Université de rennes 1
Préparation à l'agrégation externe
Année 2009-2010

Fabrice Castel
fabrice.castel@univ-rennes1.fr

Groupes finis

L'objectif de ces pages est de présenter les premiers résultats de structure et de classification des groupes finis (cas abélien, nilpotent, et groupes quelconques de petits cardinaux ou de cardinaux « sympathiques »). On développera particulièrement trois notions : les théorèmes de Sylow, les produits semi-directs, et les extensions de groupes.

Le lecteur est supposé connaître la théorie de base sur les groupes : génération de groupe, sous-groupes, sous-groupes distingués (cependant, l'essentiel sur les sous-groupes distingués est rappelé au paragraphe 3.1), morphismes, quotients, théorèmes d'isomorphisme, et présentation par générateurs et relations.

Table des matières

Résumés des chapitres

Chapitre 1. Nous rappelons quelques généralités sur les groupes et quelques pièges courants autour du théorème de Lagrange et de sa réciproque : la recherche de sous-groupes (éventuellement distingués) d'un ordre donné.

Chapitre 2. Nous abordons le cas des groupes abéliens. Nous démontrons les théorèmes de Sylow dans ce cas, nous définissons l'exposant d'un groupe abélien, et au moyen d'une proposition sur l'existence de supplémentaires, nous démontrons les théorèmes de structure des groupes abéliens. Nous montrons également d'une façon élémentaire qu'un groupe abélien admet des sous-groupes de tous ordres (réciproque du théorème de Lagrange).

Chapitre 3. Nous quittons le monde abélien pour présenter les deux notions de produits semi-directs (internes et externes). Nous verrons quelques cas simples d'isomorphismes entre différents produits semi-directs.

Chapitre 4. Nous nous concentrons sur les théorèmes de Sylow que nous démontrons de deux manières et dont nous donnons des exemples variés d'utilisation.

Chapitre 5. Nous nous penchons plus particulièrement sur les p-groupes et les groupes nilpotents. Nous montrerons en particulier que les groupes nilpotents sont exactement les produits directs de p-groupes et admettent donc des sous-groupes distingués de tous ordres (réciproque du théorème de Lagrange). Nous terminons ce chapitre en exposant le spectaculaire théorème de Frattini.

Chapitre 6. Nous classifions les groupes d'ordre inférieur ou égal à 15. Nous étudions également des groupes d'ordres supérieurs (pq, p^3, 155=3.5.17, 399=3.7.19, $147 = 3.7^2$), afin de présenter différentes techniques.

Chapitre 7. Nous présentons les problèmes d'extension de groupes. Les problèmes auxquels on tentera de répondre sont : deux groupes N et H étant donnés, combien d'extensions (à équivalence près) existe-t-il de H par N ? Combien d'extensions scindées ? A cet égard, on verra le rôle particulier de $\mathrm{Hom}(H, \mathrm{Out}(N))$. Les réponses seront plus précises dans deux cas pourtant opposés : lorsque le groupe distingué de l'extension est de centre trivial, ou au contraire lorsque ce groupe est abélien.

Chapitre 8. Nous commençons par définir rapidement la cohomologie des groupes. Puis nous poursuivons l'étude des extensions de groupes G par des groupes abéliens A et nous établissons le lien avec la cohomologie des groupes en degré 1 et 2 : $H^1(G, A)$ décrit l'ensemble des sections d'une extension scindée donnée, à conjugaison près dans A, et $H^2(G, A)$ décrit l'ensemble des extensions pour une action donnée de G dans A.

Appendice. Nous terminons par quelques mots sur William Burnside (mathématicien anglais du début du XXème siècle) qui participa avec Frobenius à l'émergence de la recherche sur les groupes finis, succédant ainsi à Galois, Lagrange, Cauchy, Cayley, et qui a laissé son nom à de nombreux lemmes et théorèmes dans cette branche des mathématiques.

1 Généralités

1.1 Quelques rappels ciblés

Les définitions ci-dessous seront centrales dans la suite de ces pages. Pour l'instant, les groupes sont quelconques, éventuellement infinis.

