

# ANNALES MATHÉMATIQUES



## BLAISE PASCAL

BRUNO DESCHAMPS & IVAN SUAREZ ATIAS

**Groupes totaux**

Volume 20, n° 2 (2013), p. 261-299.

<[http://ambp.cedram.org/item?id=AMBP\\_2013\\_\\_20\\_2\\_261\\_0](http://ambp.cedram.org/item?id=AMBP_2013__20_2_261_0)>

© Annales mathématiques Blaise Pascal, 2013, tous droits réservés.

L'accès aux articles de la revue « Annales mathématiques Blaise Pascal » (<http://ambp.cedram.org/>), implique l'accord avec les conditions générales d'utilisation (<http://ambp.cedram.org/legal/>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

*Publication éditée par le laboratoire de mathématiques  
de l'université Blaise-Pascal, UMR 6620 du CNRS  
Clermont-Ferrand — France*

**cedram**

*Article mis en ligne dans le cadre du  
Centre de diffusion des revues académiques de mathématiques  
<http://www.cedram.org/>*

# Groupes totaux

BRUNO DESCHAMPS  
IVAN SUAREZ ATIAS

## Résumé

Les «groupes totaux» sont les groupes pour lesquels la dimension du centre l'algèbre des invariants d'une algèbre simple centrale  $\mathfrak{A}_f$  associée à un 2-cocycle  $f \in Z^2(\text{Gal}(L/k), L^*)$  sous l'action d'un relevé de l'action galoisienne à  $\mathfrak{A}_f$  est constante quels que soient  $k$  et  $f$ . Dans cet article, nous montrons que les groupes quasi-CC (qui sont les groupes de centre cyclique et dont les centralisateurs des éléments hors du centre sont cycliques) sont totaux. Les groupes de type CC qui sont les groupes quasi-CC à centre trivial sont donc totaux. Nous en donnons une classification complète. Nous décrivons également une famille infinie de groupes quasi-CC qui ne sont pas de type CC : les groupes méta-dicycliques.

## *Total Groups*

### Abstract

Total groups are groups for which the dimension of the invariant algebra center of a central simple algebra  $\mathfrak{A}_f$  associated to a 2-cocycle  $f \in Z^2(\text{Gal}(L/k), L^*)$  under a lifting of the Galois action to  $\mathfrak{A}_f$  is constant for all  $k$  and  $f$ . In this article, we show that the quasi-CC groups (groups with cyclic center and for which all the centralizer of non-central elements are cyclic) are total. CC-groups, which are quasi-CC groups with trivial center, are thus total. We give a complete classification of these groups. We also describe a general family of quasi-CC groups which are not CC: the meta-dicyclic groups.

## 1. Introduction.

Dans ce texte, nous introduisons et étudions la notion de groupe total. La totalité est une propriété arithmétique liée aux algèbres simples centrales. Etant donné un groupe fini  $G$  et une extension galoisienne finie  $L/k$ ,

---

Aux Errancis.

*Mots-clés* : Algèbres simples centrales, action galoisienne, groupe CA et CC.

*Classification math.* : 20E99, 20D99, 16S35, 12E15, 16K50.

de groupe de Galois  $G$  de neutre  $e$ , on se donne un 2-cocycle  $f \in Z^2(G, L^*)$  et l'on note  $\mathfrak{A}_f$  l'algèbre muni du produit croisé relatif à  $f$  et rapportée à une  $L$ -base  $\{a_\sigma\}_{\sigma \in G}$ . Il existe un plongement tout à fait canonique du corps  $L$  dans l'algèbre  $\mathfrak{A}_f$ , donné par l'application

$$\begin{aligned} p_f : L &\longrightarrow \mathfrak{A}_f \\ \lambda &\longmapsto f^{-1}(e, e)\lambda a_e \end{aligned}$$

Dans cette situation, il se peut que le groupe  $G$  se relève en un sous-groupe de  $\text{Aut}_k(\mathfrak{A}_f)$ . Autrement dit, il peut exister un morphisme injectif  $\varphi : G \longrightarrow \text{Aut}_k(\mathfrak{A}_f)$  tel que pour tout  $\lambda \in L$  et tout  $g \in G$ , on ait

$$p_f(\lambda^g) = \varphi(g) \circ p_f(\lambda)$$

Dans le cas où un tel relevé existe, on peut considérer l'algèbre des invariants de  $\mathfrak{A}_f$  par  $G$ , notée  $\mathfrak{A}_f^G$ , ainsi que son centre  $Z(\mathfrak{A}_f^G)$ . On dit que le groupe  $G$  est total si la dimension sur  $k$  de  $Z(\mathfrak{A}_f^G)$  est indépendante du choix de  $L/k$  et de  $f$ . Le but de cet article est d'étudier cette notion et de donner une vaste série d'exemples de groupes totaux.

Bien que, de part sa définition, la totalité puisse apparaître comme une notion *a priori* improbable, les résultats établis dans ce texte montrent que de nombreuses familles classiques de groupes finis la possèdent. Parmi les plus connues, nous montrons que, pour tout entier  $n$ , le groupe cyclique  $C_n$  (proposition 3.10), le groupe diédral  $D_{4n+2}$  (corollaire 4.15), le groupe dicyclique  $Q_{4n}$  (corollaire 4.17) et le groupe spécial linéaire projectif de dimension 2 sur le corps fini à  $2^n$  éléments  $\text{PSL}_2(\mathbb{F}_{2^n})$  (corollaire 22) sont des groupes totaux. D'autres exemples plus exotiques de groupes totaux sont donnés et dans le cas de la non-totalité, le texte donne des résultats numériques qui indiquent les dimensions possibles que peut prendre  $Z(\mathfrak{A}_f^G)$  dans le cas de groupes  $G$  de petits ordres.

Cet article se compose de trois parties. Les deux premières sont assez élémentaires et concernent la question du relèvement de l'action galoisienne et l'étude du centre de l'algèbre des invariants. La troisième se consacre à l'étude des groupes totaux. Plus précisément :

Dans la première partie on s'intéresse à la question du relèvement du groupe  $G$  à  $\text{Aut}_k(\mathfrak{A}_f)$ . Cette question, ainsi que les structures des algèbres  $\mathfrak{A}_f^G$  et  $Z(\mathfrak{A}_f^G)$ , sont invariantes par cobordisme. Plus précisément, si  $f, g \in Z^2(G, L^*)$  sont deux 2-cocycles cohomologues, disons  $f = d(\mu)g$  avec  $\mu \in C^1(G, L^*)$ , il existe un isomorphisme entre  $\mathfrak{A}_f$  et  $\mathfrak{A}_g$ , donné par

l'application

$$\theta : \begin{array}{ccc} \mathfrak{A}_f & \longrightarrow & \mathfrak{A}_g \\ \sum_{\sigma \in G} \lambda_\sigma a_\sigma & \longmapsto & \sum_{\sigma \in G} \lambda_\sigma \mu(\sigma) a_\sigma \end{array}$$

Cet isomorphisme respecte les plongements de  $L$  dans  $\mathfrak{A}_f$  et  $\mathfrak{A}_g$  (i.e.  $p_g = \theta \circ p_f$ ), par ailleurs il induit un isomorphisme

$$\bar{\theta} : \begin{array}{ccc} \text{Aut}_k(\mathfrak{A}_f) & \longrightarrow & \text{Aut}_k(\mathfrak{A}_g) \\ \alpha & \longmapsto & \theta \circ \alpha \circ \theta^{-1} \end{array}$$

Puisque  $\bar{\theta}(\alpha) \circ p_g = \theta \circ \alpha \circ \theta^{-1} \circ \theta \circ p_f = \theta(\alpha \circ p_f)$ , on en déduit que  $\bar{\theta}$  applique un relevé de  $G$  dans  $\text{Aut}_k(\mathfrak{A}_f)$  à un relevé de  $G$  dans  $\text{Aut}_k(\mathfrak{A}_g)$  et que les algèbres  $\mathfrak{A}_f^G$  et  $\mathfrak{A}_g^G$  (resp.  $Z(\mathfrak{A}_f^G)$  et  $Z(\mathfrak{A}_g^G)$ ) sont  $k$ -isomorphes.

Ainsi, on peut reformuler plus globalement la problématique en la regardant sur le groupe  $H^2(G, L^*)$  : étant donné un élément  $\alpha \in H^2(G, L^*)$  on dira que  $G$  se relève à  $\alpha$ , si le groupe d'automorphismes  $G$  se relève dans  $\text{Aut}_k(\mathfrak{A}_f)$  où  $f \in Z^2(G, L^*)$  désigne n'importe quel représentant de  $\alpha$ . La collection des relevés ainsi que les algèbres invariantes et leurs centres ne dépendent donc pas, à  $k$ -isomorphisme près, du choix du représentant  $f$  de  $\alpha$ . Nous montrons dans cette partie que  $G$  se relève à  $\text{Aut}_k(\mathfrak{A}_f)$  si et seulement si  $f$  est cohomologue à un 2-cocycle à valeurs dans  $k^*$  (théorème 2.1) ce qui se traduit par le fait que les éléments du  $H^2(G, L^*)$  pour lesquels  $G$  se relève sont exactement ceux qui sont dans l'image du morphisme canonique  $H^2(G, k^*) \longrightarrow H^2(G, L^*)$ . Une fois  $f$  fixé, l'ensemble des relevés de  $G$  dans  $\text{Aut}_k(\mathfrak{A}_f)$  a naturellement une structure de groupe abélien.

La deuxième partie s'intéresse à l'algèbre des invariants,  $\mathfrak{A}_f^G$ , de  $\mathfrak{A}_f$  par un relevé de  $G$ . Nous montrons que la dimension sur  $k$  de  $\mathfrak{A}_f^G$  est toujours égale à l'ordre de  $G$  (théorème 3.4) et nous montrons que la dimension sur  $k$  du centre  $Z(\mathfrak{A}_f^G)$  de l'algèbre  $\mathfrak{A}_f^G$  correspond au cardinal d'un ensemble de classes de conjugaison de  $G$  pour lesquelles un certain morphisme est trivial (théorème 3.7). Dans le cas des groupes non-abélien nous en déduisons que l'algèbre des invariants  $\mathfrak{A}_f^G$  n'est jamais commutative (corollaire 3.8). Dans le cas des groupes abéliens, ce résultat est complété par le fait que la dimension sur  $k$  de  $Z(\mathfrak{A}_f^G)$  est un entier tel que  $o(G)/\dim_k Z(\mathfrak{A}_f^G)$  soit un carré parfait (proposition 3.9).

La troisième partie est consacrée à la propriété de totalité à proprement dite. En vertu des résultats établis dans les parties 1 et 2, un groupe fini

$G$  est total lorsque la dimension de  $Z(\mathfrak{A}_f^G)$  est égale au nombre de classes de conjugaisons de  $G$ , quels que soient le corps  $k$  et le 2-cocycle  $f$ . Cette notion est intrinsèquement liée à l'arithmétique du groupe que l'on étudie et ne reste stable pour aucune des opérations usuelles sur les groupes (passage aux quotients, au sous-groupes, au produit cartésiens ou encore aux extensions). Nous donnons toutefois plusieurs critères pour obtenir des groupes totaux. Nous montrons, par exemple, que tout groupe dont l'ordre est un entier radicalaire est total (corollaire 4.4).

Nous nous intéressons, par ailleurs, à la notion de *groupes de type CC*, qui sont les groupes pour lesquels les centralisateurs des éléments non triviaux sont cycliques. Ils sont toujours totaux. Nous donnons une classification de ces groupes (théorème 4.8) : ce sont exactement les groupes cycliques, les groupes spéciaux linéaires projectif  $\mathrm{PSL}_2(\mathbb{F}_{2^n})$  et les produits semi-direct de deux groupes cycliques pour une action ayant de "bonnes propriétés". Cette classification permet d'exhiber plusieurs familles explicites de groupes totaux. Plus généralement, les *groupes quasi-CC* (même définition que CC, mais l'on autorise le centre à être cyclique) sont totaux. Nous donnons un exemple de famille de groupes quasi-CC qui ne sont pas de type CC : les groupes méta-dicycliques. Il s'agit d'une famille obtenue en généralisant la construction des groupes dicycliques (paragraphe 3.3.). Elle compte des groupes de centre d'ordres arbitrairement grands.

## 2. Relèvement de l'action galoisienne.

On conserve les notations de l'introduction et pour ce qui est des objets cohomologiques, nous utilisons les notations standards.

**Théorème 2.1.** *Le groupe  $G$  se relève à  $\mathrm{Aut}_k(\mathfrak{A}_f)$  si et seulement si  $f$  est cohomologue à un 2-cocycle à valeurs dans  $k^*$ . En particulier, l'ensemble des  $\alpha \in \mathrm{H}^2(G, L^*)$  pour lesquelles  $G$  se relève à  $\alpha$  est exactement l'image du morphisme canonique  $\mathrm{H}^2(G, k^*) \longrightarrow \mathrm{H}^2(G, L^*)$ .*

Quand  $f$  est cohomologue à un 2-cocycle à valeurs dans  $k^*$ , l'ensemble des relevés de  $G$  à  $\mathrm{Aut}_k(\mathfrak{A}_f)$  a alors une structure de groupe, isomorphe au groupe  $d^{-1}(Z^2(G, k^*))/C^1(G, k^*)$  (où  $d : C^1(G, L^*) \longrightarrow Z^2(G, L^*)$  est l'application de cobord pour le  $G$ -groupe  $L^*$ ). Plus précisément, si  $f$  est choisi normalisé (i.e.  $f(e, e) = 1$ ) et à valeurs dans  $k^*$ , alors la correspondance annoncée s'obtient, pour  $\mu \in C^1(G, L^*)$  telle que  $d(\mu) \in Z^2(G, k^*)$ ,

GROUPES TOTAUX

par

$$\begin{aligned} G &\longrightarrow \text{Aut}_k(\mathfrak{A}_f) \\ g &\longmapsto \text{conjugaison par } \mu(g)a_g \end{aligned}$$

*Démonstration.* Commençons par montrer que si  $f$  est supposé normalisé et à valeurs dans  $k^*$  alors pour tout  $\mu \in C^1(G, L^*)$  telle que  $d(\mu) \in Z^2(G, k^*)$ , l'application

$$\theta : g \longmapsto \text{conjugaison par } \mu(g)a_g$$

est bien un relèvement. En premier lieu, puisque  $f$  est normalisé, on a pour tout  $g \in G$ ,  $f(e, g) = f(g, e) = 1$  et le plongement naturel de  $L$  dans  $\mathfrak{A}_f$  est donné par  $\lambda \longmapsto \lambda a_e$ . Ainsi, pour  $\lambda \in L$ , on a

$$\begin{aligned} \theta(g)(\lambda a_e) &= \mu(g)a_g \lambda a_e (\mu(g)a_g)^{-1} \\ &= \mu(g)a_g \lambda a_e \mu(g)^{-g^{-1}} f(g, g^{-1})^{-g^{-1}} a_{g^{-1}} \\ &= \mu(g)\lambda^g f(g, e) a_g \mu(g)^{-g^{-1}} f(g, g^{-1})^{-g^{-1}} a_{g^{-1}} \\ &= \mu(g)\lambda^g \mu(g)^{-1} f(g, g^{-1})^{-1} f(g, g^{-1}) a_e \\ &= \lambda^g a_e \end{aligned}$$

et donc l'action de  $\theta(g)$  sur  $L$  coïncide avec celle de  $g$ .

Reste à voir que  $\theta$  est bien un monomorphisme : pour tout  $g, h \in G$  on a

$$\mu(g)a_g \mu(h)a_h = \mu(g)\mu(h)^g f(g, h) a_{gh} = \mu(gh) f_0(g, h) a_{gh}$$

où  $f_0 = d(\mu)f \in Z^2(G, k^*)$ . Comme  $f_0(g, h) \in k^* = Z(\mathfrak{A}_f)^*$ , la conjugaison par l'élément  $f_0(g, h)$  vaut l'identité. Ainsi, on a  $\theta(gh) = \theta(g) \circ \theta(h)$ . Par ailleurs,  $\theta$  est bien injective car  $g \in \ker(\theta) \iff \mu(g)a_g \in k^* \implies g = e$ .

Venons-en maintenant à la preuve du coeur du théorème. Puisque la propriété de relèvement reste vraie par isomorphisme, on peut supposer que  $f$  est déjà normalisé (sous cette hypothèse le plongement de  $L$  dans  $\mathfrak{A}_f$  est canonique).

Supposons donc donné un relèvement  $G \longrightarrow \text{Aut}_k(\mathfrak{A}_f)$  et notons alors  $x^g$  l'action de l'élément  $g \in G$  sur l'élément  $x \in \mathfrak{A}_f$  via ce relèvement. Le théorème de Skolem-Noether assure qu'il existe  $x_g \in \mathfrak{A}_f$  tel que l'action de  $g$  sur  $\mathfrak{A}_f$  soit la conjugaison par  $x_g$ . Ainsi, pour tout  $\lambda \in L$ , on a  $\lambda^g x_g = x_g \lambda$ . Cependant, pour tout  $\lambda \in L$ , on a  $\lambda a_g^{-1} = a_g^{-1} \lambda^g$ , donc  $a_g^{-1} x_g \in Z(La_e) = La_e$ . Ainsi, il existe  $\mu_g \in L^*$  tel que  $x_g = \mu_g a_g$ .

