'$  sont des involutions de première espèce de même type. Par ailleurs,

$\rho(G) \cong \frac{G}{\text{Ker } \rho}$  étant un 2-groupe extra-spécial,  $A'$  est son unique composante simple de degré  $> 1$  (théorème 3.3.11) et comme la restriction de  $\sigma'$  à toutes les composantes simples de degré 1 est de type orthogonal, alors  $\rho(G)$  est ortho-ambivalent par rapport à  $\mathbb{C}$  (resp. n'est pas ortho-ambivalent par rapport à  $\mathbb{C}$ ) si et seulement si la restriction de  $\sigma$  à  $A$  est orthogonale (resp. symplectique). D'une part, d'après le théorème 2.1.20, cela est équivalent à dire que  $\chi$  est de type 1 (resp. de type  $-1$ ). D'autre part, d'après le corollaire 3.4.27, cela est équivalent au fait que  $\text{Arf}(\rho(G)) = 0$  (resp.  $\text{Arf}(\rho(G)) = 1$ ) et le résultat est ainsi établi. ■

**Corollaire 3.4.31.** *Soient  $G$  un 2-groupe spécial ambivalent et  $k$  un corps dont la caractéristique est différente de 2. Les assertions suivantes sont équivalentes :*

- (1)  $G$  est ortho-ambivalent par rapport à  $k$  ;
- (2) Pour toute représentation irréductible  $\rho$  de  $G$  de degré  $> 1$ ,

$$\text{Arf}(\rho(G)) = 0.$$

*Preuve :* Cela découle de la proposition 3.4.30 pour  $k = \mathbb{C}$ . On utilise finalement le corollaire 2.3.8 pour conclure. ■

Nous nous proposons maintenant de trouver une autre caractérisation d'un 2-groupe spécial ortho-ambivalent par rapport à un corps de caractéristique différente de 2, en utilisant des formes quadratiques induites par des formes quadratiques qui sont des transferts de l'application quadratique de  $G$  par des formes linéaires non nulles sur le centre de  $G$ . Pour y arriver, nous avons besoin de quelques résultats préliminaires.

**Proposition 3.4.32.** *Soient  $A, B, B_1$  des espaces vectoriels sur  $\mathbb{F}_2$ ,  $q \in \text{Quad}(A, B)$  et  $s \in \text{Hom}_{\mathbb{F}_2}(B, B_1)$ . L'application  $s_*(q) = sq : A \rightarrow B_1$  est quadratique d'application polaire  $b_{s_*(q)} = sb_q : A \times A \rightarrow B_1$  ; on l'appelle transfert de  $q$  par  $s$ . On suppose que  $s_*(q)(\text{rad}(b_{s_*(q)})) = 0$ .*

- (1)  $s_*(q)$  induit alors une application quadratique régulière  $q_s$  de  $A_s := \frac{A}{\text{rad}(b_{s_*(q)})}$  dans  $B_1$  définie par

$$q_s(\varepsilon_s(x)) = s_*(q)(x), \quad \forall x \in A,$$

$\varepsilon_s : A \rightarrow A_s$  étant la surjection canonique.

- (2) Soient  $\varphi$  (resp.  $\varphi_s$ ) l'isomorphisme entre  $H^2(A, B)$  et  $\text{Quad}(A, B)$  (resp. entre  $H^2(A_s, B_1)$  et  $\text{Quad}(A_s, B_1)$ ) défini dans la proposition 3.4.20 et  $c \in Z^2(A, B)$  (resp.  $c_s \in Z^2(A_s, B_1)$ ) un 2-cocycle tel que  $\varphi([c]) = q$  (resp.  $\varphi_s([c_s]) = q_s$ ). Soit  $G$  (resp.  $G_s$ ) l'extension centrale de  $B$  par  $A$  (resp. de  $B_1$  par  $A_s$ ) correspondant à  $[c]$  (resp. à  $[c_s]$ ).

- (a) Il existe alors un morphisme de groupes  $f_s : G \rightarrow G_s$  tel que le diagramme suivant (où les lignes sont exactes) est commutatif :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \xrightarrow{\alpha} & G & \xrightarrow{\pi} & A & \longrightarrow & 0 \\ & & \downarrow s & & \downarrow f_s & & \downarrow \varepsilon_s & & \\ 0 & \longrightarrow & B_1 & \xrightarrow{\alpha_s} & G_s & \xrightarrow{\pi_s} & A_s & \longrightarrow & 0 \end{array}$$

- (b) Si  $s$  est surjective, alors  $f_s$  est surjectif.

- (c) Si  $B = \text{sgr} < b_q(A \times A) >$  et  $s$  est surjective, alors

$$B_1 = \text{sgr} < b_{q_s}(A_s \times A_s) > .$$

*Preuve :* L'application  $b_{s_*(q)} : A \times A \rightarrow B_1$  définie par

$$b_{s_*(q)}(x, y) = s_*(q)(x + y) - s_*(q)(x) - s_*(q)(y), \quad \forall x, y \in A,$$

est telle que  $b_{s_*(q)} = sb_q$  ( $s$  étant linéaire). On en déduit que  $b_{s_*(q)}$  est bilinéaire, étant donné que  $s$  est linéaire et  $b_q$ , bilinéaire. Donc  $s_*(q)$  est une application quadratique d'application polaire  $b_{s_*(q)} = sb_q$ . Supposons que  $s_*(q)(\text{rad}(b_{s_*(q)})) = 0$ .



1. L'application  $q_s$  est bien définie, en effet soient  $x, y \in A$  tels que

$$\varepsilon_s(x) = x + \text{rad}(b_{s_*(q)}) = y + \text{rad}(b_{s_*(q)}) = \varepsilon_s(y);$$

il existe alors  $r \in \text{rad}(b_{s_*(q)})$  tel que  $x = y + r$ . Par suite,

$$\begin{aligned} 0 = b_{s_*(q)}(y, r) &= s_*(q)(y + r) - s_*(q)(y) - s_*(q)(r) \\ &= s_*(q)(y + r) - s_*(q)(y) \\ &= s_*(q)(x) - s_*(q)(y) \\ &= q_s(\varepsilon_s(x)) - q_s(\varepsilon_s(y)). \end{aligned}$$

$s_*(q)$  étant une application quadratique, il en est de même pour  $q_s$ . Montrons que  $q_s$  est régulière. Soit  $x \in A$  tel que  $\varepsilon_s(x) \in \text{rad}(b_{q_s})$ . Alors pour tout  $y \in A$ ,

$$\begin{aligned} 0 = b_{q_s}(\varepsilon_s(x), \varepsilon_s(y)) &= q_s(\varepsilon_s(x) + \varepsilon_s(y)) - q_s(\varepsilon_s(x)) - q_s(\varepsilon_s(y)) \\ &= s(q(x + y)) - s(q(x)) - s(q(y)) \\ &= s(b_q(x, y)) \\ &= b_{s_*(q)}(x, y) \end{aligned}$$

et donc  $x \in \text{rad}(b_{s_*(q)})$ ; par suite  $\varepsilon_s(x) = 0$  et donc  $q_s$  est régulière.

2. D'après la proposition 3.4.20,

$$q(a) = c(a, a), \quad \forall a \in A$$

et

$$q_s(a_s) = c(a_s, a_s), \quad \forall a_s \in A_s.$$

Considérons les applications  $s_*(c) : A \times A \rightarrow B_1$  et  $\text{inf}(c_s) : A \times A \rightarrow B_1$  définies par

$$s_*(c)(a, a') = s(c(a, a')) \text{ et } \text{inf}(c_s)(a, a') = c_s(\varepsilon_s(a), \varepsilon_s(a')),$$

pour tous  $a, a' \in A$ . En se servant du fait que  $s$  est linéaire et  $c$  et  $c_s$  sont des 2-cocycles normalisés, on vérifie aisément que  $s_*(c)$  et  $\text{inf}(c_s)$  sont des 2-cocycles normalisés, éléments de  $Z^2(A, B_1)$ .

$s_*(c)$  et  $\inf(c_s)$  sont appelés respectivement transfert de  $c$  par  $s$  et inflation de  $c_s$ . Montrons que  $s_*(c)$  et  $\inf(c_s)$  sont cohomologues. Pour tout  $x \in A$ , on a :

$$\begin{aligned} \inf(c_s)(x, x) &= c_s(\varepsilon_s(x), \varepsilon_s(x)) \\ &= q_s(\varepsilon_s(x)) \\ &= s(q(x)) \\ &= s(c(x, x)) \\ &= s_*(c)(x, x). \end{aligned}$$

Donc d'après la proposition 3.4.20,  $[\inf(c_s)]$  et  $[s_*(c)]$  ont même image par l'isomorphisme  $\varphi' : H^2(A, B_1) \rightarrow \text{Quad}(A, B_1)$  définie dans cette proposition. Il en résulte que  $s_*(c)$  et  $\inf(c_s)$  sont cohomologues. Il existe donc une application  $\lambda : A \rightarrow B_1$  telle que  $\lambda(0) = 0$  et

$$\inf(c_s)(x, y) = s_*(c)(x, y) + \lambda(y) - \lambda(x + y) + \lambda(x).$$

a) D'après la remarque 3.4.19,

$$G = \{(a, b) \mid a \in A, b \in B\},$$

avec

$$(a, b) \cdot (a', b') = (a + a', c(a, a') + b + b'), \quad \text{pour } a, a' \in A \text{ et } b, b' \in B$$

et

$$G_s = \{(a, b) \mid a \in A_s, b \in B_1\},$$

avec

$$(a, b) \cdot (a', b') = (a + a', c_s(a, a') + b + b'), \quad \text{pour } a, a' \in A_s \text{ et } b, b' \in B_1.$$

Soit alors  $f_s : G \rightarrow G_s$  l'application définie par

$$f_s(a, b) = (\varepsilon_s(a), s(b) - \lambda(a)), \quad \text{pour } a \in A, b \in B.$$

Pour tous  $a, a' \in A$  et  $b, b' \in B$ , on a :

$$\begin{aligned}
& f_s((a, b) \cdot (a', b')) \\
&= f_s(a + a', c(a, a') + b + b') \\
&= (\varepsilon_s(a + a'), s(c(a, a') + b + b') - \lambda(a + a')) \\
&= (\varepsilon_s(a) + \varepsilon_s(a'), s_*(c)(a, a') + s(b) + s(b') - \lambda(a + a')) \\
&= (\varepsilon_s(a) + \varepsilon_s(a'), \inf(c_s)(a, a') - \lambda(a) - \lambda(a') + \lambda(a + a') \\
&\quad + s(b) + s(b') - \lambda(a + a')) \\
&= (\varepsilon_s(a) + \varepsilon_s(a'), c_s(\varepsilon_s(a), \varepsilon_s(a')) - \lambda(a) - \lambda(a') + s(b) + s(b')) \\
&= (\varepsilon_s(a), s(b) - \lambda(a)) \cdot (\varepsilon_s(a'), s(b') - \lambda(a')) \\
&= f_s(a, b) \cdot f_s(a', b').
\end{aligned}$$

Donc  $f_s$  est un morphisme de groupes. De plus, pour tous  $a \in A$ ,  $b \in B$ , on a :

$$\pi_s f_s(a, b) = \pi_s(\varepsilon_s(a), s(b) - \lambda(a)) = \varepsilon_s(a) = \varepsilon_s \pi(a, b)$$

et

$$f_s \alpha(b) = f_s(0, b) = (\varepsilon_s(0), s(b) - \lambda(0)) = (0, s(b)) = \alpha_s s(b).$$

Donc  $\pi_s f_s = \varepsilon_s \pi$  et  $f_s \alpha = \alpha_s s$ .

**b)** Supposons  $s$  surjective. Soit  $z = (a', b') \in G_s$ , avec  $a' \in A_s$  et  $b' \in B_1$ . D'une part,  $\varepsilon_s$  et  $s$  étant surjectives, il existe  $a \in A$  et  $b \in B$  tels que  $a' = \varepsilon_s(a)$  et  $b' = s(b)$ . D'autre part, comme  $\lambda(a) \in B_1$  et  $s$  est surjective, il existe  $b'' \in B$  tel que  $\lambda(a) = s(b'')$ . D'où  $(a, b + b'') \in G$  et on a :

$$\begin{aligned}
f_s(a, b + b'') &= (\varepsilon_s(a), s(b + b'') - \lambda(a)) \\
&= (\varepsilon_s(a), s(b) + \lambda(a) - \lambda(a)) \\
&= (a', b') = z.
\end{aligned}$$

Donc  $f_s$  est surjectif.

c) Supposons que  $B = \text{sgr} < b_q(A \times A) >$  et  $s$  est surjective. Comme pour tous  $x, y \in A$ ,  $b_{q_s}(\varepsilon_s(x), \varepsilon_s(y)) = s(b_q(x, y))$ , alors

$$b_{q_s}(A_s \times A_s) = b_{q_s}(\varepsilon_s(A) \times \varepsilon_s(A)) = s(b_q(A \times A)),$$

$\varepsilon_s$  étant surjective ; d'où

$$\text{sgr} < b_{q_s}(A_s \times A_s) > = s(\text{sgr} < b_q(A \times A) >) = s(B) = B_1. \blacksquare$$

Le résultat général énoncé dans la proposition 3.4.32 s'applique aux 2-groupes spéciaux à travers le résultat suivant :

**Proposition 3.4.33.** *Soit  $G$  un 2-groupe spécial ambivalent d'application quadratique  $q : A := \frac{G}{Z(G)} \rightarrow Z(G) =: B$ .*

- (1) *Soit  $s : B \rightarrow \mathbb{F}_2$  une forme linéaire non nulle.  $s_*(q)$  induit une forme quadratique régulière  $q_s$  de  $A_s := \frac{A}{\text{rad}(b_{s_*(q)})}$  dans  $\mathbb{F}_2$  définie par*

$$q_s(\varepsilon_s(x)) = s_*(q)(x), \quad \forall x \in A,$$

*$\varepsilon_s : A \rightarrow A_s$  étant la surjection canonique. Soit  $G_s$  l'extension centrale de  $\mathbb{F}_2$  par  $A_s$  correspondant à  $q_s$ .  $G_s$  est un 2-groupe extra-spécial de forme quadratique  $q_s$  et il existe une représentation irréductible  $\rho$  de  $G$  de degré  $> 1$  tel que  $\rho(G)$  soit isomorphe à  $G_s$ .*

- (2) *Réciproquement, pour toute représentation irréductible  $\rho$  de  $G$  de degré  $> 1$ , il existe une forme linéaire non nulle  $s : B \rightarrow \mathbb{F}_2$  telle que  $\rho(G)$  soit isomorphe à  $G_s$  (avec les notations de (1)).*

La première partie de cette proposition utilise le lemme suivant :

**Lemme 3.4.34.** *Soient  $G$  un 2-groupe extra-spécial et  $\rho : G \rightarrow GL(V)$  l'unique représentation irréductible de  $G$  de degré  $> 1$ . Alors  $\rho$  est un isomorphisme de groupes de  $G$  sur  $\rho(G)$ .*

*Preuve :* Etant donné que  $G$  est fini et  $\rho : G \rightarrow \rho(G)$  est surjective, il suffit de démontrer que  $|\rho(G)| = |G|$ . D'après la définition 3.4.4,  $G$  est un 2-groupe spécial ; il est ambivalent (proposition 3.3.7).

D'où d'après le théorème 3.4.28,  $\rho(G)$  est un 2-groupe extra-spécial. Soit  $\rho_1 : \rho(G) \rightarrow GL(V_1)$  l'unique représentation irréductible de  $\rho(G)$  de degré  $> 1$ .  $\rho_1 \rho : G \rightarrow GL(V_1)$  est donc une représentation irréductible de  $G$ . De l'unicité (à isomorphisme près) d'une représentation irréductible de  $G$  de degré  $> 1$  (théorème 3.3.11), il résulte que  $\rho$  et  $\rho_1 \rho$  sont isomorphes. Donc  $\deg \rho = \deg \rho_1 \rho = \deg \rho_1$ . D'où d'après le corollaire 3.3.12,

$$|G| = 2(\deg \rho)^2 = 2(\deg \rho_1)^2 = |\rho(G)|. \blacksquare$$

**Preuve de la proposition 3.4.33 :** Pour des raisons de commodité, les  $\mathbb{F}_2$ -espaces vectoriels  $A$ ,  $B$  et  $\mathbb{F}_2 \cong \mu_2$  sont notés multiplicativement (l'élément nul est noté 1 : c'est l'élément unité du groupe).

1. Soit  $s : B \rightarrow \mathbb{F}_2$  une forme linéaire non nulle. Montrons que

$$s_*(q)(\text{rad}(b_{s_*(q)})) = 1.$$

Soit  $r \in G$  tel que  $\bar{r} := rB \in \text{rad}(b_{s_*(q)})$ . Alors pour tout  $x \in G$ ,

$$1 = b_{s_*(q)}(\bar{r}, \bar{x}) = s(b_q(\bar{r}, \bar{x})) = s([r, x]) \text{ (proposition 3.4.12).}$$

$G$  étant ambivalent, il existe  $y \in G$  tel que  $r^{-1} = y^{-1}ry$ . En particulier, pour  $x = y$ , on a :

$$\begin{aligned} 1 = s([r, y]) &= s(r^{-1}y^{-1}ry) = s(y^{-1}ryy^{-1}ry) = s(r^2) \\ &= s(q(\bar{r})) = s_*(q)(\bar{r}). \end{aligned}$$

Par suite  $s_*(q)(\text{rad}(b_{s_*(q)})) = 1$ . L'existence de  $q_s$  découle alors de la proposition 3.4.32.(1) ; de la proposition 3.4.32.(2).(a) découle l'existence d'un morphisme de groupes  $f_s : G \rightarrow G_s$  tel que le dia-

gramme suivant (où les lignes sont exactes) soit commutatif :

$$\begin{array}{ccccccccc}
 1 & \longrightarrow & B & \longrightarrow & G & \longrightarrow & A & \longrightarrow & 1 \\
 & & \downarrow s & & \downarrow f_s & & \downarrow \varepsilon_s & & \\
 1 & \longrightarrow & \mathbb{F}_2 = \mu_2 & \longrightarrow & G_s & \longrightarrow & A_s & \longrightarrow & 1
 \end{array}$$

Comme  $s$  est non nulle, alors elle est surjective.  $G$  étant un 2-groupe spécial, on a :

$$\begin{aligned}
 B = Z(G) &= G' \\
 &= \text{sgr} < [x, y] = b_q(\bar{x}, \bar{y}) \mid x, y \in G > = \text{sgr} < b_q(A \times A) > .
 \end{aligned}$$

Donc d'après la proposition 3.4.32.(2).(b)-(c),  $f_s$  est surjectif et  $\mathbb{F}_2 = \mu_2 = \text{sgr} < b_{q_s}(A_s \times A_s) >$ . D'où d'après le théorème 3.4.23,  $G_s$  est un 2-groupe spécial de forme quadratique  $q_s$ , de centre  $\mathbb{F}_2 = \mu_2$  et tel que  $A_s = \frac{G_s}{Z(G_s)}$ . Donc  $G_s$  est un 2-groupe extra-spécial. D'après le théorème 3.3.11,  $G_s$  possède une unique représentation irréductible  $\rho_s$  de degré  $> 1$ . Donc  $\rho := \rho_s f_s$  est une représentation irréductible de  $G$  telle que  $\rho(G) = \rho_s f_s(G) = \rho_s(G_s)$ ,  $f_s$  étant surjectif. D'après le lemme 3.4.34,  $\rho(G) = \rho_s(G_s)$  est isomorphe à  $G_s$ .

**2.** Soit  $\rho : G \rightarrow GL(V)$  une représentation irréductible de  $G$  de degré  $> 1$ . D'après la démonstration du théorème 3.4.28,  $\rho(Z(G)) = \mu_2 \cong \mathbb{F}_2$ . Donc la restriction  $s$  de  $\rho$  à  $Z(G) = B$  est une forme linéaire non nulle de  $B$  dans  $\mathbb{F}_2$ . La première partie de cette proposition donne donc l'existence d'un 2-groupe extra-spécial  $G_s$ , extension centrale de  $\mathbb{F}_2$  par  $A_s := \frac{A}{\text{rad}(b_{s*(q)})}$ , de forme quadratique

régulière  $q_s$  induite par  $s_*(q)$ . Par ailleurs, d'après le théorème 3.4.28,  $\rho(G)$  est un 2-groupe extra-spécial, extension centrale de  $\mathbb{F}_2 \cong \mu_2 \cong Z(\rho(G))$  par  $A_\rho := \frac{\rho(G)}{Z(\rho(G))}$ , de forme quadratique

$$q_\rho : \frac{\rho(G)}{Z(\rho(G))} \rightarrow Z(\rho(G)) : \overline{\rho(x)} \mapsto \rho(x^2),$$

avec  $\overline{\rho(x)} = \rho(x)Z(\rho(G))$ , pour tout  $x \in G$ . Pour conclure, il suffit de démontrer que les groupes  $A_s$  et  $A_\rho$  sont isomorphes et les formes quadratiques  $q_s$  et  $q_\rho$  sont isométriques (c'est-à-dire qu'il existe un isomorphisme  $\omega : A_s \rightarrow A_\rho$  tel que pour tout  $a \in A_s$ ,  $q_s(a) = q_\rho(\omega(a))$ ) pour déduire le résultat du théorème 3.4.23. Pour tout  $\bar{r} := rB \in A$ , avec  $r \in G$ ,  $\bar{r} \in \text{rad}(b_{s_*(q)})$  si et seulement si, pour tout  $x \in G$ ,

$$1 = b_{s_*(q)}(\bar{r}, \bar{x}) = \rho([r, x]) = \rho(r^{-1})\rho(x^{-1})\rho(r)\rho(x)$$

si et seulement si  $\rho(r) \in Z(\rho(G))$ . Donc

$$\text{rad}(b_{s_*(q)}) = \{\bar{r} := rB \in A \mid \rho(r) \in Z(\rho(G))\}.$$

Soit  $\omega : A \rightarrow A_\rho$  tel que pour tout  $\bar{x} := xB \in A$ , avec  $x \in G$ ,

$$\omega(\bar{x}) = \rho(x)Z(\rho(G)).$$

$\omega$  est bien définie, en effet, pour tous  $x, y \in G$ , si  $\bar{x} = \bar{y}$ , alors  $x^{-1}y \in B$  et comme  $B = \rho(Z(G)) = Z(\rho(G))$  (démonstration du théorème 3.4.28), alors  $\rho(x^{-1}y) \in Z(\rho(G))$ . D'où  $\omega(\bar{x}) = \omega(\bar{y})$ . On vérifie aisément que  $\text{Ker}\omega = \text{rad}(b_{s_*(q)})$  et comme  $\omega$  est clairement surjectif, il induit un isomorphisme de groupes  $\bar{\omega} : A_s \rightarrow A_\rho$  défini par

$$\bar{\omega}(\bar{x}\text{rad}(b_{s_*(q)})) = \rho(x)Z(\rho(G)) := \overline{\rho(x)}.$$

D'autre part, d'après la proposition 3.4.32, pour tout  $x \in G$ ,

$$\begin{aligned} q_s(\bar{x}\text{rad}(b_{s_*(q)})) &= q_s(\varepsilon_s(\bar{x})) \\ &= s_*(q)(\bar{x}) = \rho(x^2) \\ &= q_\rho(\overline{\rho(x)}) \\ &= q_\rho(\bar{\omega}(\bar{x}\text{rad}(b_{s_*(q)}))). \end{aligned}$$

Donc  $q_s$  et  $q_\rho$  sont isométriques. ■

Il est maintenant possible d'énoncer le résultat attendu sur l'ortho-ambivalence des 2-groupes spéciaux.

**Théorème 3.4.35.** *Soient  $G$  un 2-groupe spécial ambivalent d'application quadratique  $q : A =: \frac{G}{Z(G)} \rightarrow Z(G)$  et  $k$  un corps de caractéristique différente de 2. Les propositions suivantes sont équivalentes :*

- (1)  $G$  est ortho-ambivalent par rapport à  $k$ .
- (2) Pour toute  $\mathbb{F}_2$ -forme linéaire non nulle  $s$  sur  $Z(G)$ ,  $\text{Arf}(q_s) = 0$ ,  $q_s$  étant la forme quadratique sur  $A_s := \frac{A}{\text{rad}(b_{s^*(q)})}$  induite par le transfert  $s_*(q)$  de  $q$  par  $s$ .

*Preuve :* Cela découle directement du corollaire 3.4.31 et de la proposition 3.4.33, étant donné que l'invariant d'Arf d'un 2-groupe extra-spécial est l'invariant d'Arf de sa forme quadratique. ■

Pour se servir adéquatement du théorème 3.4.35, il convient de préciser une condition pour qu'un 2-groupe spécial correspondant à une application quadratique vérifiant les hypothèses du théorème 3.4.23, soit ambivalent.