Définition 1.1 (Ordre et exposant)**.**
- L'*ordre d'un groupe* est son cardinal.
- L'*ordre d'un élément* est l'ordre du sous-groupe engendré par cet élément.
- L'*exposant* d'un groupe est le ppcm des ordres (finis dans le cas de groupes infinis) de ses éléments[1].
- Un groupe est dit *périodique* si tous ses éléments sont d'ordre fini.

Définition 1.2 (p-(sous)-groupes (de Sylow))**.**
- Un *p-groupe* est un groupe pour lequel il existe un nombre premier q tel que l'ordre chaque élément est une puissance de q. Grâce au théorème de Cauchy, un *p-groupe* fini est un groupe dont l'ordre est une puissance d'un nombre premier.
- Un *p-sous-groupe* d'un groupe est un sous-groupe qui est un p-groupe.
- Un *p-sous-groupe de Sylow* (ou *p-Sylow*) d'un groupe est un p-sous-groupe maximal pour l'inclusion des p-sous-groupes.

Définition 1.3 (Actions de groupe)**.**
- Une *action du groupe G (à gauche) sur un ensemble E* est la donnée d'un morphisme de groupes φ de G dans $\mathfrak{S}(E)$, le groupe des bijections de E. L'élément $\varphi(g)(e)$ de E est noté $g.e$. Le morphisme φ est appelé le *morphisme structurel* de l'action.
- Le *stabilisateur* d'un élément e de E sous l'action de G est l'ensemble $\{g \in G \mid g.e = e\}$ et est noté $\mathrm{Stab}_G(e)$ ou G^e.
- L'*orbite* d'un élément e de E sous l'action de G est l'ensemble $\{g.e|\ g \in G\}$ et est notée $\mathrm{Orb}_G(e)$ ou $G.e$.
- Un élément e de E est un *point fixe* sous l'action de G si $\mathrm{Stab}_G(e) = G$. L'ensemble des points fixes est noté $\mathrm{Fix}_G(E)$ ou E^G.
- L'action est dite *libre* si pour tout $e \in E$, on a $\mathrm{Stab}_G(e) = \{1_G\}$.
- L'action est dite *fidèle* si $\mathrm{Ker}\,(\varphi) = \{1_G\}$.
- Une *transversale* d'une partie F de E stable sous l'action de G est un sous-ensemble F' de F contenant un et un seul élément par orbite sous G.

Remarques.

1. On a $\mathrm{Ker}\,(\varphi) = \bigcap_{e\in E} \mathrm{Stab}_G(e)$, donc $\bigcap_{e\in E} \mathrm{Stab}_G(e)$ est un sous-groupe distingué de G. On peut le voir aussi en remarquant que $\mathrm{Stab}_G(g.e) = g\mathrm{Stab}_G(e)g^{-1}$, donc $\bigcap_{e\in G} \mathrm{Stab}_G(e)$ est stable par conjugaison.

[1] Un groupe d'exposant infini signifie donc qu'il contient des éléments d'ordre fini arbitrairement grand.

2. On a la relation $|\mathrm{Orb}_G(x)| = \frac{|G|}{|\mathrm{Stab}_G(e)|}$ que l'on peut démontrer ainsi. Soit $H = \mathrm{Stab}_G(e)$, puis $f_e : G/H \to \mathrm{Orb}_G(e)$, $gH \mapsto g.e$ une application ensembliste, dont on doit vérifier la bonne définition. Il suffit ensuite de vérifier qu'elle est bijective.

3. Le plus souvent, pour étudier les groupes, on utilise des actions (en général à gauche) sur eux-mêmes ou sur des quotients.

(i) *Action par multiplication à gauche de G sur lui-même.* Pour tous g, h dans G, on pose $g.h = gh$. Le morphisme structurel va de G dans $\mathfrak{S}(G)$.