Maintenant, pour  $g, h \in G$  donnés, la conjugaison par  $(\mu_g a_g) \cdot (\mu_h a_h)$  doit être égale à celle par  $\mu_{gh} a_{gh}$ . On en déduit qu'il existe un élément

$a(g, h) \in k^* = Z(\mathfrak{A}_f)^*$  tel que  $(\mu_g a_g) \cdot (\mu_h a_h) = a(g, h) \mu_{gh} a_{gh}$ . Ceci équivaut à  $\mu_g \mu_h^g f(g, h) a_{gh} = a(g, h) \mu_{gh} a_{gh}$  ou encore

$$\forall g, h \in G, \mu_h^g \mu_{gh}^{-1} \mu_g f(g, h) = a(g, h)$$

Cette dernière propriété exprime exactement le fait que le 2-cocycle  $(g, h) \mapsto f(g, h)$  est cohomologue (par le 2-cobord associé à l'application  $g \mapsto \mu_g$ ) au 2-cocycle  $(g, h) \mapsto a(g, h)$  qui est, par définition, à valeurs dans  $k^*$ .

Si on suppose que  $f$  est déjà à valeurs dans  $k^*$ , alors les relevés sont paramétrés par les applications  $\mu$  décrites précédemment. Leur ensemble correspond alors  $d^{-1}(Z^2(G, k^*))$ , mais deux telles applications donnent le même relevé si les conjugaisons associées sont les mêmes, c'est-à-dire si elles diffèrent d'une 1-cochaîne à valeurs dans  $k^*$ .  $\square$

Il est facile de décrire des situations où le morphisme

$$H^2(G, k^*) \longrightarrow H^2(G, L^*)$$

n'est pas surjectif et donc où  $G$  ne se relève pas. Par ailleurs, signalons que l'image de  $H^2(G, k^*)$  dans  $H^2(G, L^*)$  apparaît dans d'autres questions relatives aux algèbres simples centrales : on trouvera, par exemple, dans [4]-th 3.3. une caractérisation (sous certaines hypothèses) de la décomposition en produit d'algèbres cycliques d'une algèbre simple centrale qui fait intervenir cette image.

### 3. Algèbre des invariants.

On se fixe un 2-cocycle  $f \in Z^2(G, k^*)$  normalisé et on considère un relevé de  $G$  dans  $\text{Aut}_k(\mathfrak{A}_f)$ . Quitte à modifier  $f$  par un cobord on peut supposer que le relevé en question est le relevé canonique  $g \mapsto$  conjugaison par  $a_g$ . En effet, considérons un relevé  $G$  dans  $\text{Aut}_k(\mathfrak{A}_f)$  paramétré, d'après ce qui précède, par une application  $\mu \in C^1(G, L^*)$  telle que  $d(\mu) \in Z^2(G, k^*)$ . Considérons alors le 2-cocycle  $f_0 = d(\mu)f \in Z^2(G, k^*)$  (quitte à modifier  $\mu$  par une 1-cochaîne à valeurs dans  $k^*$ , on peut supposer que  $f_0$  est aussi normalisé). Comme rappelé dans l'introduction de ce texte, l'application

$$\theta : \begin{array}{ccc} \mathfrak{A}_{f_0} & \longrightarrow & \mathfrak{A}_f \\ \sum_{\sigma} \lambda_{\sigma} a_{\sigma} & \longrightarrow & \sum_{\sigma} \lambda_{\sigma} \mu(\sigma) a_{\sigma} \end{array}$$

est alors un  $k$ -isomorphisme d'algèbres qui respecte les plongements naturels de  $L$  dans  $\mathfrak{A}_{f_0}$  et  $\mathfrak{A}_f$ . Si  $c_\lambda$  désigne la conjugaison par l'élément  $\lambda$  alors l'image par  $\theta$  de l'automorphisme  $c_{a_g}$  est l'automorphisme  $\theta \circ c_{a_g} \circ \theta^{-1}$ . Pour  $x, y$  tel que  $y = \theta(x)$ , on a

$$\theta \circ c_{a_g} \circ \theta^{-1}(y) = \theta(a_g x a_g^{-1}) = (\mu(g)a_g)y(\mu(g)a_g)^{-1} = c_{\mu(g)a_g}(y)$$

On en déduit que  $\theta^{-1}$  envoie le relevé de  $G$  dans  $\text{Aut}_k(\mathfrak{A}_f)$  relatif à  $\mu$  sur le relevé canonique de  $G$  dans  $\text{Aut}_k(\mathfrak{A}_{f_0})$ . On va s'intéresser à l'algèbre  $\mathfrak{A}_f^G$  des invariants de  $\mathfrak{A}_f$  par  $G$ . Ce que l'on vient d'expliquer montre en particulier qu'à  $k$ -isomorphisme près l'algèbre  $\mathfrak{A}_f^G$  ne dépend pas du relevé que l'on choisit pour  $G$ . Ainsi, pour ces questions, on peut toujours se ramener au cas du relevé canonique, le paramètre d'étude devenant  $f$ , le 2-cocycle normalisé à valeurs dans  $k^*$ .

Caractérisons maintenant les éléments de  $\mathfrak{A}_f^G$  :

**Proposition 3.1.** *Un élément  $x = \sum_\sigma \lambda_\sigma a_\sigma$  appartient à  $\mathfrak{A}_f^G$  si et seulement si on a*

$$(SG) \quad \forall g, \sigma \in G, \quad \lambda_\sigma^g = \lambda_{g\sigma g^{-1}} \frac{f(g\sigma g^{-1}, g)}{f(g, \sigma)}$$

*Démonstration.*

$$\begin{aligned} x \in \mathfrak{A}_f^G &\iff \forall g \in G, \quad a_g x a_g^{-1} = x \\ &\iff \forall g \in G, \quad \sum_\sigma \lambda_\sigma^g f(g, \sigma) f^{-1}(g, g^{-1}) f(g\sigma, g^{-1}) a_{g\sigma g^{-1}} = x \\ &\iff \forall g \in G, \quad \sum_\sigma \lambda_\sigma^g f(g, \sigma) f^{-1}(g\sigma g^{-1}, g) a_{g\sigma g^{-1}} = \sum_\sigma \lambda_\sigma a_\sigma \\ &\quad \left( \text{car } f(g, g^{-1})^{g\sigma g^{-1}} f(g\sigma g^{-1}, 1) = f(g\sigma, g^{-1}) f(g\sigma g^{-1}, g) \right) \\ &\iff \forall g, \sigma \in G, \quad \lambda_\sigma^g = \lambda_{g\sigma g^{-1}} \frac{f(g\sigma g^{-1}, g)}{f(g, \sigma)} \end{aligned}$$

□

Pour  $\sigma \in G$  fixé, on note  $\omega_\sigma \in C^1(G, k^*)$  l'application définie par :

$$\begin{aligned} \omega_\sigma : G &\longrightarrow k^* \\ g &\longmapsto \frac{f(g\sigma g^{-1}, g)}{f(g, \sigma)} \end{aligned}$$

**Lemme 3.2.** *Pour tout  $\sigma, g, h \in G$ , on a  $\omega_\sigma(gh) = \omega_{h\sigma h^{-1}}(g)\omega_\sigma(h)$ .*



*Démonstration.* Pour tout  $\sigma, g, h \in G$  on a

- (1)  $f(g, h)^{gh\sigma h^{-1}g^{-1}} f(gh\sigma h^{-1}g^{-1}, gh) = f(gh\sigma h^{-1}, h) f(gh\sigma h^{-1}g^{-1}, g)$
- (2)  $f(h\sigma h^{-1}, h)^g f(g, h\sigma) = f(gh\sigma h^{-1}, h) f(g, h\sigma h^{-1})$
- (3)  $f(h, \sigma)^g f(g, h\sigma) = f(gh, \sigma) f(g, h)$

En quotientant (1) et (2) on obtient

$$\frac{f(gh\sigma h^{-1}g^{-1}, g)}{f(g, h\sigma h^{-1})} = \frac{f(gh\sigma h^{-1}g^{-1}, gh)}{f(g, h\sigma)} \frac{f(g, h)}{f(h\sigma h^{-1}, h)}$$

On a donc

$$\begin{aligned} \omega_{h\sigma h^{-1}}(g)\omega_{\sigma}(h) &= \frac{f(gh\sigma h^{-1}g^{-1}, g)}{f(g, h\sigma h^{-1})} \frac{f(h\sigma h^{-1}, h)}{f(h, \sigma)} \\ &= f(gh\sigma h^{-1}g^{-1}, gh) \frac{f(g, h)}{f(g, h\sigma)f(h, \sigma)} \end{aligned}$$

Comme d'après (3) on a  $\frac{f(g, h)}{f(g, h\sigma)f(h, \sigma)} = \frac{1}{f(gh, \sigma)}$ , on en déduit finalement que

$$\omega_{h\sigma h^{-1}}(g)\omega_{\sigma}(h) = \frac{f(gh\sigma h^{-1}g^{-1}, gh)}{f(gh, \sigma)} = \omega_{\sigma}(gh)$$

Cette propriété traduit simplement le fait que, pour tout  $g, h, \sigma \in G$ , on a  $(a_{\sigma}^h)^g = a_{\sigma}^{gh}$ .  $\square$

*Notation 3.3.* Dans la suite de ce texte, pour  $\sigma \in G$ , on notera

- $\text{Cen}_G(\sigma)$ , le centralisateur de  $\sigma$  dans  $G$ ,
- $L_{\sigma}$ , le corps  $L^{\text{Cen}_G(\sigma)}$  des invariants de  $L$  par  $\text{Cen}_G(\sigma)$ ,
- $\hat{\sigma}$ , une classe de représentants de l'ensemble quotient  $G/\text{Cen}_G(\sigma)$ ,
- $\tilde{\sigma}$ , la classe de conjugaison de  $\sigma$  :  $\tilde{\sigma} = \{g\sigma g^{-1}/g \in \hat{\sigma}\}$  (description biunivoque),
- $G_{\text{conj}}$ , une classe de représentants de l'ensemble des classes de conjugaison de  $G$ .

Une première conséquence du lemme 3.2 est que la restriction de  $\omega_{\sigma}$  à  $\text{Cen}_G(\sigma)$  est un morphisme de groupes et que si  $\sigma, \sigma' \in G$  sont deux éléments conjugués, alors les fonctions  $\omega_{\sigma}$  et  $\omega_{\sigma'}$  restreintes aux centralisateurs de  $\sigma$  et  $\sigma'$  sont égales. Plus précisément, si  $\sigma' = g\sigma g^{-1}$ , alors on a  $\text{Cen}_G(\sigma') = g\text{Cen}_G(\sigma)g^{-1}$  et, pour tout  $h \in \text{Cen}_G(\sigma)$ , si l'on considère

$h' = ghg^{-1}$ , on a

$$\omega_{\sigma'}(h') = \omega_{g\sigma g^{-1}}(h') = \frac{\omega_{\sigma}(h'g)}{\omega_{\sigma}(g)} = \frac{\omega_{\sigma}(gh)}{\omega_{\sigma}(g)} = \frac{\omega_{h\sigma h^{-1}}(g)\omega_{\sigma}(h)}{\omega_{\sigma}(g)} = \omega_{\sigma}(h)$$

Cette propriété va être importante pour l'étude du centre  $Z(\mathfrak{A}_f^G)$  à venir. Mais commençons par étudier l'algèbre  $\mathfrak{A}_f^G$  elle-même : on considère, pour  $\sigma \in G$  donné, le sous- $L$ -espace vectoriel de  $\mathfrak{A}_f$

$$E_{\sigma} = \left\{ x = \sum_{g \in \widehat{\sigma}} \lambda_{g\sigma g^{-1}} a_{g\sigma g^{-1}} \right\}$$

On a bien sur  $\mathfrak{A}_f = \bigoplus_{\sigma \in G_{\text{conj}}} E_{\sigma}$ . La relation  $(SG)$  montre que l'action de  $G$  laisse stable chaque  $E_{\sigma}$ , on en déduit donc que

$$\mathfrak{A}_f^G = \bigoplus_{\sigma \in G_{\text{conj}}} E_{\sigma}^G$$

où  $E_{\sigma}^G$  désigne l'ensemble des invariants de  $E_{\sigma}$  par  $G$ .

**Théorème 3.4.** *Pour tout  $\sigma \in G_{\text{conj}}$ , l'ensemble  $E_{\sigma}^G$  est (non canoniquement) un sous- $L_{\sigma}$ -espaces vectoriels de  $\mathfrak{A}_f$ . On a  $\dim_{L_{\sigma}} E_{\sigma}^G = 1$  et plus précisément,*

$$E_{\sigma}^G = \text{Vect}_{L_{\sigma}}(u) \text{ avec } u = \sum_{g \in \widehat{\sigma}} \frac{\lambda_0^g}{\omega_{\sigma}(g)} a_{g\sigma g^{-1}}$$

où  $\lambda_0 \in L$  est un élément non nul qui vérifie  $\lambda_0^g = \lambda_0 \omega_{\sigma}(g)$  pour tout  $g \in \text{Cen}_G(\sigma)$ .

En conséquence de quoi on a  $\dim_k \mathfrak{A}_f^G = o(G)$ .

*Démonstration.* Le sous-groupe  $E_{\sigma}^G$  est un  $L_{\sigma}$ -espaces vectoriels, pour la loi de composition externe suivante :

$$\begin{aligned} L_{\sigma} \times E_{\sigma}^G &\longrightarrow E_{\sigma}^G \\ \left( \lambda, x = \sum_{g \in \widehat{\sigma}} \lambda_{g\sigma g^{-1}} a_{g\sigma g^{-1}} \right) &\longmapsto \lambda \cdot x = \sum_{g \in \widehat{\sigma}} \lambda^g \lambda_{g\sigma g^{-1}} a_{g\sigma g^{-1}} \end{aligned}$$

En effet, il est clair que les axiomes définissant la structure d'espace vectoriel sont bien vérifiés, la seule chose à détailler est que la loi de

composition est bien à valeurs dans  $E_\sigma^G$ . Considérons  $\lambda \in L_\sigma$  et  $x = \sum_{g \in \widehat{\sigma}} \lambda_{g\sigma g^{-1}} a_{g\sigma g^{-1}} \in E_\sigma^G$ , pour tout  $h \in G$  et  $g \in \widehat{\sigma}$  on a

$$(\lambda^g \lambda_{g\sigma g^{-1}})^h = \lambda^{hg} \lambda_{hg\sigma g^{-1}}^h = \lambda^{hg} \lambda_{hg\sigma g^{-1}h^{-1}} \frac{f(hg\sigma g^{-1}h^{-1}, h)}{f(h, g\sigma g^{-1})}$$

Pour montrer que  $\lambda.x \in E_\sigma^G$  il faut donc montrer que pour tout  $h \in G$  et tout  $g \in \widehat{\sigma}$ , on a  $\lambda^{hg} = \lambda^{g'}$  où  $g' \in \widehat{\sigma}$  est le représentant de  $hg$  modulo  $\text{Cen}_G(\sigma)$ . Or, il existe  $\tau \in \text{Cen}_G(\sigma)$  tel  $hg = g'\tau$ , et donc comme  $\lambda \in L_\sigma$ , on a  $\lambda^{hg} = \lambda^{g'\tau} = \lambda^{g'}$ . Ainsi,  $\lambda.x \in E_\sigma^G$ .

On remarque, au passage, qu'en considérant  $k$  comme sous-corps de  $L_\sigma$  alors la structure induite par cette loi à  $k$  redonne la structure de  $k$ -espace vectoriel naturel de  $E_\sigma^G$  (c'est-à-dire celle obtenue par la multiplication à gauche).

Si  $x = \sum_{g \in \widehat{\sigma}} \lambda_{g\sigma g^{-1}} a_{g\sigma g^{-1}}$  et  $y = \sum_{g \in \widehat{\sigma}} \mu_{g\sigma g^{-1}} a_{g\sigma g^{-1}}$  sont deux éléments non nuls de  $E_\sigma^G$ , alors pour tout  $g \in \text{Cen}_G(\sigma)$ , on a

$$\lambda_\sigma^g = \lambda_\sigma \omega_\sigma(g) \text{ et } \mu_\sigma^g = \mu_\sigma \omega_\sigma(g)$$

et donc  $\lambda_\sigma / \mu_\sigma$  est invariant par  $\text{Cen}_G(\sigma)$ . Il existe donc  $\alpha \in L_\sigma$  tel que  $\mu_\sigma = \alpha \lambda_\sigma$ . On a alors

$$\begin{aligned} \alpha.x &= \sum_{g \in \widehat{\sigma}} \alpha^g \lambda_{g\sigma g^{-1}} a_{g\sigma g^{-1}} = \sum_{g \in \widehat{\sigma}} \alpha^g \lambda_\sigma^g \omega_\sigma(g)^{-1} a_{g\sigma g^{-1}} \\ &= \sum_{g \in \widehat{\sigma}} (\alpha \lambda_\sigma)^g \omega_\sigma(g)^{-1} a_{g\sigma g^{-1}} = \sum_{g \in \widehat{\sigma}} (\mu_\sigma)^g \omega_\sigma(g)^{-1} a_{g\sigma g^{-1}} \\ &= \sum_{g \in \widehat{\sigma}} \mu_{g\sigma g^{-1}} \omega_\sigma(g) \omega_\sigma(g)^{-1} a_{g\sigma g^{-1}} = y \end{aligned}$$

Ceci prouve que  $E_\sigma^G$  est au plus une droite  $L_\sigma$ -vectorielle. Reste donc à montrer que  $E_\sigma^G \neq \{0\}$ .