**Théorème 3.4.36.** *Soit  $G$  le 2-groupe spécial (d'application quadratique  $q : A = \frac{G}{Z(G)} \rightarrow B = Z(G)$ ) donné par le théorème 3.4.23. Les assertions suivantes sont équivalentes :*

- (1)  $G$  est ambivalent ;
- (2) pour tout  $a \in A$ , il existe  $a' \in A$  tel que  $q(a') = q(a + a')$  ;
- (3) pour tout  $a \in A$ , il existe  $a' \in A$  tel que  $q(a) = b_q(a, a')$ .

*Preuve :*

(1)  $\Rightarrow$  (2) : Si  $G$  est ambivalent, alors pour tout  $x \in G$ , il existe  $y \in G$  tel que  $x^{-1} = y^{-1}xy$  et donc

$$q(\bar{y}) = y^2 = yx^{-1}xy = yy^{-1}xyxy = (xy)^2 = q(\overline{xy}) = q(\bar{x} \bar{y}),$$

avec  $\bar{x} = xZ(G)$ , pour  $x \in G$ .



(2)  $\Rightarrow$  (1) : Supposons la condition (2) réalisée. Soit alors  $c \in Z^2(A, B)$  un 2-cocycle tel que  $\varphi([c]) = q$ ,  $\varphi : H^2(A, B) \rightarrow \text{Quad}(A, B)$  étant l'isomorphisme de groupes défini par la proposition 3.4.20 ; d'après cette proposition, pour tous  $a, a' \in A$ ,

$$q(a) = c(a, a) \text{ et } b_q(a, a') = c(a, a') - c(a', a).$$

D'après la remarque 3.4.19,

$$G = \{(a, b) | a \in A, b \in B\},$$

la multiplication dans  $G$  étant définie par :

$$(a, b) \cdot (a', b') = (a + a', c(a, a') + b + b'), \text{ pour } a, a' \in A \text{ et } b, b' \in B.$$

Soit  $x = (a, b) \in G$ , avec  $a \in A$  et  $b \in B$ . Par hypothèse, il existe  $a' \in A$  tel que  $q(a') = q(a + a')$  et donc

$$b_q(a, a') = q(a + a') - q(a) - q(a') = -q(a) = q(a);$$

par suite

$$c(a, a') - c(a', a) = c(a, a). \quad (3.33)$$

La relation de cocycle donne :

$$c(a', a') - c(a + a', a') + c(a, a' + a') - c(a, a') = 0;$$

donc

$$c(a', a') + c(a + a', a') = c(a, a'). \quad (3.34)$$

Pour  $y = (a', b')$ , avec  $b' \in B$ ,  $y^{-1} = (a', c(a', a') + b')$  et donc

$$yxy^{-1}$$

$$\begin{aligned} &= (a' + a, c(a', a) + b' + b) \cdot (a', c(a', a') + b') \\ &= (a' + a + a', c(a' + a, a') + c(a', a) + b' + b + c(a', a') + b') \\ &= (a, c(a' + a, a') + c(a', a) + c(a', a') + b) \\ &= (a, c(a, a') + c(a', a) + b) \quad \text{d'après (3.34)} \\ &= (a, c(a, a) + b) \quad \text{d'après (3.33)} \\ &= x^{-1}. \end{aligned}$$

Il en résulte que  $G$  est ambivalent.

(2)  $\Leftrightarrow$  (3) : c'est évident par définition de  $b_q$ . ■

**Existence des 2-groupes spéciaux non ambivalents.** En nous servant des conditions d'ambivalence d'un 2-groupe spécial, données par le théorème 3.4.36, nous allons donner un exemple d'un 2-groupe spécial non ambivalent.

Soit  $A$  un  $\mathbb{F}_2$ -espace vectoriel de dimension finie  $n$ . Soit  $\wedge^2 A = A \wedge A$  la deuxième puissance extérieure de  $A$  (pour la définition, voir [37, page 323]). Soit  $(e_1, e_2, \dots, e_n)$  une base de  $A$ ; alors  $(e_i \wedge e_j)_{1 \leq i < j \leq n}$  est une base de  $\wedge^2 A$ .  $\wedge^2 A$  est un  $\mathbb{F}_2$ -espace vectoriel de dimension  $\binom{n}{2}$ . Rappelons que pour tous  $x, y \in A$ , si  $x = \sum_{i=1}^n \alpha_i e_i$  et  $y = \sum_{i=1}^n \beta_i e_i$ , avec  $\alpha_i, \beta_i \in \mathbb{F}_2$ , pour tout  $i$ , on a (voir [37, page 316]) :

$$x \wedge y = \sum_{1 \leq i < j \leq n} (\alpha_i \beta_j - \beta_i \alpha_j) e_i \wedge e_j.$$

Soit  $q : A \rightarrow \wedge^2 A$  l'application définie par

$$\begin{aligned} & q\left(\sum_{i=1}^n \alpha_i e_i\right) \\ &= \sum_{i=1}^{n-2} \alpha_i^2 e_{i+1} \wedge e_{i+2} + \alpha_{n-1}^2 e_1 \wedge e_n + \alpha_n^2 e_1 \wedge e_2 + \sum_{1 \leq i < j \leq n} \alpha_i \alpha_j e_i \wedge e_j, \end{aligned}$$

pour  $\alpha_i \in \mathbb{F}_2$ , pour tout  $i$ . Pour tous  $x, y \in A$  tels que  $x = \sum_{i=1}^n \alpha_i e_i$  et  $y = \sum_{i=1}^n \beta_i e_i$ , avec  $\alpha_i, \beta_i \in \mathbb{F}_2$ , pour tout  $i$ , on a :

$$\begin{aligned}
 b_q(x, y) &= q(x + y) - q(x) - q(y) \\
 &= \sum_{i=1}^{n-2} ((\alpha_i + \beta_i)^2 - \alpha_i^2 - \beta_i^2) e_{i+1} \wedge e_{i+2} \\
 &\quad + ((\alpha_{n-1} + \beta_{n-1})^2 - \alpha_{n-1}^2 - \beta_{n-1}^2) e_1 \wedge e_n \\
 &\quad + ((\alpha_n + \beta_n)^2 - \alpha_n^2 - \beta_n^2) e_1 \wedge e_2 \\
 &\quad + \sum_{1 \leq i < j \leq n} ((\alpha_i + \beta_i)(\alpha_j + \beta_j) - \alpha_i \alpha_j - \beta_i \beta_j) e_i \wedge e_j \\
 &= \sum_{1 \leq i < j \leq n} (\alpha_i \beta_j - \beta_i \alpha_j) e_i \wedge e_j \\
 &= x \wedge y.
 \end{aligned}$$

L'opérateur  $\wedge : A \times A \longrightarrow \wedge^2 A$  étant bilinéaire [37, (9.2.1), page 321],  $b_q$  est une application bilinéaire ; donc  $q$  est une application quadratique.

Montrons que  $q$  est régulière. Soit  $x = \sum_{i=1}^n \alpha_i e_i \in \text{rad}(b_q)$ , avec  $\alpha_i \in \mathbb{F}_2$ , pour tout  $i$ . Alors pour tout  $y \in A$ ,  $b_q(x, y) = 0$ . En particulier  $b_q(x, e_1) = 0$ . Or

$$b_q(x, e_1) = x \wedge e_1 = \sum_{i=2}^n \alpha_i e_i \wedge e_1 = \sum_{i=2}^n \alpha_i e_1 \wedge e_i$$

et le système  $(e_1 \wedge e_i)_{i=2}^n$  est libre ; donc  $\alpha_2 = \alpha_3 = \dots = \alpha_n = 0$ . De même, de l'égalité  $b_q(x, e_2) = 0$ , il résulte que  $\alpha_1 = 0$  et alors  $x = 0$ . Par suite  $\text{rad}(b_q) = 0$  et donc  $q$  est régulière.

Comme pour tous  $x, y \in A$ ,  $x \wedge y = b_q(x, y) \in b_q(A \times A)$ , alors  $\wedge^2 A = b_q(A \times A) = \text{sgr} < b_q(A \times A) >$ . Donc d'après le théorème 3.4.23, il existe un unique 2-groupe spécial  $G$  d'application quadratique  $q$  tel que  $Z(G) = \wedge^2 A$  et  $\frac{G}{Z(G)} = A$ .

Montrons que  $G$  n'est pas ambivalent. En vertu du théorème 3.4.36, il suffit de montrer qu'il existe  $a \in A$  tel que pour tout  $x \in A$ ,  $q(a) \neq b_q(a, x)$ . Par définition de  $q$ ,  $q(e_1) = e_2 \wedge e_3$ . Supposons qu'il existe  $x \in A$  tel que  $q(e_1) = b_q(e_1, x) = e_1 \wedge x$ . Alors  $e_2 \wedge e_3 = e_1 \wedge x$ . D'où si  $x = \sum_{i=1}^n \alpha_i e_i$ , avec  $\alpha_i \in \mathbb{F}_2$ , pour tout  $i$ , on a :

$$e_2 \wedge e_3 - \alpha_2 e_1 \wedge e_2 - \alpha_3 e_1 \wedge e_3 - \cdots - \alpha_n e_1 \wedge e_n = 0;$$

et comme le système  $(e_2 \wedge e_3, e_1 \wedge e_2, e_1 \wedge e_3, \dots, e_1 \wedge e_n)$  est libre, alors  $1 = -\alpha_2 = -\alpha_3 = \cdots = -\alpha_n = 0$ , ce qui est absurde. Le 2-groupe spécial  $G$  n'est donc pas ambivalent.

Pour clôturer ce chapitre, nous allons illustrer par quelques exemples l'usage du théorème 3.4.35, pour vérifier l'ortho-ambivalence d'un 2-groupe spécial ambivalent donné par rapport à un corps de caractéristique différente de 2. Nous avons besoin du résultat suivant :

**Proposition 3.4.37.** *Soient  $A$  un espace vectoriel de dimension finie  $2m$  sur le corps  $\mathbb{F}_{2^n}$  (avec  $n, m \in \mathbb{N}_0$ ) et  $q : A \rightarrow \mathbb{F}_{2^n}$  une forme quadratique régulière.*

- (1) *Il existe alors un unique 2-groupe spécial ambivalent  $G$  d'application quadratique  $q$  et tel que  $Z(G) = \mathbb{F}_{2^n}$  et  $\frac{G}{Z(G)} = A$ .*
- (2) *Soit  $s : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$  une forme linéaire non nulle. Le transfert  $s_*(q) : A \rightarrow \mathbb{F}_2$  est une forme quadratique régulière (elle est donc isométrique à  $q_s$ ).*

*Preuve :*

- 1) Soit  $(e_i, f_i)_{i=1}^m$  une base symplectique de l'espace symétrique alterné  $(A, b_q)$  (voir définition 3.4.16). Rappelons qu'alors

$$b_q(e_i, e_i) = b_q(f_i, f_i) = 0, \quad \forall i,$$

$$b_q(e_i, f_i) = b_q(f_i, e_i) = 1, \quad \forall i$$

et

$$b_q(e_i, e_j) = b_q(e_i, f_j) = b_q(f_i, e_j) = b_q(f_i, f_j) = 0, \quad \forall i \neq j.$$

Il est connu que le corps fini  $\mathbb{F}_{2^n}$  est l'ensemble des solutions de l'équation  $X^{2^n} - X = 0$  dans une clôture algébrique  $K_2$  de  $\mathbb{F}_2$  et on a :

$$\mathbb{F}_{2^n} = \{0, 1, a, a^2, \dots, a^{2^n-2}\},$$

$a$  étant une racine primitive  $(2^n - 1)$ -ième de l'unité dans  $K_2$ , laquelle vérifie la relation

$$\sum_{j=0}^{2^n-2} a^j = 0.$$

**a)** Montrons que  $\mathbb{F}_{2^n} = \text{sg}r < b_q(A \times A) >$ . Comme  $b_q(e_1, f_1) = 1$ , alors pour tout  $j = 0, 1, 2, \dots, 2^n - 2$ ,

$$a^j = b_q(a^j e_1, f_1) \in b_q(A \times A)$$

et donc  $b_q(A \times A) = \mathbb{F}_{2^n}$  et le résultat s'ensuit.

**b)** Montrons que pour tout  $x \in A$ , il existe  $x' \in A$  tel que  $q(x) = b_q(x, x')$ . Soit alors  $x \in A$  tel que  $x = \sum_{i=1}^m (x_i e_i + y_i f_i)$ , avec  $x_i, y_i \in \mathbb{F}_{2^n}$ , pour  $i = 1, 2, \dots, m$ . D'une part, la base  $(e_i, f_i)_{i=1}^m$  étant symplectique, on a :

$$q(x) = \sum_{i=1}^m (x_i^2 q(e_i) + x_i y_i + y_i^2 q(f_i)).$$

D'autre part, en prenant

$$x' = \sum_{i=1}^m (y_i q(f_i) e_i + (x_i q(e_i) + y_i) f_i),$$

on a :

$$\begin{aligned}
 b_q(x, x') &= \sum_{i=1}^m (x_i(x_i q(e_i) + y_i) + y_i^2 q(f_i)) \\
 &= \sum_{i=1}^m (x_i^2 q(e_i) + x_i y_i + y_i^2 q(f_i)) \\
 &= q(x).
 \end{aligned}$$

c) De a) et b), il résulte que  $q$  est une application quadratique vérifiant les hypothèses du théorème 3.4.23 et la condition (3) du théorème 3.4.36. Le résultat découle donc de ce dernier théorème.

2) Soit  $x \in A$  tel que  $x \neq 0$ . Comme  $q$  est une forme quadratique régulière, alors il existe  $y \in A$  tel que  $b_q(x, y) = 1$ .  $s$  étant non nulle, elle est surjective et donc il existe  $\alpha \in \mathbb{F}_{2^n}$  tel que  $s(\alpha) = 1$ . Par suite

$$b_{s_*(q)}(x, \alpha y) = s(\alpha) = 1$$

et donc  $x \notin \text{rad}(b_{s_*(q)})$ . Il en résulte que  $\text{rad}(b_{s_*(q)}) = 0$  et alors  $s_*(q)$  est régulière. ■

**Remarque 3.4.38.** Avec les notations utilisées dans la démonstration de la proposition 3.4.37, en théorie des formes quadratiques en caractéristique 2, la forme quadratique régulière  $q$  telle que

$$q(x) = \sum_{i=1}^m (x_i^2 q(e_i) + x_i y_i + y_i^2 q(f_i))$$

pour  $x = \sum_{i=1}^m (x_i e_i + y_i f_i)$  (avec  $x_i, y_i \in \mathbb{F}_{2^n}$ , pour  $i = 1, 2, \dots, m$ ) s'identifie au polynôme homogène

$$\sum_{i=1}^m (x_i^2 q(e_i) + x_i y_i + y_i^2 q(f_i))$$

de l'anneau  $\mathbb{F}_{2^n}[x_1, y_1, x_2, y_2, \dots, x_m, y_m]$  et se note simplement par

$$q = [q(e_1), q(f_1)] \perp [q(e_2), q(f_2)] \perp \dots \perp [q(e_m), q(f_m)],$$

$\perp$  étant la somme orthogonale des formes quadratiques. On pose aussi

$$p \times [a_i, b_i] := \underbrace{[a_i, b_i] \perp [a_i, b_i] \perp \cdots \perp [a_i, b_i]}_{p \text{ termes}},$$

pour  $p \in \mathbb{N}_0$  et  $a_i, b_i \in \mathbb{F}_{2^n}$ .

Pour nous permettre de donner aisément les illustrations annoncées, il nous importe de rappeler certaines propriétés des formes quadratiques en caractéristique 2. Rappelons d'abord quelques définitions.

Soient  $k$  un corps de caractéristique 2,  $A$  un  $k$ -espace vectoriel de dimension finie paire et  $q : A \rightarrow k$  une forme quadratique régulière.

- (a) La dimension de  $A$  est appelée dimension de  $q$  et se note  $\dim q$ .
- (b) Si  $\dim q = 2$  et  $q$  est isométrique à  $[0, 0]$  (on note  $q \cong [0, 0]$ ), on dit que  $q$  est un plan hyperbolique.
- (c) Si  $q$  est somme orthogonale des plans hyperboliques, on dit que  $q$  est hyperbolique.
- (d)  $q$  est dite isotrope s'il existe un vecteur  $x$  non nul de  $A$  tel que  $q(x) = 0$ ; dans le cas contraire,  $q$  est dite anisotrope.

La proposition suivante reprend certaines isométries de formes quadratiques.

**Proposition 3.4.39.** [28, lemme D.3.10, page 177] *Pour tous  $\alpha, \beta, \gamma, \delta \in k$ , on a :*

- (1)  $[\gamma\alpha, \gamma^{-1}\beta] \cong \gamma[\alpha, \beta]$  si  $\gamma \neq 0$ ;
- (2)  $[\alpha, \beta] \cong [\alpha, \alpha + \beta + 1]$ ;
- (3)  $[\alpha, \beta] \perp [\gamma, \delta] \cong [\alpha + \gamma, \beta] \perp [\gamma, \beta + \delta]$ .

On en déduit alors que pour tous  $\alpha, \beta \in k$ , pour tout  $m \in \mathbb{N}_0$ ,

- (e) si  $\alpha \neq 0$ , alors  $[0, \alpha] \cong \alpha^{-1}[0, 1] \cong \alpha^{-1}[0, 0]$  (après usage successif des formules (1) et (2) de la proposition 3.4.39); donc la forme quadratique  $[0, \alpha]$  est un plan hyperbolique;

- (f) si  $\alpha \neq 0$ , alors  $[\alpha, \beta] \cong \alpha[1, \alpha\beta]$ , d'après la proposition 3.4.39.(1) ;
- (g)  $2 \times [1, \alpha] = [1, \alpha] \perp [1, \alpha] \cong [0, \alpha] \perp [1, 0]$  (d'après la proposition 3.4.39.(3)) ; donc  $2 \times [1, \alpha]$  est hyperbolique et donc :
- (h) la forme quadratique  $m \times [1, \alpha]$  est hyperbolique pour  $m$  pair ; elle est somme orthogonale d'une forme quadratique hyperbolique avec  $[1, \alpha]$  pour  $m$  impair.

Enfin, d'après [29, théorème 1.3.1, page 14], on a :

**Proposition 3.4.40.** *Si  $k$  est un corps fini, alors à isométrie près, toute  $k$ -forme quadratique régulière  $q$  est ou bien hyperbolique, ou bien une somme orthogonale de la forme*

$$q = q_{hyp} \perp [\alpha, \beta]$$

où  $q_{hyp}$  est une forme quadratique hyperbolique (appelée partie hyperbolique de  $q$ ) et la forme quadratique  $[\alpha, \beta]$  (avec  $\alpha, \beta \in k^\times$ ) est anisotrope. ■

Le 2-groupe spécial  $G$  donné par la proposition 3.4.37 étant ambivalent, on peut lui appliquer le théorème 3.4.35 tel que nous le verrons dans les illustrations ultérieures. Rappelons que si  $A$  est un  $\mathbb{F}_2$ -espace vectoriel de dimension finie,  $q : A \rightarrow \mathbb{F}_2$  une forme quadratique régulière et  $s : \mathbb{F}_2 \rightarrow \mathbb{F}_2$  une forme linéaire non nulle,  $q_s$  désigne la  $\mathbb{F}_2$ -forme quadratique sur  $A_s := \frac{A}{\text{rad}(b_{s_*(q)})}$  induite par le transfert  $s_*(q)$  de  $q$  par  $s$  et définie par  $q_s(\varepsilon_s(x)) = s_*(q)(x)$ , pour  $x \in A$ ,  $\varepsilon_s : A \rightarrow A_s$  étant la surjection canonique. Le résultat suivant nous facilitera les calculs.

**Proposition 3.4.41.** *Soient  $A_1, A_2$  des  $\mathbb{F}_2$ -espaces vectoriels,  $q_1 : A_1 \rightarrow \mathbb{F}_2$ ,  $q_2 : A_2 \rightarrow \mathbb{F}_2$  des formes quadratiques régulières et  $s : \mathbb{F}_2 \rightarrow \mathbb{F}_2$  une forme linéaire non nulle. Alors :*

- (1)  $s_*(q_1 \perp q_2) = s_*(q_1) \perp s_*(q_2)$  ;
- (2)  $b_{s_*(q_1 \perp q_2)} = b_{s_*(q_1)} \perp b_{s_*(q_2)}$  ;
- (3)  $\text{rad}(b_{s_*(q_1 \perp q_2)}) = \text{rad}(b_{s_*(q_1)}) \times \text{rad}(b_{s_*(q_2)})$  ;
- (4)  $(q_1 \perp q_2)_s = (q_1)_s \perp (q_2)_s$ .

*Preuve :*



1) Pour tout  $(x, y) \in A_1 \times A_2$ , on a :

$$\begin{aligned} s_*(q_1 \perp q_2)(x, y) &= s(q_1(x) + q_2(y)) = s(q_1(x)) + s(q_2(y)) \\ &= s_*(q_1)(x) + s_*(q_2)(y) = (s_*(q_1) \perp s_*(q_2))(x, y); \end{aligned}$$

donc  $s_*(q_1 \perp q_2) = s_*(q_1) \perp s_*(q_2)$ .

2) Pour tout  $(x, y), (x', y') \in A_1 \times A_2$ , en se servant de (1), on a :

$$\begin{aligned} b_{s_*(q_1 \perp q_2)}((x, y), (x', y')) &= s_*(q_1 \perp q_2)(x + x', y + y') \\ &\quad - s_*(q_1 \perp q_2)(x, y) - s_*(q_1 \perp q_2)(x', y') \\ &= s_*(q_1)(x + x') + s_*(q_2)(y + y') \\ &\quad - s_*(q_1)(x) - s_*(q_2)(y) \\ &\quad - s_*(q_1)(x') - s_*(q_2)(y') \\ &= b_{s_*(q_1)}(x, x') + b_{s_*(q_2)}(y, y') \\ &= [b_{s_*(q_1)} \perp b_{s_*(q_2)}]((x, y), (x', y')); \end{aligned}$$

donc  $b_{s_*(q_1 \perp q_2)} = b_{s_*(q_1)} \perp b_{s_*(q_2)}$ .