(ii) *Action par conjugaison de G sur lui-même.* Pour tous g, h dans G, on pose[2] $g.h = ghg^{-1}$. Dans ce cas, le morphisme structurel va de G dans $\mathrm{Int}(G)$, le groupe des automorphismes intérieurs de G.

(iii) *Action de G sur un ensemble quotient G/H.* Soit H un sous-groupe quelconque de G. Pour tous g, g' dans G, notons $\bar{g}'$ la classe de g' dans l'ensemble quotient G/H et posons $g.\bar{g}' = \overline{gg'}$.

Trois exemples d'action de groupes

Les trois exemples choisis ci-dessous illustrent les trois actions décrites ci-dessus.

Proposition 1.4 (Théorème de Cayley, 1854)**.**
Si G est un groupe d'ordre n, alors G est isomorphe à un sous-groupe du groupe symétrique $\mathfrak{S}_n$.

Démonstration (action par multiplication à gauche).
Le morphisme structurel φ de l'action par multiplication à gauche de G sur lui-même est un morphisme de G dans $\mathfrak{S}(G)$ qui est injectif, car cette action est libre, donc fidèle, donc $\mathrm{Ker}\,(\varphi) = \{1_G\}$. Ainsi G est isomorphe à un sous-groupe du groupe symétrique $\mathfrak{S}(G)$. □

Lemme 1.5 (L'équation aux classes)**.**
Etant donné un groupe G opérant sur un ensemble E, soient E' une transversale de E et E'' une transversale de $E \smallsetminus E^G$. Alors ,

$$|E| = \sum_{e \in E'} \frac{|G|}{|\mathrm{Stab}_G(e)|}, \qquad (EC1)$$

$$|E| = |E^G| + \sum_{e \in E''} \frac{|G|}{|\mathrm{Stab}_G(e)|}, \qquad (EC2)$$

et si G est un p-groupe, on a :

$$|E| \equiv |E^G| \pmod{p}. \qquad (EC3)$$

Démonstration (action par conjugaison).
Prouvons (EC1). On part de la partition E en orbites sous G. Puisque $|\mathrm{Orb}_G(e)| = \frac{|G|}{|\mathrm{Stab}_G(e)|}$, l'équation aux classes (EC1) en découle. Prouvons (EC2). Pour tout point fixe e de E sous l'action de G, on a $\mathrm{Stab}_G(e) = G$, donc $\frac{|G|}{|\mathrm{Stab}_G(e)|} = 1$. En écartant dans (EC1) les points fixes, on obtient (EC2). Prouvons (EC3). Supposons que G est un p-groupe.

[2] ou alors $h.g = g^{-1}hg$, et l'action serait à droite.

Alors dès que e n'est pas un point fixe, $|\mathrm{Stab}_G(e)|$ est un diviseur propre de $|G|$, donc $\frac{|G|}{|\mathrm{Stab}_G(e)|}$ est une puissance non nulle de p, donc p divise $\sum_{e\in E''} \frac{|G|}{|\mathrm{Stab}_G(e)|}$. Le résultat se déduit alors de (EC2). □

Proposition 1.6 (Théorème de Lagrange)**.**
L'ordre de tout sous-groupe divise l'ordre du groupe.

Démonstration (action par multiplication sur les classes selon un sous-groupe). Soit H un sous-groupe de G. L'action de H sur G par multiplication à gauche est libre, donc l'équation aux classes associée est :

$$|G| = \sum_{g\in G'} |H|,$$

donc l'ordre de H divise celui de G. □

Proposition 1.7 (Un corollaire important du théorème de Lagrange)**.**
Deux sous-groupes H et K d'ordre m et n avec $m\wedge n = 1$ d'un groupe G sont d'intersection triviale : $H \cap K = \{1_G\}$.

Démonstration. Soit x un élément de $H \cap K$. Le cardinal du sous-groupe engendré par x doit diviser m et n d'après le théorème de Lagrange, donc doit diviser le pgcd de m et n. Donc $x = 1_G$. □

1.2 Quelques contre-vérités

– *Soit G un groupe de cardinal n. Pour tout diviseur d de n, il existe un élément de G d'ordre d.*

VRAI : pour tous les groupes cycliques et eux seulement.
FAUX : pour tous les autres, puisqu'un groupe non cyclique d'ordre n ne contient pas d'élément d'ordre n.