Commençons par regarder la condition (SG) quand  $g$  parcourt  $\text{Cen}_G(\sigma)$ . Dans cette situation,  $\omega_\sigma$  est un élément de  $\text{Hom}(\text{Cen}_G(\sigma), k^*)$ . Si  $d = o(\text{Im}(\omega_\sigma))$ , on a  $\text{Im}(\omega_\sigma) = \mu_d \subset k^*$ . Considérons le sous-groupe  $H = \ker(\omega_\sigma)$ , on a alors  $\text{Cen}_G(\sigma)/H \simeq \mu_d$  et l'extension  $L^H/L_\sigma$  est cyclique de degré  $d$ . Comme  $\mu_d \subset k^*$  et que  $d$  est premier à la caractéristique de  $k$  (puisque  $\#\mu_d = d$ ), l'extension  $L^H/L_\sigma$  est kummérienne et il existe donc un élément  $\alpha \in k^*$  tel que  $\ell = \sqrt[d]{\alpha} \in L^H$  soit un élément primitif. On

considère alors l'épimorphisme canonique

$$\begin{aligned} \varphi : G = \text{Gal}(L/L_\sigma) &\longrightarrow \frac{\mu_d}{\ell^g} \\ g &\longrightarrow \frac{\ell^g}{\ell} \end{aligned}$$

Puisque  $\omega_\sigma$  et  $\varphi$  ont même noyau  $H$ , il existe  $\theta \in \text{Aut}(\mu_d)$  tel que  $\omega_\sigma = \theta \circ \varphi$ .

Comme  $\text{Aut}(\mu_d) \simeq (\mathbb{Z}/d\mathbb{Z})^*$ , il existe alors  $r \in (\mathbb{Z}/d\mathbb{Z})^*$  tel que  $\theta(\xi) = \xi^r$  pour tout  $\xi \in \mu_d$ . Posons  $\lambda_0 = \ell^r$ , on a alors pour tout  $g \in G$ ,

$$\lambda_0^g = (\ell^r)^g = (\ell^g)^r = \varphi(g)^r \ell^r = \theta \circ \varphi(g) \lambda_0 = \omega_\sigma(g) \lambda_0$$

Prenons maintenant un élément  $g \in G$  quelconque et posons

$$\lambda_{g\sigma g^{-1}} = \frac{\lambda_0^g}{\omega_\sigma(g)}$$

Cette définition est sans ambiguïté car, si  $g, g' \in G$  sont tels que  $g\sigma g^{-1} = g'\sigma g'^{-1}$ , alors il existe  $h \in \text{Cen}_G(\sigma)$  tel que  $g' = gh$  et donc

$$\begin{aligned} \frac{\lambda_0^{g'}}{\omega_\sigma(g')} &= \frac{\lambda_0^{gh}}{\omega_\sigma(gh)} = \frac{(\lambda_0^h)^g}{\omega_\sigma(g)\omega_\sigma(h)} \quad (\text{d'après le lemme 3.2}) \\ &= \lambda_0^g \frac{\omega_\sigma(h)^g}{\omega_\sigma(g)\omega_\sigma(h)} = \frac{\lambda_0^g}{\omega_\sigma(g)} \end{aligned}$$

Vérifions maintenant que  $x = \sum_{g \in \widehat{\sigma}} \lambda_{g\sigma g^{-1}} a_{g\sigma g^{-1}}$  est bien un élément de  $E_\sigma^G$ . Si  $g_0 \in G$ , alors pour tout  $g \in \widehat{\sigma}$ , on a

$$\begin{aligned} \lambda_{g_0\sigma g_0^{-1}}^{g_0} &= \frac{\lambda_0^{g_0 g_0}}{\omega_\sigma(g_0)} = \lambda_{g_0\sigma g_0^{-1} g_0^{-1}} \frac{\omega_\sigma(g_0 g_0)}{\omega_\sigma(g_0)} \\ &= \lambda_{g_0\sigma g_0^{-1} g_0^{-1}} \frac{\omega_{g_0\sigma g_0^{-1}}(g_0)\omega_\sigma(g_0)}{\omega_\sigma(g_0)} \quad (\text{d'après le lemme 3.2}) \\ &= \lambda_{g_0\sigma g_0^{-1} g_0^{-1}} \omega_{g_0\sigma g_0^{-1}}(g_0) \end{aligned}$$

et donc  $x$  vérifie bien la condition  $(SG)$ . Ainsi, on a bien

$$E_\sigma^G = \text{Vect}_{L_\sigma}(u) \text{ avec } u = \sum_{g \in \widehat{\sigma}} \frac{\lambda_0^g}{\omega_\sigma(g)} a_{g\sigma g^{-1}}$$

où  $\lambda_0 \in L$  est un élément non nul qui vérifie  $\lambda_0^g = \lambda_0 \omega_\sigma(g)$  pour tout  $g \in \text{Cen}_G(\sigma)$ . On remarque que, réciproquement, pour n'importe quel choix de  $\lambda_0 \in L$  non nul vérifiant que pour tout  $g \in \text{Cen}_G(\sigma)$  on ait  $\lambda_0^g = \lambda_0 \omega_\sigma(g)$ , l'élément  $u = \sum_{g \in \widehat{\sigma}} \frac{\lambda_0^g}{\omega_\sigma(g)} a_{g\sigma g^{-1}}$  engendre bien sur  $L_\sigma$  l'espace  $E_\sigma^G$ .

On déduit de cela que

$$\dim_k(E_\sigma^G) = \dim_k(L_\sigma)\dim_{L_\sigma}(E_\sigma^G) = [G : \text{Cen}_G(\sigma)]$$

et donc, l'équation des classes permet d'écrire

$$\dim_k \mathfrak{A}_f^G = \dim_k \bigoplus_{\sigma \in G_{\text{conj}}} E_\sigma^G = \sum_{\sigma \in G_{\text{conj}}} [G : \text{Cen}_G(\sigma)] = o(G)$$

□

Abordons maintenant l'étude du centre  $\mathfrak{A}_f^G$  et établissons préalablement deux lemmes à cette fin.

**Lemme 3.5.** *Posons  $n = o(G)$ . Il existe une  $L$ -base,  $(e_1, \dots, e_n)$ , de  $L^n$  telle que si l'on pose pour  $i = 1, \dots, n$ ,  $e_i = (\lambda_\sigma^{(i)})_{\sigma \in G}$  alors  $\sum_{\sigma \in G} \lambda_\sigma^{(i)} a_\sigma \in \mathfrak{A}_f^G$ .*

*Démonstration.* Posons  $G_{\text{conj}} = \{\sigma_1, \dots, \sigma_r\}$  et, pour tout  $i \in \{1, \dots, r\}$ ,  $\hat{\sigma}_i = \{g_{i,1}, \dots, g_{i,h_i}\}$  (on convient que  $g_{i,1} = e$ ). Pour  $i \in \{1, \dots, r\}$  fixé, on considère un élément non nul

$$x = \sum_{j=1}^{h_i} \lambda_{g_{i,j}\sigma_i g_{i,j}^{-1}} a_{g_{i,j}\sigma_i g_{i,j}^{-1}} \in E_{\sigma_i}^G$$

On sait qu'aucun des  $\lambda_{g_{i,j}\sigma_i g_{i,j}^{-1}}$  n'est nul, et que pour tout  $j = 1, \dots, h_i$ , on a

$$\lambda_{g_{i,j}\sigma_i g_{i,j}^{-1}} = \frac{\lambda_{\sigma_i}^{g_{i,j}}}{\omega_{\sigma_i}(g_{i,j})}$$

Comme  $h_i = [G : \text{Cen}_G(\sigma)]$ , on a  $h_i = \dim_k L_{\sigma_i}$  et l'on considère  $\{\alpha_1, \dots, \alpha_{h_i}\}$  une  $k$ -base de  $L_{\sigma_i}$ . Pour tout  $s = 1, \dots, h_i$ , on pose

$$(e_{\sigma_i})_s = \left( \frac{(\alpha_s \lambda_{\sigma_i})^{g_{i,1}}}{\omega_{\sigma_i}(g_{i,1})}, \dots, \frac{(\alpha_s \lambda_{\sigma_i})^{g_{i,h_i}}}{\omega_{\sigma_i}(g_{i,h_i})} \right) \in L^{h_i}$$

On remarque que  $\sum_{j=1}^{h_i} \frac{(\alpha_s \lambda_{\sigma_i})^{g_{i,j}}}{\omega_{\sigma_i}(g_{i,j})} a_{g_{i,j}\sigma_i g_{i,j}^{-1}} = \alpha_s \cdot x \in E_\sigma^G$  (structure de  $L_\sigma$ -espace vectoriel de  $E_\sigma^G$  introduite dans le théorème 3.4) et donc le vecteur  $(e_{\sigma_i})_s$  est à coordonnées dans  $E_\sigma^G$ . On a, par ailleurs,

$$\det(\{(e_{\sigma_i})_s\}_{1 \leq s \leq h_i}) = \prod_{j=1}^{h_i} \frac{\lambda_{\sigma_i}^{g_{i,j}}}{\omega_{\sigma_i}(g_{i,j})} \begin{vmatrix} \alpha_1^{g_{i,1}} & \dots & \alpha_1^{g_{i,h_i}} \\ \vdots & & \vdots \\ \alpha_s^{g_{i,1}} & \dots & \alpha_s^{g_{i,h_i}} \end{vmatrix}$$

GROUPES TOTAUX

Ce dernier déterminant est certainement non nul, car si tel était le cas, il existerait une équation de  $L$ -dépendance linéaire pour les  $g_{i,1}, \dots, g_{i,h_i} \in \text{Isom}_k(L_{\sigma_i}, L)$ , ce qui est contraire au lemme de Dedekind.

Ainsi, la famille  $\{(e_{\sigma_i})_s\}_{1 \leq s \leq h_i}$  est une  $L$ -base de  $L^{h_i}$ . On rajoute alors des zéros aux coordonnées manquantes des vecteurs  $(e_{\sigma_i})_s$ ,

$$(e_{\sigma_i})_s = \left( \overbrace{0, \dots, 0}^{\# \hat{\sigma}_1}, \dots, \frac{(\alpha_s \lambda_{\sigma_i})^{g_{i,1}}}{\omega_{\sigma_i}(g_{i,1})}, \dots, \frac{(\alpha_s \lambda_{\sigma_i})^{g_{i,h_i}}}{\omega_{\sigma_i}(g_{i,h_i})}, \dots, \dots, \overbrace{0, \dots, 0}^{\# \hat{\sigma}_r} \right)$$

et  $\{(e_{\sigma_i})_s\}_{1 \leq s \leq h_i}$  devient alors une famille  $L$ -libre de  $L^n$ .

La famille  $\{(e_{\sigma_i})_s\}_{1 \leq i \leq r, 1 \leq s \leq h_i}$  est visiblement une famille  $L$ -libre de  $L^n$  satisfaisant aux conditions demandées, mais comme cette dernière est de cardinal

$$\sum_{i=1}^r h_i = \sum_{\sigma \in G_{\text{conj}}} [G : \text{Cen}_G(\sigma)] = o(G) = n$$

on en déduit finalement qu'il s'agit bien d'une base. □

Notons maintenant  $\mathfrak{A}_f(k) = \bigoplus_{\sigma \in G} k a_{\sigma}$  (c'est une sous-algèbre de  $\mathfrak{A}_f$  puisque  $f$  est à valeurs dans  $k^*$ ) et considérons, pour  $\sigma \in G$ ,

$$E_{\sigma}^G(k) = E_{\sigma}^G \cap \mathfrak{A}_f(k)$$

**Lemme 3.6.** *Pour tout  $\sigma \in G$ ,  $E_{\sigma}^G(k)$  est un  $k$ -espace vectoriel de dimension 0 ou 1 et l'on a*

$$\dim_k E_{\sigma}^G(k) = 1 \iff \omega_{\sigma|_{\text{Cen}_G(\sigma)}} \equiv 1$$

*Démonstration.* L'ensemble  $E_{\sigma}^G(k)$  est visiblement un  $k$ -espace vectoriel (intersection de deux  $k$ -espaces vectoriels). Un élément  $x \in E_{\sigma}^G(k)$  s'écrit

$$x = \sum_{g \in \hat{\sigma}} \lambda_{g\sigma g^{-1}} a_{g\sigma g^{-1}} = \sum_{g \in \hat{\sigma}} \frac{\lambda_{\sigma}^g}{\omega_{\sigma}(g)} a_{g\sigma g^{-1}} = \lambda_{\sigma} \sum_{g \in \hat{\sigma}} \frac{1}{\omega_{\sigma}(g)} a_{g\sigma g^{-1}}$$

ce qui prouve que  $E_{\sigma}^G(k)$  est au plus une droite vectorielle.

Supposons que  $E_{\sigma}^G(k) \neq \{0\}$  et considérons un élément  $\lambda_{\sigma} \in k^*$  tel que  $\lambda_{\sigma} \sum_{g \in \hat{\sigma}} \frac{1}{\omega_{\sigma}(g)} a_{g\sigma g^{-1}} \in E_{\sigma}^G(k)$ . Pour tout  $g \in \text{Cen}_G(\sigma)$ , on a

$$\lambda_{\sigma} = \lambda_{\sigma}^g = \lambda_{g\sigma g^{-1}} \omega_{\sigma}(g) = \lambda_{\sigma} \omega_{\sigma}(g)$$

et donc  $\omega_{\sigma}(g) = 1$ .

Réciproquement, supposons que  $\omega_{\sigma|_{\text{Cen}_G(\sigma)}} \equiv 1$ . Le choix de  $\lambda_0 = 1$  dans le théorème 3.4 montre que

$$E_{\sigma}^G = \left\{ \sum_{g \in \widehat{\sigma}} \frac{\lambda^g}{\omega_{\sigma}(g)} a_{g\sigma g^{-1}} / \lambda \in L_{\sigma} \right\}$$

et donc, on en déduit que

$$E_{\sigma}^G(k) = k \cdot \left( \sum_{g \in \widehat{\sigma}} \frac{1}{\omega_{\sigma}(g)} a_{g\sigma g^{-1}} \right) \neq \{0\}.$$

□

**Théorème 3.7.** *On a  $Z(\mathfrak{A}_f^G) = \mathfrak{A}_f^G \cap \mathfrak{A}_f(k) = \bigoplus_{\sigma \in G_{\text{conj}}} E_{\sigma}^G(k)$ , en conséquence de quoi, on a  $\dim_k Z(\mathfrak{A}_f^G) = \#S$  où  $S = \{\sigma \in G_{\text{conj}} / \omega_{\sigma|_{\text{Cen}_G(\sigma)}} \equiv 1\}$ .*

*Démonstration.* Soit  $y = \sum_{\tau \in G} \mu_{\tau} a_{\tau} \in \mathfrak{A}_f^G$ , on a

$$\begin{aligned} y \in Z(\mathfrak{A}_f^G) &\iff \forall x = \sum_{\sigma \in G} \lambda_{\sigma} a_{\sigma} \in \mathfrak{A}_f^G, \quad xy = yx \\ &\iff \sum_{\sigma, \tau \in G} \lambda_{\sigma} \mu_{\tau}^{\sigma} f(\sigma, \tau) a_{\sigma\tau} = \sum_{\sigma, \tau \in G} \lambda_{\sigma}^{\tau} \mu_{\tau} f(\tau, \sigma) a_{\tau\sigma} \\ &\iff \sum_{\sigma, \tau \in G} \lambda_{\sigma} \mu_{\tau}^{\sigma} f(\sigma, \tau) a_{\sigma\tau} = \sum_{\sigma, \tau \in G} \lambda_{\tau\sigma\tau^{-1}} \mu_{\tau} f(\tau\sigma\tau^{-1}, \tau) a_{\tau\sigma} \\ &\iff \sum_{\rho \in G} \left( \sum_{\sigma \in G} \lambda_{\sigma} \mu_{\sigma^{-1}\rho}^{\sigma} f(\sigma, \sigma^{-1}\rho) \right) a_{\rho} = \sum_{\rho \in G} \left( \sum_{\tau \in G} \lambda_{\rho\tau^{-1}} \mu_{\tau} f(\rho\tau^{-1}, \tau) \right) a_{\rho} \\ &\iff \forall \rho \in G, \quad \sum_{\sigma \in G} \lambda_{\sigma} \mu_{\sigma^{-1}\rho}^{\sigma} f(\sigma, \sigma^{-1}\rho) = \sum_{\tau \in G} \lambda_{\rho\tau^{-1}} \mu_{\tau} f(\rho\tau^{-1}, \tau) \\ &\iff \forall \rho \in G, \quad \sum_{\sigma \in G} \lambda_{\sigma} \mu_{\sigma^{-1}\rho}^{\sigma} f(\sigma, \sigma^{-1}\rho) = \sum_{\sigma \in G} \lambda_{\sigma} \mu_{\sigma^{-1}\rho} f(\sigma, \sigma^{-1}\rho) \\ &\quad \text{(On a effectué le changement de variables } \sigma = \rho\tau^{-1}\text{)} \\ &\iff \forall \rho \in G, \quad \sum_{\sigma \in G} \lambda_{\sigma} f(\sigma, \sigma^{-1}\rho) \left( \mu_{\sigma^{-1}\rho}^{\sigma} - \mu_{\sigma^{-1}\rho} \right) = 0 \end{aligned}$$