3) Soit  $(a, b) \in \text{rad}(b_{s_*(q_1 \perp q_2)})$ ; alors pour tout  $(x, y) \in A_1 \times A_2$ ,

$$0 = b_{s_*(q_1 \perp q_2)}((a, b), (x, y)) = b_{s_*(q_1)}(a, x) + b_{s_*(q_2)}(b, y).$$

En particulier,

$$0 = b_{s_*(q_1)}(a, x) + b_{s_*(q_2)}(b, b) = b_{s_*(q_1)}(a, x), \text{ pour tout } x \in A_1$$

et

$$0 = b_{s_*(q_1)}(a, a) + b_{s_*(q_2)}(b, y) = b_{s_*(q_2)}(b, y), \text{ pour tout } y \in A_2.$$

Donc  $a \in \text{rad}(b_{s_*(q_1)})$  et  $b \in \text{rad}(b_{s_*(q_2)})$  et alors

$$(a, b) \in \text{rad}(b_{s_*(q_1)}) \times \text{rad}(b_{s_*(q_2)});$$

d'où

$$\text{rad}(b_{s_*(q_1 \perp q_2)}) \subset \text{rad}(b_{s_*(q_1)}) \times \text{rad}(b_{s_*(q_2)}).$$

On vérifie de même que

$$\text{rad}(b_{s_*(q_1 \perp q_2)}) \supset \text{rad}(b_{s_*(q_1)}) \times \text{rad}(b_{s_*(q_2)}).$$

4) On sait que

$$(A_1 \times A_2)_s = \frac{A_1 \times A_2}{\text{rad}(b_{s_*(q_1 \perp q_2)})} = \frac{A_1 \times A_2}{\text{rad}(b_{s_*(q_1)}) \times \text{rad}(b_{s_*(q_2)})}$$

est isomorphe à

$$\frac{A_1}{\text{rad}(b_{s_*(q_1)})} \times \frac{A_2}{\text{rad}(b_{s_*(q_2)})} = (A_1)_s \times (A_2)_s$$

(d'après le lemme 3.3.2.(2) appliqué aux  $\mathbb{F}_2$ -espaces vectoriels via la structure de groupe sous-jacente à ceux-ci). Par l'intermédiaire de cet isomorphisme, la surjection canonique  $\varepsilon_s : A_1 \times A_2 \rightarrow (A_1 \times A_2)_s$  s'identifie à l'application  $\varepsilon_s^1 \times \varepsilon_s^2$  définie par

$$(\varepsilon_s^1 \times \varepsilon_s^2)(x, y) = (\varepsilon_s^1(x), \varepsilon_s^2(y)), \text{ pour } (x, y) \in A_1 \times A_2,$$

où  $\varepsilon_s^1 : A_1 \rightarrow (A_1)_s$  et  $\varepsilon_s^2 : A_2 \rightarrow (A_2)_s$  désignent les surjections canoniques. Pour tout  $(x, y) \in A_1 \times A_2$ , on a :

$$\begin{aligned} (q_1 \perp q_2)_s(\varepsilon_s(x, y)) &= s_*(q_1 \perp q_2)(x, y) \\ &= (s_*(q_1) \perp s_*(q_2))(x, y) \\ &= s_*(q_1)(x) + s_*(q_2)(y) \\ &= (q_1)_s(\varepsilon_s^1(x)) + (q_2)_s(\varepsilon_s^2(x)) \\ &= ((q_1)_s \perp (q_2)_s)(\varepsilon_s^1(x), \varepsilon_s^2(y)) \\ &= ((q_1)_s \perp (q_2)_s)(\varepsilon_s(x, y)); \end{aligned}$$

donc  $(q_1 \perp q_2)_s = (q_1)_s \perp (q_2)_s$ . ■

Avant de traiter le cas général, intéressons nous d'abord au cas particulier  $n = 2$  c'est-à-dire aux  $\mathbb{F}_4$ -formes quadratiques régulières, avec

$$\mathbb{F}_4 = \{0, 1, a, a^2 = 1 + a\}.$$

Remarquons d'abord que sur  $\mathbb{F}_4$  on a les particularités suivantes :

- (a) la forme quadratique  $[1, 1] = x^2 + xy + y^2$  est isotrope car  $a^2 + a \cdot 1 + 1^2 = 0$  ; elle est donc isométrique à la forme hyperbolique  $[0, 0]$ , d'après [28, lemme 1.2.8, page 5] ;

- (b) les formes quadratiques  $[1, a]$  et  $[1, a^2]$  sont isométriques, en effet, posons  $q = [1, a] : V \rightarrow \mathbb{F}_4$ . Soit  $(e, f)$  une base symplectique de  $(V, b_q)$ ; alors  $q(e) = 1$ ,  $q(f) = a$  et  $b_q(e, f) = 1$ .  $(e, ae + f)$  est donc une base de  $V$  telle que

$$b_q(e, ae + f) = 1, \quad q(e) = 1$$

et

$$q(ae + f) = b_q(ae, f) + q(ae) + q(f) = a + a^2 + a = a^2;$$

par suite  $(e, ae + f)$  est une base symplectique de  $(V, b_q)$  et alors  $q$  est isométrique à  $[1, a^2]$ .

**Proposition 3.4.42.** *Soit  $q : A \rightarrow \mathbb{F}_4$  une forme quadratique régulière de dimension 2 et  $s : \mathbb{F}_4 \rightarrow \mathbb{F}_2$  une forme linéaire non nulle.*

- (1) Si  $q = [0, 0]$ , alors  $Arf(q_s) = 0$ .  
 (2) Si  $q = [1, a]$ , alors  $Arf(q_s) = 1$ .

*Preuve :* D'après la proposition 3.4.37,  $s_*(q)$  est régulière, donc isométrique à  $q_s$ . Supposons que  $q = [\alpha, \beta]$  par rapport à une base symplectique  $(e, f)$  de l'espace symétrique alternée  $(A, b_q)$ . La forme linéaire  $s : \mathbb{F}_4 \rightarrow \mathbb{F}_2$  étant non nulle, elle est surjective; donc  $\frac{\mathbb{F}_4}{Kers}$  est isomorphe à  $\mathbb{F}_2$  et alors  $|Kers| = 2$ . Il existe donc un unique entier  $i$  tel que  $0 \leq i \leq 2$  et  $s(a^i) = 0$ .

a) Si  $i = 0$ , alors  $s(a) = s(a^2) = 1$ . Comme

$$b_q(e, f) = 1, \quad \text{et} \quad b_q(e, e) = b_q(f, f) = 0,$$

alors pour tout  $j = 1, 2$ , on a :

$$b_{s_*(q)}(a^j e, a^j f) = b_{s_*(q)}(a^j e, a^j f) = s(a^{2j}) = 1, \quad (3.35)$$

et

$$b_{s_*(q)}(a^j e, a^{2j} f) = b_{s_*(q)}(a^{2j} e, a^j f) = s(a^{3j}) = s(1) = 0. \quad (3.36)$$

Comme  $(a, a^2)$  est une base de  $\mathbb{F}_4$  sur  $\mathbb{F}_2$ , alors  $(ae, af, a^2e, a^2f)$  est une base de  $A$  sur  $\mathbb{F}_2$  et d'après (3.35) et (3.36), c'est une base symplectique de  $(A, b_{s_*(q)}) \cong (A_s, b_{q_s})$ . D'où

$$\begin{aligned} Arf(q_s) &= Arf(s_*(q)) \\ &= s(q(ae))s(q(af)) + s(q(a^2e))s(q(a^2f)) \\ &= s(a^2q(e))s(a^2q(f)) + s(aq(e))s(aq(f)) \\ &= s(a^2\alpha)s(a^2\beta) + s(a\alpha)s(a\beta). \end{aligned}$$

En particulier,

**(a.1)** pour  $q = [0, 0]$ ,  $Arf(q_s) = 0$ ;

**(a.2)** pour  $q = [1, a]$ ,  $Arf(q_s) = s(a^2)s(a^3) + s(a)s(a^2) = 0 + 1 = 1$ .

**b)** Si  $i \in \{1, 2\}$ , alors  $s(1) = s(a^{2i}) = 1$ . Par suite

$$b_{s_*(q)}(e, f) = s(1) = 1 \quad (3.37)$$

et on a :

$$b_{s_*(q)}(a^i e, f) = b_{s_*(q)}(e, a^i f) = s(a^i) = 0 \quad (3.38)$$

et

$$b_{s_*(q)}(a^i e, a^i f) = s(a^{2i}) = 1. \quad (3.39)$$

Comme  $(1, a^i)$  est une base de  $\mathbb{F}_4$  sur  $\mathbb{F}_2$ , alors  $(e, f, a^i e, a^i f)$  est une base de  $A$  sur  $\mathbb{F}_2$  et d'après (3.37), (3.38) et (3.39), c'est une base symplectique de  $(A, b_{s_*(q)}) \cong (A_s, b_{q_s})$ . D'où

$$\begin{aligned} Arf(q_s) &= Arf(s_*(q)) \\ &= s(q(e))s(q(f)) + s(q(a^i e))s(q(a^i f)) \\ &= s(\alpha)s(\beta) + s(a^{2i}\alpha)s(a^{2i}\beta). \end{aligned}$$

En particulier,

**(b.1)** pour  $q = [0, 0]$ ,  $Arf(q_s) = 0$ ;

**(b.2)** pour  $q = [1, a]$ ,  $Arf(q_s) = s(1)s(a) + s(a^{2i})s(a^{2i+1}) = 1$ .

Le résultat est ainsi établi. ■

Des illustrations du théorème 3.4.35 sont données par la proposition suivante :

**Proposition 3.4.43.** *Soient  $A$  un  $\mathbb{F}_4$ -espace vectoriel de dimension finie  $2m$  (avec  $m \in \mathbb{N}_0$ ),  $q : A \rightarrow \mathbb{F}_4$  une forme quadratique régulière et  $k$  un corps de caractéristique différente de 2. Notons par  $q_{hyp}$  la partie hyperbolique de  $q$ . Soit  $G$  le 2-groupe spécial ambivalent d'application quadratique  $q$ , tel que  $Z(G) = \mathbb{F}_4$  et  $\frac{G}{Z(G)} = A$  (voir proposition 3.4.37).*

- (1) *Si  $q$  est hyperbolique, alors  $G$  est ortho-ambivalent par rapport à  $k$ .*
- (2) *Si  $q = q_{hyp} \perp [1, a]$ , alors  $G$  n'est pas ortho-ambivalent par rapport à  $k$ .*

*Preuve :* Soit  $s : \mathbb{F}_4 \rightarrow \mathbb{F}_2$  une forme linéaire non nulle.

- 1) Si  $q$  est hyperbolique, alors

$$q \cong \underbrace{[0, 0] \perp [0, 0] \perp \cdots \perp [0, 0]}_{m \text{ facteurs}}.$$

En utilisant successivement les propositions 3.4.41.(4), 3.4.17 et 3.4.42, on a :

$$\begin{aligned} \text{Arf}(q_s) &= \underbrace{\text{Arf}([0, 0]_s) + \text{Arf}([0, 0]_s) + \cdots + \text{Arf}([0, 0]_s)}_{m \text{ facteurs}} \\ &= \underbrace{0 + 0 + \cdots + 0}_{m \text{ facteurs}} = 0. \end{aligned}$$

De façon analogue et en utilisant 1), on obtient :

- 2) Si  $q = q_{hyp} \perp [1, a]$ , alors

$$\text{Arf}(q_s) = \text{Arf}((q_{hyp})_s) + \text{Arf}([1, a]_s) = 0 + 1 = 1.$$

Le résultat découle alors du théorème 3.4.35. ■

Pour réaliser une étude complète de l'ortho-ambivalence du 2-groupe spécial donné par la proposition 3.4.37, par rapport à un corps de caractéristique différente de 2, il faut répondre à la question suivante :

**Question 3.4.44.** *Trouver une généralisation de la proposition 3.4.43, en remplaçant  $\mathbb{F}_4$  par  $\mathbb{F}_{2^n}$  pour  $n$  entier  $> 2$ .*

Pour y arriver, nous allons démontrer que si  $k$  est un corps fini de caractéristique 2, toute  $\mathbb{F}_2$ -forme linéaire non nulle sur  $k$  se définit à l'aide de la forme trace  $Tr_{k/\mathbb{F}_2}$  de l'extension  $k/\mathbb{F}_2$ . Pour faciliter les calculs, nous allons opérer dans le groupe de Witt  $W_q(k)$  des espaces quadratiques sur  $k$  (qui est en fait un module sur l'anneau de Witt  $W(k)$  des espaces bilinéaires symétriques sur  $k$ ) et utiliser le transfert  $(Tr_{k/\mathbb{F}_2})_* : W_q(k) \rightarrow W_q(\mathbb{F}_2)$  pour opérer dans  $W_q(\mathbb{F}_2)$ . Nous réaliserons qu'alors pour toute forme quadratique régulière  $q : V \rightarrow k$ , pour toute  $\mathbb{F}_2$ -forme linéaire  $s : k \rightarrow \mathbb{F}_2$ , dans  $W_q(\mathbb{F}_2)$ , on a :  $[s_*(q)] = [(Tr_{k/\mathbb{F}_2})_*(q)]$  et donc  $Arf(s_*(q)) = Arf(Tr_{k/\mathbb{F}_2})_*(q)$ . Cela constituera une clé de recherche de solution à la question 3.4.44.

Il est indispensable de rappeler brièvement les ingrédients à utiliser, tirés en grande partie de [2, pages 1-21]. Soit  $k/F$  une extension finie de corps de caractéristique 2.

**Définition 3.4.45.** *Un espace quadratique sur  $k$  est un couple  $(V, q)$ , où  $V$  est un  $k$ -espace vectoriel de dimension finie et  $q : V \rightarrow k$  est une forme quadratique régulière. On note par  $Quad(k)$  l'ensemble des espaces quadratiques sur  $k$ . Si  $V$  est un  $k$ -espace vectoriel de dimension finie, l'application  $q_V : V \oplus V^* \rightarrow k$  définie par*

$$q_V(x + f) = f(x), \text{ pour } x \in V \text{ et } f \in V^* = Hom_k(V, k),$$

*est une forme quadratique régulière et l'espace quadratique  $(V \oplus V^*, q_V)$  se note  $\mathbb{H}(V)$  et est appelé espace hyperbolique associé à  $V$ .*

Un espace quadratique sur  $k$  est dit hyperbolique s'il est isométrique à  $\mathbb{H}(V)$  pour un certain  $k$ -espace vectoriel  $V$ .

**Définition 3.4.46.** Un espace bilinéaire symétrique sur  $k$  est un couple  $(V, b)$ , où  $V$  est un  $k$ -espace vectoriel de dimension finie et  $b : V \times V \rightarrow k$  est une forme bilinéaire régulière (c'est-à-dire de radical nul). On note par  $\text{Bil}(k)$  l'ensemble des espaces bilinéaires symétriques sur  $k$ . Si  $b : V \times V \rightarrow k$  est une forme bilinéaire symétrique, l'application  $b_V : (V \oplus V^*) \times (V \oplus V^*) \rightarrow k$  définie par

$$b_V(x + f, y + g) = f(y) + g(x) + b(x, y), \quad \text{pour } x, y \in V \text{ et } f, g \in V^*,$$

est une forme bilinéaire symétrique régulière et l'espace bilinéaire symétrique  $(V \oplus V^*, b_V)$  se note  $\mathbb{M}(V)$  et est appelé espace métabolique associé à  $V$ . Si  $b = 0$ ,  $\mathbb{M}(V)$  se note  $\mathbb{H}_0(V)$  et est appelé espace bilinéaire hyperbolique associé à  $V$ . Un espace bilinéaire symétrique sur  $k$  est dit métabolique s'il est isométrique à  $\mathbb{M}(V)$  pour un certain  $k$ -espace vectoriel  $V$ .

Soient  $(V_1, q_1), (V_2, q_2) \in \text{Quad}(k)$  et  $(W_1, b_1), (W_2, b_2) \in \text{Bil}(k)$ . On pose :

$$(V_1, q_1) \perp (V_2, q_2) = (V_1 \oplus V_2, q_1 \perp q_2), \quad (3.40)$$

$$(W_1, b_1) \otimes (V_1, q_1) = (W_1 \otimes V_1, b_1 \otimes q_1), \quad (3.41)$$

$$(W_1, b_1) \perp (W_2, b_2) = (W_1 \oplus W_2, b_1 \perp b_2) \quad (3.42)$$

et

$$(W_1, b_1) \otimes (W_2, b_2) = (W_1 \otimes W_2, b_1 \otimes b_2) \quad (3.43)$$

avec

$$(q_1 \perp q_2)(x + y) = q_1(x) + q_2(x), \quad \text{pour } x \in V_1 \text{ et } y \in V_2,$$

$$(b_1 \otimes q_1)(x \otimes y) = b_1(x, x)q_1(y), \quad \text{pour } x \in W_1 \text{ et } y \in V_1$$

et

$$(b_1 \perp b_2)(x + x', y + y') = b_1(x, y) + b_2(x', y'),$$

$$(b_1 \otimes b_2)(x \otimes x', y \otimes y') = b_1(x, y)b_2(x', y'),$$

pour  $x, y \in W_1$  et  $x', y' \in W_2$ .

**Définition 3.4.47.** On note par  $\widehat{W}(k)$  (resp.  $\widehat{W}_q(k)$ ) l'anneau de Grothendieck-Witt des espaces bilinéaires symétriques sur  $k$  (resp. le groupe de Grothendieck-Witt des espaces quadratiques sur  $k$ ). C'est en fait l'anneau de Grothendieck des classes d'isométrie des espaces bilinéaires symétriques sur  $k$  (resp. le groupe de Grothendieck des classes d'isométrie des espaces quadratiques sur  $k$ ) dans lequel l'addition est induite par la somme orthogonale et la multiplication, par le produit tensoriel sur  $\text{Bil}(k)$  (resp. dans lequel l'addition est induite par la somme orthogonale sur  $\text{Quad}(k)$ ). On pose

$$\widehat{\mathbb{H}}_q(k) = \{[\mathbb{H}(V)] - [\mathbb{H}(V')] \mid V \text{ et } V' \text{ des } k\text{-espaces vectoriels}\}$$

et

$$\widehat{\mathbb{M}}(k) = \{[\mathbb{M}(V)] - [\mathbb{M}(V')] \mid V \text{ et } V' \text{ des } k\text{-espaces vectoriels}\}.$$

$\widehat{\mathbb{H}}_q(k)$  (resp.  $\widehat{\mathbb{M}}(k)$ ) est un sous-groupe de  $\widehat{W}_q(k)$  (resp. un idéal de  $\widehat{W}(k)$ ). On pose :

$$W(k) = \frac{\widehat{W}(k)}{\widehat{\mathbb{M}}(k)} \quad \text{et} \quad W_q(k) = \frac{\widehat{W}_q(k)}{\widehat{\mathbb{H}}_q(k)}.$$

$W(k)$  (resp.  $W_q(k)$ ) est appelé l'anneau de Witt des espaces bilinéaires symétriques sur  $k$  (resp. le groupe de Witt des espaces quadratiques sur  $k$ ).

L'anneau  $W(k)$  a pour élément unité la classe de l'espace bilinéaire symétrique  $(k, b)$ , où  $b : k \times k \rightarrow k$  est définie par  $b(x, y) = xy$ , pour  $x, y \in k$  : cet espace se note simplement par  $< 1 >$ , en conformité avec la notation des espaces bilinéaires symétriques diagonalisables tel que nous allons le préciser ci-dessous.

Le produit tensoriel défini par (3.41) induit une multiplication externe  $W(k) \times W_q(k) \rightarrow W_q(k)$  qui, avec l'addition dans  $W_q(k)$ , font de  $W_q(k)$  un  $W(k)$ -module.



Soit  $(V, b)$  un espace bilinéaire symétrique sur  $k$ . Si  $(V, b)$  est diagonalisable c'est-à-dire s'il existe une base de  $V$  dans laquelle la matrice de Gram de  $b$  est diagonale de la forme

$$\begin{pmatrix} \alpha_1 & 0 & \cdots & 0 \\ 0 & \alpha_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha_r \end{pmatrix},$$

avec  $r = \dim_k V$  et  $\alpha_i \in k$ , pour tout  $i$ , on pose

$$(V, b) := \langle \alpha_1, \alpha_2, \dots, \alpha_r \rangle.$$

Supposons l'extension  $k/F$  galoisienne finie de groupe de Galois  $G = \text{Gal}(k/F)$ . La  $F$ -forme linéaire trace  $Tr_{k/F} : k \rightarrow F$  de l'extension  $k/F$  est définie par

$$Tr_{k/F}(x) = \sum_{\tau \in G} \tau(x).$$

D'une part, l'application

$$(Tr_{k/F})_* : \text{Quad}(k) \rightarrow \text{Quad}(F) : (V, q) \mapsto (V, (Tr_{k/F})_*(q))$$

(resp. l'application

$$(Tr_{k/F})_* : \text{Bil}(k) \rightarrow \text{Bil}(F) : (V, b) \mapsto (V, (Tr_{k/F})_*(b)))$$

induit un morphisme de groupes

$$(Tr_{k/F})_* : W_q(k) \rightarrow W_q(F)$$

(resp. un morphisme de groupes

$$(Tr_{k/F})_* : W(k) \rightarrow W(F) )$$

appelé transfert (d'après [2, page 19]).

D'autre part, l'inclusion  $i : F \rightarrow k$  induit un morphisme de groupes  $i_q^* : W_q(F) \rightarrow W_q(k)$  via l'application  $i_q^* : Quad(F) \rightarrow Quad(k)$  définie par

$$i_q^*(V, q) = (V \otimes_F k, q \otimes id_k), \text{ pour } (V, q) \in Quad(F),$$

avec

$$(q \otimes id_k)(x \otimes \alpha) = q(x) \otimes \alpha^2, \text{ pour } x \in V \text{ et } \alpha \in k.$$

Cette inclusion induit de façon analogue un morphisme d'anneaux  $i^* : W(F) \rightarrow W(k)$  par extension des scalaires à  $k$ . Les morphismes de groupes  $(Tr_{k/F})_*$ ,  $i_q^*$  et  $i^*$  vérifient les relations suivantes :

**Proposition 3.4.48.** (Réciprocité de Frobenius)

(1) Pour tout  $x \in W(F)$ , pour tout  $y \in W_q(k)$ ,

$$(Tr_{k/F})_*(i^*(x)y) = x(Tr_{k/F})_*(y).$$

(2) Pour tout  $x \in W(k)$ , pour tout  $y \in W_q(F)$ ,

$$(Tr_{k/F})_*(xi_q^*(y)) = (Tr_{k/F})_*(x)y.$$

*Preuve :* Voir [2, proposition 2.12, page 8]. ■

**Définition 3.4.49.** Une extension de corps est dite quadratique si elle est de degré 2. Soit  $(V, b)$  un espace bilinéaire symétrique sur  $k$ . Un vecteur non nul  $x$  de  $V$  est dit isotrope si  $b(x, x) = 0$ . Si  $(V, b)$  contient un vecteur isotrope, il est dit isotrope. Dans le cas contraire, il est dit anisotrope.

**Lemme 3.4.50.** On suppose que les corps  $k$  et  $F$  sont finis. Si  $k/F$  est de degré impair, la  $F$ -forme bilinéaire symétrique  $T : k \times k \rightarrow F$  définie par

$$T(x, y) = Tr_{k/F}(xy), \text{ pour } x, y \in k,$$

est non alternée.

*Preuve :* Supposons que  $[k : F] = d$  ; par définition

$$T(1, 1) = \text{Tr}_{k/F}(1) = d.1 = 1,$$

$d$  étant impair. Donc  $T$  n'est pas alternée. ■

**Lemme 3.4.51.** *On suppose que les corps  $k$  et  $F$  sont finis.*

(1) *Si  $k/F$  est de degré impair et  $a \in F$ , alors dans  $W_q(F)$ ,*

$$(\text{Tr}_{k/F})_*([1, a]) = [1, a].$$

(2) *Si  $k/F$  est quadratique et  $a \in k$ , alors dans  $W_q(F)$ ,*

$$(\text{Tr}_{k/F})_*([1, a]) = [1, \text{Tr}_{k/F}(a)].$$

*Preuve :* Sauvageons les notations de la proposition 3.4.48.

1) Soit  $a \in F$ . Supposons que  $d = [k : F]$  est impair. Dans  $W_q(k)$ , on a :

$$[1, a] = \langle 1 \rangle [1, a] = \langle 1 \rangle i_q^*([1, a]).$$

Donc d'après la proposition 3.4.48,(2), dans  $W_q(F)$  on a :

$$(\text{Tr}_{k/F})_*([1, a]) = (\text{Tr}_{k/F})_*(\langle 1 \rangle i_q^*([1, a])) = (\text{Tr}_{k/F})_*(\langle 1 \rangle)[1, a].$$

Pour obtenir le résultat, il suffit donc de vérifier que dans  $W(F)$ ,

$$(\text{Tr}_{k/F})_*(\langle 1 \rangle) = \langle 1 \rangle.$$

Pour tous  $x, y \in k$ ,  $(\text{Tr}_{k/F})_*(\langle 1 \rangle)(x, y) = \text{Tr}_{k/F}(xy)$ . Donc d'après le lemme 3.4.50, la forme bilinéaire  $(\text{Tr}_{k/F})_*(\langle 1 \rangle)$  est non alternée ; par suite d'après [2, proposition 3.5, page 13], elle est diagonalisable et alors isométrique à  $\langle \alpha_1, \alpha_2, \dots, \alpha_d \rangle$ , avec  $\alpha_1, \alpha_2, \dots, \alpha_d \in F^\times$ . Or  $F$  étant fini de caractéristique 2, l'application  $F \rightarrow F : x \mapsto x^2$  est un automorphisme de  $F$  (c'est l'automorphisme de Frobenius de  $F$ ). Donc  $\alpha_i^{-1}$  est un carré dans  $F$  pour tout  $i$ . D'où d'après [39, lemme 3.7, page 8],

$$\langle \alpha_1, \alpha_2, \dots, \alpha_d \rangle \cong \langle \alpha_1 \alpha_1^{-1}, \alpha_2 \alpha_2^{-1}, \dots, \alpha_d \alpha_d^{-1} \rangle \cong \underbrace{\langle 1, 1, \dots, 1 \rangle}_{d \text{ termes}}$$

Par ailleurs,

$$\underbrace{\langle 1, 1, \dots, 1 \rangle}_{d \text{ termes}} \cong \underbrace{\langle 1, 1 \rangle \perp \dots \perp \langle 1, 1 \rangle}_{\frac{d-1}{2} \text{ termes}} \perp \langle 1 \rangle$$

et  $\langle 1, 1 \rangle \cong \langle 1, -1 \rangle$  est un plan métabolique. Donc dans  $W(F)$ ,

$$\underbrace{\langle 1, 1, \dots, 1 \rangle}_{d \text{ termes}} = \langle 1 \rangle$$

et alors  $(Tr_{k/F})_*(\langle 1 \rangle) = \langle 1 \rangle$ , d'où le résultat.