– *Soit G un groupe de cardinal n. Pour tout diviseur d de n, il existe sous-groupe de G d'ordre d.*

VRAI : pour tous les groupes abéliens[3] et les p-groupes[4]. Vrai pour tous les groupes d'ordre pq où p et q sont premiers entre eux (en utilisant le théorème de Cauchy, tels $\mathfrak{S}_3$. Vrai plus généralement pour les groupes nilpotents, puisqu'ils sont le produit direct de leurs p-Sylow (cf. théorème 5.14).
FAUX : pour les groupes symétriques $\mathfrak{S}_p$ où p est premier supérieur ou égal à 5, car un sous-groupe d'ordre $2p$ contient un élément d'ordre p et un élément d'ordre 2, mais on peut montrer que deux tels éléments de $\mathfrak{S}_p$ engendrent un sous-groupe d'ordre strictement supérieur à $2p$. Faux également pour les groupes simples non cycliques, puisque d'une part, d'après le théorème de Feit-Thomson

[3]Cf. propositions 2.5.
[4]Cf. propositions 5.5.

(extrêmement difficile) de tels groupes sont d'ordre pair (tel $\mathfrak{A}_5$), d'autre part, si un tel groupe contenait un sous-groupe d'indice 2, il serait distingué, ce qui contredirait la simplicité du groupe. En fait, l'énoncé en question est faux pour tous les groupes non nilpotents (cf. proposition 5.15).

– *Soit G un groupe de cardinal n et soient p et q deux nombre premiers distincts divisant n. Alors il existe un élément de G d'ordre pq.*

VRAI : pour tous les groupes abéliens.
FAUX : pour les groupes d'ordre pq (p et q premiers distincts) non cycliques (par exemple les groupes diédraux) car ils ne contiennent pas d'éléments d'ordre pq, pour $\mathfrak{S}_p$ ne contenant pas d'éléments d'ordre $2p$, pour $\mathfrak{A}_4$ ne contenant aucun élément d'ordre 6.

– *a) Un groupe finiment engendré et périodique est fini.*
b) Un groupe finiment engendré, périodique et d'exposant fini est fini.

VRAI : Le b) est vrai pour les groupes linéaires[5].
FAUX : ces deux contre-vérités ont été conjecturées par Burnside au début du XXème siècle, et il a fallu plus de cinquante ans avant de trouver des contre-exemples. Ce type de questions continue d'influencer la recherche dans les groupes.

2 Groupes abéliens

Dans ce paragraphe, tous les groupes sont abéliens et finis. On utilisera sans le mentionner le fait suivant : Si x et y sont d'ordre respectivement m et n dans G abélien, alors l'ordre du sous-groupe engendré par x et y divise mn et l'ordre des éléments d'un tel sous-groupe divise le ppcm de m et n.

2.1 Théorèmes de Sylow pour les groupes abéliens

D'après le théorème de Lagrange, l'ordre de tout sous-groupe divise l'ordre du groupe. Dans le cas des groupes abéliens, la réciproque est vraie. C'est ce que l'on va établir, en démontrant le théorème de Sylow pour les groupes abéliens. Une notion essentielle est celle d'exposant d'un groupe fini.

Proposition 2.1 (Théorème de Cauchy pour les groupes abéliens)**.**
Soient G un groupe abélien d'ordre n et p un nombre premier qui divise n. Alors, il existe un élément dans G d'ordre p.

[5] i.e. les sous-groupes de $\mathcal{GL}(V)$, V étant un espace vectoriel ; le groupe étant finiment engendré, V doit être de dimension finie. Tous les groupes finis sont des groupes linéaires, puisqu'ils sont isomorphes à des sous-groupes de groupes symétriques, eux-mêmes isomorphes au groupe de matrices (dans les dimensions convenables) d'interversion de lignes et de colonnes.