On en déduit que pour tout  $x = \sum_{\sigma \in G} \lambda_{\sigma} a_{\sigma} \in \mathfrak{A}_f^G$ , le vecteur  $(\lambda_{\sigma})_{\sigma \in G} \in L^n$  est solution du système linéaire défini par l'ensemble de constantes

$$\left\{ f(\sigma, \sigma^{-1}\rho) \left( \mu_{\sigma^{-1}\rho}^{\sigma} - \mu_{\sigma^{-1}\rho} \right) \right\}_{\sigma, \rho}$$

Le lemme 3.5 affirmant qu'il existe une  $L$ -base de  $L^n$  constitué de vecteurs  $(\lambda_\sigma)_{\sigma \in G} \in L^n$  tel que  $\sum_{\sigma \in G} \lambda_\sigma a_\sigma \in \mathfrak{A}_f^G$ , on en déduit que toutes les constantes du système sont nulles. Ainsi, on a

$$y \in Z(\mathfrak{A}_f^G) \iff \forall \rho, \sigma \in G, f(\sigma, \sigma^{-1}\rho) (\mu_{\sigma^{-1}\rho}^\sigma - \mu_{\sigma^{-1}\rho}) = 0$$

ce qui équivaut, après le changement de variables  $\tau = \sigma^{-1}\rho$ , à

$$y = \sum_{\tau \in G} \mu_\tau a_\tau \in Z(\mathfrak{A}_f^G) \iff \forall \sigma, \tau \in G, \mu_\tau^\sigma = \mu_\tau$$

ce qui prouve que  $Z(\mathfrak{A}_f^G) = \mathfrak{A}_f^G \cap \mathfrak{A}_f(k) = \bigoplus_{\sigma \in G_{\text{conj}}} E_\sigma^G(k)$ . La suite du théorème découle immédiatement du lemme 3.6.  $\square$

**Corollaire 3.8.** *Si  $G$  n'est pas abélien, alors l'algèbre  $\mathfrak{A}_f^G$  n'est pas commutative.*

*Démonstration.* Si  $G$  n'est pas abélien, alors  $G_{\text{conj}}$  compte strictement moins d'éléments que  $G$  et donc  $\dim_k Z(\mathfrak{A}_f^G) < o(G)$ . Le théorème 3.4 affirme que  $\dim_k \mathfrak{A}_f^G = o(G)$ , ce qui prouve le corollaire.  $\square$

**Cas où  $G$  est abélien.** Dans le cas où  $G$  est abélien, l'application  $(\sigma, g) \mapsto \omega_\sigma(g)$  est donc un homomorphisme de groupes relativement à chaque variable  $\sigma$  et  $g$ . On en déduit que cette application est un élément de  $Z^2(G, k^*)$  (l'action de  $G$  sur  $k^*$  étant triviale). En particulier, l'application  $(g, h) \mapsto f(h, g)$  est aussi un élément de  $Z^2(G, k^*)$ .

En appliquant ce qui précède, pour  $\sigma \in G$  fixé, on peut écrire  $E_\sigma^G = A_\sigma a_\sigma$  avec  $A_\sigma = \{\lambda \in L / \forall g \in G, \lambda^g = \lambda \omega_\sigma(g)\}$  qui est un  $k$ -espace vectoriel de dimension 1 et l'on a  $\mathfrak{A}_f^G = \bigoplus_{\sigma \in G} A_\sigma a_\sigma$ . Le noyau du morphisme

$\omega : \sigma \mapsto \omega_\sigma$  est constitué des éléments  $\sigma \in G$  vérifiant  $A_\sigma = k$ . Ainsi, on a  $\sigma \in \ker(\omega)$  si et seulement si  $A_\sigma = k$ . Dans le cas abélien, on a donc

$$Z(\mathfrak{A}_f^G) = \bigoplus_{\sigma \in \ker(\omega)} A_\sigma a_\sigma = \bigoplus_{\sigma \in \ker(\omega)} k a_\sigma$$

En particulier,  $\dim_k Z(\mathfrak{A}_f^G)$  divise  $o(G)$ , mais on peut être plus précis sur ce point :

**Proposition 3.9.** *Si  $G$  est un groupe abélien alors  $o(G)/\dim_k Z(\mathfrak{A}_f^G)$  est un carré parfait.*



*Démonstration.* L'application  $\omega$  est une forme bilinéaire alternée et la dimension  $\dim_k Z(\mathfrak{A}_f^G)$  est égale à l'ordre du noyau de  $\omega$ . La forme  $\omega$  induit sur le groupe quotient  $A = G/\ker(\omega)$  une forme bilinéaire alternée non dégénérée. On sait alors (voir par exemple [1]) qu'il existe un sous-groupe isotropique  $A_0$  tel que  $A \cong A_0 \times \widehat{A_0}$ , où  $\widehat{A_0}$  désigne le groupe des caractères de  $A_0$ . En particulier, on a  $o(A) = o(A_0)^2$  et notre proposition découle alors de cette propriété.  $\square$

Lorsque  $G = C_n$  est cyclique, il est célèbre que

$$H^2(G, L^*) \simeq k^*/N(L^*)$$

et que tout 2-cocycle est cohomologue à un cocycle paramétré par des éléments de  $k^*/N(L^*)$  et donc à valeurs dans  $k^*$ . Ces cocycles sont donc tous éléments de  $Z^2(G, k^*)$  si bien que l'application naturelle  $H^2(G, k^*) \rightarrow H^2(G, L^*)$  est surjective.

Par ailleurs, les éléments de  $Z^2(G, k^*)$  sont symétriques (i.e.  $\forall g, h \in G, f(g, h) = f(h, g)$ ). On en déduit que

**Proposition 3.10.** *Si  $G$  est cyclique, alors pour toute extension galoisienne  $L/k$  de groupe  $G$  et pour tout  $f \in Z^2(G, L^*)$ ,  $G$  se relève à  $\text{Aut}_k(\mathfrak{A}_f)$  et l'on a*

$$\mathfrak{A}_f^G = Z(\mathfrak{A}_f^G) = \bigoplus_{\sigma} ka_{\sigma}$$

Pour les groupes abéliens de rang  $\geq 2$ , les choses se compliquent. Le calcul machine montre que, même dans le cas non cyclique, les dimensions possibles pour  $Z(\mathfrak{A}_f^G)$  n'atteignent pas nécessairement tous les entiers  $o(G)/d^2$  pour les  $d^2|o(G)$ . Nous donnons ici quelques résultats numériques :

$G$	$C_2^2$	$C_2 \times C_4$	$C_3^2$	$C_2 \times C_6$	$C_2 \times C_8$
$o(G)$	4	8	9	12	16
$\dim_k Z(\mathfrak{A}_f^G)$	1 ou 4	2 ou 8	1 ou 9	3 ou 12	4 ou 16
$G$	$C_4^2$	$C_3 \times C_6$	$C_2 \times C_{10}$	$C_2 \times C_{12}$	$C_4 \times C_6$
$o(G)$	16	18	20	24	24
$\dim_k Z(\mathfrak{A}_f^G)$	1, 4 ou 16	2 ou 18	5 ou 20	6 ou 24	6 ou 24

GROUPES TOTAUX

$G$	$C_5^2$	$C_3 \times C_9$	$C_2 \times C_{14}$	$C_2 \times C_{16}$	$C_4 \times C_8$
$o(G)$	25	27	28	32	32
$\dim_k Z(\mathfrak{A}_f^G)$	1 ou 25	3 ou 27	7 ou 28	8 ou 32	2, 8 ou 32
$G$	$C_6^2$	$C_2^3$	$C_2^2 \times C_4$	$C_2^2 \times C_6$	$C_3^3$
$o(G)$	36	8	16	24	27
$\dim_k Z(\mathfrak{A}_f^G)$	1, 4, 9 ou 36	2 ou 8	4 ou 16	6 ou 24	3 ou 27
$G$	$C_2 \times C_4^2$	$C_2^2 \times C_8$	$C_2^4$	$C_2^3 \times C_4$	$C_2^5$
$o(G)$	32	32	16	32	32
$\dim_k Z(\mathfrak{A}_f^G)$	2, 8 ou 32	8 ou 32	1, 4 ou 16	2, 8 ou 32	2, 8 ou 32

On remarque que dans ce tableau, pour les groupes d'ordre 32,  $G = C_2 \times C_{16}$  et  $G = C_2^2 \times C_8$ , la dimension 2 n'est pas atteinte (alors que  $2 = 32/(4)^2$ ) et que pour le groupe d'ordre 16,  $G = C_2^2 \times C_4$ , la dimension 1 n'est pas atteinte (alors que  $1 = 16/(4)^2$ ).

**Note :** Dans le tableau ci dessus, ainsi que dans tous les tableaux numériques du même acabit que nous donnerons dans la suite de ce texte, les dimensions indiquées pour  $Z(\mathfrak{A}_f^G)$  sont toutes atteintes pour un bon choix de  $f$ . Ces résultats numériques sont obtenus par calcul formel sous le logiciel maxima.

## 4. Totalité.

### 4.1. Généralités.

La dimension du centre de  $\mathfrak{A}_f^G$  est intimement liée à l'arithmétique du groupe  $G$ . Nous allons maintenant étudier les groupes pour lesquels cette dimension est toujours maximale :

**Définition 4.1.** Soit  $k$  un corps et  $G$  un groupe fini se réalisant comme groupe de Galois sur  $k$ . On dit que  $G$  est total pour  $k$  si, pour toute extension galoisienne  $L/k$  de groupe  $G$  et tout élément  $f \in \text{Im}(H^2(G, k^*) \rightarrow H^2(G, L^*))$ , la dimension de  $Z(\mathfrak{A}_f^G)$  (pour n'importe quel relevé de  $G$ ) est maximale (i.e. égale au nombre de classes de conjugaison de  $G$ ).

Par exemple, conséquemment à l'étude mené sur le groupe de Klein dans le paragraphe 1, on voit que si ce dernier se réalise sur un corps  $k$  alors il est total pour  $k$  si et seulement si  $k$  est de caractéristique 2.

La totalité équivaut donc à dire que l'application  $f \mapsto \dim_k \mathbb{Z}(\mathfrak{A}_f^G)$  est constante, puisque le choix pour  $f$  du cocycle trivial donne pour  $\dim_k \mathbb{Z}(\mathfrak{A}_f^G)$  une valeur maximale. L'étude précédente montre que la totalité d'un groupe  $G$  pour un corps  $k$  ne dépend pas du corps  $L$  qui réalise  $G$ . Si  $G$  se réalise comme groupe de Galois sur  $k$ , la question de sa totalité pour  $k$  est équivalente à (avec les notations des paragraphes précédents)

$$(T) \quad \forall f \in \mathbb{Z}^2(G, k^*), \forall \sigma \in G, \omega_{\sigma|_{\text{Cen}_G(\sigma)}} \equiv 1$$

La propriété (T) existe indépendamment du fait que  $G$  se réalise sur  $k$ . Quand un groupe  $G$  satisfait à la condition (T) pour tous les corps  $k$ , on dira que  $G$  est *vraiment total*. Plus globalement, étant donné un groupe  $G$  et un élément  $\sigma \in G$ , on dira que  $\sigma$  est *vraiment total* si

$$\forall k \text{ corps}, \forall f \in \mathbb{Z}^2(G, k^*), \forall g \in \text{Cen}_G(\sigma), \omega_{\sigma}(g) = 1$$

On considérera alors *l'ensemble de totalité* de  $G$  :

$$T_G = \{\sigma \in G / \sigma \text{ vraiment total}\}$$

Cet ensemble étant stable par l'action de conjugaison, on notera  $\tilde{T}_G$  le quotient de  $T_G$  par cette action. Dire que  $G$  est vraiment total équivaut à dire que  $T_G = G$  et, sous cette condition, la dimension (toujours maximale) de  $\mathbb{Z}(\mathfrak{A}_f^G)$  vaut exactement  $\sharp \tilde{T}_G = \sharp G_{\text{conj}}$ . Ceci incite à considérer, en toute généralité, l'entier  $\sharp \tilde{T}_G$  que nous appelons *ordre de totalité* du groupe  $G$ .

**Proposition 4.2.** *Le groupe  $\text{Aut}(G)$  agit (par restriction) sur l'ensemble  $T_G$  et, par suite, le groupe des automorphismes extérieurs de  $G$ ,  $\text{Out}(G)$ , agit naturellement sur l'ensemble  $\tilde{T}_G$ . En conséquence de quoi, si  $G$  est abélien,  $T_G$  est un sous-groupe caractéristique de  $G$ .*

*Démonstration.* Commençons par remarquer que si  $f \in \mathbb{Z}^2(G, k^*)$  et  $\varphi \in \text{Aut}(G)$  alors l'application

$$\begin{aligned} f^\varphi : G \times G &\longrightarrow k^* \\ (g, h) &\longmapsto f(\varphi(g), \varphi(h)) \end{aligned}$$

est bien un élément de  $\mathbb{Z}^2(G, k^*)$  (ce fait est immédiat, une fois pris en compte que l'action de  $G$  sur  $k^*$  est triviale). Il s'agit de montrer que si  $\sigma \in G$  est vraiment total alors  $\varphi(\sigma)$  l'est aussi pour tout  $\varphi \in \text{Aut}(G)$ . Pour  $f \in \mathbb{Z}^2(G, k^*)$ , on notera  $\omega_\sigma^f$  l'application  $\omega_\sigma$  relative au choix de  $f$ . Comme  $\text{Cen}_G(\varphi(\sigma)) = \varphi(\text{Cen}_G(\sigma))$ , pour tout  $h \in \text{Cen}_G(\sigma)$ , on a

$$\omega_{\varphi(\sigma)}^f(\varphi(h)) = \omega_\sigma^{f^\varphi}(h)$$

Si  $\sigma$  est supposé vraiment total, alors  $\omega_\sigma^{f^\sigma} \equiv 1$  sur  $\text{Cen}_G(\sigma)$ . On en déduit que  $\omega_{\varphi(\sigma)}^f \equiv 1$  sur  $\text{Cen}_G(\varphi(\sigma))$  et ce, en toute généralité sur  $f \in Z^2(G, k^*)$ . L'élément  $\varphi(\sigma)$  est donc lui aussi vraiment total.  $\square$

Nous avons vu (proposition 3.10) que les groupes cycliques étaient des groupes vraiment totaux. Cette propriété va permettre de construire d'autres exemples.

**Proposition 4.3.** *Soit  $G$  un groupe fini de centre  $Z(G)$ . Si  $Z(G)$  est vraiment total et si, pour tout  $\sigma \in G - Z(G)$ , le centralisateur  $\text{Cen}_G(\sigma)$  de  $\sigma$  est vraiment total, alors  $G$  est vraiment total.*

*Démonstration.* Considérons un corps  $k$ , un 2-cocycle  $f \in Z^2(G, k^*)$ , un élément  $\sigma \in G$  et un sous-groupe  $G'$  contenant  $\sigma$ . L'application de restriction  $Z^2(G, k^*) \rightarrow Z^2(G', k^*)$  associée à  $f$  un élément  $f' \in Z^2(G', k^*)$  et les fonctions  $\omega_\sigma$  associées à  $f$  et à  $f'$  coïncident sur  $G'$ .

Prenons un élément  $\sigma \in G - Z(G)$  et posons  $G' = \text{Cen}_{G'}(\sigma)$ . Puisque  $G'$  est vraiment total par hypothèse, on en déduit que  $\omega_\sigma$  est trivial sur  $G'$ .