**2)** Posons  $q = [1, a] : V \rightarrow k$ ,  $V$  étant un  $k$ -espace vectoriel de dimension 2. Soit  $(e, f)$  une base symplectique de  $(V, b_q)$ . Alors  $q(e) = 1$ ,  $q(f) = a$ ,  $b_q(e, f) = 1$ ,  $b_q(e, e) = b_q(f, f) = 0$ . Comme  $k/F$  est une extension quadratique de corps de caractéristique 2, alors  $k = F(\alpha)$  pour un certain  $\alpha \in k - F$  tel que  $\alpha^2 + \alpha = u \in F$ . Notons que le polynôme minimal de  $\alpha$  sur  $F$  est donc  $X^2 + X + u$  et a pour racines  $\alpha$  et  $1 + \alpha$ . Donc  $Tr_{k/F}(\alpha) = 1$  et alors pour tous  $x_0, x_1 \in F$ ,  $Tr_{k/F}(x_0) = 0$  et  $Tr_{k/F}(x_0 + x_1\alpha) = x_1$ . Posons

$$V_1 = \text{sev} \langle e, \alpha f \rangle \quad \text{et} \quad V_2 = \text{sev} \langle (1 + \alpha)e, f \rangle.$$

Comme  $(e, \alpha f, (1 + \alpha)e, f)$  est clairement une base de  $V$  sur  $F$ , alors  $V = V_1 \oplus V_2$ .

- D'une part, dans l'espace bilinéaire symétrique  $(V, (Tr_{k/F})_*(b_q))$ ,  $V_1^\perp = V_2$ , en effet,

$$Tr_{k/F}(b_q(e, f)) = Tr_{k/F}(1) = 0,$$

$$Tr_{k/F}(b_q(e, (1 + \alpha)e)) = Tr_{k/F}(0) = 0,$$

$$Tr_{k/F}(b_q(\alpha f, (1 + \alpha)e)) = Tr_{k/F}(\alpha(1 + \alpha)) = Tr_{k/F}(u) = 0$$

et

$$Tr_{k/F}(b_q(\alpha f, f)) = Tr_{k/F}(0) = 0.$$

- D'autre part, comme  $Tr_{k/F}(q(e)) = Tr_{k/F}(1) = 0$ , alors la restriction  $q_1$  de  $(Tr_{k/F})_*(q)$  à  $V_1$  est une forme quadratique régulière isotrope de dimension 2. Donc d'après [28, lemme 1.2.8, page 5],  $(V_1, q_1)$  est un plan hyperbolique.

- De plus, on a :

$$Tr_{k/F}(q((1 + \alpha)e)) = Tr_{k/F}((1 + \alpha)^2) = 1,$$

$$Tr_{k/F}(q(f)) = Tr_{k/F}(a),$$

et

$$Tr_{k/F}(b_q((1 + \alpha)e, f)) = Tr_{k/F}(1 + \alpha) = 1.$$

Donc si  $q_2$  désigne la restriction de  $(Tr_{k/F})_*(q)$  à  $V_2$ , alors  $((1 + \alpha)e, f)$  est une base symplectique de  $(V_2, b_{q_2})$  et l'espace quadratique  $(V_2, q_2)$  est isométrique à  $[1, Tr_{k/F}(a)]$ .

- On en déduit finalement que

$$(V, (Tr_{k/F})_*(q)) \cong (V_1, q_1) \perp (V_2, q_2) \cong (V_1, q_1) \perp [1, Tr_{k/F}(a)]$$

et étant donné que  $(V_1, q_1)$  est un plan hyperbolique, alors dans  $W_q(F)$ ,

$$(Tr_{k/F})_*(q) = [1, Tr_{k/F}(a)]. \blacksquare$$

Nous allons maintenant démontrer que si  $k/F$  est une extension quadratique de corps finis de caractéristique 2, alors la forme  $Tr_{k/F} : k \rightarrow F$  induit de façon naturelle un isomorphisme de groupes noté aussi  $Tr_{k/F}$  de  $\frac{k}{\wp(k)}$  sur  $\frac{F}{\wp(F)}$ . Après avoir vérifié que les groupes  $\frac{k}{\wp(k)}$  et  $\frac{F}{\wp(F)}$  sont d'ordre 2, il sera alors clair que l'isomorphisme entre ces deux groupes envoie l'unique élément non nul du premier sur l'unique élément non nul du second. Cela nous sera d'une grande utilité pour calculer l'invariant d'Arf du transfert par la  $F$ -forme linéaire  $Tr_{k/F}$  d'une forme quadratique régulière  $q$  sur  $k$  à partir de l'invariant d'Arf de  $q$ .

Supposons que  $k/F$  est une extension quadratique de corps finis de caractéristique 2. Rappelons que l'application  $\wp : F \rightarrow F$  est définie par  $\wp(x) = x^2 + x$ , pour  $x \in F$ . Rappelons aussi que  $k = F(\alpha)$  pour un certain  $\alpha \in k - F$  tel que  $\alpha^2 + \alpha = u \in F$ .

L'application  $\wp : F \rightarrow F$  est telle que pour tous  $x, x' \in F$

$$\wp(x) = \wp(x') \Leftrightarrow x' = x \text{ ou } x' = 1 + x;$$

et comme l'application  $F \rightarrow F : x \mapsto 1 + x$  est bijective et pour tout  $x \in F$ ,  $x \neq 1 + x$ , alors  $\wp(F)$  est un sous-groupe de  $F$  d'ordre  $\frac{|F|}{2}$ . Donc  $\frac{F}{\wp(F)}$  est un groupe d'ordre 2. C'est clair que  $u \notin \wp(F)$  sinon il existe  $v \in F$  tel que  $\wp(v) = u = \wp(\alpha)$  et alors  $\alpha = v \in F$  ou  $\alpha = 1 + v \in F$ , ce qui est absurde. Donc  $\{\wp(F), u + \wp(F)\}$  est un sous-groupe de  $\frac{F}{\wp(F)}$  d'ordre 2 et alors

$$\frac{F}{\wp(F)} = \{\wp(F), u + \wp(F)\}.$$

Considérons l'application  $Tr_{k/F} : \frac{k}{\wp(k)} \longrightarrow \frac{F}{\wp(F)}$  définie par

$$Tr_{k/F}(x + \wp(k)) = Tr_{k/F}(x) + \wp(F) \text{ pour } x \in k.$$

Pour montrer que cette application est bien définie, il suffit de vérifier que  $Tr_{k/F}(\wp(k)) \subset \wp(F)$ . Soit  $y \in \wp(k)$ ; il existe alors  $x \in k$  tel que  $y = \wp(x) = x^2 + x$ . Supposons que  $x = x_0 + x_1\alpha$ , avec  $x_0, x_1 \in F$ . Alors

$$x^2 = x_0^2 + x_1^2\alpha^2 = x_0^2 + x_1^2u + x_1^2\alpha$$

et donc

$$Tr_{k/F}(x^2) = x_1^2 = (Tr_{k/F}(x))^2.$$

Par suite,

$$Tr_{k/F}(y) = Tr_{k/F}(x^2 + x) = (Tr_{k/F}(x))^2 + Tr_{k/F}(x) \in \wp(F)$$

et alors  $Tr_{k/F}(\wp(k)) \subset \wp(F)$ . Soient maintenant  $x, x' \in k$  tels que  $x + \wp(k) = x' + \wp(k)$ . Alors  $x - x' \in \wp(k)$  et donc

$$Tr_{k/F}(x - x') \in Tr_{k/F}(\wp(k)) \subset \wp(F).$$

D'où  $Tr_{k/F}(x) + \wp(F) = Tr_{k/F}(x') + \wp(F)$  et l'application précédente est bien définie. Montrons qu'elle est surjective. Soit  $z \in F$ . D'après [29, 1.3, page 12], l'application  $Tr_{k/F} : k \rightarrow F$  est surjective. Donc il existe  $x \in k$  tel que  $z = Tr_{k/F}(x)$  et alors

$$Tr_{k/F}(x + \wp(k)) = Tr_{k/F}(x) + \wp(F) = z + \wp(F).$$

Donc  $Tr_{k/F} : \frac{k}{\wp(k)} \longrightarrow \frac{F}{\wp(F)}$  est surjective. On en déduit que l'application  $Tr_{k/F} : \frac{k}{\wp(k)} \longrightarrow \frac{F}{\wp(F)}$  est un isomorphisme de groupes, les groupes  $\frac{k}{\wp(k)}$  et  $\frac{F}{\wp(F)}$  étant finis de même ordre 2. Nous avons ainsi établi le résultat suivant :

**Proposition 3.4.52.** *Soit  $k/F$  une extension quadratique de corps finis de caractéristique 2, telle que  $k = F(\alpha)$  pour un certain  $\alpha \in k - F$  tel que  $\alpha^2 + \alpha = u \in F$ .  $u$  représente l'unique élément non nul de  $\frac{F}{\wp(F)}$  et l'application*

$$Tr_{k/F} : \frac{k}{\wp(k)} \longrightarrow \frac{F}{\wp(F)}$$

*est un isomorphisme de groupes. ■*

On en déduit alors que :

**Corollaire 3.4.53.** *Avec les hypothèses de la proposition 3.4.52, si  $a \in k$  représente l'unique élément non nul de  $\frac{k}{\wp(k)}$ , alors  $Tr_{k/F}(a)$  représente l'unique élément non nul de  $\frac{F}{\wp(F)}$ .*

*Preuve :* cela découle de la proposition 3.4.52. ■

On a alors le résultat suivant pour des extensions finies de corps finis de caractéristique 2.

**Proposition 3.4.54.** *Soit  $k/F$  une extension finie de corps finis de caractéristique 2 et  $a \in k$  tel que  $a$  représente l'unique élément non nul de  $\frac{k}{\wp(k)}$ . Alors dans  $W_q(F)$ ,*

$$(Tr_{k/F})_*([1, a]) = [1, u],$$

où  $u$  représente l'unique élément non nul de  $\frac{F}{\wp(F)}$ .

*Preuve :*  $k/F$  se décompose en une suite d'extensions de corps de la forme

$$k = k_0 \supset k_1 \supset k_2 \supset \cdots \supset k_{r-1} \supset k_r \supset F$$

telle que pour tout  $i = 1, 2, \dots, r$ ,  $k_{i-1}/k_i$  est une extension quadratique et  $k_r/F$  est une extension de degré impair. Comme d'après [11, proposition 2, page V.48],

$$Tr_{k/F} = Tr_{k_r/F} \circ Tr_{k_{r-1}/k_r} \circ Tr_{k_{r-2}/k_{r-1}} \circ \cdots \circ Tr_{k_1/k_2} \circ Tr_{k/k_1},$$

alors dans  $W_q(F)$ , on a :

$$\begin{aligned} (Tr_{k/F})_*([1, a]) \\ = (Tr_{k_r/F})_*(Tr_{k_{r-1}/k_r})_* \cdots (Tr_{k_1/k_2})_*(Tr_{k/k_1})_*([1, a]). \end{aligned}$$

Le lemme 3.4.51.(2) appliqué  $r$  fois dans  $W_q(F)$  donne :

$$\begin{aligned} (Tr_{k_{r-1}/k_r})_*(Tr_{k_{r-2}/k_{r-1}})_* \cdots (Tr_{k_1/k_2})_*(Tr_{k/k_1})_*([1, a]) \\ = [1, Tr_{k_{r-1}/k_r} \circ Tr_{k_{r-2}/k_{r-1}} \circ \cdots \circ Tr_{k_1/k_2} \circ Tr_{k/k_1}(a)] \\ = [1, Tr_{k/k_r}(a)]. \end{aligned}$$

D'où

$$(Tr_{k/F})_*([1, a]) = (Tr_{k_r/F})_*([1, Tr_{k/k_r}(a)]).$$



Posons  $a_r = \text{Tr}_{k/k_r}(a)$ . Par simple induction et usage du corollaire 3.4.53,  $a_r$  représente l'unique élément non nul de  $\frac{k_r}{\wp(k_r)}$  et donc  $k_{r-1} = k_r(\alpha_r)$ , avec  $\alpha_r \in k_{r-1} - k_r$  et  $\wp(\alpha_r) = \alpha_r^2 + \alpha_r = a_r \in k_r$ . Soit  $L$  l'unique extension quadratique de  $F$ . Alors  $L = F(\alpha)$ , avec  $\alpha \in L - F$  et  $\alpha^2 + \alpha = u \in F$ ;  $u$  représente donc l'unique élément non nul de  $\frac{F}{\wp(F)}$ . C'est clair que  $\alpha \notin k_r$  sinon  $F \subset F(\alpha) \subset k_r$  et alors  $2 = [F(\alpha) : F]$  divise  $[k_r : F]$  qui est impair, ce qui est absurde. Donc le polynôme minimal de  $\alpha$  sur  $k_r$  est  $X^2 + X + u$  et alors  $[k_r(\alpha) : k_r] = 2$ ; par suite  $k_r(\alpha)/k_r$  est une extension quadratique. De l'unicité de l'extension quadratique de  $k_r$ , il résulte que  $k_{r-1} = k_r(\alpha_r) = k_r(\alpha)$ . On a donc les extensions suivantes :

$$\begin{array}{ccc} k_r(\alpha_r) & \text{---} & k_r \\ | & & | \\ F(\alpha) & \text{---} & F \end{array}$$

Comme  $k_{r-1} = k_r(\alpha)$  et  $\wp(\alpha) = \alpha^2 + \alpha = u$ , alors  $u$  représente aussi l'unique élément non nul de  $\frac{k_r}{\wp(k_r)}$ . On en déduit que dans  $W_q(k_r)$ ,  $[1, a_r] = [1, u]$ . Il en résulte que dans  $W_q(F)$ , étant donné que  $[k_r : F]$  est impair et  $u \in F$ , le lemme 3.4.51.(1) donne

$$\begin{aligned} (\text{Tr}_{k/F})_*([1, a]) &= (\text{Tr}_{k_r/F})_*([1, a_r]) \\ &= (\text{Tr}_{k_r/F})_*([1, u]) \\ &= [1, u]. \quad \blacksquare \end{aligned}$$

Le lemme suivant nous permet de comprendre que si  $k$  est un corps fini de caractéristique 2, toute  $\mathbb{F}_2$ -forme linéaire non nulle s'exprime en fonction de la forme trace de l'extension  $k/\mathbb{F}_2$ . Cela nous permettra alors d'utiliser les résultats précédents.

**Lemme 3.4.55.** *Soit  $k$  un corps fini de caractéristique 2. L'application  $\omega : k \rightarrow k^* := \text{Hom}_{\mathbb{F}_2}(k, \mathbb{F}_2)$  définie par*

$$\omega(a)(x) = \text{Tr}_{k/\mathbb{F}_2}(ax), \quad \text{pour } a, x \in k,$$

est un isomorphisme de  $\mathbb{F}_2$ -espaces vectoriels.

*Preuve :* La linéarité de  $\omega$  découle de celle de la forme  $Tr_{k/\mathbb{F}_2}$ . Montrons que  $\omega$  est injective. Soit  $a \in Ker\omega$ . Alors pour tout  $x \in k$ ,  $Tr_{k/\mathbb{F}_2}(ax) = 0$ .  $a$  est donc un élément du radical de la forme bilinéaire  $T : k \times k \rightarrow \mathbb{F}_2$  définie par

$$T(x, y) = Tr_{k/\mathbb{F}_2}(xy), \quad \text{pour } x, y \in k.$$

D'après [11, proposition 1, page V.47],  $T$  est une forme bilinéaire symétrique régulière ; son radical est donc nul et alors  $a = 0$ . Donc  $\omega$  est injective et comme  $dim_{\mathbb{F}_2}k = dim_{\mathbb{F}_2}k^*$ , alors  $\omega$  est un isomorphisme de  $\mathbb{F}_2$ -espaces vectoriels. ■

Nous avons le résultat suivant :

**Proposition 3.4.56.** *Soient  $k$  un corps fini de caractéristique 2,  $(V, q)$  un espace quadratique sur  $k$  et  $s$  une  $\mathbb{F}_2$ -forme linéaire non nulle sur  $k$ . Alors dans  $W_q(\mathbb{F}_2)$ ,*

$$[s_*(q)] = [(Tr_{k/\mathbb{F}_2})_*(q)].$$

*Preuve :* D'après le lemme 3.4.55, il existe  $a \in k^\times$  tel que pour tout  $x \in k$ ,  $s(x) = Tr_{k/\mathbb{F}_2}(ax)$ . Donc pour tout  $x \in V$ , on a :

$$s_*(q)(x) = s(q(x)) = Tr_{k/\mathbb{F}_2}(aq(x)).$$

Donc

$$s_*(q) = (Tr_{k/\mathbb{F}_2})_*(\langle a \rangle q).$$

Comme  $a \neq 0$  et  $a^{-1}$  est un carré dans  $k$ , d'après [39, lemme 3.7, page 8], la forme bilinéaire symétrique régulière  $\langle a \rangle$  est isométrique à  $\langle aa^{-1} \rangle = \langle 1 \rangle$ . Donc dans  $W_q(k)$ ,

$$[\langle a \rangle q] = [\langle 1 \rangle q] = [q].$$

Il en résulte que dans  $W_q(\mathbb{F}_2)$ , on a :

$$[s_*(q)] = [(Tr_{k/\mathbb{F}_2})_*(q)]. \quad \blacksquare$$

Avant d'établir le résultat tant attendu, rappelons une caractérisation des formes quadratiques hyperboliques.

**Proposition 3.4.57.** *Soient  $k$  un corps fini de caractéristique 2,  $A$  un  $k$ -espace vectoriel de dimension paire et  $q : A \rightarrow k$  une forme quadratique régulière. Les assertions suivantes sont équivalentes :*

- (1)  $q$  est hyperbolique ;
- (2)  $\text{Arf}(q) = 0$  ;
- (3)  $A$  contient un sous-espace vectoriel  $V$  tel que  $q(V) = 0$  et

$$\dim_k V = \frac{1}{2} \dim_k A.$$

$V$  est appelé sous-espace totalement isotrope de l'espace quadratique  $(A, q)$ .

*Preuve :*

(1)  $\Leftrightarrow$  (2) : d'après [29, exercice 1, pages 13-14] ;

(1)  $\Leftrightarrow$  (3) : d'après [28, corollaire 1.2.13, page 6]. ■

De la proposition 3.4.57, avec les notations de cette proposition, il résulte que si deux espaces quadratiques sur  $k$  sont dans la même classe dans  $W_q(k)$ , ils ont même invariant d'Arf. C'est pour cette raison que nous opérons essentiellement dans ce groupe de Witt pour établir des résultats qui amènent au calcul de l'invariant d'Arf d'une forme quadratique régulière. Nous pouvons finalement établir le résultat clé suivant :

**Proposition 3.4.58.** *Soit  $k$  un corps fini de caractéristique 2,  $A$  un  $k$ -espace vectoriel de dimension paire,  $q : A \rightarrow k$  une forme quadratique régulière et  $s : k \rightarrow \mathbb{F}_2$  une forme linéaire non nulle.*

- (1) *Si  $q$  est de dimension 2 et anisotrope, alors  $s_*(q)$  n'est pas hyperbolique.*

- (2) Si  $q$  est hyperbolique, alors  $s_*(q)$  est hyperbolique.  
 (3) Si  $q$  n'est pas hyperbolique, alors  $s_*(q)$  n'est pas hyperbolique.

*Preuve :* D'après la proposition 3.4.37,  $s_*(q)$  est régulière.

- 1) Supposons que  $q = [\alpha, \beta]$ , avec  $\alpha, \beta \in k^\times$ . On a donc :

$$q \cong \alpha[1, \alpha\beta] \cong \langle \alpha \rangle [1, \alpha\beta] \cong \langle 1 \rangle [1, \alpha\beta].$$

Donc dans  $W_q(k)$ ,

$$[q] = [\langle 1 \rangle [1, \alpha\beta]] = [1, \alpha\beta].$$

$q$  étant anisotrope,  $\text{Arf}(q) = \alpha\beta + \wp(k)$  est non nul dans  $\frac{k}{\wp(k)}$  (proposition 3.4.57) et alors  $\alpha\beta$  représente l'unique élément non nul de  $\frac{k}{\wp(k)}$ . Par suite, d'après la proposition 3.4.52, dans  $W_q(\mathbb{F}_2)$ ,

$$(Tr_{k/\mathbb{F}_2})_*([1, \alpha\beta]) = [1, 1],$$

car 1 représente l'unique élément non nul de  $\frac{\mathbb{F}_2}{\wp(\mathbb{F}_2)}$ . D'après la proposition 3.4.56, dans  $W_q(\mathbb{F}_2)$ ,

$$[s_*(q)] = [(Tr_{k/\mathbb{F}_2})_*(q)] = [(Tr_{k/\mathbb{F}_2})_*([1, \alpha\beta])] = [1, 1].$$

Donc  $\text{Arf}(s_*(q)) = 1$  et alors  $s_*(q)$  n'est pas hyperbolique (proposition 3.4.57).

- 2) Supposons  $q$  hyperbolique. Il existe alors un sous-espace vectoriel  $V$  de  $A$  tel que  $q(V) = 0$  et  $\dim_k V = \frac{1}{2}\dim_k A$ . D'une part,  $s_*(q)(V) = s(q(V)) = 0$ . D'autre part,

$$\dim_{\mathbb{F}_2} V = (\dim_{\mathbb{F}_2} k)(\dim_k V) = (\dim_{\mathbb{F}_2} k)\left(\frac{1}{2}\dim_k A\right) = \frac{1}{2}\dim_{\mathbb{F}_2} A.$$

Donc  $s_*(q)$  est hyperbolique.

**3)** Supposons  $q$  non hyperbolique. Elle s'écrit donc (à isométrie près) sous la forme  $q = q_{hyp} \perp [\alpha, \beta]$ , où  $q_{hyp}$  est la partie hyperbolique et  $[\alpha, \beta]$  (avec  $\alpha, \beta \in k^\times$ ), la partie anisotrope de  $q$  (proposition 3.4.40). D'après la proposition 3.4.41,

$$s_*(q) = s_*(q_{hyp}) \perp s_*([\alpha, \beta]).$$

$s_*(q_{hyp})$  est hyperbolique (d'après (2)) et  $s_*([\alpha, \beta])$  n'est pas hyperbolique (d'après (1)). Donc  $s_*(q)$  n'est pas hyperbolique. ■

Il est maintenant possible de passer à la généralisation de la proposition 3.4.43.

**Proposition 3.4.59.** *Soient  $A$  un  $\mathbb{F}_{2^n}$ -espace vectoriel de dimension finie  $2m$  (avec  $m, n \in \mathbb{N}_0$ ),  $q : A \rightarrow \mathbb{F}_{2^n}$  une forme quadratique régulière et  $k$  un corps de caractéristique différente de 2. Soit  $G$  le 2-groupe spécial ambivalent d'application quadratique  $q$ , tel que  $Z(G) = \mathbb{F}_{2^n}$  et  $\frac{G}{Z(G)} = A$  (voir proposition 3.4.37).*

- (1) *Si  $q$  est hyperbolique, alors  $G$  est ortho-ambivalent par rapport à  $k$ .*
- (2) *Si  $q$  n'est pas hyperbolique, alors  $G$  n'est pas ortho-ambivalent par rapport à  $k$ .*

*Preuve :* Soit  $s : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$  une forme linéaire non nulle. D'après la proposition 3.4.58,  $q$  est hyperbolique si et seulement si  $s_*(q)$  est hyperbolique. D'après la proposition 3.4.57, il est équivalent de dire que  $0 = \text{Arf}(s_*(q)) = \text{Arf}(q_s)$  (car d'après la proposition 3.4.37, les formes quadratiques  $s_*(q)$  et  $q_s$  sont isométriques). Le résultat découle alors du théorème 3.4.35. ■



# Chapitre 4

## Groupes de Witt

Soient  $G$  un groupe fini,  $k$  un corps dont la caractéristique ne divise pas l'ordre de  $G$  et est différente de deux et  $R$  une  $k$ -algèbre semi-simple. Soit  $\sigma$  une involution sur  $R$ . Soit  $R-lib$  (resp.  $R-proj$ ) la catégorie des  $R$ -modules libres (resp.  $R$ -modules projectifs) à gauche finiment engendrés.  $R-lib$  est une sous-catégorie de  $R-proj$ . Nous définissons sur chacune de ces catégories une dualité qui dépend de l'involution  $\sigma$ . Les catégories  $R-lib$  et  $R-proj$  munies de cette dualité sont des catégories avec dualité notées respectivement  $R_\sigma-lib$  et  $R_\sigma-proj$ . Pour chacune de ces catégories, nous définissons le groupe de Witt usuel, le groupe de Witt dérivé et les groupes de Witt tordus. Nous mettons en évidence une suite dodécagonale reliant les groupes de Witt tordus des catégories avec dualité  $R_\sigma-lib$  et  $R_\sigma-proj$  avec certains groupes de cohomologie de Tate. Nous relevons quelques relations existant entre les groupes de Witt tordus de  $R_\sigma-lib$  et le type de la restriction de  $\sigma$  à chaque composante simple de  $R$  telles que données dans [4]. Ces relations sont enfin utilisées dans le cas particulier où  $R = kG$  et  $\sigma$  est l'involution canonique de  $kG$ ; elles débouchent sur une condition nécessaire et suffisante pour que  $G$  soit ortho-ambivalent par rapport à  $k$ , ceci, en termes de groupes de Witt tordus.