Démonstration. Soient $x_1, \ldots, x_r$ r éléments dans G qui engendrent G. Soit

$$\begin{array}{rccc} \varphi : & \langle x_1\rangle \times \cdots \times \langle x_r\rangle & \longrightarrow & G \\ & (y_1, \ldots, y_n) & \longmapsto & y_1 \ldots y_n \end{array}$$

un morphisme de groupe (bien défini grâce à la commutativité de G). D'après le théorème d'isomorphisme, on a

$$\prod_{1 \leqslant i \leqslant r} |\langle x_i\rangle| = |G|.|\mathrm{Ker}\,(\varphi)|.$$

Or p divise $|G|$, donc p divise l'un des $|\langle x_i\rangle|$ pour $i \in \{1, \ldots, r\}$, donc l'une des puissances de l'un des x_i est d'ordre p. □

Proposition 2.2 (Théorèmes de Sylow pour les groupes abéliens)**.**
Soit G un groupe abélien d'ordre $p^\alpha m$ où p est premier, α est non nul, et m est premier avec p. Alors :

(i) il existe des p-sous-groupes de G d'ordre p^β pour tout $\beta \leqslant \alpha$,

(ii) le p-sous-groupe de G d'ordre p^β (le p-Sylow) est unique.

Démonstration.

Montrons le point (i). Par récurrence sur α. Lorsque $\alpha = 1$, le théorème de Cauchy fournit un élément d'ordre p, donc le sous-groupe engendré par cet élément convient. Maintenant, supposons que $\alpha > 1$. Supposons que (i) est vrai pour tout groupe dont l'ordre a une p-valuation strictement inférieur à α. Soit $\beta \leqslant \alpha$. Nous allons trouver un p-sous-groupe de G d'ordre p^β. Soit x un élément d'ordre p dans G. Soit H le sous-groupe de G engendré par x et soit $\pi : G \to G/H$ le morphisme de passage au quotient. L'hypothèse de récurrence appliquée à G/H fournit un sous-groupe $\bar{K}$ de G/H d'ordre $p^{\beta-1}$. Alors le groupe $K = \pi^{-1}(\bar{K})$ est d'ordre p^β par le théorème d'isomorphisme.

Montrons le point (ii). Soit H et K deux p-Sylow de G. Soit W le sous-groupe de G engendré par H et K. Puisque l'ordre des éléments de H et K divise p^α et que G est abélien, l'ordre des éléments de W divise également p^α. Or si l'ordre de W n'était pas une puissance de p, d'après le théorème de Cauchy, il existerait un élément dont l'ordre ne serait pas une puissance de p. Donc il existe β tel que $|W| = p^\beta$. On a $\beta \geqslant \alpha$ car $H \subset W$, et on a aussi $\beta \leqslant \alpha$ car $|W|$ divise $|G|$ d'après le théorème de Lagrange, mais $p^{\alpha+1}$ ne divise pas $|G|$. Donc W est de même cardinal que H et K tout en les contenant, donc $W = H = K$. □

Lemme 2.3 (Lemme chinois pour les sous-groupes d'un groupe abélien)**.**
Soient G un groupe abélien et $(H_i)_{1 \leqslant i \leqslant r}$ une famille de sous-groupes d'ordre deux à deux premiers. Alors ces sous-groupes sont en somme directe dans G.