Prenons maintenant un élément  $\sigma \in Z(G)$  et un élément quelconque  $g \in G$ . Et distinguons deux cas :

- $g \notin Z(G)$ , on  $\sigma \in \text{Cen}_G(g)$  et alors

$$\omega_\sigma(g) = \frac{f(\sigma, g)}{f(g, \sigma)} = \frac{1}{\omega_g(\sigma)} = 1$$

d'après ce qui précède.

- $g \in Z(G)$ , puisque  $Z(G)$  est supposé vraiment total, on a  $\omega_\sigma(g) = 1$ .

On en déduit finalement que  $G$  est vraiment total.  $\square$

**Corollaire 4.4.** *Si  $n$  désigne un entier radicalaire (i.e.  $n$  est produit de nombres premiers distincts deux à deux) alors tout groupe d'ordre  $n$  est vraiment total.*

*Démonstration.* La preuve va s'effectuer par récurrence sur la longueur  $k$  de l'entier radicalaire  $n = p_1 \cdots p_k$ .

Pour  $k = 1$ , un groupe d'ordre  $n = p_1$  est cyclique et donc, d'après la proposition 3.10, est total.

Supposons la propriété vraie pour jusqu'au rang  $k \geq 1$  et considérons un groupe  $G$  d'ordre  $n = p_1 \cdots p_{k+1}$  radicalaire.

Le centre  $Z(G)$  de  $G$  est d'ordre divisant  $n$  et est donc d'ordre un produit de nombres premiers distincts deux à deux. Le centre  $Z(G)$  étant abélien, il est donc cyclique et par conséquent vraiment total.

Considérons maintenant un élément  $\sigma \in G - Z(G)$ . Le centralisateur  $\text{Cen}_G(\sigma)$  de  $\sigma$  est un sous-groupe strict de  $G$  d'ordre divisant  $n$ . Cet ordre est donc égal à un produit d'au plus  $k$  nombres premiers distincts deux à deux et, par hypothèse de récurrence, c'est donc un groupe vraiment total. La proposition 4.3 assure alors que  $G$  est vraiment total.  $\square$

Ce corollaire fournit déjà une vaste famille de groupes totaux. Nous allons nous intéresser dans la suite de ce texte à une autre famille de groupes totaux : *les groupes quasi-CC*.

**Définition 4.5.** Un groupe  $G$  sera dit de type CC (sigle pour "centralisateurs cycliques") si pour tout  $g \in G - \{e\}$ , le centralisateur  $\text{Cen}_G(g)$  de  $g$  dans  $G$  est un groupe cyclique.

Plus généralement, on dira de  $G$  qu'il est *quasi-CC* si son centre,  $Z(G)$ , est un groupe cyclique et si pour tout  $g \in G - Z(G)$ , le centralisateur  $\text{Cen}_G(g)$  de  $g$  dans  $G$  est un groupe cyclique.

Les groupes de type CC sont bien sûr quasi-CC. En effet, si  $G$  est un groupe de type CC possédant un centre non-trivial, alors le centralisateur de n'importe quel élément  $\neq e$  de ce centre vaut  $G$  et donc  $G$  est cyclique.

Les propositions 3.10 et 4.3 impliquent immédiatement qu'un groupe quasi-CC est vraiment total. Tout groupe  $G$  d'ordre  $pq$ , un produit de deux nombres premiers  $p \neq q$ , est quasi-CC. En effet, si  $G$  est abélien alors il est cyclique et si  $G$  est non abélien, le centre  $Z(G)$  de  $G$  est donc d'ordre 1,  $p$  ou  $q$  et donc dans tous les cas est cyclique. Si l'on prend maintenant un élément  $g \in G - Z(G)$ , alors son centralisateur  $\text{Cen}_G(g)$  n'est pas égal à  $G$  et donc, son ordre vaut  $p$  ou  $q$  et est lui aussi cyclique.

## 4.2. Classification des groupes de type CC.

La classification que nous allons établir repose sur plusieurs résultats profonds de théorie des groupes, en particulier la classification des groupes de type CA (même définition que pour CC, mais l'on remplace la condition "centralisateurs cycliques" par "centralisateurs abéliens").

Cette classification des groupes de type CA est due, en plusieurs étapes, à Brauer, Suzuki et Wall (voir [2] et [3]) et a constitué un préliminaire

important au fameux théorème de Feit-Thompson sur la résolubilité des groupes d'ordre impair. Elle se résume ainsi :

**Théorème 4.6.** (*Brauer-Suzuki-Wall*) *Si  $G$  désigne un groupe de type CA, alors  $G$  satisfait une des conditions suivantes :*

- $G$  est abélien.
- $G$  est isomorphe à  $\text{PSL}_2(\mathbb{F}_{2^n})$  pour un certain entier  $n \geq 1$ .
- $G$  est un groupe de Frobenius.

Rappelons qu'un groupe de Frobenius  $G$  peut s'écrire comme produit semi-direct non trivial  $H \rtimes K$  et donc qu'en particulier un groupe de Frobenius n'est jamais simple.

Nous aurons besoin dans la suite de ce texte de deux résultats sur l'arithmétique des groupes de type CA :

1/ Un groupe de type CA est soit simple, soit résoluble (voir [5]).

2/ Un groupe  $G$ , fini, résoluble et de type CA est le produit semi-direct  $H \rtimes F$  où  $F$  est le groupe de Fitting de  $G$  (qui dans cette situation est nécessairement abélien) et  $H$  est un certain sous-groupe de  $\text{Aut}(F)$  (voir [6]-th 9)).

*Notation 4.7.* Pour deux entiers  $n, m \geq 2$  et  $a \in C_m^*$  d'ordre divisant  $n$ , on notera  $C_n \rtimes_a C_m$  le produit semi-direct de  $C_n$  par  $C_m$  où l'action de  $\lambda \in C_n$  sur  $x \in C_m$  est donnée par  $x^\lambda = a^\lambda x$ .

**Théorème 4.8.** *La collection des groupes de type CC est exactement la réunion des trois classes de groupes suivantes :*

- Les groupes cycliques.
- Les groupe spéciaux linéaires projectifs de dimension 2 sur les corps finis de caractéristique 2,  $\text{PSL}_2(\mathbb{F}_{2^n})$ .
- Les produits semi-directs de deux groupes cycliques  $G = C_n \rtimes_a C_m$  où  $a \in C_m^*$  est d'ordre  $n$  et vérifie  $\forall x \in C_n - \{0\}, a^x - 1 \in C_m^*$ .

*Démonstration.* Si  $G$  est un groupe de type CC, il est alors de type CA. On est donc dans une des trois situations suivantes :

1/  $G$  est abélien. Sous cette hypothèse, être de type CC équivaut immédiatement à être cyclique.

2/  $G$  est isomorphe à  $\mathrm{PSL}_2(\mathbb{F}_q)$  pour  $q = 2^n$ . Montrons que, sous cette hypothèse,  $G$  est de type CC.

Remarquons pour commencer que, puisque  $\mathbb{F}_q$  est un corps de caractéristique 2, le groupe  $G$  s'identifie au groupe  $\mathrm{SL}_2(\mathbb{F}_q)$ . Prenons maintenant une matrice  $M \in \mathrm{SL}_2(\mathbb{F}_q)$  et distinguons deux cas :

a) *Le polynôme caractéristique  $P$  de  $M$  est séparable.* Sous cette hypothèse, il existe un entier  $m$  tel que  $P$  se décompose dans  $\mathbb{F}_{q^m}$  et comme  $M$  est de déterminant 1, il existe  $\alpha \in \mathbb{F}_{q^m}^* - \{1\}$  tel que  $M$  soit semblable dans  $\mathrm{SL}_2(\mathbb{F}_{q^m})$  à la matrice diagonale  $D = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}$ . Maintenant, la matrice  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_{q^m})$  commute avec  $D$  si et seulement si  $b = c = 0$ , on en déduit que

$$\mathrm{Cen}_{\mathrm{SL}_2(\mathbb{F}_{q^m})}(D) = \left\{ \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix} / u \in \mathbb{F}_{q^m}^* \right\} \simeq \mathbb{F}_{q^m}^*$$

Comme les matrices  $M$  et  $D$  sont semblables, les groupes  $\mathrm{Cen}_{\mathrm{SL}_2(\mathbb{F}_{q^m})}(D)$  et  $\mathrm{Cen}_{\mathrm{SL}_2(\mathbb{F}_{q^m})}(M)$  sont conjugués et donc  $\mathrm{Cen}_{\mathrm{SL}_2(\mathbb{F}_{q^m})}(M)$  est cyclique. Maintenant,  $\mathrm{Cen}_{\mathrm{SL}_2(\mathbb{F}_q)}(M)$  est un sous-groupe de  $\mathrm{Cen}_{\mathrm{SL}_2(\mathbb{F}_{q^m})}(M)$ , il est par conséquent lui aussi cyclique.

b) *Le polynôme caractéristique  $P$  de  $M$  est inséparable.* Il possède donc une racine double dans  $\overline{\mathbb{F}_q}$ , mais puisque  $M$  est de déterminant 1, cette racine vaut nécessairement 1. Ainsi,  $M$  est semblable à une matrice de  $\mathrm{SL}_2(\mathbb{F}_q)$  de la forme  $T = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$  avec  $\lambda \in \mathbb{F}_q$  (on suppose que  $\lambda \neq 0$ , car on s'intéresse au stabilisateur de  $M \neq I$ ). Maintenant, la matrice  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_q)$  commute avec  $T$  si et seulement si  $c = 0$  et  $a = d$ , on en déduit que

$$\mathrm{Cen}_{\mathrm{SL}_2(\mathbb{F}_q)}(T) = \left\{ \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} / u \in \mathbb{F}_q \right\} \simeq \mathbb{F}_q$$

qui est bien un groupe cyclique. Comme précédemment, on en déduit que le centralisateur  $\mathrm{Cen}_{\mathrm{SL}_2(\mathbb{F}_q)}(M)$  est bien cyclique.

3/  $G$  est un groupe de Frobenius. Dans ces conditions, puisque  $G$  n'est pas simple, il est résoluble d'après [5]. Donc  $G$  est de type CA et est résoluble, ce qui implique d'après [6] qu'il est le produit semi-direct  $H \rtimes F$  avec  $F$

abélien et  $H$  un sous-groupe de  $\text{Aut}(F)$ . Comme  $G$  est de type CC, il en est de même de  $F$  et donc  $F$  est cyclique. On en déduit que  $\text{Aut}(F)$  et donc  $H$  sont abéliens, et comme  $H$  est de type CC, il est lui aussi cyclique. Finalement,  $G$  est de la forme  $G = C_n \rtimes_a C_m$  avec  $a \in C_m^*$  d'ordre divisant  $n$ . Pour finir la preuve, nous allons caractériser les produits  $C_n \rtimes_a C_m$  qui sont de type CC :

**Lemme 4.9.** *Soient  $n, m \geq 2$  des entiers et  $a \in C_m^*$  d'ordre divisant  $n$ . Les conditions suivantes*

*i)  $G = C_n \rtimes_a C_m$  est de type CC,*

*ii)  $\forall x \in C_n - \{0\}, a^x - 1 \in C_m^*$ ,*

*sont équivalentes. Dans ces conditions, on a nécessairement  $o(a) = n$ .*

*Démonstration.* *ii)  $\implies$  i) Il est clair que, sous l'hypothèse ii),  $a$  est d'ordre  $n$ . Soit  $\sigma = (x, y) \in C_n \rtimes_a C_m$  non trivial, le centralisateur  $\text{Cen}_G(\sigma)$  est un groupe cyclique. En effet, soit  $\sigma' = (x', y') \in C_n \rtimes_a C_m$ , on a*

$$\begin{aligned} \sigma' \in \text{Cen}_G(\sigma) &\iff (x, y)(x', y') = (x', y')(x, y) \\ &\iff (x + x', y + a^x y') = (x' + x, y' + a^{x'} y) \\ &\iff y + a^x y' = y' + a^{x'} y \\ &\iff y'(1 - a^x) = y(1 - a^{x'}) \end{aligned}$$

Si  $x = 0$  alors  $y \neq 0$  et donc  $x' = 0$  et ainsi  $\text{Cen}_G(\sigma) = C_m$ .

Si  $x \neq 0$  alors  $y' = y(1 - a^x)^{-1}(1 - a^{x'})$  et donc

$$\text{Cen}_G(\sigma) = \left\{ (\lambda, y(1 - a^x)^{-1}(1 - a^\lambda)) / \lambda \in C_n \right\} \simeq C_n$$

non ii)  $\implies$  non i) Soit  $x_0 \in C_n - \{0\}$  tel que  $a^{x_0} - 1 \notin C_m^*$ . Distinguons deux cas :

1/  $a - 1 \notin C_m^*$ . Considérons alors un entier  $d \neq 0$  divisant  $m$  tel que  $d(a - 1) \equiv 0 \pmod{m}$ . On a alors  $a \equiv 1 \pmod{m/d}$  et donc pour tout  $x$ ,  $a^x \equiv 1 \pmod{m/d}$ , ce qui implique que  $a^x d \equiv d \pmod{m}$ . Pour tout  $(x, h) \in C_n \rtimes_a C_m$ , on a alors

$$(0, d)(x, h) = (x, d + h) = (x, a^x d + h) = (x, h)(0, d)$$

et donc  $C_n \rtimes_a C_m$  a un centre non trivial, ce qui rend impossible le fait qu'il soit de type CC.



2/  $a - 1 \in C_m^*$ . On a donc  $x_0 \neq 1$ . Soit  $d \not\equiv 0 \pmod{m}$  un entier divisant  $m$  tel que  $d(a^{x_0} - 1) \equiv 0 \pmod{m}$ . Pour tout  $x \in C_n$ , on a

$$(x_0, 0)(x, d) = (x_0 + x, a^{x_0}d) = (x + x_0, d) = (x, d)(x_0, 0)$$

et donc le centralisateur de  $(x_0, 0)$  contient le sous-groupe  $\langle (x, d) \rangle_{x \in C_n}$ . Par ailleurs, on a

$$(1, d)(0, -d) = (1, d(1 - a)) \neq (1, 0) = (0, -d)(1, d)$$

ce qui montre que ce centralisateur n'est pas abélien et donc que  $C_n \rtimes_a C_m$  n'est pas de type CC. □

Le lemme 4.9 achève la preuve du théorème 4.8. □

On obtient alors comme corollaires :

**Corollaire 4.10.** *Pour  $n \geq 1$ , les groupes  $\text{PSL}_2(\mathbb{F}_{2^n})$  sont vraiment totaux. Si le groupe  $\text{PSL}_2(\mathbb{F}_{2^n})$  se réalise sur un corps  $k$  alors, pour tout  $f \in \mathbb{Z}^2(\text{PSL}_2(\mathbb{F}_{2^n}), k^*)$ , on a*

$$\dim_k Z(\mathfrak{A}_f^{\text{PSL}_2(\mathbb{F}_{2^n})}) = 2^n + 1$$

*Démonstration.* La totalité de  $\text{PSL}_2(\mathbb{F}_{2^n})$  découle du fait qu'il est de type CC. La preuve de ce corollaire va donc consister en un dénombrement de ses classes de conjugaisons.

Pour  $n = 1$ , on a  $\text{PSL}_2(\mathbb{F}_2) \simeq S_3$  et l'on a vu que  $S_3$  contenait bien  $3 = 2^1 + 1$  classes de conjugaisons. On va donc supposer maintenant que  $n \geq 2$  et l'on va poser  $q = 2^n$ . Puisque nous travaillons en caractéristique 2, on a  $\text{PSL}_2(\mathbb{F}_q) = \text{SL}_2(\mathbb{F}_q)$ . Pour  $M \in M_2(\mathbb{F}_q)$ , on notera  $\Pi_M$  son polynôme caractéristique.

Montrons préalablement deux résultats élémentaires d'algèbre linéaire :

1/ Si  $M, N \in M_2(\mathbb{F}_q)$  sont semblables alors il existe  $P_0 \in \text{SL}_2(\mathbb{F}_q)$  telle que  $M = P_0 N P_0^{-1}$ . Autrement dit, l'orbite de conjugaison d'une matrice de  $M_2(\mathbb{F}_q)$  est la même sous l'action de  $\text{GL}_2(\mathbb{F}_q)$  que sous l'action de  $\text{SL}_2(\mathbb{F}_q)$ .

Cette propriété découle du fait que, puisque  $\mathbb{F}_q$  est de caractéristique 2, alors tous les éléments de  $\mathbb{F}_q$  sont des carrés. Si  $P \in \text{GL}_2(\mathbb{F}_q)$  est telle que  $M = P N P^{-1}$  alors  $P_0 = \frac{1}{\sqrt{\det(P)}} P$  est un élément de  $\text{SL}_2(\mathbb{F}_q)$  qui vérifie  $M = P_0 N P_0^{-1}$ .

2/ Deux matrices  $M, N \in M_2(\mathbb{F}_q)$  sont semblables dans  $M_2(\mathbb{F}_q)$  si et seulement si  $\Pi_M = \Pi_N$ .