Dans ce chapitre, sauf mention contraire,  $G$  désigne un groupe fini,  $k$ , un corps dont la caractéristique ne divise pas l'ordre de  $G$  et est différente de deux,  $R$ , une  $k$ -algèbre semi-simple et  $\sigma$ , une involution sur  $R$ .

## 4.1 Groupe de Witt usuel

**Définition 4.1.1.** [5, définition 1, page 540] Une catégorie avec dualité est un triple  $(\mathcal{C}, *, \varpi)$ , où  $\mathcal{C}$  est une catégorie,  $*$  :  $\mathcal{C} \rightarrow \mathcal{C}$  est un foncteur contravariant et  $\varpi : Id_{\mathcal{C}} \rightarrow * \circ *$  est un isomorphisme naturel tel que pour tout objet  $M$  de  $\mathcal{C}$ , l'isomorphisme  $\varpi_M : M \rightarrow (M^*)^* = M^{**}$  est tel que  $(\varpi_M)^* \circ \varpi_{M^*} = id_{M^*}$ .

**Remarque 4.1.2.** Sur les catégories  $R$ -lib et  $R$ -proj, on définit une dualité  $(*, \varpi)$  de la manière suivante : soient  $M$  et  $N$  deux objets de l'une ou l'autre de ces deux catégories et  $g$  un morphisme de  $M$  dans  $N$ .

- Le dual de  $M$  noté  $M^*$  est défini par  $M^* = Hom_R(M, R)$  ; c'est un  $R$ -module à gauche lorsqu'il est muni de l'addition naturelle et de la multiplication externe définie par :

$$(\alpha.f)(m) := f(m)\sigma(\alpha) \quad (4.1)$$

pour tous  $\alpha \in R$ ,  $f \in M^*$ ,  $m \in M$ .

- Le dual de  $g$  noté par  $g^*$ , est le morphisme de  $N^*$  dans  $M^*$  défini par :

$$g^*(y)(m) := \sigma(y(g(m))) \quad (4.2)$$

pour tous  $y \in N^*$ ,  $m \in M$ .

- L'isomorphisme naturel  $\varpi$  est tel que l'isomorphisme  $\varpi_M : M \rightarrow M^{**}$  est défini par :

$$(\varpi_M(m))(f) := \sigma(f(m)) \quad (4.3)$$

pour tous  $f \in M^*$ ,  $m \in M$ .



On vérifie aisément que  $(R - \text{lib}, *, \varpi)$  et  $(R - \text{proj}, *, \varpi)$  sont des catégories avec dualité,  $(*, \varpi)$  étant la dualité définie par (4.1), (4.2) et (4.3) (qui dépend en fait de  $\sigma$ ), qui sont exactes, additives et essentiellement petites (c'est-à-dire dont la classe des classes d'isomorphismes d'objets est un ensemble). Ce résultat est donné dans [5, page 554]. Posons désormais

$$R_\sigma - \text{lib} := (R - \text{lib}, *, \varpi) \quad \text{et} \quad R_\sigma - \text{proj} := (R - \text{proj}, *, \varpi). \quad (4.4)$$

**Remarque 4.1.3.** Soient  $p, q, r \in \mathbb{N}_0$ .  $R^p$ ,  $R^q$  et  $R^r$  sont des objets de  $R_\sigma - \text{lib}$ . Si  $g$  est un morphisme de  $R^p$  dans  $R^q$  dont la matrice par rapport aux  $R$ -bases canoniques de  $R^p$  et  $R^q$  est  $A = (a_{ij})_{i,j}$ , en utilisant (4.2), on démontre que la matrice de  $g^*$  par rapport aux bases canoniques respectives de  $(R^q)^* = R^q$  et  $(R^p)^* = R^p$  est  $A^* = \sigma(A^t) = (\sigma(A))^t$ , avec  $\sigma(A) = (\sigma(a_{ij}))_{i,j}$ .  $g$  s'identifie à sa matrice et on pourra simplement noter que

$$g^* = (\sigma(g))^t = \sigma(g^t).$$

On vérifie sans peine que si  $f, g : R^p \rightarrow R^q$  et  $h : R^q \rightarrow R^r$  sont des morphismes de  $R$ -modules libres, alors  $(g^*)^* = g$ ,  $(f + g)^* = f^* + g^*$  et  $(hg)^* = g^*h^*$ . De plus, si  $f$  est un isomorphisme de  $R$ -modules libres,  $(f^{-1})^* = (f^*)^{-1}$ .

**Remarque 4.1.4.** Dans toute la suite, sauf mention contraire,  $\mathcal{C}$  désigne la catégorie avec dualité  $R_\sigma - \text{lib}$  ou  $R_\sigma - \text{proj}$  donnée par (4.4).

**Définition 4.1.5.** [5, définition 2, page 541] Dans  $\mathcal{C}$ , on appelle espace  $\varepsilon$ -symétrique, avec  $\varepsilon = \pm 1$ , une paire  $(M, \varphi)$ , où  $M$  est un objet de  $\mathcal{C}$  et  $\varphi : M \rightarrow M^*$  est un isomorphisme  $\varepsilon$ -symétrique (appelé forme  $\varepsilon$ -symétrique de l'espace  $(M, \varphi)$ ) c'est-à-dire un isomorphisme tel que  $\varphi^* \circ (\varepsilon \varpi_M) = \varphi$ ; cela signifie que lorsqu'on identifie  $M$  et  $M^{**}$  par l'isomorphisme  $\varepsilon \varpi_M$ ,  $\varphi^*$  s'identifie à  $\varphi$ . Le diagramme suivant est commutatif :

$$\begin{array}{ccc}
M & \xrightarrow{\varphi} & M^* \\
\downarrow \varepsilon \varpi_M & & \parallel \\
M^{**} & \xrightarrow{\varphi^*} & M^*.
\end{array}$$

**Définition 4.1.6.** [7, définition 1.2, 1.3, page 354-355] Dans  $\mathcal{C}$ , soient  $(M, \varphi)$  et  $(N, \psi)$  deux espaces  $\varepsilon$ -symétriques. On dit que  $(M, \varphi)$  et  $(N, \psi)$  sont isométriques s'il existe un isomorphisme  $h : M \rightarrow N$  (appelé isométrie entre  $(M, \varphi)$  et  $(N, \psi)$ ) tel que  $h^* \psi h = \varphi$ . On appelle somme orthogonale de  $(M, \varphi)$  et  $(N, \psi)$  et on note  $(M, \varphi) \perp (N, \psi)$ , l'espace  $\varepsilon$ -symétrique  $(M \oplus N, \begin{pmatrix} \varphi & 0 \\ 0 & \psi \end{pmatrix})$ . L'isométrie est une relation d'équivalence dans l'ensemble des espaces  $\varepsilon$ -symétriques et elle préserve la somme orthogonale. L'ensemble des classes d'isométrie des espaces  $\varepsilon$ -symétriques, muni de la somme orthogonale est un monoïde, appelé monoïde de Witt- $(\varepsilon)$  de  $\mathcal{C}$  ; on le note par  $MW^\varepsilon(\mathcal{C})$ .

**Définition 4.1.7.** [7, définition 1.4, page 355] Dans  $\mathcal{C}$ , soit  $(M, \varphi)$  un espace  $\varepsilon$ -symétrique. On appelle lagrangien de  $(M, \varphi)$  un morphisme injectif  $\alpha : L \rightarrow M$  tel que la suite suivante soit exacte :

$$L \xrightarrow{\alpha} M \xrightarrow{\alpha^* \varphi} L^*.$$

On dit que  $(M, \varphi)$  est métabolique s'il possède un lagrangien. On vérifie que tout espace  $\varepsilon$ -symétrique isométrique à un espace métabolique est métabolique, et la somme orthogonale de deux espaces métaboliques est un espace métabolique. L'ensemble des classes d'isométrie des espaces  $\varepsilon$ -symétriques métaboliques de  $\mathcal{C}$  est un sous-monoïde de  $MW^\varepsilon(\mathcal{C})$  ; on le note par  $NW^\varepsilon(\mathcal{C})$ .

**Remarque 4.1.8.** [5, remarque 26, page 546] Soit  $(M, +)$  un monoïde abélien d'élément neutre 0 et  $N$  un sous-monoïde de  $M$  tel que pour tout  $m \in M$ , il existe  $m' \in M$  tel que  $m + m' \in N$ . On considère la relation  $\sim$  définie sur  $M$  par : pour tous  $m, m' \in M$ ,  $m \sim m'$  si et seulement s'il existe  $n, n' \in N$  tels que  $m + n = m' + n'$ .

$\sim$  est une relation d'équivalence sur  $M$  et l'ensemble quotient  $M/\sim$  muni de l'addition définie par  $[m] + [m'] := [m + m']$  (avec  $m, m' \in M$  et  $[m]$  étant la classe de  $m$  par  $\sim$ ), est un groupe commutatif noté  $\frac{M}{N}$ ; dans ce groupe, pour tout  $m \in M$ ,  $-[m] = [m']$ , où  $m'$  est un élément de  $M$  tel que  $m + m' \in N$ .

**Définition 4.1.9.** [7, définition 1.6, page 356] On appelle groupe de Witt- $(\varepsilon)$  de  $\mathcal{C}$  et on note  $W^\varepsilon(\mathcal{C})$  le groupe quotient (commutatif) défini par :

$$W^\varepsilon(\mathcal{C}) := \frac{MW^\varepsilon(\mathcal{C})}{NW^\varepsilon(\mathcal{C})}$$

Dans  $W^\varepsilon(\mathcal{C})$ , la classe d'un espace  $\varepsilon$ -symétrique  $(M, \varphi)$  se note par  $[M, \varphi]$  et on dit que deux espaces  $\varepsilon$ -symétriques sont Witt-équivalents si leurs classes coïncident dans  $W^\varepsilon(\mathcal{C})$ .

**Remarque 4.1.10.** Un espace 1-symétrique (resp. -1-symétrique) est appelé simplement espace symétrique (resp. antisymétrique). De plus on pose :

$$MW^{+1}(\mathcal{C}) := MW(\mathcal{C}) \quad \text{et} \quad MW^{-1}(\mathcal{C}) := MW^-(\mathcal{C});$$

$$NW^{+1}(\mathcal{C}) := NW(\mathcal{C}) \quad \text{et} \quad NW^{-1}(\mathcal{C}) := NW^-(\mathcal{C});$$

et

$$W^{+1}(\mathcal{C}) := W(\mathcal{C}) := W_{us}(\mathcal{C}) \quad \text{et} \quad W^{-1}(\mathcal{C}) := W^-(\mathcal{C}) := W_{us}^-(\mathcal{C}).$$

$W_{us}(\mathcal{C})$  (resp.  $W_{us}^-(\mathcal{C})$ ) est appelé groupe de Witt usuel (resp. groupe de Witt-(-1) usuel) de  $\mathcal{C}$ .

## 4.2 Groupe de Witt dérivé

**Définition 4.2.1.** [7, def.2.6, page 358] Catégorie homotopique de  $\mathcal{C}$ . Soit  $K^b(\mathcal{C})$  la catégorie dont les objets sont des complexes de chaînes limités des objets de  $\mathcal{C}$  et les morphismes sont des morphismes de complexes de chaînes à homotopie près.  $K^b(\mathcal{C})$  est appelée catégorie homotopique de  $\mathcal{C}$ . Rappelons que si  $A_\bullet = (A_n, d_n^A)_{n \in \mathbb{Z}}$

et  $B_\bullet = (B_n, d_n^B)_{n \in \mathbb{Z}}$  sont des complexes de chaînes dans  $K^b(\mathcal{C})$ , deux morphismes de complexes  $\varphi_\bullet : A_\bullet \rightarrow B_\bullet$  et  $\varphi'_\bullet : A_\bullet \rightarrow B_\bullet$  sont dits homotopes s'il existe des morphismes  $s_n : A_{n-1} \rightarrow B_{n+1}$  tels que  $s_n d_n^A + d_{n+1}^B s_{n+1} = \varphi'_n - \varphi_n$ , pour tout  $n \in \mathbb{Z}$ .

$K^b(\mathcal{C})$  possède une famille de suites exactes données par la construction des cônes des morphismes de complexes de chaînes (voir [43, paragraphe 1.5, page 18-19]) de la manière suivante : Soient  $A_\bullet = (A_n, d_n)_{n \in \mathbb{Z}}$  et  $B_\bullet = (B_n, d'_n)_{n \in \mathbb{Z}}$  des complexes de chaînes limités des objets de  $\mathcal{C}$  et  $u_\bullet : A_\bullet \rightarrow B_\bullet$  un morphisme de complexes ; on note par  $C(u_\bullet)$  ou  $Cone(u_\bullet)$  le cône de  $u_\bullet$  défini par

$$C(u_\bullet) := \cdots \rightarrow A_{n-1} \oplus B_n \xrightarrow{\begin{pmatrix} -d_{n-1} & 0 \\ -u_{n-1} & d'_n \end{pmatrix}} A_{n-2} \oplus B_{n-1} \longrightarrow \cdots .$$

On pose  $T(A_\bullet) = A_\bullet[-1]$  c'est-à-dire que pour tout entier  $n$ ,

$$T(A_\bullet)_n = A_\bullet[-1]_n = A_{n-1},$$

les différentielles du complexe  $T(A_\bullet)$  étant les morphismes  $-d_n$ , les  $d_n$  étant les différentielles du complexe  $A_\bullet$ . Plus précisément, pour

$$\begin{array}{c} \text{degré } n \\ \vdots \\ A_\bullet := \cdots \rightarrow A_n \xrightarrow{d_n} A_{n-1} \xrightarrow{d_{n-1}} \cdots , \\ \vdots \\ \text{degré } n \\ \vdots \\ T(A_\bullet) := \cdots \rightarrow A_{n-1} \xrightarrow{-d_{n-1}} A_{n-2} \xrightarrow{-d_{n-2}} \cdots . \end{array}$$

On a la suite des morphismes de complexes ci-dessous :

$$\begin{array}{ccccccc}
& & \text{degré } n & & & & \\
& & \vdots & & & & \\
A_{\bullet} = & \cdots \longrightarrow & A_n & \xrightarrow{d_n} & A_{n-1} & \xrightarrow{d_{n-1}} & \cdots \\
\downarrow u_{\bullet} & & \downarrow u_n & & \downarrow u_{n-1} & & \\
B_{\bullet} = & \cdots \longrightarrow & B_n & \xrightarrow{d'_n} & B_{n-1} & \xrightarrow{d'_{n-1}} & \cdots \\
\downarrow v_{\bullet} & & \downarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix} & & \downarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix} & & \\
C(u_{\bullet}) := & \cdots \longrightarrow & A_{n-1} \oplus B_n & \xrightarrow{\begin{pmatrix} -d_{n-1} & 0 \\ -u_{n-1} & d'_n \end{pmatrix}} & A_{n-2} \oplus B_{n-1} & \longrightarrow & \cdots \\
\downarrow w_{\bullet} & & \downarrow \begin{pmatrix} -1 & 0 \end{pmatrix} & & \downarrow \begin{pmatrix} -1 & 0 \end{pmatrix} & & \\
T(A_{\bullet}) := & \cdots \longrightarrow & A_{n-1} & \xrightarrow{-d_{n-1}} & A_{n-2} & \xrightarrow{-d_{n-2}} & \cdots
\end{array}$$

D'après [43, paragraphe 1.5.2, page 19],

$$0 \longrightarrow B_{\bullet} \xrightarrow{v_{\bullet}} C(u_{\bullet}) \xrightarrow{w_{\bullet}} T(A_{\bullet}) \longrightarrow 0 \quad (4.5)$$

est une suite exacte ; par définition (voir [43, définition 10.1.3, page 371]) le triple  $(u_{\bullet}, v_{\bullet}, w_{\bullet})$  est appelé triangle strict dans  $K^b(\mathcal{C})$  ; on dit alors que la suite

$$A_{\bullet} \xrightarrow{u_{\bullet}} B_{\bullet} \xrightarrow{v_{\bullet}} C(u_{\bullet}) \xrightarrow{w_{\bullet}} T(A_{\bullet})$$

est un triangle strict.

Soient  $A, B, C$  des objets de  $K^b(\mathcal{C})$  et des morphismes  $u : A \rightarrow B$ ,  $v : B \rightarrow C$ ,  $w : C \rightarrow T(A)$ . On dit que  $(u, v, w)$  est un triangle exact sur  $(A, B, C)$  ou que la suite

$$A \xrightarrow{u} B \xrightarrow{v} C \xrightarrow{w} T(A)$$

est un triangle exact si elle est isomorphe à un triangle strict.

**Remarque 4.2.2.** *Le foncteur  $T$  défini ci-dessus sur  $K^b(\mathcal{C})$  est un automorphisme tel que pour tous objets  $A_\bullet$  et  $B_\bullet$  de  $K^b(\mathcal{C})$ , pour tout morphisme  $f_\bullet : A_\bullet \rightarrow B_\bullet$ ,  $T(f_\bullet)_n = f_{n-1}$  (voir [3, paragraphe 3, page 4]).*

*$K^b(\mathcal{C})$  est naturellement muni d'une dualité  $\#$  définie par : pour tout objet  $A_\bullet$  de  $K^b(\mathcal{C})$ , avec  $A_\bullet = (A_n, d_n)_{n \in \mathbb{Z}}$ , les  $d_n$  étant les différentielles,*

$$(A_\bullet)^\# := ((A_{-n})^*, (d_{-n+1})^*)_{n \in \mathbb{Z}}$$

*De plus, pour tous objets  $A_\bullet$  et  $B_\bullet$  de  $K^b(\mathcal{C})$ , pour tout morphisme  $f_\bullet : A_\bullet \rightarrow B_\bullet$ ,*

$$(f_\bullet)^\# = ((f_n)_{n \in \mathbb{Z}})^\# = ((f_{-n})^*)_{n \in \mathbb{Z}}.$$

*D'autre part,  $K^b(\mathcal{C})$  est muni d'un isomorphisme naturel*

$$\pi : Id_{K^b(\mathcal{C})} \rightarrow \# \circ \#$$

*défini par : pour tout objet  $A_\bullet$  de  $K^b(\mathcal{C})$ ,*

$$\pi_{A_\bullet} = ((\pi_{A_n})_{n \in \mathbb{Z}}) := (\varpi_{A_n})_{n \in \mathbb{Z}}$$

*(voir [7, paragraphe 2.6, page 358]).*

**Définition 4.2.3.** [43, exercice 1.1.5, page 3]. *Un objet  $A_\bullet$  de  $K^b(\mathcal{C})$  est dit acyclique si pour tout  $n \in \mathbb{Z}$ ,  $H_n(A_\bullet) = 0$ .*

**Définition 4.2.4.** [7, paragraphe 2.8, page 360] *Un quasi-isomorphisme de  $K^b(\mathcal{C})$  est un morphisme de  $K^b(\mathcal{C})$  dont le cône est acyclique.*

**Proposition 4.2.5.** *Soit  $A_\bullet = (A_i, d_i)$  un complexe limité d'objets de  $\mathcal{C}$ . Si  $A_\bullet$  est acyclique, alors  $A_\bullet$  est une suite exacte.*

*Preuve :* Supposons  $A_\bullet$  acyclique. Alors pour tout  $n \in \mathbb{Z}$ ,

$$\frac{\text{Ker } d_n}{\text{Im } d_{n+1}} = H_n(A_\bullet) = 0$$

et donc  $\text{Ker } d_n = \text{Im } d_{n+1}$  ; donc  $A_\bullet$  est une suite exacte. ■

**Définition 4.2.6.** [43, def.10.3.1, page 379]. Soit  $P$  une collection de morphismes dans une catégorie  $\mathcal{A}$ ; on appelle localisation de  $\mathcal{A}$  par rapport à  $P$  et on note  $P^{-1}\mathcal{A}$ , la catégorie munie d'un foncteur  $q : \mathcal{A} \rightarrow P^{-1}\mathcal{A}$  vérifiant les conditions suivantes :

- (1) Pour tout  $s \in P$ ,  $q(s)$  est un isomorphisme dans la catégorie  $P^{-1}\mathcal{A}$ .
- (2) Pour toute catégorie  $\mathcal{B}$ , tout foncteur  $F : \mathcal{A} \rightarrow \mathcal{B}$  tel que  $F(s)$  est un isomorphisme pour tout  $s \in P$ , se factorise de façon unique à travers  $q$ , c'est-à-dire qu'il existe un et un seul foncteur  $G : P^{-1}\mathcal{A} \rightarrow \mathcal{B}$  tel que  $F = G \circ q$ . Donc  $P^{-1}\mathcal{A}$  est unique à équivalence près.

**Définition 4.2.7.** [43, définition 10.3.4, page 380]. Soit  $P$  une collection de morphismes dans une catégorie  $\mathcal{A}$ ; on dit que  $P$  est un système multiplicatif dans  $\mathcal{A}$  si les trois conditions suivantes sont vérifiées :

- (1) Pour tous  $s, t \in P$ , si  $s$  et  $t$  sont composables alors  $st \in P$ ; pour tout objet  $X$  de  $\mathcal{A}$ ,  $\text{id}_X \in P$ .
- (2) (Condition d'Ore) Si  $t : Z \rightarrow Y$  est dans  $P$ , alors pour tout morphisme  $g : X \rightarrow Y$  de  $\mathcal{A}$ , il existe un morphisme  $s : W \rightarrow X$  dans  $P$  et un morphisme  $f : W \rightarrow Z$  dans  $\mathcal{A}$  tel que  $gs = tf$ .
- (3) (simplification) Si  $f, g : X \rightarrow Y$  sont des morphismes dans  $\mathcal{A}$ , alors les 2 conditions suivantes sont équivalentes :
  - (a)  $sf = sg$ , pour un certain morphisme  $s : Y \rightarrow W$  dans  $P$ ;
  - (b)  $ft = gt$ , pour un certain morphisme  $t : V \rightarrow X$  dans  $P$ .

**Remarque 4.2.8.** Soit  $Q$  la collection des quasi-isomorphismes de  $K^b(\mathcal{C})$ . D'après [43, proposition 10.4.1, page 385],  $Q$  est un système multiplicatif et si  $Q^{-1}K^b(\mathcal{C})$  est la localisation de  $K^b(\mathcal{C})$  par  $Q$ , de foncteur  $q_0 : K^b(\mathcal{C}) \rightarrow Q^{-1}K^b(\mathcal{C})$ , ce foncteur est additif, commute avec le foncteur  $T$  défini ci-dessus (après la définition 4.2.1) et transforme un triangle exact en un triangle exact [43, définition 10.2.6, page 377].

**Définition 4.2.9.** [43, paragraphe 10.3, page 379]. *La catégorie  $Q^{-1}K^b(\mathcal{C})$  donnée dans la remarque 4.2.8, est appelée catégorie dérivée de  $\mathcal{C}$  et se note simplement par  $D^b(\mathcal{C})$ .*

La dualité sur  $D^b(\mathcal{C})$  se définit de la même façon que la dualité sur  $K^b(\mathcal{C})$  par l'intermédiaire du foncteur  $q_0 : K^b(\mathcal{C}) \rightarrow Q^{-1}K^b(\mathcal{C}) = D^b(\mathcal{C})$ ; nous pouvons la noter de la même façon que sur  $K^b(\mathcal{C})$  par  $\#$ . Il en est de même de l'isomorphisme naturel que nous noterons par  $\pi$  sur  $D^b(\mathcal{C})$  et sur  $K^b(\mathcal{C})$  et de la translation que nous noterons par  $T$  sur  $D^b(\mathcal{C})$  et sur  $K^b(\mathcal{C})$ .

**Proposition 4.2.10.** [7, paragraphe 2.8, page 360]  $(D^b(\mathcal{C}), \#, \pi)$  est une catégorie avec dualité. De plus,  $T \circ \# \cong \# \circ T^{-1}$  et pour tout objet  $M$  de  $D^b(\mathcal{C})$ ,  $\pi_{T(M)} = T(\pi_M)$  et  $(\pi_M)^\# \circ \pi_{M^\#} = \text{id}_{M^\#}$ .