Démonstration. Appelons d_1, ..., d_r les différents ordres des sous-groupes H_1, ..., H_r correspondants. Tout repose sur la remarque suivante : dans un groupe abélien, si a est d'ordre m et b d'ordre n avec m et n premiers entre eux, alors ab est d'ordre mn. Ainsi, pour tout i, l'ordre de tout élément de $\sum_{j \neq i} H_j$ divise le ppcm des d_j avec $j \neq i$, donc est premier avec d_i. Donc pour tout i, $H_i \cap (\sum_{j \neq i} H_j) = \{1\}$. Donc ces groupes H_i, $1 \leqslant i \leqslant r$ sont en somme directe. □

Corollaire 2.4 (Décomposition de Sylow dans un groupe abélien)**.**
Un groupe abélien fini est la somme directe de ses sous-groupes de Sylow[6]*.*

Démonstration. D'après le lemme 2.3, les différents p-Sylow de G sont en somme directe. L'égalité des cardinaux permet de conclure. □

Proposition 2.5 (Réciproque du théorème de Lagrange pour les groupes abéliens)**.**
Soit G un groupe abélien fini. Pour tout diviseur d de l'ordre de G, G admet un sous-groupe d'ordre d.

Démonstration. Soit n l'ordre de G que l'on factorise en nombres premiers : $n = \prod p_i^{\alpha_i}$. Soit d un diviseur de n que l'on factorise en nombres premiers : $d = \prod p_i^{\beta_i}$. D'après le théorème de Sylow, pour tout i, il existe un p-sous-groupe de G d'ordre $p_i^{\beta_i}$. D'après le lemme 2.3, les sous-groupes H_i sont en somme directe, donc le sous-groupe résultant est d'ordre d. □

2.2 Classification des groupes abéliens finis

Les théorèmes de Sylow nous mettent sur la voie de la classification des groupes abéliens finis. Pour conclure, il nous faut un résultat sur l'existence de supplémentaire. L'existence d'un supplémentaire est fausse en général, par exemple, un sous-groupe propre d'un groupe cyclique n'admet pas de supplémentaire. Par contre, (et c'est une utilisation remarquable de l'exposant d'un groupe abélien) tout sous-groupe cyclique engendré par un élément d'ordre maximal du groupe admet un supplémentaire, cf. proposition 2.8.

Rappelons que l'exposant d'un groupe fini est le ppcm des ordres des éléments de ce groupe.

Proposition 2.6 (Propriétés de l'exposant pour un groupe abélien fini)**.**
*Soit G un groupe **abélien fini**. Alors :*
(i) l'exposant de G est le maximum des ordres des éléments de G ;
(ii) il existe un élément de x dont l'ordre est l'exposant de G ;
(iii) l'ordre de tout élément divise l'exposant du groupe ;
(iv) l'exposant d'un groupe a les mêmes facteurs premiers que l'ordre du groupe ;
(v) l'exposant d'un groupe divise l'ordre du groupe.

Démonstration. Montrons l'assertion (i). Soit m le maximum des ordres des éléments de G et soit x un élément d'ordre m. Nous allons montrer que l'ordre de tout élément de G divise m. On fait un raisonnement par l'absurde : on suppose qu'il existe y dans G d'ordre q tel que q ne divise pas m. Soient α, β, m' et q' tels que :

[6] D'autres groupes que les groupes abéliens vérifient cette propriété. En fait, parmi les groupes finis, être la somme directe de ses sous-groupes de Sylow est équivalent n'avoir qu'un seul p-Sylow par nombre premier p, ce qui est encore équivalent à être nilpotent (voir la note au bas de la page **??**).

$$\begin{cases} m = p^\alpha m' & \text{avec} \quad p \wedge m' = 1, \\ q = p^\beta q' & \text{avec} \quad \beta > \alpha. \end{cases}$$

Remarquons que l'élément x^{p^α} est d'ordre m' et que l'élément $y^{q'}$ est d'ordre p^β. Puisque p^β et m' sont premiers entre eux, l'élément $x^{p^\alpha}y^{q'}$ est d'ordre $p^\beta m'$ qui est strictement supérieur à m. C'est absurde. Finalement, l'ordre de tout élément de G divise m, donc m est égal au ppcm des ordres des éléments de G, c'est donc l'exposant de G.

- L'assertions (ii) est incluse dans (i).
- L'assertion (iii) est un corollaire de la définition de l'exposant.
- L'assertion (iv) découle du *théorème de Cauchy.*
- L'assertion (v) découle du *théorème de Lagrange.* □

Remarques.