## GROUPES TOTAUX

Pour cette propriété, le sens direct est évident. Pour la réciproque, si  $\Pi = \Pi_M = \Pi_N$  est inséparable alors en notant  $\lambda \in M_2(\mathbb{F}_{q^2})$  la racine double de  $\Pi$ , on a que, soit  $M = N = \lambda I$ , soit  $M$  et  $N$  sont semblables à la matrice  $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ . Si  $\Pi$  est séparable, comme c'est un polynôme de degré 2,  $M$  et  $N$  sont diagonalisables dans  $M_2(\mathbb{F}_{q^2})$  et toutes deux semblables à une même matrice diagonale de  $M_2(\mathbb{F}_{q^2})$ . Dans tous les cas,  $M$  et  $N$  sont semblables dans  $M_2(\mathbb{F}_{q^2})$ .

Montrons que cela implique qu'elles le sont aussi dans  $M_2(\mathbb{F}_q)$ . Notons  $\alpha \in \mathbb{F}_{q^2}$  un élément primitif et considérons une matrice  $P \in \text{GL}_2(\mathbb{F}_{q^2})$  tel que  $PM = NP$ . Il existe  $R, Q \in M_2(\mathbb{F}_q)$  tels que  $P = R + \alpha Q$  et par suite on a  $RM = NR$  et  $QM = NQ$  et donc pour tout  $x \in \mathbb{F}_{q^2}$ , on a  $(R + xQ)M = N(R + xQ)$ . L'application  $x \mapsto \det(R + xQ)$  est alors un polynôme de degré au plus 2 qui n'est pas nul (puisque non nul en  $x = \alpha$ ), il possède au plus deux racines, mais comme  $q \geq 4$ , il existe donc  $x \in \mathbb{F}_q$  tel que  $(R + xQ) \in \text{GL}_2(\mathbb{F}_q)$ .

Dénombrons maintenant les classes de conjugaison et considérons une matrice  $M \in \text{SL}_2(\mathbb{F}_q)$ . Distinguons deux cas :

a) Le polynôme  $\Pi_M$  est inséparable. Puisque  $\det(M) = 1$ , on a  $\Pi_M(X) = X^2 - 1$  et donc, soit  $M = I$ , soit  $M$  est semblable à la matrice  $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ . Il y a donc deux classes de conjugaison correspondant à des matrices à polynômes caractéristiques inséparables.

b) Le polynôme  $\Pi_M$  est séparable. Puisque  $d^\circ \Pi_M = 2$  et que  $\det(M) = 1$ , il existe un élément  $\alpha \in \mathbb{F}_{q^2} - \{0, 1\}$  tel que  $\alpha + \alpha^{-1} \in \mathbb{F}_q$  et tel que  $\Pi_M(X) = X^2 - (\alpha + \alpha^{-1})X + 1$ .

Réciproquement, pour tout  $\alpha \in \mathbb{F}_{q^2} - \{0, 1\}$  tel que  $\alpha + \alpha^{-1} \in \mathbb{F}_q$  il existe  $M \in \text{SL}_2(\mathbb{F}_q)$  tel que  $\Pi_M(X) = X^2 - (\alpha + \alpha^{-1})X + 1$ . Pour voir ce fait, il suffit de considérer la matrice de Frobenius  $M = \begin{pmatrix} 0 & -1 \\ 1 & \alpha + \alpha^{-1} \end{pmatrix}$ . Ainsi, l'ensemble des classes de conjugaison des matrices de  $\text{SL}_2(\mathbb{F}_q)$  à polynômes caractéristiques séparables est biunivoquement décrit par l'ensemble  $E_1$  constitué des éléments  $\alpha + \alpha^{-1} \in \mathbb{F}_q$  avec  $\alpha \in \mathbb{F}_{q^2} - \{0, 1\}$ .

On a  $\alpha + \alpha^{-1} = \beta + \beta^{-1}$  si et seulement si  $\alpha = \beta$  ou  $\alpha = \beta^{-1}$ . Comme  $\alpha \neq 1$ , on en déduit que le cardinal de  $E_1$  vaut exactement la moitié du cardinal de l'ensemble  $E_2$  constitué des éléments  $\alpha \in \mathbb{F}_{q^2} - \{0, 1\}$  tels que

$\alpha + \alpha^{-1} \in \mathbb{F}_q$ . Dénombrons ce dernier ensemble : il contient  $\mathbb{F}_q - \{0, 1\}$ , ce qui fait déjà  $q - 2$  éléments. Soit maintenant  $\alpha \in E_2 - \mathbb{F}_q$ . Puisque  $\alpha$  est racine de  $\Pi_M$ , on en déduit que  $\alpha^{-1}$  est le conjugué de  $\alpha$ , ce qui équivaut à dire que  $\alpha^q = \alpha^{-1}$  ou encore que  $\alpha^{q+1} = 1$ . Réciproquement, tout  $\alpha \in \mathbb{F}_{q^2} - \{1\}$  vérifiant  $\alpha^{q+1} = 1$  est un élément de  $E_2 - \mathbb{F}_q$ . Puisque  $\mathbb{F}_{q^2}^*$  est cyclique d'ordre  $q^2 - 1 = (q - 1)(q + 1)$ , il existe un sous-groupe d'ordre  $q + 1$  dans  $\mathbb{F}_{q^2}^*$  et donc, il y a  $q + 1$  éléments de  $\mathbb{F}_{q^2}$  vérifiant  $\alpha^{q+1} = 1$ . Ainsi  $E_2 - \mathbb{F}_q$  compte  $q$  éléments et, par suite,  $E_2$  compte  $2q - 2$  éléments.

Il y a donc  $q - 1$  classes de conjugaison de matrices de  $SL_2(\mathbb{F}_q)$  à polynômes caractéristiques séparables, ce qui, ajouté au 2 autres classes trouvées dans le cas inséparable, donne finalement  $q + 1$  classes de conjugaison dans  $SL_2(\mathbb{F}_q)$ .  $\square$

**Corollaire 4.11.** *Soient  $n, m \geq 2$  des entiers et  $a \in C_m^*$  d'ordre  $o(a) = n$ . Si la condition*

$$\forall x \in C_n - \{0\}, a^x - 1 \in C_m^*$$

*est vérifiée, alors le groupe  $G = C_n \rtimes_a C_m$  est vraiment total.*

*Dans cette situation, si  $G$  se réalise sur un corps  $k$  alors, pour tout  $f \in Z^2(G, k^*)$ , on a*

$$\dim_k Z(\mathfrak{A}_f^G) = n + \frac{m - 1}{n}$$

*Démonstration.* La totalité de  $G$  découle du fait qu'il est de type CC. La preuve de ce corollaire va donc consister en un dénombrement des classes de conjugaison dans  $G$ .

•  $\sigma = (x, 0)$ ,  $x \neq 0$  : pour tout  $y \in C_m$ , on a

$$(0, y)(x, 0)(0, -y) = (x, y(1 - a^x))$$

Comme  $(1 - a^x)$  est un élément inversible de  $C_m$ , on en déduit que  $\{(x, \lambda) / \lambda \in C_m\} \subset \widetilde{(x, 0)}$ .

Comme  $C_n \subset \text{Cen}_G(\sigma)$ , on a  $\#(\widetilde{(x, 0)}) = [G : \text{Cen}_G(\sigma)] \leq m$  et, par suite, on a finalement que

$$\widetilde{(x, 0)} = \{(x, \lambda) / \lambda \in C_m\}$$

Ceci détermine  $n - 1$  classes de conjugaisons paramétrées par les  $x \in C_n$  non nuls.

## GROUPES TOTAUX

•  $\sigma = (0, y)$ ,  $y \neq 0$  : pour tout  $x \in C_n$ , on a

$$(x, 0)(0, y)(-x, 0) = (0, a^x y)$$

Soient  $x, x' \in C_n$  tels que  $a^x y = a^{x'} y$ , ce équivaut à  $y(1 - a^{x-x'}) = 0$ . Si on avait  $x \neq x'$  alors, comme  $(1 - a^{x-x'})$  est inversible, on aurait  $y = 0$ , ce qui est absurde. On en déduit que  $\{(0, a^x y) / x \in C_n\} \subset \widetilde{(0, y)}$  et que cet ensemble compte exactement  $n$  éléments. Puisque  $C_m \subset \text{Cen}_G(\sigma)$ , on a  $\sharp \widetilde{(0, y)} = [G : \text{Cen}_G(\sigma)] \leq n$ . Il s'ensuit que

$$\widetilde{(0, y)} = \{(0, a^x y) / x \in C_n\}$$

Il y a donc  $\frac{m-1}{n}$  classes de conjugaisons paramétrées par les  $y \in C_m$  non nuls. En rajoutant à ce décompte la classe neutre, on obtient bien pour nombre de classes de conjugaison  $n + \frac{m-1}{n}$  dans  $G$ .  $\square$

*Remarque 4.12.* a) Le fait que l'entier  $n$  divise l'entier  $m - 1$  n'est pas du tout naturel, cette propriété découle bien sur du fait que  $\forall x \in C_n - \{0\}$ ,  $a^x - 1 \in C_m^*$ .

b) La condition  $\forall x \in C_n - \{0\}$ ,  $a^x - 1 \in C_m^*$  implique que  $m$  est un entier impair, car dans le cas contraire, on constate que si  $a$  est impair alors  $a - 1$  ne l'est pas et n'est donc pas inversible modulo  $m$ . On peut préciser un peu la condition, en regardant la décomposition en facteurs premiers de  $m$  :

**Lemme 4.13.** *Si  $m = \prod p_i^{r_i}$  est la décomposition en produit de facteurs premiers d'un entier impair  $m \geq 3$ , et si  $a \in C_m^*$  est un élément d'ordre multiplicatif  $o(a) = n$ , alors les propriétés suivantes*

- i) pour tout  $x \in C_n - \{0\}$ ,  $a^x - 1 \in C_m^*$ ,*
  - ii) pour tout indice  $i$ , l'ordre multiplicatif de  $a$  modulo  $p_i^{r_i}$  vaut  $n$  et  $n | p_i - 1$ ,*
- sont équivalentes.*

*Démonstration.* *i)  $\implies$  ii)* L'isomorphisme  $C_m^* \simeq \prod C_{p_i^{r_i}}^*$  assure que l'ordre de  $a$  modulo  $p_i^{r_i}$  vaut bien  $n$  pour tout  $i$ . En effet, pour tout  $x \in C_n - \{0\}$ , on a  $a^x - 1 \in C_m^*$  et donc  $a^x - 1$  est inversible modulo  $p_i^{r_i}$  et donc non nul. On peut donc se limiter maintenant au cas où  $m = p^r$ . Les éléments de  $C_{p^r}^*$  d'ordre une puissance de  $p$  sont exactement les éléments congrus à 1 modulo  $p$  et aucun d'eux ne vérifie la condition i). Donc, aucun élément non trivial de  $\langle a \rangle$  n'est d'ordre une puissance de  $p$ . Comme  $C_{p^r}^* \simeq$

$C_{p-1} \times C_{p^{r-1}}$ , on en déduit que  $a$  appartient au facteur  $C_{p-1}$  et donc que  $n|p-1$ .

*ii)  $\implies$  i)* En utilisant à nouveau l'isomorphisme  $C_{p^r}^* \simeq C_{p-1} \times C_{p^{r-1}}$ , on voit que la condition  $n|p-1$  implique que l'ordre de  $a$  modulo  $p^r$  est le même que l'ordre de  $a$  modulo  $p$  et donc pour tout  $x \in C_n - \{0\}$ , on a  $a^x \neq 1$ . L'isomorphisme  $C_m^* \simeq \prod C_{p_i^{r_i}}^*$  implique finalement le i).  $\square$

Cette remarque permet d'exhiber plus efficacement des produits  $C_n \rtimes_a C_m$  de type CC. Pour  $m = 341 = 11 \cdot 31$  ou  $8281 = 7^2 \cdot 13^2$  on trouve  $C_{10} \rtimes_{244} C_{341}$ ,  $C_{10} \rtimes_{277} C_{341}$ ,  $C_{10} \rtimes_{46} C_{341}$ ,  $C_{10} \rtimes_{178} C_{341}$ ,  $C_6 \rtimes_{3020} C_{8281}$ ,  $C_6 \rtimes_{2175} C_{8281}$  comme exemples possibles.

c) La question de la classe d'isomorphisme d'un produit  $C_n \rtimes_a C_m$  se pose. Dans le cas où ils sont de type CC, on peut caractériser simplement cette classe.

**Lemme 4.14.** *Soient  $n, m, n', m' \geq 2$  des entiers,  $a \in C_m^*$  un élément d'ordre  $n$  vérifiant, pour tout  $x \in C_n - \{0\}$ ,  $a^x - 1 \in C_m^*$  et  $b \in C_{m'}^*$  un élément d'ordre  $n'$  vérifiant, pour tout  $x \in C_{n'} - \{0\}$ ,  $b^x - 1 \in C_{m'}^*$ . Les conditions suivantes*

*i) les groupes  $C_n \rtimes_a C_m$  et  $C_{n'} \rtimes_b C_{m'}$  sont isomorphes,*

*ii)  $n = n'$ ,  $m = m'$  et  $a$  et  $b$  engendrent le même sous-groupe de  $C_m^*$ , sont équivalentes.*

*Démonstration.* *ii)  $\implies$  i)* Par hypothèse, il existe un entier  $k$  premier à  $n$  tel que  $b^k = a$ . L'application

$$\begin{aligned} C_n \rtimes_a C_m &\longrightarrow C_n \rtimes_b C_m \\ (x, \alpha) &\longmapsto (kx, \alpha) \end{aligned}$$

est alors un isomorphisme de groupes.

*i)  $\implies$  ii)* Rappelons deux propriétés classiques sur les groupes de Frobenius :

- Un produit semi-direct  $G = H \rtimes K$  est un groupe de Frobenius de complément de Frobenius  $H$  si et seulement si pour tout  $k \in K - \{e\}$  on a  $\text{Cen}_H(k) = \{e\}$ .

- Le noyau de Frobenius d'un groupe de Frobenius  $G$  est égal au sous-groupe de Fitting  $F(G)$  de  $G$ , c'est-à-dire au plus grand sous-groupe normal nilpotent de  $G$ .

GROUPES TOTAUX

A cause des hypothèses faites et de ce qui précède, le groupe  $G = C_n \rtimes_a C_m$  (resp.  $G' = C_{n'} \rtimes_b C_{m'}$ ) est un groupe de Frobenius. Soit  $\alpha \in C_m - \{0\}$  et  $x \in C_n$ , on a

$$(x, 0)(0, \alpha) = (0, \alpha)(x, 0) \iff a^x \alpha = \alpha \iff \alpha(a^x - 1) = 0$$

Puisque, pour tout  $x \in C_n - \{0\}$ , l'élément  $a^x - 1$  est inversible, on en déduit que  $\text{Cen}_{C_n}(\alpha) = \{0\}$  et donc que  $C_n$  (resp.  $C_{n'}$ ) est le complément de Frobenius de  $G$  (resp.  $G'$ ).

Le groupe  $C_m$  étant abélien, c'est un sous-groupe de  $G$  qui est distingué et nilpotent. On a donc  $C_m \subset F(G)$ , mais comme le complément de Frobenius de  $G$  est  $C_n$ , on a que  $G \simeq C_n \rtimes F(G)$  et, pour des raisons évidentes de cardinalité, on en déduit que  $C_m = F(G)$  (resp.  $C_{m'} = F(G')$ ).