**Remarque 4.2.11.** [7, définition 2.3, page 357] *Dans la catégorie avec dualité  $(D^b(\mathcal{C}), \#, \pi)$ , les espaces symétriques, les sommes orthogonales, les espaces isométriques se définissent de la même façon que dans la catégorie exacte avec dualité  $\mathcal{C}$  (voir définitions 4.1.5 et 4.1.6); il en est donc de même du monoïde de Witt  $MW(D^b(\mathcal{C}))$  de  $(D^b(\mathcal{C}), \#, \pi)$ . Il ne reste qu'à préciser ce que signifie un espace symétrique métabolique dans  $(D^b(\mathcal{C}), \#, \pi)$  pour définir le groupe de Witt de cette catégorie.*

**Définition 4.2.12.** [7, paragraphe 2.3, page 357]. *Dans la catégorie  $(D^b(\mathcal{C}), \#, \pi)$ , un espace symétrique  $(M, \varphi)$  est dit métabolique s'il possède un lagrangien, c'est-à-dire un triple  $(L, \alpha, z)$ ,  $L$  étant un objet de  $D^b(\mathcal{C})$ ,  $\alpha : L \rightarrow M$  et  $z : T^{-1}(L^\#) \rightarrow L$  des morphismes vérifiant les deux conditions suivantes :*

(1) *le triangle suivant est exact*

$$T^{-1}(L^\#) \xrightarrow{z} L \xrightarrow{\alpha} M \xrightarrow{\alpha^\# \varphi} L^\#;$$

(2)  *$z$  est symétrique pour  $T^{-1} \circ \#$  c'est-à-dire  $T^{-1}(z^\#) = \pi_L \circ z$ .  $NW(D^b(\mathcal{C}))$  étant le sous-monoïde de  $MW(D^b(\mathcal{C}))$  constitué des classes d'espaces symétriques métaboliques, le groupe de Witt de*



$(D^b(\mathcal{C}), \#, \pi)$  est défini par :

$$W(D^b(\mathcal{C}), \#, \pi) := W(D^b(\mathcal{C})) = \frac{MW(D^b(\mathcal{C}))}{NW(D^b(\mathcal{C}))}.$$

**Définition 4.2.13.** [7, paragraphe 2.8, page 360]. On appelle groupe de Witt dérivé de la catégorie avec dualité  $\mathcal{C}$  et on note  $W_{der}(\mathcal{C})$ , le groupe de Witt de la catégorie  $(D^b(\mathcal{C}), \#, \pi)$ .

$$W_{der}(\mathcal{C}) := W(D^b(\mathcal{C}), \#, \pi).$$

**Proposition 4.2.14.** [7, proposition 2.9, page 361] Le groupe  $W_{der}(\mathcal{C})$  est isomorphe au groupe  $W_{us}(\mathcal{C})$ .

**Remarque 4.2.15.** La catégorie  $\mathcal{C}$  se plonge dans  $(D^b(\mathcal{C}), \#, \pi)$  de la manière suivante : on associe à tout objet  $M$  de  $\mathcal{C}$  le complexe

$$\cdots \rightarrow 0 \rightarrow 0 \rightarrow M \rightarrow 0 \rightarrow 0 \rightarrow \cdots$$

( $M$  étant repris en degré 0); à  $M^*$ , on associe le complexe

$$M^\# := \cdots \rightarrow 0 \rightarrow 0 \rightarrow M^* \rightarrow 0 \rightarrow 0 \rightarrow \cdots.$$

### 4.3 Groupes de Witt tordus et dodécagone

En sauvegardant les notations de la section précédente, sur la catégorie avec dualité  $(D^b(\mathcal{C}), \#, \pi)$ , il y a lieu de considérer d'autres dualités (appelées dualités tordues) qui donnent lieu à d'autres groupes de Witt (appelés groupes de Witt tordus).

**Définition 4.3.1.** [7, paragraphe 5.1, page 377] Pour tout  $n \in \mathbb{Z}$ , on pose

$$T^n(D^b(\mathcal{C}), \#, \pi) := (D^b(\mathcal{C}), T^n \circ \#, (-1)^{\frac{n(n+1)}{2}} \cdot \pi)$$

et on définit le  $n$ -ième groupe de Witt de  $(D^b(\mathcal{C}), \#, \pi)$ , noté  $W^n(D^b(\mathcal{C}), \#, \pi)$  par

$$W^n(D^b(\mathcal{C}), \#, \pi) := W(T^n(D^b(\mathcal{C}), \#, \pi)).$$

Il est appelé  $n$ -ième groupe de Witt tordu de  $\mathcal{C}$  et se note simplement par  $W^n(\mathcal{C})$ .

**Remarque 4.3.2** (Groupes de Witt réduits à quatre). *Pour tout  $n \in \mathbb{Z}$ ,  $W^n(\mathcal{C})$  est isomorphe à  $W^{n+4}(\mathcal{C})$ . De plus, on a :*

- (1)  $W^0(\mathcal{C}) = W(D^b(\mathcal{C}), \#, \pi) = W_{der}(\mathcal{C}) \cong W_{us}(\mathcal{C})$  (Voir [7, paragraphe 5.1.(5), page 378] et [41, théorème 6.1, page 20]).
- (2)  $W^1(\mathcal{C}) = W(D^b(\mathcal{C}), T \circ \#, -\pi)$ .
- (3)  $W^2(\mathcal{C}) = W(D^b(\mathcal{C}), T^2 \circ \#, -\pi)$  est un groupe isomorphe au groupe  $W_{us}^-(\mathcal{C})$  (voir [7, paragraphe 5.1.(5), page 378] et [41, théorème 6.1, page 20]).
- (4)  $W^3(\mathcal{C}) = W(D^b(\mathcal{C}), T^3 \circ \#, \pi)$ .

Les groupes  $W^1(\mathcal{C})$  et  $W^3(\mathcal{C})$  peuvent être calculés en utilisant les complexes courts, comme Walter [41, paragraphe 7, pages 22-24] le démontre. Avant de voir comment cela peut se réaliser, précisons ce que signifie un complexe supporté sur un intervalle d'entiers.

**Définition 4.3.3.** [7, définition 3.4, page 363] Soit  $A = (A_i, d_i)_{i \in \mathbb{Z}}$  un complexe de chaîne limité d'objets de  $\mathcal{C}$  ; on dit que  $A$  est supporté en  $[m, n]$ , avec  $m, n \in \mathbb{Z}$ , si pour tout  $i \in \mathbb{Z} - [m, n]$ ,  $A_i = 0$ .

$$A = \cdots \rightarrow 0 \rightarrow A_m \xrightarrow{d_m} A_{m-1} \xrightarrow{d_{m-1}} \cdots \xrightarrow{d_{n+2}} A_{n+1} \xrightarrow{d_{n+1}} A_n \rightarrow 0 \rightarrow \cdots$$

Soit  $Sh(\mathcal{C})$  la sous-catégorie de  $K^b(\mathcal{C})$ , dont les objets sont des complexes de chaînes limités supportés sur des intervalles d'entiers à deux points et les morphismes sont des morphismes de complexes de chaînes à homotopie près.  $Sh(\mathcal{C})$  est appelée catégorie des complexes courts de  $\mathcal{C}$ .  $(Sh(\mathcal{C}), T \circ \#, -\pi)$  est une catégorie exacte avec dualité,  $T$ ,  $\#$  et  $\pi$  étant respectivement la translation, la dualité et l'isomorphisme naturel définis sur  $K^b(\mathcal{C})$  dans la section 4.2. Soit  $\varepsilon = \pm 1$

**Définition 4.3.4.** Dans la catégorie  $(Sh(\mathcal{C}), T \circ \#, -\pi)$ , un espace  $\varepsilon$ -symétrique est une paire  $(M, \varphi)$  telle que  $M$  est un objet de  $Sh(\mathcal{C})$  et  $\varphi : M \rightarrow T(M^\#)$  est un quasi-isomorphisme tel que  $T(\varphi^\#) \circ (-\varepsilon\pi_M) = \varphi$ . Plus précisément, si

$$M = \cdots \rightarrow 0 \rightarrow 0 \rightarrow M_1 \xrightarrow{d} M_0 \rightarrow 0 \rightarrow 0 \rightarrow \cdots,$$

en tenant compte du fait que

$$T((T(M^\#))^\#) = T \circ \# \circ T \circ \#(M) = \# \circ T^{-1} \circ T \circ \#(M) = M^{\#\#},$$

le diagramme suivant est commutatif :

$$\begin{array}{ccccccc}
 M = & \cdots 0 & \longrightarrow & M_1 & \xrightarrow{d} & M_0 & \longrightarrow 0 \cdots \\
 \swarrow \varphi & & & \swarrow f & & \swarrow g & \\
 T(M^\#) = & \cdots 0 & \longrightarrow & M_0^* & \xrightarrow{-d^*} & M_1^* & \longrightarrow 0 \cdots \\
 \swarrow T(\varphi^\#) & & & \swarrow g^* & & \swarrow f^* & \\
 M^{\#\#} = & \cdots 0 & \longrightarrow & M_1^{**} & \xrightarrow{d^{**}} & M_0^{**} & \longrightarrow 0 \cdots \\
 & & & \downarrow -\varepsilon\pi_{M_1} & & \downarrow -\varepsilon\pi_{M_0} & \\
 & & & M_1^* & & M_0^* & 
 \end{array}$$

Et par identification de tout objet  $N$  de  $\mathcal{C}$  à son bidual  $N^{**}$  par l'isomorphisme naturel  $\varpi_N$ ,  $g = -\varepsilon f^*$ .

**Remarque 4.3.5.** Dans la catégorie  $(Sh(\mathcal{C}), T \circ \#, -\pi)$ , soit  $(M, \varphi)$  un espace  $\varepsilon$ -symétrique donné par

$$\begin{array}{ccccccc}
 M = & \cdots \rightarrow & 0 & \rightarrow & M_1 & \xrightarrow{d} & M_0 \rightarrow 0 \rightarrow \cdots \\
 \downarrow \varphi = & & \downarrow & & \downarrow f & & \downarrow -\varepsilon f^* \\
 T(M^\#) = & \cdots \rightarrow & 0 & \rightarrow & M_0^* & \xrightarrow{-d^*} & M_1^* \rightarrow 0 \rightarrow \cdots
 \end{array}$$

$\varphi$  étant un quasi-isomorphisme, son cône est acyclique et donc d'après la proposition 4.2.5, la suite suivante est exacte :

$$\cdots \longrightarrow 0 \longrightarrow M_1 \xrightarrow{\begin{pmatrix} d \\ f \end{pmatrix}} M_0 \oplus M_0^* \xrightarrow{\begin{pmatrix} -\varepsilon f^* & d^* \end{pmatrix}} M_1 \longrightarrow 0 \longrightarrow \cdots$$

**Définition 4.3.6.** Dans la catégorie  $\mathcal{C}$ , pour tout objet  $X$  de  $\mathcal{C}$ , un morphisme  $u : X \rightarrow X^*$  est dit  $\varepsilon$ -symétrique si  $u = u^* \circ (\varepsilon \varpi_X)$ . Dans la catégorie  $(Sh(\mathcal{C}), T \circ \#, -\pi)$ , on appelle complexe graphe d'un morphisme  $\varepsilon$ -symétrique  $u : X \rightarrow X^*$  de  $\mathcal{C}$  et on note  $\Gamma_{X,u}$ , l'espace  $\varepsilon$ -symétrique de  $Sh(\mathcal{C})$  défini par

$$\begin{array}{ccccccccc}
 \cdots 0 & \longrightarrow & 0 & \longrightarrow & X & \xrightarrow{u} & X^* & \longrightarrow & 0 & \longrightarrow & 0 \cdots \\
 \downarrow & & \downarrow & & \downarrow -\varepsilon \varpi_X & & \downarrow id_{X^*} & & \downarrow & & \downarrow \\
 \cdots 0 & \longrightarrow & 0 & \longrightarrow & X^{**} & \xrightarrow{-u^*} & X^* & \longrightarrow & 0 & \longrightarrow & 0 \cdots
 \end{array}$$

Le complexe graphe trivial  $\Gamma_{X,0}$  se note simplement par  $\mathbb{H}(X)$  et est appelé complexe graphe trivial associé au complexe graphe  $\Gamma_{X,u}$ . Dans  $(Sh(\mathcal{C}), T \circ \#, -\pi)$ , on définit les espaces  $\varepsilon$ -symétriques isométriques et la somme orthogonale des classes d'isométrie de la même façon que dans  $\mathcal{C}$ . Le groupe de Grothendieck de Witt des complexes courts  $\varepsilon$ -symétriques dans  $\mathcal{C}$ , noté  $GW_{sh}^\varepsilon(\mathcal{C})$  est le quotient du groupe abélien libre des classes d'isométrie des espaces  $\varepsilon$ -symétriques de la catégorie  $(Sh(\mathcal{C}), T \circ \#, -\pi)$ , modulo quatre types de relations :

- (1) Pour tous espaces  $\varepsilon$ -symétriques  $(M, \varphi)$  et  $(N, \psi)$ ,

$$[(M, \varphi) \perp (N, \psi)] = [(M, \varphi)] + [(N, \psi)].$$

- (2) Deux espaces  $\varepsilon$ -symétriques homotopiques se trouvent dans la même classe.

- (3) Pour tout espace  $\varepsilon$ -symétriques  $(M, \varphi)$ , pour tout objet  $N$  de  $(Sh(\mathcal{C}), T \circ \#, -\pi)$ , si  $s : N \rightarrow M$  est un quasi isomorphisme, alors  $(N, T(s^\#) \circ \varphi \circ s)$  est un espace  $\varepsilon$ -symétrique et

$$[(M, \varphi)] = [(N, T(s^\#) \circ \varphi \circ s)].$$

- (4) Chaque complexe graphe se trouve dans la même classe que le complexe graphe trivial associé

$$[\Gamma_{X,u}] = [\mathbb{H}(X)].$$

Le groupe de Witt des complexes courts  $\varepsilon$ -symétriques dans  $\mathcal{C}$ , noté  $W_{sh}^\varepsilon(\mathcal{C})$  est le quotient du groupe  $GW_{sh}^\varepsilon(\mathcal{C})$  par les classes d'isométrie des complexes graphes de morphismes  $\varepsilon$ -symétriques.

Le théorème suivant nous permet de calculer  $W^1(\mathcal{C})$  et  $W^3(\mathcal{C})$  en passant par la catégorie  $(Sh(\mathcal{C}), T \circ \#, -\pi)$  :

**Théorème 4.3.7.** *Les groupes  $W^1(\mathcal{C})$  et  $W^3(\mathcal{C})$  sont respectivement isomorphes à  $W_{sh}^{+1}(\mathcal{C}) := W_{sh}^+(\mathcal{C})$  et  $W_{sh}^{-1}(\mathcal{C}) := W_{sh}^-(\mathcal{C})$ .*

**Preuve :** Voir Walter [41, th.7.1, page 24].

**Corollaire 4.3.8.** *Les groupes  $W_{sh}^\varepsilon(\mathcal{C})$  et  $W^{\varepsilon+4}(\mathcal{C})$  sont isomorphes.*

**Preuve :** Cela découle du théorème 4.3.7 et du fait que  $W^1(\mathcal{C})$  et  $W^5(\mathcal{C})$  sont isomorphes (remarque 4.3.2).

Le résultat suivant est un cas particulier où la  $k$ -algèbre  $R$  est de dimension finie.

**Proposition 4.3.9.** *On suppose que  $R$  est de dimension finie sur  $k$ . Tout élément du groupe  $W_{sh}^\varepsilon(R_\sigma - lib)$  est classe d'isométrie d'un espace  $\varepsilon$ -symétrique  $(M, \varphi)$  de la forme*

$$\begin{array}{ccccccc} M = & \cdots \rightarrow & 0 & \rightarrow & R^n & \xrightarrow{d} & R^n \rightarrow 0 \rightarrow \cdots \\ \downarrow \varphi = & & \downarrow & & \downarrow f & & \downarrow -\varepsilon f^* \\ T(M^\#) = & \cdots \rightarrow & 0 & \rightarrow & R^n & \xrightarrow{-d^*} & R^n \rightarrow 0 \rightarrow \cdots, \end{array}$$

$\varphi$  étant un quasi-isomorphisme.

**Preuve :** Par définition, tout élément du groupe  $W_{sh}^\varepsilon(R_\sigma - lib)$  est classe d'isométrie d'un espace  $\varepsilon$ -symétrique  $(M, \varphi)$  de la forme

$$\begin{array}{ccccccc} M = & \cdots \rightarrow & 0 & \rightarrow & R^n & \xrightarrow{d} & R^m \rightarrow 0 \rightarrow \cdots \\ \downarrow \varphi = & & \downarrow & & \downarrow f & & \downarrow -\varepsilon f^* \\ T(M^\#) = & \cdots \rightarrow & 0 & \rightarrow & R^m & \xrightarrow{-d^*} & R^n \rightarrow 0 \rightarrow \cdots \end{array}$$

$\varphi$  étant un quasi-isomorphisme. D'après la remarque 4.3.5, la suite suivante est exacte :

$$\cdots \longrightarrow 0 \longrightarrow R^n \xrightarrow{\begin{pmatrix} d \\ f \end{pmatrix}} R^m \oplus R^m \xrightarrow{\begin{pmatrix} -\varepsilon f^* & d^* \end{pmatrix}} R^n \longrightarrow 0 \longrightarrow \cdots$$

Il en résulte que les  $R$ -modules libres  $R^{2n} = R^n \oplus R^n$  et  $R^{2m} = R^m \oplus R^m$  sont isomorphes ; en particulier, ce sont des  $k$ -espaces vectoriels isomorphes et alors  $\dim_k R^{2n} = \dim_k R^{2m}$  c'est-à-dire que  $2n \dim_k R = 2m \dim_k R$  ; d'où  $n = m$  et le résultat s'ensuit. ■

**Remarque 4.3.10.** Avec les hypothèses et notations de la proposition 4.3.9, dans le groupe  $W_{sh}^\varepsilon(R_\sigma - lib)$ , la classe d'isométrie de l'espace  $\varepsilon$ -symétrique  $(M, \varphi)$  donné par

$$\begin{array}{ccccccc} M = & \cdots \rightarrow & 0 & \rightarrow & R^n & \xrightarrow{d} & R^n & \rightarrow & 0 & \rightarrow \cdots \\ \downarrow \varphi = & & \downarrow & & \downarrow f & & \downarrow -\varepsilon f^* & & \downarrow & \\ T(M^\#) = & \cdots \rightarrow & 0 & \rightarrow & R^n & \xrightarrow{-d^*} & R^n & \rightarrow & 0 & \rightarrow \cdots, \end{array}$$

$\varphi$  étant un quasi-isomorphisme, peut se noter simplement par

$$[(M, \varphi)] := [n, d, f]^\varepsilon.$$

**Remarque 4.3.11.** Avec les hypothèses et notations de la proposition 4.3.9, du théorème 4.3.7 et de la proposition 4.3.9, il suit que :

- (1) Tout élément de  $W^1(R_\sigma - lib) \cong W_{sh}^+(R_\sigma - lib)$  est classe d'isométrie d'un espace +1-symétrique  $(M, \varphi)$  donné par

$$\begin{array}{ccccccc} M = & \cdots \rightarrow & 0 & \rightarrow & R^n & \xrightarrow{d} & R^n & \rightarrow & 0 & \rightarrow \cdots \\ \downarrow \varphi = & & \downarrow & & \downarrow f & & \downarrow -f^* & & \downarrow & \\ T(M^\#) = & \cdots \rightarrow & 0 & \rightarrow & R^n & \xrightarrow{-d^*} & R^n & \rightarrow & 0 & \rightarrow \cdots \end{array},$$

$\varphi$  étant un quasi-isomorphisme, et est noté par  $[(M, \varphi)] := [n, d, f]^{+1}$  ou simplement par  $[(M, \varphi)] := [n, d, f]^+$ .

- (2) Tout élément de  $W^3(R_\sigma - lib) \cong W_{sh}^-(R_\sigma - lib)$  est classe d'isométrie d'un espace -1-symétrique  $(M, \varphi)$  donné par

$$\begin{array}{ccccccc} M = & \cdots \rightarrow & 0 & \rightarrow & R^n & \xrightarrow{d} & R^n & \rightarrow & 0 & \rightarrow \cdots \\ \downarrow \varphi = & & \downarrow & & \downarrow f & & \downarrow f^* & & \downarrow & \\ T(M^\#) = & \cdots \rightarrow & 0 & \rightarrow & R^n & \xrightarrow{-d^*} & R^n & \rightarrow & 0 & \rightarrow \cdots, \end{array}$$

$\varphi$  étant un quasi-isomorphisme, et est noté par  $[(M, \varphi)] := [n, d, f]^{-1}$  ou simplement par  $[(M, \varphi)] := [n, d, f]^-$ .

Il est temps de donner une suite exacte dodécagonale qui relie les groupes de Witt tordus de  $\mathcal{C}$  à certains groupes de cohomologie de Tate. Pour y arriver, nous avons besoin de préciser les ingrédients qui interviennent dans cette suite.

**Définition 4.3.12.** Soient  $A$  un groupe commutatif et  $\tau$  un automorphisme de  $A$  tel que  $\tau^2 = id_A$ .  $\tau$  induit une action du groupe  $\frac{\mathbb{Z}}{2\mathbb{Z}}$  sur  $A$  définie par

$$0.a = a \quad \text{et} \quad 1.a = \tau(a), \quad \text{pour tout } a \in A.$$

$id - \tau$  et  $id + \tau$  sont des endomorphismes de  $A$  tels que

$$(id - \tau)(id + \tau) = (id + \tau)(id - \tau) = 0.$$

On pose

$$\widehat{H}^0\left(\frac{\mathbb{Z}}{2\mathbb{Z}}, A\right) := \frac{Ker(id - \tau)}{Im(id + \tau)}$$

et

$$\widehat{H}^1\left(\frac{\mathbb{Z}}{2\mathbb{Z}}, A\right) := \frac{Ker(id + \tau)}{Im(id - \tau)}$$

Pour  $i = 0, 1$ ,  $\widehat{H}^i(\frac{\mathbb{Z}}{2\mathbb{Z}}, A)$  est appelé le  $i$ -ième groupe de cohomologie de Tate de  $\frac{\mathbb{Z}}{2\mathbb{Z}}$  à coefficients dans  $A$ . On peut le lire aisément sur le complexe de groupes suivant

$$\begin{array}{ccccccc} \dots & \xrightarrow{id-\tau} & A & \xrightarrow{id+\tau} & A & \xrightarrow{id-\tau} & A & \xrightarrow{id+\tau} & \dots \\ & & & & \vdots & & \vdots & & \\ & & & & \text{degré } 0 & & \text{degré } 1 & & \end{array}.$$

**Définition 4.3.13.** [1, page 2] Soit  $\overline{R - proj}$  la collection des classes d'isomorphisme des  $R$ -modules projectifs à gauche finiment engendrés.

$(\overline{R - proj}, \oplus)$  est un semi-groupe. Soit  $Gr(\overline{R - proj}, \oplus)$  le groupe

de Grothendieck de  $(\overline{R - proj}, \oplus)$  : on l'appelle le 0-ième groupe de  $K$ -théorie de  $R$  et on le note  $K_0R$  :

$$K_0R := Gr(\overline{R - proj}, \oplus).$$

L'application  $i : \mathbb{Z} \rightarrow K_0R : n \mapsto n[R]$  est un morphisme de groupes. On appelle 0-ième groupe réduit de  $K$ -théorie de  $R$  et on note  $\tilde{K}_0R$  le groupe quotient

$$\tilde{K}_0R := \frac{K_0R}{i(\mathbb{Z})}.$$

**Remarque 4.3.14.** Avec les notations de la définition 4.3.13, l'application  $\tau : \tilde{K}_0R \rightarrow \tilde{K}_0R$  telle que pour tout objet  $M$  de  $R_\sigma - proj$ ,

$$\tau([M] + i(\mathbb{Z})) = [M^*] + i(\mathbb{Z}),$$

est bien définie car pour tout entier naturel  $n$ , les modules  $R^n$  et  $(R^n)^*$  sont isomorphes. C'est un automorphisme de  $\tilde{K}_0R$  tel que  $\tau^2 = id_{\tilde{K}_0R}$ . Par l'action de  $\frac{\mathbb{Z}}{2\mathbb{Z}}$  sur  $\tilde{K}_0R$  induite par  $\tau$ , on définit le  $i$ -ième groupe de cohomologie de Tate de  $\frac{\mathbb{Z}}{2\mathbb{Z}}$  à coefficients dans  $\tilde{K}_0R$  pour  $i = 0, 1$  comme dans la définition 4.3.12.