1. Les assertions (iii), (iv) et (v) sont vraies en général, mais les assertions (i) et (ii) ne le sont pas en général (par exemple les groupes symétriques $\mathfrak{S}_n$ avec $n \geqslant 3$).
2. On peut adapter ces résultats dans le cas de groupes infinis.
3. La notion d'exposant simplifie de nombreuses preuves classiques, comme la suivante.

Corollaire 2.7 (Groupe multiplicatif d'un corps commutatif)**.**
Tout sous-groupe fini d'un corps commutatif est cyclique. En particulier, pour tout nombre premier p, le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z}^*, .)$ est cyclique.

Démonstration. Soit $\mathbb{K}$ un corps et G un sous-groupe du groupe multiplicatif $(\mathbb{K}^*, .)$. Soit r l'exposant de G. Alors pour tout $x \in G$, on a $x^r = 1$. Par ailleurs, le polynôme $X^r - 1$ de $\mathbb{K}[X]$ possède au plus r solutions puisque $\mathbb{K}$ est un corps commutatif. On en déduit que G est de cardinal au plus r. Il est donc de cardinal r. Or puisque r est l'exposant de G, il existe un élément a dans G d'ordre r. D'après l'ordre de a et l'ordre de G, on constate que G est un groupe cyclique engendré par a. □

Proposition 2.8 (Prolongement de morphismes et existence d'un supplémentaire)**.**
Soit G un groupe abélien fini et x un élément d'ordre maximal dans G. Alors :

(i) il existe un morphisme de G dans $\langle x \rangle$ qui envoie x sur x,

(ii) il existe un sous-groupe K de G tel que $G = \langle x \rangle \oplus K$.

Démonstration. La partie (ii) est une conséquence de la partie (i). Prenons $K = \mathrm{Ker}\,(\varphi)$ où φ est le morphisme trouvé en (i). Alors $K \cap \langle x \rangle = \{1_G\}$ car φ est l'identité sur $\langle x \rangle$. Or $|G| = |\langle x \rangle||K|$ d'après le théorème d'isomorphisme, d'où le résultat.

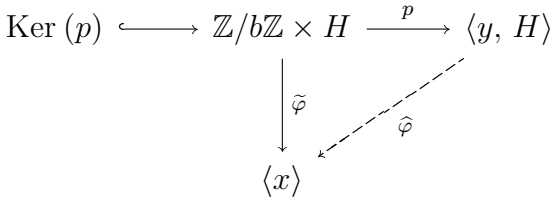
Passons à la démonstration de la partie (i). Soit H un sous-groupe propre de G contenant x. Supposons qu'on ait déjà un morphisme φ de H dans $\langle x \rangle$ envoyant x sur x. Soit a l'ordre x. Soit $y \in G \setminus H$ dont on note b l'ordre. Soient

$$\widetilde{\varphi} : \begin{array}{ccc} \mathbb{Z}/b\mathbb{Z} \times H & \longrightarrow & \langle x \rangle \\ (\bar{k},\, h) & \longmapsto & x^{k\ell}\varphi(h) \end{array} \quad \text{et } p : \begin{array}{ccc} \mathbb{Z}/b\mathbb{Z} \times H & \longrightarrow & \langle y,\, H \rangle \\ (\bar{k},\, h) & \longmapsto & y^k h \end{array},$$

des morphismes, où ℓ est un entier à déterminer. Remarquons que $\widetilde{\varphi}$ est bien défini si et seulement si $x^{b\ell} = 1$. Or x est d'ordre a, donc il faut et il suffit que :

$$a \text{ divise } b\ell. \qquad (*)$$

Considérons le diagramme suivant :



dans lequel on cherche à définir $\widehat{\varphi}$. Puisque p est surjectif, on a $\langle y,\ H\rangle \cong \frac{\mathbb{Z}/b\mathbb{Z}\times H}{\mathrm{Ker}\ (p)}$, et d'après le théorème de passage au quotient, $\widetilde{\varphi}$ passe au quotient sous Ker (p) si et seulement si :

$$\mathrm{Ker}\ (p) \subset \mathrm{Ker}\ (\widetilde{\varphi}). \qquad (**)$$

Il suffit alors de vérifier qu'en choisissant bien l'entier ℓ, $(**)$ est vérifié :