Considérons un isomorphisme  $\varphi : G \rightarrow G'$ . Puisque  $\varphi$  envoie isomorphiquement  $F(G)$  sur  $F(G')$ , on en déduit que  $m = m'$  et, par suite, que  $n = n'$ . L'application  $\varphi$  définit alors, par restriction, un automorphisme de  $C_m$  et il existe donc un élément  $u \in C_m^*$  tel que  $\varphi(0, 1) = (0, u)$ . Posons formellement  $\varphi(1, 0) = (v, w)$ , on a alors

$$\begin{aligned} (v, w + b^v u) &= (v, w).(0, u) = \varphi(1, 0).\varphi(0, 1) = \varphi((1, 0).(0, 1)) \\ &= \varphi(1, a) = \varphi((0, a).(1, 0)) = \varphi(0, a).\varphi(1, 0) \\ &= (0, au).(v, w) = (v, w + au) \end{aligned}$$

et donc  $au = b^v u$ , ce qui implique (puisque  $u$  est inversible) que  $a = b^v \in \langle b \rangle$ . Le même raisonnement effectué sur  $\varphi^{-1}$  montre finalement que  $\langle a \rangle = \langle b \rangle$ .  $\square$

Un cas pratique d'application du corollaire 4.11 est celui où  $m = p \geq 3$  est un nombre premier,  $n \geq 2$  un entier divisant  $p - 1$  et  $a$  un générateur du sous-groupe d'ordre  $n$  de  $C_p^*$ . Par exemple  $G = C_2 \rtimes_2 C_3, C_2 \rtimes_4 C_5, C_4 \rtimes_2 C_5, C_2 \rtimes_6 C_7, C_3 \rtimes_2 C_7, C_6 \rtimes_3 C_7 \dots$ . Un autre cas intéressant concerne le groupe diédral :

**Corollaire 4.15.** *a) Pour tout  $n \geq 1$ , le groupe diédral  $D_{4n+2}$  est vraiment total et quand il se réalise sur un corps  $k$ , on a pour tout  $f \in Z^2(D_{4n+2}, k^*)$ ,*

$$\dim_k Z(\mathfrak{A}_f^{D_{4n+2}}) = n + 2$$

*b) Pour tout  $n \geq 1$ , si le groupe diédral  $G = D_{4n}$  se réalise sur un corps  $k$ , alors pour tout  $f \in Z^2(D_{4n}, k^*)$ , on a*

$$\dim_k Z(\mathfrak{A}_f^{D_{4n}}) = n \text{ ou } n + 3$$

*Démonstration.* Le a) découle du corollaire 4.11 pour le choix  $n = 2$ ,  $m = 2n + 1$  et  $a = -1$ .

b) Pour ce qui est du groupe diédral

$$D_{4n} = C_2 \rtimes_{-1} C_{2n} = \{e, \rho, \dots, \rho^{2n-1}, \sigma, \sigma\rho, \dots, \sigma\rho^{2n-1}\}$$

on a  $Z(D_{4n}) = \{e, \rho^n\}$  et les classes de conjugaisons et centralisateurs dans  $D_{4n}$  sont :

- $\tilde{e} = \{e\}$ ,  $\text{Cen}_{D_{4n}}(e) = D_{2n}$
  - $\tilde{\rho^n} = \{\rho^n\}$ ,  $\text{Cen}_{D_{4n}}(\rho^n) = D_{2n}$
  - $\tilde{\rho^k} = \{\rho^k, \rho^{-k}\}$ ,  $\text{Cen}_{D_{4n}}(\rho^k) = C_{2n}$  pour tout  $k = 1, \dots, n-1$
  - $\tilde{\sigma} = \{\sigma, \sigma\rho^2, \dots, \sigma\rho^{2n-2}\}$ ,  $\text{Cen}_{D_{4n}}(\sigma) = \{e, \rho^n, \sigma, \sigma\rho^n\} \simeq C_2 \times C_2$
  - $\tilde{\sigma\rho} = \{\sigma\rho, \sigma\rho^3, \dots, \sigma\rho^{2n-1}\}$ ,  $\text{Cen}_{D_{4n}}(\sigma) = \{e, \rho^n, \sigma\rho, \sigma\rho^{n+1}\} \simeq C_2 \times C_2$
- Posons  $D_{4n\text{conj}} = \{e, \rho, \dots, \rho^n, \sigma, \sigma\rho\}$  et

$$S = \{\sigma \in D_{4n\text{conj}} / \omega_{\sigma|_{\text{Cen}_{D_{4n}}(\sigma)}} \equiv 1\}$$

Comme pour tout  $k = 1, \dots, n-1$ ,  $\text{Cen}_{D_{2n}}(\rho^k)$  est cyclique on en déduit que  $\rho^k \in S$  et donc que  $S$  compte au moins  $n$  éléments. La fin de la preuve va consister à montrer que les trois éléments  $\rho^n$ ,  $\sigma$  et  $\sigma\rho$  sont, soit simultanément dans  $S$ , soit simultanément hors de  $S$ . Remarquons préalablement que comme  $\rho^n \in C_{2n}$ , on a  $\omega_{\rho^n|_{C_{2n}}} \equiv 1$ .

Posons  $\lambda = \omega_{\sigma}(\rho^n)$ . Comme  $1 = \omega_{\sigma}(e) = \omega_{\sigma}(\rho^n \rho^n) = \omega_{\sigma}(\rho^n)^2 = \lambda^2$  on en déduit que  $\lambda = \pm 1$ .

- Si  $\lambda = 1$  alors
  - $\omega_{\rho^n|_{C_{2n}}} \equiv 1$  et  $\omega_{\rho^n}(\sigma\rho^k) = \omega_{\rho^n}(\sigma)\omega_{\rho^n}(\rho^k) = \omega_{\rho^n}(\sigma) = \lambda^{-1} = 1$ , pour tout  $k = 0, \dots, 2n-1$ . Ainsi,  $\omega_{\rho^n|_{D_{4n}}} \equiv 1$  et donc  $\rho^n \in S$ .
  - $\omega_{\sigma}(e) = 1$ ,  $\omega_{\sigma}(\sigma) = 1$ ,  $\omega_{\sigma}(\rho^n) = \lambda = 1$ ,  $\omega_{\sigma}(\sigma\rho^n) = \omega_{\sigma}(\sigma)\omega_{\sigma}(\rho^n) = \lambda = 1$ . Donc  $\sigma \in S$ .
  - $\omega_{\sigma\rho}(e) = 1$ ,  $\omega_{\sigma\rho}(\sigma\rho) = 1$ ,  $\omega_{\sigma\rho}(\rho^n) = \omega_{\rho^n}(\sigma\rho)^{-1} = \omega_{\rho^n}(\sigma)^{-1}\omega_{\rho^n}(\rho)^{-1} = \lambda = 1$ ,  $\omega_{\sigma\rho}(\sigma\rho^{n+1}) = \omega_{\sigma\rho}(\sigma\rho\rho^n) = \omega_{\sigma\rho}(\sigma\rho)\omega_{\sigma\rho}(\rho^n) = \omega_{\rho^n}(\sigma\rho)^{-1} = 1$ . Donc  $\sigma\rho \in S$ .

Si  $\lambda = -1$  alors

- $\omega_{\rho^n}(\sigma) = \lambda^{-1} = -1$  et ainsi  $\omega_{\rho^n|_{D_{4n}}} \not\equiv 1$ . Donc  $\rho^n \notin S$ .
- $\omega_{\sigma}(\rho^n) = -1$  et ainsi  $\omega_{\sigma|_{\text{Cen}_{D_{4n}}(\sigma)}} \not\equiv 1$ . Donc  $\sigma \notin S$ .

GROUPES TOTAUX

•  $\omega_{\sigma\rho}(\rho^n) = \omega_\sigma(\rho^n)\omega_\rho(\rho^n) = -1$  et ainsi  $\omega_{\sigma\rho|_{\text{Cen}_{D_{4n}}(\sigma\rho)}} \neq 1$ . Donc  $\sigma\rho \notin S$ . □

Pour le cas du groupe  $D_{4n}$ , nous n'affirmons pas qu'il n'est pas vraiment total. Pour autant, le calcul numérique montre que les groupes  $D_{4n}$  ne sont pas vraiment totaux pour  $n = 1, \dots, 8$ .

Si l'on exclut le cas du groupe diédral et celui où  $m$  est un nombre premier, les cas possibles rentrant dans le cadre du corollaire 4.11 et restants pour  $m \leq 100$  sont alors

$C_4 \rtimes_7 C_{25}$	$C_4 \rtimes_{18} C_{25}$	$C_3 \rtimes_{18} C_{49}$	$C_6 \rtimes_{19} C_{49}$	$C_3 \rtimes_{30} C_{49}$
$C_6 \rtimes_{31} C_{49}$	$C_4 \rtimes_8 C_{65}$	$C_4 \rtimes_{18} C_{65}$	$C_4 \rtimes_{47} C_{65}$	$C_4 \rtimes_{57} C_{65}$
$C_4 \rtimes_{13} C_{85}$	$C_4 \rtimes_{38} C_{85}$	$C_4 \rtimes_{47} C_{85}$	$C_4 \rtimes_{72} C_{85}$	$C_3 \rtimes_9 C_{91}$
$C_6 \rtimes_{10} C_{91}$	$C_3 \rtimes_{16} C_{91}$	$C_6 \rtimes_{17} C_{91}$	$C_3 \rtimes_{74} C_{91}$	$C_6 \rtimes_{75} C_{91}$
$C_3 \rtimes_{81} C_{91}$	$C_6 \rtimes_{82} C_{91}$			

Pour compléter ces résultats, nous donnons quelques autres exemples pour des produits semi-directs de groupe cycliques. Nous rappelons que dans ces tableaux, les dimensions  $\dim_k Z(\mathfrak{A}_f^G)$  données, quand il y en a plus d'une, sont toutes atteintes pour un bon choix de corps  $k$  et de cocycle  $f$ .

a) *Exemples de produits semi-directs de deux groupes cycliques qui ne sont pas des groupes totaux.*

$G$	$C_2 \rtimes_5 C_{12}$	$C_2 \rtimes_7 C_{12}$	$C_4 \rtimes_3 C_4$	$C_4 \rtimes_5 C_6$
$o(G)$	24	24	16	24
$\#G_{\text{conj}}$	12	15	10	12
$\dim_k Z(\mathfrak{A}_f^G)$	6 ou 12	6 ou 15	4 ou 10	6 ou 12
$G$	$C_6 \rtimes_3 C_4$	$C_8 \rtimes_3 C_4$	$C_6 \rtimes_5 C_6$	
$o(G)$	24	32	36	
$\#G_{\text{conj}}$	15	20	18	
$\dim_k Z(\mathfrak{A}_f^G)$	6 ou 15	8 ou 20	9 ou 18	

b) *Exemples de produits semi-directs de deux groupes cycliques qui ne sont pas de type CC mais qui sont totaux.*



$G$	$C_2 \times_3 C_8$	$C_2 \times_5 C_8$	$C_3 \times_4 C_9$	$C_3 \times_7 C_9$
$o(G)$	16	16	27	27
$\sharp G_{\text{conj}}$	7	10	11	11
$\dim_k Z(\mathfrak{A}_f^G)$	7	10	11	11
$G$	$C_4 \times_2 C_3$	$C_4 \times_4 C_5$	$C_4 \times_6 C_7$	$C_6 \times_2 C_3$
$o(G)$	12	20	28	18
$\sharp G_{\text{conj}}$	6	8	10	9
$\dim_k Z(\mathfrak{A}_f^G)$	6	8	10	9

### 4.3. Les groupes méta-dicycliques.

Dans ce paragraphe nous présentons l'exemple d'une famille de groupes finis quasi-CC qui ne sont pas de type CC.

On se donne deux entiers  $n, m \geq 1$  et l'on considère le groupe  $\Gamma = C_{4m} \times_{-1} C_{2n}$ . On considère le sous-groupe d'ordre 2,  $H = \langle (2m, n) \rangle$  qui est visiblement distingué dans  $\Gamma$  puisque contenu dans le centre de  $\Gamma$ .

On considère alors le groupe quotient d'ordre  $4mn$ ,  $\Delta_m^n = \Gamma/H$ . On appelle les groupes  $\Delta_m^n$  les *groupes méta-dicycliques*. Cette terminologie provient du fait que pour  $m = 1$ , le groupe  $\Delta_1^n$  est égal au groupe dicyclique  $Q_{4n}$ .

**Proposition 4.16.** *Si  $n$  et  $m$  sont premiers entre eux, alors le groupe méta-dicyclique  $\Delta_m^n$  est un groupe quasi-CC. Par ailleurs, si en plus  $n \geq 2$  alors le groupe  $\Delta_m^n$  n'est pas de type CC.*

*Démonstration.* Posons  $G = \Delta_m^n$ . Lorsque  $n = 1$ , on a  $\Gamma = C_{4m} \times C_2$  et, par suite,  $\Delta_m^1 \simeq C_{4m}$  qui est bien de type CC, donc quasi-CC. Supposons maintenant que  $n > 1$ .

Le premier point à observer est que, si l'on note  $s : \Gamma \rightarrow G$  la surjection canonique, on a  $Z(\Gamma) = s^{-1}(Z(G))$  et pour tout  $\alpha \in \Gamma$ ,  $\text{Cen}_\Gamma(\alpha) = s^{-1}(\text{Cen}_G(s(\alpha)))$ . En effet, si  $h, h' \in G$  ont pour représentants  $\alpha = (x, g)$  et  $\alpha' = (x', g')$  dans  $\Gamma$ , alors la condition  $hh' = h'h$  équivaut à

$$(x + x', g + (-1)^x g') = (x' + x, g' + (-1)^{x'} g) \text{ mod } H$$

mais du fait de l'égalité  $x + x' = x' + x$ , l'égalité modulo  $H$  ci-dessus équivaut à l'égalité tout court, c'est-à-dire à  $\alpha\alpha' = \alpha'\alpha$ . On en déduit que  $Z(G) = Z(\Gamma)/H$  et que pour tout  $\alpha \in \Gamma$ ,  $\text{Cen}_G(s(\alpha)) = \text{Cen}_\Gamma(\alpha)/H$ .

GROUPES TOTAUX

Un élément  $(x, g) \in \Gamma$  est dans le centre de  $\Gamma$  si et seulement si, pour tout  $(x', g')$ , on a

$$(1 - (-1)^{x'})g = (1 - (-1)^x)g'$$

Le choix  $g' = 0$  et  $x' = 1$  montre que  $2g = 0$  et donc que  $g = 0$  ou  $n$ . Le choix  $x' = 0$  et  $g' = 1$  montre que  $x \in 2C_{4m}$ . On en déduit que le centre de  $\Gamma$  est égal à  $Z(\Gamma) = 2C_{4m} \times nC_{2n}$ . On a donc  $Z(G) = Z(\Gamma)/H = 2C_{4m} \times nC_{2n}/(2m, n) = s(2C_{4m}) \simeq C_{2m}$ , et le centre de  $G$  est bien cyclique non-trivial. En particulier,  $G$  n'est pas de type CC.

Étudions maintenant les centralisateurs. Soit  $\alpha = (x, g) \in \Gamma$ , alors  $\alpha' = (x', g') \in \text{Cen}_\Gamma(\alpha)$  si et seulement si

$$(C) \quad (1 - (-1)^{x'})g = (1 - (-1)^x)g'$$

Distinguons deux cas :

1/  $x \notin 2C_{4m}$  : la condition (C) équivaut alors à  $2g' = (1 - (-1)^{x'})g$ .

- Si  $x' \in 2C_{4m}$  alors  $g' = 0$  ou  $n$  et les éléments  $\alpha'$  correspondent alors à  $2C_{4m} \times nC_{2n} = Z(\Gamma)$ .

- Si  $x' \notin 2C_{4m}$  alors  $2g' = 2g$ , ce qui équivaut à  $g' = g$  ou  $g + n$ .

Ainsi, l'ordre de  $\text{Cen}_\Gamma(\alpha)$  vaut  $8m$ . Pour tout entier  $k$ , on a  $(1, g)^k = (k, \frac{1-(-1)^k}{2}g)$ , on en déduit que, modulo  $H$ , l'élément  $(1, g)$  est d'ordre  $4m$ . Par ailleurs, puisque  $\text{Cen}_G(s(\alpha)) = \text{Cen}_\Gamma(\alpha)/H$ , l'ordre de  $\text{Cen}_G(s(\alpha))$  vaut  $4m$  et donc, on en déduit finalement que

$$\text{Cen}_G(s(\alpha)) = \langle s(1, g) \rangle \simeq C_{4m}$$

est cyclique.

2/  $x \in 2C_{4m}$  : la condition (C) équivaut alors à  $(1 - (-1)^{x'})g = 0$ . On s'intéresse aux centralisateurs des éléments qui ne sont pas dans le centre, on peut donc exclure le cas  $g = 0$  ou  $n$ . Dans cette situation on a nécessairement  $x' \in 2C_{4m}$  et, par suite, on a  $\text{Cen}_\Gamma(\alpha) = 2C_{4m} \times C_{2n}$ .

- Si  $n$  et  $m$  sont impairs, puisqu'ils sont premiers entre eux, on a

$$\begin{aligned} \text{Cen}_G(s(\alpha)) &= \frac{2C_{4m} \times C_{2n}}{H} \simeq \frac{C_{2m} \times C_{2n}}{C_2} \simeq \frac{C_2 \times C_2 \times C_m \times C_n}{C_2} \\ &\simeq C_2 \times C_m \times C_n \simeq C_{2mn} \end{aligned}$$

qui est bien cyclique.