**Théorème 4.3.15.** [4, théorème 4.2, page 15]

$$W^1(R_\sigma - proj) = W^3(R_\sigma - proj) = 0.$$

*Preuve :* Voir Ranicki [36, page 242],  $R$  étant semi-simple. ■

**Théorème 4.3.16.** [4, paragraphe 3, page 13] La suite dodéca-gonale suivante est exacte

$$\begin{array}{ccccc}
 W^0(R_\sigma - lib) & \rightarrow & W^0(R_\sigma - proj) & \rightarrow & \hat{H}^0(\frac{\mathbb{Z}}{2\mathbb{Z}}; \tilde{K}_0R) \\
 \uparrow & & & & \downarrow \\
 \hat{H}^1(\frac{\mathbb{Z}}{2\mathbb{Z}}; \tilde{K}_0R) & & & & W^1(R_\sigma - lib) \\
 \uparrow & & & & \downarrow \\
 W^3(R_\sigma - proj) & & & & W^1(R_\sigma - proj) \\
 \uparrow & & & & \downarrow \\
 W^3(R_\sigma - lib) & & & & \hat{H}^1(\frac{\mathbb{Z}}{2\mathbb{Z}}; \tilde{K}_0R) \\
 \uparrow & & & & \downarrow \\
 \hat{H}^0(\frac{\mathbb{Z}}{2\mathbb{Z}}; \tilde{K}_0R) & \leftarrow & W^2(R_\sigma - proj) & \leftarrow & W^2(R_\sigma - lib).
 \end{array} \tag{4.6}$$



Il est important de rappeler comment sont définis les différents morphismes de groupes qui interviennent dans la suite exacte dodéca-gonale ( 4.6) (voir [24, Appendice A]). Si  $\mathcal{C}$  désigne l'une ou l'autre des catégories avec dualité  $R_\sigma - proj$  ou  $R_\sigma - lib$ , on rappelle que pour  $r = 0, 1, 2, 3$ ,

$$W^r(\mathcal{C}) = W(D^b(\mathcal{C}), T^r \circ \#, (-1)^{\frac{r(r+1)}{2}} \pi) \text{ (voir définition 4.3.1) .}$$

Il est donc question de préciser les morphismes  $j_r$ ,  $\alpha_r$  et  $\beta_r$  dans la suite exacte suivante :

$$W^r(R_\sigma - lib) \xrightarrow{j_r} W^r(R_\sigma - proj) \xrightarrow{\alpha_r} \frac{Ker(id - (-1)^r \tau)}{Im(id + (-1)^r \tau)} \xrightarrow{\beta_r} W^{r+1}(R_\sigma - lib) \quad (4.7)$$

( $\tau$  étant l'automorphisme de  $\tilde{K}_0 R$  défini dans la remarque 4.3.14), en tenant compte du fait que

$$\frac{Ker(id - (-1)^r \tau)}{Im(id + (-1)^r \tau)} = \begin{cases} \widehat{H}^0(\frac{\mathbb{Z}}{2\mathbb{Z}}, \tilde{K}_0 R) & \text{si } r \text{ est pair} \\ \widehat{H}^1(\frac{\mathbb{Z}}{2\mathbb{Z}}, \tilde{K}_0 R) & \text{si } r \text{ est impair.} \end{cases}$$

Le morphisme  $j_r$  est induit par l'inclusion  $R_\sigma - lib \subset R_\sigma - proj$ .

Le morphisme  $\alpha_r$  est défini de la manière suivante. Si  $r$  est impair,  $\alpha_r = 0$  (en vertu du théorème 4.3.15). Si  $r$  est pair, d'après la remarque 4.3.2,

$$W^r(R_\sigma - proj) \cong W(R - proj, *, (-1)^{\frac{r}{2}} \varpi).$$

Soit  $(M, \varphi)$  un espace  $(-1)^{\frac{r}{2}}$ -symétrique de  $(R - proj, *, (-1)^{\frac{r}{2}} \varpi)$ .  $\varphi : M \rightarrow M^*$  est un isomorphisme et donc dans  $\tilde{K}_0 R$ ,

$$\tau([M] + i(\mathbb{Z})) = [M^*] + i(\mathbb{Z}) = [M] + i(\mathbb{Z});$$

d'où  $[M] + i(\mathbb{Z}) \in Ker(id - \tau)$ . Si  $(M, \varphi)$  est métabolique, il possède un lagrangien  $\alpha : L \rightarrow M$  et donc la suite

$$L \xrightarrow{\alpha} M \xrightarrow{\alpha^* \varphi} L^*$$

est exacte. Par suite  $M \cong L \oplus L^*$  et alors

$$[M] + i(\mathbb{Z}) = [L] + i(\mathbb{Z}) + \tau([L] + i(\mathbb{Z})) \in \text{Im}(id + \tau).$$

Donc l'application  $\alpha_r$  définie par

$$\alpha_r([(M, \varphi)]) = [M] + i(\mathbb{Z}) \quad \text{modulo } \text{Im}(id + \tau),$$

est bien définie.

Enfin, le morphisme  $\beta_r$  est, quant à lui, défini comme suit. Soit  $M$  un objet de  $R - \text{proj}$  tel que  $[M] + i(\mathbb{Z}) \in \ker(id - (-1)^r \tau)$ . Alors

$$[M] + i(\mathbb{Z}) = (-1)^r [M^*] + i(\mathbb{Z}).$$

- Si  $r$  est impair, comme  $M^* \cong M^\# \cong T^{r+1}(M^\#)$ , alors

$$[M \oplus T^{r+1}(M^\#)] + i(\mathbb{Z}) = i(\mathbb{Z})$$

et donc  $M \oplus T^{r+1}(M^\#)$  est un objet de  $D^b(R - \text{lib})$ .

Soit  $H_r(M)$  l'espace hyperbolique associé à  $M$  pour la dualité  $(T^{r+1} \circ \#, (-1)^{\frac{(r+1)(r+2)}{2}} \pi)$  sur  $D^b(R - \text{proj})$ , c'est-à-dire

$$H_r(M) = (M \oplus T^{r+1}(M^\#), \begin{pmatrix} 0 & 1 \\ (-1)^{\frac{(r+1)(r+2)}{2}} \pi_M & 0 \end{pmatrix}). \quad (4.8)$$

$H_r(M)$  est un espace symétrique dans la catégorie avec dualité  $(D^b(R - \text{lib}), T^{r+1} \circ \#, (-1)^{\frac{(r+1)(r+2)}{2}} \pi)$ . Si  $[M] + i(\mathbb{Z})$  est un élément de  $\text{Im}(id + (-1)^r \tau)$ , il existe un objet  $N$  de  $R - \text{proj} \hookrightarrow D^b(R - \text{proj})$  tel que

$$[M] + i(\mathbb{Z}) = [N] + (-1)^r [N^*] + i(\mathbb{Z});$$

on vérifie que l'espace hyperbolique  $H_r(N)$  est métabolique et qu'alors l'application  $\beta_r$  définie par  $\beta_r([M]) = [H_r(M)]$  ( $[M]$  étant la classe de  $[M] + i(\mathbb{Z})$  modulo  $\text{Im}(id + (-1)^r \tau)$ ) est bien définie.

- Si  $r$  est pair, d'après [4, paragraphe 3, page 14],  $\beta_r$  se définit comme dans le cas où  $r$  est impair. Toutefois dans ce cas, il faut noter que l'espace hyperbolique  $H_r(M)$  (définie par (4.8)) est en réalité dans  $K^b(R_\sigma - proj)$  et non dans  $K^b(R_\sigma - lib)$ , étant donné qu'il ne possède pas de lagrangien dans cette sous-catégorie; mais la classe de Witt de  $H_r(M)$  est un élément de  $W^{r+1}(R_\sigma - lib)$ .

**Remarque 4.3.17.** *Vu le théorème 4.3.15, le théorème 4.3.16 donne les deux suites exactes suivantes :*

$$\begin{array}{ccccc}
 W^0(R_\sigma - lib) & \xrightarrow{j_0} & W^0(R_\sigma - proj) & \xrightarrow{\alpha_0} & \widehat{H}^0(\frac{\mathbb{Z}}{2\mathbb{Z}}; \widetilde{K}_0 R) \\
 \beta_3 \uparrow & & & & \downarrow \beta_0 \\
 \widehat{H}^1(\frac{\mathbb{Z}}{2\mathbb{Z}}; \widetilde{K}_0 R) & & & & W^1(R_\sigma - lib) \\
 \uparrow & & & & \downarrow \\
 0 & & & & 0
 \end{array}$$

et

$$\begin{array}{ccccc}
 W^2(R_\sigma - lib) & \xrightarrow{j_2} & W^2(R_\sigma - proj) & \xrightarrow{\alpha_2} & \widehat{H}^0(\frac{\mathbb{Z}}{2\mathbb{Z}}; \widetilde{K}_0 R) \\
 \beta_1 \uparrow & & & & \downarrow \beta_2 \\
 \widehat{H}^1(\frac{\mathbb{Z}}{2\mathbb{Z}}; \widetilde{K}_0 R) & & & & W^3(R_\sigma - lib) \\
 \uparrow & & & & \downarrow \\
 0 & & & & 0
 \end{array}$$

Dans la suite, nous nous intéressons plus particulièrement aux  $n$ -ièmes groupes de Witt de la catégorie  $R_\sigma - lib$  pour  $n$  impair, à cause des liens qui existent entre ceux-ci et le type de la restriction de l'involution  $\sigma$  à chaque composante simple de  $R$ . La proposition suivante donne certains des liens précités lorsqu'on suppose  $R$  simple.

**Proposition 4.3.18.** *Soit  $A$  une composante simple de  $R$  telle que  $A \cong M_l(D)$ , pour un entier naturel  $l$  et une  $k$ -algèbre à division  $D$ .*

(1) *Si  $\sigma(A) = A$ , notons par  $\sigma$  la restriction de l'involution  $\sigma$  à  $A$ .*

(a) *Si  $l$  est impair, alors  $\widehat{H}^0(\frac{\mathbb{Z}}{2\mathbb{Z}}; \widetilde{K}_0 A) = \widehat{H}^1(\frac{\mathbb{Z}}{2\mathbb{Z}}; \widetilde{K}_0 A) = 0$ .*

- (b) Si  $l$  est pair, alors  $\widehat{H}^0(\frac{\mathbb{Z}}{2\mathbb{Z}}; \widetilde{K}_0 A) \cong \widehat{H}^1(\frac{\mathbb{Z}}{2\mathbb{Z}}; \widetilde{K}_0 A) \cong \frac{\mathbb{Z}}{2\mathbb{Z}}$ .
- (c) Si  $\sigma$  est orthogonale sur  $A$ , alors  $W^1(A_\sigma - lib) = 0$  et  $W^3(A_\sigma - lib)$  est nul si  $l$  est impair et isomorphe à  $\frac{\mathbb{Z}}{2\mathbb{Z}}$  si  $l$  est pair.
- (d) Si  $\sigma$  est symplectique sur  $A$ , alors

$$W^1(A_\sigma - lib) \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \text{ et } W^3(A_\sigma - lib) = 0.$$

- (e) Si  $\sigma$  est unitaire sur  $A$ , alors

$$W^1(A_\sigma - lib) = W^3(A_\sigma - lib) = 0.$$

- (2) Si  $\sigma(A) \neq A$ , Notons par  $\sigma$  la restriction de  $\sigma$  à  $A \times \sigma(A) = A \times A^{op}$ . Pour tout entier  $n$ ,

$$W^n((A \times A^{op})_\sigma - proj) = W^n((A \times A^{op})_\sigma - lib) = 0.$$

*Preuve :* Voir [4, proposition 4.1, page 14] pour (1a) et (1b); voir [4, théorème 4.14, page 18] pour (1c), (1d) et (1e). Voir [4, exemple 1.13, page 8] pour (2). ■

Rappelons une description des éléments non triviaux des groupes à deux éléments repris dans la proposition 4.3.18. Avec les notations de cette proposition, comme  $A \cong M_l(D)$  est une  $k$ -algèbre simple, tout  $A$ -module est isomorphe à  $I^r$  pour un certain entier naturel  $r$ ,  $I$  étant un idéal à gauche minimal de  $A$ . Plus précisément,  $I$  est isomorphe à l'idéal à gauche

$$\left\{ \begin{pmatrix} a & 0 \end{pmatrix} \mid a \in D^{l \times 1} \text{ et } 0 \text{ est la matrice nulle de } D^{l \times (l-1)} \right\}$$

des matrices  $l \times l$  à entrées dans  $D$  telles que les  $(l-1)$  dernières colonnes sont nulles. L'application  $r \mapsto [I^r]$  est un isomorphisme de groupes de  $\mathbb{Z}$  sur  $K_0 A$ ; donc  $K_0 A$  est le groupe cyclique engendré par  $[I]$ . Comme  $A$  est isomorphe à  $I^l$ , alors le morphisme de groupes  $i : \mathbb{Z} \rightarrow K_0 A : m \mapsto m[A]$  est tel que  $i(\mathbb{Z}) = sgr < l[I] > \cong l\mathbb{Z}$ . Donc

$$\widetilde{K}_0 A = \frac{K_0 A}{i(\mathbb{Z})} = sgr < [I] + sgr < l[I] > > \cong \frac{\mathbb{Z}}{l\mathbb{Z}}.$$

#### 4.3. GROUPES DE WITT TORDUS ET DODÉCAGONE 167

Soit  $\tau$  l'automorphisme de  $\tilde{K}_0 A$  induisant une action de  $\frac{\mathbb{Z}}{2\mathbb{Z}}$  sur  $\tilde{K}_0 A$  (voir remarque 4.3.14).

$$\tau([I] + sgr < l[I] >) = [I^*] + sgr < l[I] > = [I] + sgr < l[I] >;$$

donc pour tout  $x \in \tilde{K}_0 A$ ,  $\tau(x) = x$ . Il en résulte que

$$Ker(id - \tau) = \tilde{K}_0 A,$$

$$Im(id + \tau) = 2\tilde{K}_0 A,$$

$$Ker(id + \tau) = \{x \in \tilde{K}_0 A / 2x = 0\}$$

et

$$Im(id - \tau) = 0.$$

Il en résulte que

$$\begin{aligned} \widehat{H}^0(\frac{\mathbb{Z}}{2\mathbb{Z}}, \tilde{K}_0 A) &= \frac{Ker(id - \tau)}{Im(id + \tau)} = \frac{\tilde{K}_0 A}{2\tilde{K}_0 A} \\ &= \begin{cases} 0 & \text{si } l \text{ est impair} \\ \{0, [I] + sgr < l[I] > + 2\tilde{K}_0 A\} & \text{si } l \text{ est pair} \end{cases} \end{aligned}$$

et

$$\begin{aligned} \widehat{H}^1(\frac{\mathbb{Z}}{2\mathbb{Z}}, \tilde{K}_0 A) &= \frac{Ker(id + \tau)}{Im(id - \tau)} = \{x \in \tilde{K}_0 A / 2x = 0\} \\ &= \begin{cases} 0 & \text{si } l \text{ est impair} \\ \{0, [I^{\frac{l}{2}}] + sgr < l[I] >\} & \text{si } l \text{ est pair.} \end{cases} \end{aligned}$$

D'autre part, la suite exacte dodécagonale 4.6, où on fait jouer à  $A$  le rôle de  $R$ , donne la suite exacte suivante

$$W^{2r}(A_\sigma - lib) \xrightarrow{j_{2r}} W^{2r}(A_\sigma - proj) \xrightarrow{\alpha_{2r}} \widehat{H}^0(\frac{\mathbb{Z}}{2\mathbb{Z}}, \tilde{K}_0 A) \xrightarrow{\beta_{2r}} W^{2r+1}(A_\sigma - lib) \rightarrow 0$$

pour  $r = 0, 1$ , en utilisant les mêmes notations des morphismes que dans (4.7). Donc  $\beta_{2r}$  est surjectif.

Si  $\sigma$  est orthogonale sur  $A$  et  $l$  est pair, il est établi que les groupes  $\widehat{H}^0(\frac{\mathbb{Z}}{2\mathbb{Z}}; \widetilde{K}_0 A)$  et  $W^3(A_\sigma - lib)$  sont isomorphes à  $\frac{\mathbb{Z}}{2\mathbb{Z}}$ . Donc

$$\beta_2 : \widehat{H}^0(\frac{\mathbb{Z}}{2\mathbb{Z}}, \widetilde{K}_0 A) \longrightarrow W^3(A_\sigma - lib)$$

est un isomorphisme de groupes. Par suite, l'élément non nul de  $W^3(A_\sigma - lib)$  est

$$\beta_2([I] + sgr < l[I] > + 2\widetilde{K}_0 A) = [H_2(I)]$$

avec

$$H_2(I) = (I \oplus T^3(I^\#), \begin{pmatrix} 0 & 1 \\ \pi_I & 0 \end{pmatrix}) \quad (\text{voir (4.8)}).$$

Si  $\sigma$  est symplectique sur  $A$ , alors  $l$  est pair et par un raisonnement analogue, l'élément non nul de  $W^1(A_\sigma - lib)$  est

$$\beta_0([I] + sgr < l[I] > + 2\widetilde{K}_0 A) = [H_0(I)]$$

avec

$$H_0(I) = (I \oplus T(I^\#), \begin{pmatrix} 0 & 1 \\ -\pi_I & 0 \end{pmatrix}).$$

Le résultat suivant donne certains liens entre les groupes de Witt de  $R_\sigma - lib$  et le type de l'involution  $\sigma$  sur les composantes simples de  $R$ .

**Théorème 4.3.19.** [4, proposition 5.4, page 20 et théorème 5.6, page 21] *On suppose que  $R$  se décompose comme somme directe de ses composantes simples sous la forme*

$$R = (\prod_{i=1}^n A_i) \times (\prod_{j=1}^m B_j \times B_j^{op})$$

*où, pour tout  $1 \leq i \leq n$ ,  $A_i$  est une composante simple de  $R$  telle que  $\sigma(A_i) = A_i$  (et alors  $A_i \cong M_{l_i}(D_i)$ , pour un certain entier naturel  $l_i$  et une certaine algèbre à division  $D_i$ ) et pour tout  $1 \leq j \leq m$ ,*

$B_j$  est une composante simple de  $R$  telle que  $\sigma(B_j) = B_j^{op}$ . Soit  $s(R)$  (resp.  $o(R)$ ) le nombre de composantes simples de  $R$  sur lesquelles la restriction de  $\sigma$  est symplectique (resp. orthogonale). Alors :

(1) si pour tout  $i$ ,  $l_i$  est pair, alors

$$\widehat{H}^0(\frac{\mathbb{Z}}{2\mathbb{Z}}; \widetilde{K}_0 R) \simeq (\frac{\mathbb{Z}}{2\mathbb{Z}})^n \quad \text{et} \quad \widehat{H}^1(\frac{\mathbb{Z}}{2\mathbb{Z}}; \widetilde{K}_0 R) \simeq \frac{\mathbb{Z}}{2\mathbb{Z}};$$

(2) s'il existe  $i$  tel que  $l_i$  est impair, alors

$$\widehat{H}^0(\frac{\mathbb{Z}}{2\mathbb{Z}}; \widetilde{K}_0 R) \simeq (\frac{\mathbb{Z}}{2\mathbb{Z}})^{n-1} \quad \text{et} \quad \widehat{H}^1(\frac{\mathbb{Z}}{2\mathbb{Z}}; \widetilde{K}_0 R) = 0;$$

(3)  $W^1(R_\sigma - lib) \simeq (\frac{\mathbb{Z}}{2\mathbb{Z}})^{s(R)}$  ;

(4) si pour tout  $i$  tel que  $\sigma$  est orthogonale sur  $A_i$ ,  $l_i$  est pair, alors

$$W^3(R_\sigma - lib) \simeq (\frac{\mathbb{Z}}{2\mathbb{Z}})^{o(R)};$$

(5) s'il existe  $i$  tel que  $\sigma$  est orthogonale sur  $A_i$  et  $l_i$  est impair, alors

$$W^3(R_\sigma - lib) \simeq (\frac{\mathbb{Z}}{2\mathbb{Z}})^{o(R)-1}. \quad \blacksquare$$

## 4.4 Application à une algèbre de groupe

Dans cette section,  $S$  désigne l'algèbre de groupe  $kG$ , et  $\sigma$ , l'involution canonique sur  $S$ .

**Théorème 4.4.1.** Soit  $s(S)$  (resp.  $o(S)$ ) le nombre de composantes simples de  $S$  sur lesquelles la restriction de  $\sigma$  est symplectique (resp. orthogonale) et  $n$  le nombre de composantes simples de  $S$  fixées par  $\sigma$ . Alors :

(1)  $\widehat{H}^0(\frac{\mathbb{Z}}{2\mathbb{Z}}; \widetilde{K}_0 S) \simeq (\frac{\mathbb{Z}}{2\mathbb{Z}})^{n-1}$  ;

(2)  $\widehat{H}^1(\frac{\mathbb{Z}}{2\mathbb{Z}}; \widetilde{K}_0 S) = 0$  ;

(3)  $W^1(S_\sigma - lib) \simeq (\frac{\mathbb{Z}}{2\mathbb{Z}})^{s(S)}$  ;

$$(4) \quad W^3(S_\sigma - lib) \simeq (\frac{\mathbb{Z}}{2\mathbb{Z}})^{o(S)-1}.$$

*Preuve :* Cela découle du théorème 4.3.19 et du fait que la restriction de  $\sigma$  à la composante simple de  $S$ , correspondant au caractère trivial, est une involution orthogonale ; de plus, cette composante simple est bien isomorphe à  $k = M_1(k)$ . ■

**Théorème 4.4.2.** *Les propositions suivantes sont équivalentes :*

- (1)  $G$  est ambivalent et  $W^1(S_\sigma - lib) = 0$  ;
- (2)  $G$  est ortho-ambivalent par rapport à  $k$ .

*Preuve :*  $G$  étant ambivalent dans les deux propositions, d'après la proposition 1.3.3, la restriction de  $\sigma$  à chaque composante simple de  $S$  est une involution de première espèce.

(a) (2)  $\Rightarrow$  (1). Supposons que  $G$  est ortho-ambivalent par rapport à  $k$  ; alors la restriction de  $\sigma$  à toute composante simple de  $S$  est orthogonale. Donc  $s(S) = 0$ . D'après le théorème 4.4.1,

$$W^1(S_\sigma - lib) \simeq (\frac{\mathbb{Z}}{2\mathbb{Z}})^{s(S)} = 0.$$

(b) (1)  $\Rightarrow$  (2). Supposons que  $W^1(S_\sigma - lib) = 0$ . Alors

$$0 = W^1(S_\sigma - lib) \simeq (\frac{\mathbb{Z}}{2\mathbb{Z}})^{s(S)}$$

et donc  $s(S) = 0$ . D'où la restriction de  $\sigma$  à chaque composante simple de  $S$  étant de première espèce, est orthogonale. ■

**Théorème 4.4.3.** *Si  $G$  est ortho-ambivalent par rapport à  $k$ , alors*

(1) *La suite*

$$0 \longrightarrow W^0(S_\sigma - lib) \longrightarrow W^0(S_\sigma - proj) \longrightarrow (\frac{\mathbb{Z}}{2\mathbb{Z}})^{o(S)-1} \longrightarrow 0$$

*est exacte ;*

(2)  $W^2(S_\sigma - proj) \simeq W^2(S_\sigma - lib)$ .



**Preuve :** D'après le théorème 4.4.2,  $G$  est ambivalent et  $W^1(S_\sigma - lib) = 0$ . Donc d'après la proposition 1.3.3, la restriction de  $\sigma$  à chaque composante simple de  $S$  est une involution de première espèce. Donc avec les notations du théorème 4.4.1, le nombre de composantes simples de  $S$  est  $n = o(S) + s(S) = o(S)$  (car  $s(S) = 0$ ). D'après le théorème 4.4.1,

$$\hat{H}^0\left(\frac{\mathbb{Z}}{2\mathbb{Z}}; \tilde{K}_0 S\right) \simeq \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{n-1} \simeq \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{o(S)-1} \simeq W^3(S_\sigma - lib)$$

et

$$\hat{H}^1\left(\frac{\mathbb{Z}}{2\mathbb{Z}}; \tilde{K}_0 S\right) = 0.$$

D'après le théorème 4.3.15,

$$W^1(S_\sigma - proj) = W^3(S_\sigma - proj) = 0.$$

La suite exacte dodécaagonale ( 4.6) donnée par le théorème 4.3.16, se subdivise donc en les deux suites exactes suivantes :

$$0 \longrightarrow W^2(S_\sigma - lib) \longrightarrow W^2(S_\sigma - proj) \longrightarrow \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{o(S)-1} \longrightarrow \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{o(S)-1} \longrightarrow 0 \quad (4.9)$$

et

$$0 \longrightarrow W^0(S_\sigma - lib) \longrightarrow W^0(S_\sigma - proj) \longrightarrow \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{o(S)-1} \longrightarrow 0. \quad (4.10)$$

D'une part, le premier résultat est donné par ( 4.10). D'autre part, l'exactitude de la suite ( 4.9) implique que le morphisme

$$\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{o(S)-1} \longrightarrow \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{o(S)-1}$$

est un isomorphisme de groupes, que

$$0 = Ker\left(\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{o(S)-1} \longrightarrow \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{o(S)-1}\right) = Im(W^2(S_\sigma - proj) \longrightarrow \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{o(S)-1})$$

et donc que la suite

$$0 \longrightarrow W^2(S_\sigma - lib) \longrightarrow W^2(S_\sigma - proj) \longrightarrow 0$$

est exacte. On en déduit que

$$W^2(S_\sigma - proj) \simeq W^2(S_\sigma - lib). \quad \blacksquare$$

Le résultat suivant donne des conditions nécessaires et suffisantes pour que  $G$  soit ortho-ambivalent par rapport à  $k$ .

**Corollaire 4.4.4.** *Les propositions suivantes sont équivalentes :*

- (1)  $G$  est ortho-ambivalent par rapport à  $k$  ;
- (2)  $G$  est ortho-ambivalent par rapport à  $\mathbb{C}$  ;
- (3)  $G$  est ambivalent et pour tout caractère irréductible  $\chi$  de  $G$ ,  $\nu(\chi) = 1$  ;
- (4)  $G$  est ambivalent et  $t(1) = \sum_{\chi \in \text{Irr}(G)} \chi(1)$  ;
- (5)  $G$  est totalement orthogonal ;
- (6)  $G$  est ambivalent et  $W^1(S_\sigma - \text{lib}) = 0$ .

*Preuve :* Conséquence directe des corollaires 2.1.21, 2.3.8, de la proposition 2.4.2 et du théorème 4.4.2. ■

Pour clôturer ce chapitre, utilisons les résultats précédents pour calculer les  $n$ -ièmes groupes de Witt de la catégorie  $S_\sigma - \text{lib}$  pour  $n$  impair,  $S = kG$ ,  $G$  étant un groupe diédral ou quaternionique ambivalent ou symétrique ou un 2-groupe abélien élémentaire ou un 2-groupe extra-spécial ou un  $p$ -groupe ( $p$  entier premier  $> 2$ ) et  $k$ , un corps dont la caractéristique ne divise pas l'ordre de  $G$  et est différente de 2.

Afin d'y arriver pour les groupes symétriques, nous avons besoin de rappeler ce que l'on appelle partition d'un entier naturel non nul.

**Définition 4.4.5.** *Soit  $n$  un entier naturel non nul. On appelle partition de  $n$  toute suite  $(\alpha_i)_{i \geq 1} = (\alpha_1, \alpha_2, \alpha_3, \dots, \dots)$  d'entiers naturels telle que  $\sum_{i \geq 1} \alpha_i = n$  et pour tout  $i \in \mathbb{N}_0$ ,  $\alpha_i \geq \alpha_{i+1}$ . On note par  $\mathcal{P}(n)$  le nombre de partitions de  $n$ .*

On a le résultat suivant :

**Proposition 4.4.6.** *Soient  $G$  un groupe fini,  $k$  un corps algébriquement clos dont la caractéristique ne divise pas l'ordre de  $G$  (et est différente de 2) et  $\sigma$  l'involution canonique de l'algèbre de groupe  $S = kG$ . Soit  $n$  un entier naturel non nul.*

(1) *Si  $G$  est un 2-groupe abélien élémentaire, alors*

$$W^1(S_\sigma - \text{lib}) = 0 \quad \text{et} \quad W^3(S_\sigma - \text{lib}) \cong \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{|G|-1}.$$

(2) *Si  $G$  est un  $p$ -groupe ( $p$  entier premier  $> 2$ ), alors*

$$W^1(S_\sigma - \text{lib}) = 0 \quad \text{et} \quad W^3(S_\sigma - \text{lib}) = 0.$$

(3) *Si  $G$  est le groupe diédral  $D_n$  d'ordre  $2n$ , alors*

$$W^1(S_\sigma - \text{lib}) = 0$$

*et*

$$W^3(S_\sigma - \text{lib}) \cong \begin{cases} \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{\frac{n+4}{2}} & \text{si } n \text{ est pair} \\ \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{\frac{n+1}{2}} & \text{si } n \text{ est impair.} \end{cases}$$

(4) *Si  $G$  est le groupe quaternionique  $Q_{2n}$  d'ordre  $8n$ , alors*

$$W^1(S_\sigma - \text{lib}) \cong \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^n \quad \text{et} \quad W^3(S_\sigma - \text{lib}) \cong \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{n+2}.$$

(5) *Si  $G$  est le groupe symétrique  $S_n$ , alors*

$$W^1(S_\sigma - \text{lib}) = 0 \quad \text{et} \quad W^3(S_\sigma - \text{lib}) \cong \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{\mathcal{P}(n)-1},$$

$\mathcal{P}(n)$  étant le nombre de partitions de  $n$ .

(6) *Si  $G$  est le 2-groupe extra-spécial  $2_+^{1+2n}$  (voir proposition 3.3.5), alors*

$$W^1(S_\sigma - \text{lib}) = 0 \quad \text{et} \quad W^3(S_\sigma - \text{lib}) \cong \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{2^{2n}}.$$

(7) Si  $G$  est le 2-groupe extra-spécial  $2_-^{1+2n}$  (voir proposition 3.3.5), alors

$$W^1(S_\sigma - \text{lib}) \cong \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right) \quad \text{et} \quad W^3(S_\sigma - \text{lib}) \cong \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{2^{2n}-1}.$$

*Preuve :* Notons d'abord que si  $G$  est ambivalent, alors le nombre de classes de conjugaison de  $G$  (qui est, d'après la proposition 1.1.4, le nombre de caractères irréductibles de  $G$  et donc le nombre de composantes simples de  $S = kG$ ) est égal à  $o(S) + s(S)$ ,  $o(S)$  (resp.  $s(S)$ ) étant le nombre de composantes simples de  $S$  sur lesquelles la restriction de  $\sigma$  est orthogonale (resp. symplectique). Que  $G$  soit ambivalent ou pas, il suffit de calculer  $s(S)$  et  $o(S)$  et d'utiliser ensuite le théorème 4.4.1.

1. Si  $G$  est un 2-groupe abélien élémentaire, il est ambivalent et comme tous ses caractères irréductibles sont de degré 1, alors  $s(S) = 0$  et  $o(S) = |G|$ .

2. Si  $G$  est un  $p$ -groupe fini, avec  $p$  entier naturel premier strictement supérieur à 2 et  $k = \mathbb{C}$ , alors d'après le théorème 3.2.1, une seule composante simple de  $S$  est fixée par  $\sigma$ , à savoir celle correspondant au caractère trivial et la restriction de  $\sigma$  à cette composante est orthogonale. Cela reste valable pour  $k$  algébriquement clos (par extension de corps ou par changement de caractéristique). Donc  $o(S) = 1$  et  $s(S) = 0$ .

3. Si  $G = D_n$ , d'après le corollaire 2.3.10,  $G$  est ortho-ambivalent par rapport à  $k$ . Donc  $s(S) = 0$  et  $o(S)$  est le nombre de caractères irréductibles de  $G$ . D'après [38, page 37] et [33, pages 12-14], le nombre de ces caractères est  $\frac{n}{2} + 3$  (resp.  $\frac{n-1}{2} + 2$ ) si  $n$  est pair (resp. impair). Donc

$$o(S) = \begin{cases} \frac{n}{2} + 3 & \text{si } n \text{ est pair} \\ \frac{n-1}{2} + 2 & \text{si } n \text{ est impair.} \end{cases}$$

4. Si  $G = Q_{2n}$ , d'après la proposition 2.1.8,  $G$  est ambivalent. D'après [33, page 15-19],  $G$  possède exactement  $n$  caractères irréductibles de type  $-1$  et  $n + 3$  caractères irréductibles de type  $1$ . Donc  $s(S) = n$  et  $o(S) = n + 3$ .

5. Si  $G = S_n$ , d'après le corollaire 2.3.9,  $G$  est ortho-ambivalent par rapport à  $k$ . Donc  $s(S) = 0$  et  $o(S)$  est le nombre de classes de conjugaison de  $G$  qui est égal à  $\mathcal{P}(n)$ , d'après [27, lemme 1.2.6, page 11].

6. Si  $G = 2_+^{1+2n}$ , d'après le théorème 3.3.11,  $G$  est ortho-ambivalent par rapport à  $k$ . Par suite  $s(S) = 0$  et  $o(S)$  est le nombre de composantes simples de  $S$  lequel, en vertu du corollaire 3.3.12, est égal à  $1 + \frac{1}{2}|G| = 1 + 2^{2n}$ .

7. Si  $G = 2_-^{1+2n}$ , d'après la proposition 3.3.7,  $G$  est ambivalent. De la démonstration du théorème 3.3.11, il ressort que  $S$  possède une unique composante simple de degré  $> 1$  et la restriction de  $\sigma$  à cette composante est symplectique. D'après (3.1), page 74,  $S$  possède  $\frac{1}{2}|G| = 2^{2n}$  composantes simples de degré  $1$ . Donc  $s(S) = 1$  et  $o(S) = 2^{2n}$ . Les résultats de (1) à (7) découlent alors immédiatement du théorème 4.4.1. ■



# Conclusion

Les résultats de cette thèse méritent d'être synthétisés et analysés pour en déduire des perspectives d'avenir.

Soit  $G$  un groupe fini et  $k$  un corps dont la caractéristique ne divise pas l'ordre de  $G$ . Nous pouvons mettre en évidence les résultats suivants :

**I)** Les assertions suivantes sont équivalentes :

- (1)  $G$  est ortho-ambivalent par rapport à  $k$  ;
- (2)  $G$  est ortho-ambivalent par rapport à  $\mathbb{C}$  ;
- (3)  $G$  est ambivalent et pour tout caractère irréductible  $\chi$  de  $G$ ,  $\nu(\chi) = 1$  ;
- (4)  $G$  est ambivalent et  $t(1) = \sum_{\chi \in Irr(G)} \chi(1)$  ;
- (5)  $G$  est totalement orthogonal.

De plus, si la caractéristique de  $k$  est différente de 2, les propositions ci-dessus sont équivalentes à la proposition suivante :

- (6)  $G$  est ambivalent et  $W^1(S_\sigma - lib) = 0$ ,  $S$  étant l'algèbre de groupe  $kG$  et  $\sigma$ , l'involution canonique sur  $S$ .

**II)** Si  $G$  est un 2-groupe et la caractéristique de  $k$  est différente de 2, les assertions suivantes sont équivalentes :

- (1)  $G$  est ortho-ambivalent par rapport à  $k$ .

- (2)  $G$  est ambivalent, engendré par des involutions et aucun sous-groupe de  $G$  d'indice 2 ne possède un caractère irréductible de type  $-1$ .

**III)** Si  $G$  est un 2-groupe spécial ambivalent d'application quadratique  $q : A =: \frac{G}{Z(G)} \rightarrow Z(G)$  et la caractéristique de  $k$  est différente de 2, les assertions suivantes sont équivalentes :

- (1)  $G$  est ortho-ambivalent par rapport à  $k$ .  
 (2) Pour toute représentation irréductible  $\rho$  de  $G$  de degré  $> 1$ ,  $Arf(\rho(G)) = 0$   
 (3) Pour toute  $\mathbb{F}_2$ -forme linéaire non nulle  $s$  sur  $Z(G)$ ,  $Arf(q_s) = 0$ ,  $q_s$  étant la forme quadratique sur  $A_s := \frac{A}{rad(b_{s^*(q)})}$  induite par le transfert  $s_*(q)$  de  $q$  par  $s$ .

**IV)** Le tableau suivant synthétise les résultats obtenus pour certains groupes "familiers"  $G$ ,  $n$  étant un entier naturel non nul.

| $G$                                            | Ambivalent ? | Ortho-ambivalent par rapport à $k$ ? |
|------------------------------------------------|--------------|--------------------------------------|
| $(\frac{\mathbb{Z}}{2\mathbb{Z}})^n$           | oui          | oui                                  |
| $S_n$                                          | oui          | oui                                  |
| $D_n$                                          | oui          | oui                                  |
| $Q_n$ , pour $n$ impair                        | non          | non                                  |
| $Q_n$ , pour $n$ pair                          | oui          | non                                  |
| $A_n$ , pour $n \in \{1, 2, 5, 6, 10, 14\}$    | oui          | oui                                  |
| $A_n$ , pour $n \notin \{1, 2, 5, 6, 10, 14\}$ | non          | non                                  |
| $2_+^{1+2n}$                                   | oui          | oui                                  |
| $2_-^{1+2n}$                                   | oui          | non                                  |
| 2-sous groupe de Sylow de $S_n$ ou de $A_n$    | oui          | oui                                  |

Il nous convient d'analyser ces résultats.



- Pour qu'un groupe fini soit ortho-ambivalent par rapport à un corps  $k$  dont la caractéristique ne divise pas l'ordre de  $G$ , il faut et il suffit qu'il soit totalement orthogonal. Nous débouchons ici sur le cas extrême du problème de Brauer, toujours ouvert. Ce que l'on sait simplement, c'est que le groupe  $G$  est, dans ces conditions, engendré par des involutions. Nous souhaiterions arriver à trouver une condition explicite en termes de relations entre les éléments du groupe  $G$ , par analogie avec ce qui se passe pour les groupes dont tous les caractères irréductibles sont réels. Nous prétendons avoir à notre disposition une solution à notre problème pour les 2-groupes ; c'est vrai, mais elle s'exprime en fonction des caractères comme la plupart des conditions obtenues dans le corollaire 4.4.4.

- Nous trouvons une condition nécessaire et suffisante pour qu'un groupe fini soit ortho-ambivalent par rapport à un corps  $k$  dont la caractéristique ne divise pas l'ordre de  $G$ , en termes de groupe de Witt. Les groupes de Witt ne sont pas faciles à calculer.

- Une condition nécessaire et suffisante pour qu'un 2-groupe spécial soit ortho-ambivalent par rapport à un corps de caractéristique différente de 2 est obtenue en termes d'invariant d'Arf des formes quadratiques régulières. Le calcul de cet invariant est un travail de longue haleine, surtout étant donné qu'il y a souvent plusieurs formes quadratiques à considérer (il y en a autant qu'il y a d'éléments dans le centre du groupe privé de l'élément unité).

Il ressort de ce qui précède que la recherche d'une solution à notre problème mérite d'être poursuivie en répondant à la question 4.4.7 qui constitue un problème ouvert :

**Question 4.4.7.** *Trouver une caractérisation (en termes de relations) de tous les groupes  $G$  ortho-ambivalents par rapport à un corps  $k$  dont la caractéristique ne divise pas l'ordre de  $G$ .*



# Bibliographie

- [1] C. Ausoni, *An introduction to Algebraic K-theory*, lecture at the 20th Winter School for Geometry and Physics at Srni, Zurich.
- [2] R. Baeza, *Quadratic Forms over Semilocal Rings*, Lecture Notes in Mathematics, vol. 655, Springer-Verlag (1978).
- [3] P. Balmer, *An introduction to Triangular Witt Groups and a survey of applications*, Contemporary Mathematics, Volume 00(2000).
- [4] P. Balmer, R. Preeti, *Shifted Witt groups of semi-local rings*, manuscripta math.117,1-27, DOI/10.1007/s00229-005-0546-5, Springer-Verlag (2005).
- [5] P. Balmer, *Witt Groups*, Handbook of K-Theory, Springer, vol. 2, 539-576 (2005).
- [6] P. Balmer, *Triangular Witt Groups Part I : The 12-term localization exact sequence*, K-theory 19, n° 4, p. 311-363 (2000).
- [7] P. Balmer, *Triangular Witt Groups Part II : From usual to derived*, Mathematische Zeitschrift 236, 351-382 (2001), DOI/10.1007/s002090000182 Spring Verlag (2000).
- [8] J.L. Berggren, *Finite groups in which every element is conjugate to its inverse*, Pacific journal of mathematics vol. 28, N° 2, 289-293 (1969).
- [9] M. Boulagouaz, L. Oukhtite, *Involutions of semisimple group algebras*, The Arabian Journal for Science and Engineering, Volume 25, Number 2C, 133-149, (December 2000).

- [10] M. Boulagouaz, L. Oukhtite, *Sur les involutions de l'algèbre de groupe semi-simple*, Prépublication, Département de Mathématique, Fès.
- [11] N. Bourbaki, *Eléments de mathématique*, Masson, Paris (1981) Algèbre. Chapitres 4 à 7.
- [12] W. Burnside, *Theory of groups of finite order*, Cambridge University press, Dover publications, inc., Second edition, New York (1955).
- [13] Arjeh M. Cohen, D.E. Taylor *On a certain Lie algebra defined by a finite group*, University of Sydney, NSW (2006).
- [14] P.M. Cohn, *Algebra*, Second Edition, Volume 2, John Wiley and Sons, New-York (1989).
- [15] P.M. Cohn, *Further Algebra and Applications*, Springer, London (2003).
- [16] L.E. Dickson, *Algebras and their arithmetics*, University of Chicago, Chicago (1923), Reprinted by G.E. Stechert and Co., New york (1938).
- [17] W. Feit, *Characters of finite groups*, W. A. Benjamin, inc., NewYork (1967).
- [18] R. Gow, *Real valued characters and the Schur index*, J. Algebra 40, 258-270 (1976).
- [19] R. Gow, *Real valued and 2-rational group characters*, J. Algebra 61, 388-413 (1979).
- [20] Ph. Gille, T. Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Univ. Press (2006).
- [21] D. Gorenstein, *Finite groups*, Harper and Row, NewYork (1968).
- [22] D. Gorenstein, *Finite simple groups*, Plenum Press, NewYork (1982).
- [23] M. Hall jr, *The theory of groups*, Macmillan (1959).
- [24] J. Hornbostel, M. Schlichting, *Localization in hermitian K-theory of rings*, J. London Math. Soc.(2) 70, 77-124 (2004).

- [25] I.M. Isaacs, *Character theory of finite groups*, American Mathematical Society, Providence (2006).
- [26] N. Jacobson, *Basic Algebra II*, Second Edition, W. H. Freeman and Company, New York (1995).
- [27] G. James, A. Kerber, *The representation theory of the symmetric group*, Encyclopedia of mathematics and its applications, Vol.16, Addison-Wesley, London (1981).
- [28] B. Kahn, *Formes quadratiques sur un corps, avec un appendice de A. Laghrabi*, rédaction d'un cours de troisième cycle donné à l'Université de Paris 7 en 1998, article soumis à publication (2000).
- [29] Y. Kitaoka, *Arithmetic of quadratic forms*, Cambridge University Press (1993).
- [30] M.-A. Knus, A. Merkurjev, M. Rost, J.-P. Tignol, *The Book of Involutions*, Colloquium Publications, Vol.44, American Mathematical Society, Providence, R.I. (1998).
- [31] H. Kurzweil, B. Stellmacher, *The Theory of Finite Groups, an introduction*, Springer-Verlag, New-York, Inc. (2004).
- [32] T.Y. Lam, *A first course in noncommutative rings*, Springer-Verlag, New-York, Inc. (1991).
- [33] O. Ntabuhashe Zahinda, *Involution canonique sur une algèbre de groupe ambivalent, semi-simple*, Mémoire D.E.A., Université Catholique de Louvain (2001-2002).
- [34] D.S. Passman, *The Algebraic Structure of Group Rings*, John Wiley and Sons, New-York (1977).
- [35] R. Quinlan, *Real elements and real-valued characters of covering groups of elementary abelian 2-groups*, Journal of Algebra 275, 191-211 (2004).
- [36] A. Ranicki, *On the algebraic L-theory of semisimple rings*, Journal of Algebra 50, 242-243 (1978).
- [37] J.R. Ruiz-Tolosa, E. Castillo, *From vectors to tensors*, Springer, New York (2000).

- [38] J.-P. Serre, *Linear Representations of Finite Groups*, Springer-Verlag, New-York (1977).
- [39] W. Scharlau, *Quadratic and Hermitian Forms*, Springer-Verlag, Berlin Heidelberg New-York Tokyo (1985).
- [40] I. Stewart, *Galois Theory*, Chapman and Hall, Second edition, New-York (1989).
- [41] C. Walter, *Grothendieck-Witt Groups of Triangulated Categories*, Preprint (2003).
- [42] K.S. Wang, L.C. Grove *Realizability of representations of finite groups*, Journal of Pure and Applied Algebra 54, 299-310, (1988).
- [43] C.A. Weibel, *An Introduction to Homological Algebra*, University Press, Cambridge (1994).

# Index

- élémentaire
  - 2-groupe commutatif, 66
- acyclique (complexe), 152
- algèbre
  - à division, 4
  - centrale, 4
  - de groupe, 11
  - des quaternions
    - en caractéristique 2, 8
    - en caractéristique différente de 2, 8
  - opposée de ..., 4
  - semi-simple, 4
  - simple, 4
- Brauer (problème de), xii
- caractère, 3
  - contragrédient de..., 3
  - irréductible, 3
  - orthogonal, xi
- catégorie
  - avec dualité, 146
  - dérivée de  $\mathcal{C}$ , 154
  - homotopique de..., 149
- cocycle normalisé
  - 2-cocycle, 84
- degré
  - d'un caractère, 3
  - d'un idempotent centralement primitif, 13
  - d'une algèbre simple centrale, 5
  - d'une représentation, 1
- espace  $\varepsilon$ -symétrique, 147
  - espaces isométriques, 148
  - métabolique, 148
  - somme orthogonale, 148
- espace hyperbolique, 164
- espace symétrique métabolique
  - dans  $(D^b(\mathcal{C}), \#, \pi)$ , 154
- forme bilinéaire
  - $G$ -invariante, 11
- Fratini (sous-groupe de), 75
- groupe
  - 2-uniforme, 49
  - ambivalent, xii, 11
  - de cohomologie de Tate ( $i$ -ième), 161
  - de  $K$ -théorie de  $R$  (0-ième), 162
  - de Frobenius, xi, 49
  - de Witt dérivé de  $\mathcal{C}$ , 155

- de Witt des complexes courts
  - $\varepsilon$ -symétriques, 159
- de Witt tordu de  $\mathcal{C}$  (n-ième), 156
- de Witt usuel de  $\mathcal{C}$ , 149
- de Witt- $(\varepsilon)$  de  $\mathcal{C}$ , 149
- de Witt- $(-1)$  usuel de  $\mathcal{C}$ , 149
- diédral, 20
- extra-spécial (2-groupe), 66
- ortho-ambivalent par rapport
  - à un corps, xiii, 20
- quaternionique, 20
- réduit de  $K$ -théorie de  $R$  (0-ième), 162
- spécial (2-groupe), 76
- symétrique, 20
- totalement orthogonal, xi, 48
- homotopes
  - morphismes de complexes, 150
- idempotent centralement primitif, 12
- indicateur de Schur-Frobenius, xi, 22
- indice de Schur de..., 5
- inflation
  - d'un 2-cocycle, 108
- invariant d'Arf, 81
  - d'un 2-groupe extra-spécial, 102
- involution
  - adjointe de..., 6
  - canonique
    - ...algèbre de groupe, 11
    - ...algèbre des quaternions, 8
  - d'un groupe, 49
  - de deuxième espèce, unitaire, 5
  - de première espèce, 5
    - orthogonale, 6
    - symplectique, 6
  - sur une algèbre, 5
- isométriques
  - formes quadratiques, 113
- lagrangien, 148
  - dans  $(D^b(\mathcal{C}), \#, \pi)$ , 154
- localisation d'une catégorie, 153
- partition de  $n$ , 172
- place, 32
- polaire (application), 78
- produit central, 67
- quadratique (application), 78
  - d'un 2-groupe spécial, 80
- quasi-isomorphisme, 152
- représentation, 1
  - contragrédiente de ..., 3
  - irréductible, 2
  - réalisable, rationnelle sur..., 2
- représentations semblables, isomorphes, 1
- somme orthogonale
  - de formes quadratiques, 82
- sous-groupe dérivé, 61
- symplectique (base), 81



transfert

  d'un 2-cocycle, 108

  d'une application quadratique,  
    105

triangle exact, 151

triangle strict, 151

type

  d'un caractère irréductible, xi,  
    23