- Si un des deux entiers  $n$  ou  $m$  est pair alors étudions l'ordre modulo  $H$  de l'élément  $(2, 1) \in \text{Cen}_\Gamma(\alpha)$ . On a, pour tout entier  $k$ ,  $(2, 1)^k = (2k, k)$

et donc

$$\begin{aligned}
 (2, 1)^k = (0, 0) &\iff \begin{cases} 2k \equiv 0 \pmod{4m} \\ k \equiv 0 \pmod{2n} \end{cases} \\
 &\iff \begin{cases} k \equiv 0 \pmod{2m} \\ k \equiv 0 \pmod{2n} \end{cases} \\
 &\iff k \equiv 0 \pmod{2mn} \\
 \\
 (2, 1)^k = (2m, n) &\iff \begin{cases} 2k \equiv 2m \pmod{4m} \\ k \equiv n \pmod{2n} \end{cases} \\
 &\iff \begin{cases} k \equiv m \pmod{2m} \\ k \equiv n \pmod{2n} \end{cases} \\
 &\iff \begin{cases} \exists h \in \mathbb{Z} / k = m(1 + 2h) \\ \exists t \in \mathbb{Z} / k = n(1 + 2t) \end{cases}
 \end{aligned}$$

Comme  $n$  et  $m$  sont des entiers premiers entre eux, les dernières relations montrent qu'ils divisent tous deux des entiers impairs, ce qui est contradictoire avec l'hypothèse. On en déduit donc que  $(2, 1)$  est d'ordre  $2nm$  modulo  $H$ , ce qui est exactement l'ordre de  $\text{Cen}_G(s(\alpha)) = 2C_{4m} \times C_{2n}/H$ . Ainsi,  $\text{Cen}_G(s(\alpha)) \simeq C_{2mn}$  est cyclique, ce qui achève la preuve.  $\square$

**Corollaire 4.17.** *Les groupes méta-dicycliques  $\Delta_m^n$  sont vraiment totaux dès que  $n$  et  $m$  sont premiers entre eux. Dans cette situation, si  $\Delta_m^n$  se réalise sur un corps  $k$ , alors pour tout  $f \in Z^2(\Delta_m^n, k^*)$ , on a*

$$\dim_k Z(\mathfrak{A}_f^{\Delta_m^n}) = m(n + 3)$$

*En particulier, pour tout  $n \geq 1$ , le groupe dicyclique  $Q_{4n}$  est vraiment total et, si  $Q_{4n}$  se réalise sur un corps  $k$ , alors pour tout  $f \in Z^2(Q_{4n}, k^*)$ , on a*

$$\dim_k Z(\mathfrak{A}_f^{Q_{4n}}) = n + 3$$

*Démonstration.* Il s'agit de dénombrer les classes de conjugaisons de  $\Delta_m^n$ . On reprend les notations précédentes et l'on commence par décrire les classes de conjugaison de  $\Gamma$ . Soit  $(x, g) \in \Gamma$ , pour tout  $(y, h) \in \Gamma$ , on a

$$\begin{aligned}
 (y, h)(x, g)(y, h)^{-1} &= (y + x, h + (-1)^y g)(-y, -(-1)^y h) \\
 &= (x, (-1)^y g + h(1 - (-1)^x))
 \end{aligned}$$

1/ Si  $x \in 2C_{4m}$ , alors le produit précédent vaut  $(x, (-1)^y g)$  et on en déduit que

$$\widetilde{(x, g)} = \{(x, g), (x, -g)\}$$

L'ensemble de classes correspondantes est donc

$$\left\{ \widetilde{(x, g)} / x \in 2C_{4m}, g = 0, \dots, n \right\}$$

ensemble qui compte  $2m(n + 1)$  éléments.

2/ Si  $x \notin 2C_{4m}$ , alors le produit précédent vaut  $(x, (-1)^y g + 2h)$  et on en déduit que si  $g \in 2C_{2n}$  alors

$$\widetilde{(x, g)} = \{(x, 0), (x, 2), \dots, (x, 2n - 2)\}$$

et si  $g \notin 2C_{2n}$  alors

$$\widetilde{(x, g)} = \{(x, 1), (x, 3), \dots, (x, 2n - 1)\}$$

L'ensemble de classes correspondantes est donc

$$\left\{ \widetilde{(x, 0)}, \widetilde{(x, 1)} / x \notin 2C_{4m} \right\}$$

ensemble qui compte  $4m$  éléments.

En conclusion, il y a  $2m(n + 3)$  classes de conjugaison dans  $\Gamma$ . Par passage au quotient, on en déduit que les classes de conjugaisons de  $G$  sont la réunion des deux ensembles suivants

$$\left\{ \widetilde{s(x, g)} / x = 0, 2, \dots, 2m - 2, g = 0, \dots, n \right\}$$

et

$$\left\{ \widetilde{s(x, 0)}, \widetilde{s(x, 1)} / x = 1, 3, \dots, 2m - 1 \right\}$$

Il y a donc  $m(n + 3)$  classes de conjugaison dans  $G$ , ce qui achève la preuve.  $\square$

#### 4.4. Totalité et opérations sur les groupes.

L'ensemble des groupes vraiment totaux n'est stable par aucune opération usuelle sur les groupes. Plus précisément :

- Si  $G$  est vraiment total et si  $H$  est un sous-groupe de  $G$ , alors  $H$  n'est pas forcément vraiment total. Par exemple, le groupe  $G = C_2 \times_3 C_8$  est vraiment total, mais l'action de  $C_2$  sur le sous-groupe d'ordre 2 de  $C_8$  étant trivial, on en déduit que  $G$  possède un sous-groupe isomorphe à  $C_2 \times C_2$  qui n'est pas vraiment total.

- Si  $G$  est vraiment total et  $H$  est un sous-groupe distingué de  $G$ , alors le groupe quotient  $G/H$  n'est pas forcément vraiment total. Par exemple  $G = Q_8$  possède un quotient isomorphe à  $C_2 \times C_2$ .
- Si  $G$  est extension de deux groupes vraiment totaux  $H$  et  $N$ , alors  $G$  n'est pas forcément vraiment total. Par exemple,  $H = Q_8$  et  $N = C_2$  sont vraiment totaux, mais  $G = C_4 \times_{-1} C_4$  qui est extension de  $N$  par  $H$  ne l'est pas.
- Si  $G$  et  $H$  sont vraiment totaux, le produit cartésien  $G \times H$  ne l'est pas forcément. Par exemple, pour  $G = H = C_2$ , le groupe  $C_2 \times C_2$  n'est pas vraiment total.

On peut toutefois obtenir des résultats sur la totalité si l'on impose quelques hypothèses. Pour les produits cartésiens, on a :

**Proposition 4.18.** *Soient  $G$  et  $H$  deux groupes vraiment totaux. Si  $o(G)$  et  $o(H)$  sont des entiers premiers entre eux, alors le groupe produit  $G \times H$  est vraiment total.*

*Démonstration.* On identifie  $G$  et  $H$  à leurs images canoniques dans  $G \times H$ . Considérons un élément  $\sigma = \alpha\beta \in G \times H$  avec  $\alpha \in G$  et  $\beta \in H$ . On a  $\text{Cen}_{G \times H}(\sigma) = \text{Cen}_G(\alpha) \times \text{Cen}_H(\beta)$  et il s'agit de montrer que pour tout  $x \in \text{Cen}_{G \times H}(\sigma)$ , on a  $\omega_\sigma(x) = 1$ . Écrivons  $x = gh$  avec  $g \in \text{Cen}_G(\alpha)$  et  $h \in \text{Cen}_H(\beta)$ , remarquons que  $\alpha, \beta, g, h$  commutent deux à deux et donc

$$\begin{aligned} \omega_\sigma(x) &= \omega_{\alpha\beta}(gh) = \omega_{\alpha\beta}(g)\omega_{\alpha\beta}(h) = \omega_g^{-1}(\alpha\beta)\omega_h^{-1}(\alpha\beta) \\ &= \omega_g^{-1}(\alpha)\omega_g^{-1}(\beta)\omega_h^{-1}(\alpha)\omega_h^{-1}(\beta) = \omega_\alpha(g)\omega_\alpha(h)\omega_\beta(g)\omega_\beta(h) \\ &= \omega_\alpha(h)\omega_\beta(g) \quad (\text{car } \alpha, \beta, g, h \in H \text{ et } G, H \text{ sont totaux.}) \end{aligned}$$

Comme  $h \in H$ ,  $\omega_\alpha(h)$  est une racine  $o(H)$ -ème de l'unité, mais comme  $\omega_h(\alpha) = \omega_\alpha(h)^{-1}$  et que  $\alpha \in G$ , on en déduit que  $\omega_\alpha(h)$  est aussi une racine  $o(G)$ -ème de l'unité, et comme  $o(H)$  et  $o(G)$  sont premiers entre eux, on en déduit finalement que  $\omega_\alpha(h) = 1$ . On montre de la même façon que  $\omega_\beta(g) = 1$  et ainsi,  $\omega_\sigma(x) = 1$ .  $\square$

GROUPES TOTAUX

Complétons le cas des produits par quelques résultats obtenus sur machine :

$G$	$C_2 \times S_3$	$C_3 \times S_3$	$C_2 \times Q_8$	$C_2 \times A_4$
$o(G)$	12	18	16	24
$\#G_{\text{conj}}$	6	9	10	8
$\dim_k Z(\mathfrak{A}_f^G)$	3 ou 6	9	4 ou 10	6 ou 8
$G$	$C_2 \times Q_{12}$	$C_4 \times S_3$	$C_2 \times C_2 \times S_3$	$C_2 \times D_{10}$
$o(G)$	24	24	24	20
$\#G_{\text{conj}}$	12	12	12	8
$\dim_k Z(\mathfrak{A}_f^G)$	6 ou 12	6 ou 12	3, 6 ou 12	5 ou 8
$G$	$C_2 \times D_8$	$C_3 \times D_8$	$C_2 \times D_{12}$	$C_2 \times D_{14}$
$o(G)$	16	24	24	28
$\#G_{\text{conj}}$	10	15	12	10
$\dim_k Z(\mathfrak{A}_f^G)$	1, 4 ou 10	6 ou 15	3, 6 ou 12	7 ou 10

Le cas du groupe  $G = C_3 \times S_3$  est intéressant puisqu'il constitue un contre-exemple, dans le cas non-abélien, à la réciproque de la proposition 4.18. Par ailleurs, puisque le centralisateur du couple  $(1, \rho)$  est isomorphe à  $C_3 \times C_3$ , ce groupe constitue un exemple de groupe total qui n'est pas quasi-CC.

La proposition 4.18 couplée à l'étude des groupes quasi-CC permet d'exhiber une large famille de groupes totaux dont aucun n'est quasi-CC : on prend les produits cartésiens  $G \times H$  où  $G$  et  $H$  sont des groupes quasi-CC non cycliques d'ordre premier entre eux (les éléments non centraux des facteurs  $G$  et  $H$  n'ont alors pas de centralisateurs cycliques). Par exemple, les groupes  $\text{PSL}_2(\mathbb{F}_{2^n}) \times (C_{11} \rtimes_4 C_{23})$  sont totaux mais pas quasi-CC dès que  $n \not\equiv 11 \pmod{23}$  et  $n \not\equiv 5 \pmod{11}$ .

Le fait que la totalité ne soit pas stable par passage au quotient est lié au fait que les stabilisateurs d'un groupe quotient peuvent "grossir". Si l'on peut contrôler ces stabilisateurs, on peut alors conclure :

**Proposition 4.19.** *Soient  $G$  un groupe vraiment total,  $H$  un sous-groupe distingué de  $G$  et  $s : G \rightarrow G/H$  la surjection canonique. Si, pour tout  $\alpha \in G - H$  on a*

$$s(\text{Cen}_G(\alpha)) = \text{Cen}_{G/H}(s(\alpha))$$

*alors le groupe quotient  $G/H$  est vraiment total.*

*Démonstration.* Considérons un 2-cocycle  $f \in Z^2(G/H, k^*)$  et  $f'$  l'image de  $f$  par l'application d'inflation  $Z^2(G/H, k^*) \rightarrow Z^2(G, k^*)$ . On a, par définition, pour tout  $g, h \in G$ ,  $f'(g, h) = f(\bar{g}, \bar{h})$ . Soit donc  $\sigma \in G - H$ , par hypothèse quand  $g$  parcourt  $\text{Cen}_G(\sigma)$ ,  $\bar{g}$  parcourt  $\text{Cen}_{G/H}(\bar{\sigma})$  et donc on a

$$\omega_{\bar{\sigma}}(\bar{g}) = \omega_{\sigma}(g) = 1$$

ce qui prouve que  $G/H$  est vraiment total.  $\square$

Une illustration pertinente de cette propriété consiste à regarder l'épimorphisme  $Q_{4n} \rightarrow D_{2n}$ . Si l'on présente ces groupes de la manière suivante :

$$\begin{aligned} Q_{4n} &= \langle \alpha, \beta \mid \alpha^{2n} = e, \beta^2 = \alpha^n, \beta\alpha\beta^{-1} = \alpha^{-1} \rangle \\ D_{2n} &= \langle \rho, \sigma \mid \rho^n = e, \sigma^2 = e, \sigma\rho\sigma = \rho^{-1} \rangle \end{aligned}$$

alors  $Z(Q_{4n}) = \langle \alpha^n \rangle = \langle \beta^2 \rangle$  est d'ordre 2 et l'on a la suite exacte

$$1 \longrightarrow Z(Q_{4n}) \longrightarrow Q_{4n} \xrightarrow{s} D_{2n} \longrightarrow 1$$

où  $s(\alpha) = \rho$  et  $s(\beta) = \sigma$ .

Si  $n = 2m$  est pair, alors  $\text{Cen}_{Q_{4n}}(\alpha^m) = \langle \alpha \rangle$  puisque  $\beta\alpha^m\beta^{-1} = \alpha^{-m} \neq \alpha^m$ . Cependant,

$$\text{Cen}_{D_{2n}}(s(\alpha^m)) = \text{Cen}_{D_{2n}}(\rho^m) = D_{2n} \neq s(\text{Cen}_{D_{2n}}(\alpha^m)) = \langle \rho \rangle$$

ce qui montre que les hypothèses de la proposition 4.19 ne sont pas vérifiées lorsque  $n$  est pair.

Si  $n = 2m+1$  est impair, les classes de conjugaison et les centralisateurs sont :  $\tilde{e} = \{e\}$ ,  $\text{Cen}_{Q_{4n}}(e) = Q_{4n}$ ,  $\text{Cen}_{D_{2n}}(e) = D_{2n} = s(Q_{4n})$

$$\tilde{\alpha}^n = \{\alpha^n\}, \text{Cen}_{Q_{4n}}(\alpha^n) = Q_{4n}, \text{Cen}_{D_{2n}}(s(\alpha^n)) = s(\text{Cen}_{Q_{4n}}(\alpha^n))$$

$$\tilde{\alpha}^k = \{\alpha^k, \alpha^{-k}\}, \text{Cen}_{Q_{4n}}(\alpha^k) = \langle \alpha \rangle \text{ pour tout } k = 1, \dots, n-1$$

$$\tilde{\rho}^k = \{\rho^k, \rho^{-k}\}, \text{Cen}_{D_{2n}}(s(\alpha^k)) = \langle \rho \rangle = s(\text{Cen}_{Q_{4n}}(\alpha^k)) = s(\text{Cen}_{Q_{4n}}(\alpha^{k+m}))$$

pour tout  $k = 1, \dots, m$

$$\tilde{\beta} = \{\beta, \beta\alpha^2, \dots, \beta\alpha^{2n-2}\}, \text{Cen}_{Q_{4n}}(\beta) = \langle \beta \rangle$$

$$\tilde{\beta}\alpha = \{\beta\alpha, \beta\alpha^3, \dots, \beta\alpha^{2n-1}\}, \text{Cen}_{Q_{4n}}(\beta\alpha) = \langle \beta\alpha \rangle \text{ d'ordre } 4$$

$$\tilde{\sigma} = \{\sigma, \sigma\rho, \dots, \sigma\rho^{2m}\}, \text{Cen}_{D_{2n}}(\sigma) = \langle \sigma \rangle = s(\text{Cen}_{Q_{4n}}(\beta)) = s(\text{Cen}_{Q_{4n}}(\beta^3))$$

et nous sommes là en pleine application de la proposition 4.19, ce qui donne une autre preuve de la proposition 4.15.a).

Références

- [1] A. DAVYDOV – « Twisted automorphisms of group algebras », *arXiv :0708.2758* (2007).
- [2] M. S. R. BRAUER & G. WALL – « A characterization of the one-dimensional unimodular projective groups over finite fields », *Illinois Journal of Mathematics* **2** (1958), p. 718–745.
- [3] M. SUZUKI – « The nonexistence of a certain type of simple groups of odd order », *Proceedings of the American Mathematical Society (American Mathematical Society)* **8** (1957), no. 4, p. 686–695.
- [4] J.-P. TIGNOL – « Sur les décompositions des algèbres à division en produit tensoriel d’algèbres cycliques », *Lecture Notes in Math.*, vol. 917, p. 126–145, *Lecture Notes in Math.*, Springer, Berlin-New York, 1982.
- [5] L. WEISNER – « Groups in which the normaliser of every element except identity is abelian », *Bull. Amer. Math. Soc.* **31** (1925), no. 8, p. 413–416.
- [6] Y.-F. WU – « Groups in which commutativity is a transitive relation », *J. Algebra* **207** (1998), no. 1, p. 165–181.

BRUNO DESCHAMPS  
 Département de Mathématiques  
 Université du Maine  
 Avenue Olivier Messiaen  
 72085 Le Mans cedex 9  
 FRANCE  
 bruno.deschamps@univ-lemans.fr

IVAN SUAREZ ATIAS  
 Département de Mathématiques  
 Université du Maine  
 Avenue Olivier Messiaen  
 72085 Le Mans cedex 9  
 FRANCE  
 ivan.suarez-atias@@univ-lemans.fr