- *Déterminons* Ker (p). Soit β (un diviseur de b) tel que $\langle y\rangle \cap H = \langle y^\beta\rangle$. Alors $p((k,h)) = 1_G$ si et seulement si β divise k et $h = y^{-k}$. Donc Ker $(p) = \langle(\beta,\ x^{-\beta})\rangle$.
- *Choix de ℓ a priori pour satisfaire* $(**)$. Puisque Ker (p) est engendré par $(\beta,\ x^{-\beta})$, calculons $\widetilde{\varphi}(\beta,\ y^{-\beta})$. Posons α tel que $\varphi(y^\beta) = x^\alpha$. Alors :
$$\widetilde{\varphi}(\beta,\ y^{-\beta}) = x^{\ell\beta}\varphi(y^{-\beta}) = x^{\ell\beta-\alpha}.$$
Pour que $\widetilde{\varphi}(\beta,\ y^{-\beta}) = 1_G$, il suffit alors de poser :
$$\ell = \tfrac{\alpha}{\beta}. \qquad (***)$$
- *Vérifions que le choix de ℓ est légal, i.e. vérifions que $(***)$ est compatible avec $(*)$ et que ℓ est entier.* Par définition, β divise b, et $\varphi(y^\beta) = x^\alpha$, donc $x^{\alpha\frac{b}{\beta}} = 1_G$, donc a divise $\alpha\frac{b}{\beta}$, autrement dit, a divise $b\ell$ et $(*)$ est vérifié. Vérifions enfin que ℓ est entier. Puisque a est l'exposant de G (*c'est seulement ici que cela intervient, mais c'est essentiel*[7]), b divise a. Or on a vu que a divise $\alpha\frac{b}{\beta}$, donc $\frac{\alpha}{\beta}$ est entier. □

Théorème 2.9 (Structure des groupes abéliens finis)**.**
Pour tout groupe abélien fini non trivial, il existe r entiers $d_1,\ d_2,\ \ldots,\ d_r$ tels que

- $d_1 \geqslant 2$
- *pour tout $i \in \{1,\ldots,\ r-1\}$, d_i divise d_{i+1}*
- *on a l'isomorphisme :*
$$G \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_r\mathbb{Z}.$$

De plus, sous ces conditions, une telle liste $(d_1,\ d_2,\ \ldots,\ d_r)$ est unique.

[7] Si l'on avait simplement voulu étendre un morphisme injectif (sinon, cela n'a pas d'intérêt) de $\langle x\rangle$ dans $\mathbb{Q}/\mathbb{Z}$ en un morphisme de G dans $\mathbb{Q}/\mathbb{Z}$, on n'aurait pas eu besoin de vérifier que ℓ était entier puisque $\mathbb{Q}/\mathbb{Z}$ est un groupe divisible (i.e. qui admet pour chacun de ses éléments des racines n-ièmes pour tout n). Et de fait, un tel énoncé est vrai, même sans supposer que x est d'ordre maximal. En contre partie, l'image d'un tel morphisme χ (parfois appelé caractère) est un sous-groupe fini de $\mathbb{Q}/\mathbb{Z}$ contenant des racines n-ièmes de $\chi(x)$ sans que x ne possède lui-même de telles racines dans G, autrement dit, Im (χ) peut ne pas être isomorphe à $\langle x\rangle$. C'est uniquement en prenant x d'ordre maximal et en invoquant les propriétés de l'exposant qu'on peut affirmer que Im (χ) est isomorphe à $\langle x\rangle$ et retrouver le résultat tel que nous l'avons dans la partie (i) de cette proposition.

Démonstration.

Existence. L'existence découle de la proposition précédente : Dans G, soit x_1 un élément d'ordre maximal n_1, et soit H_1 le sous-groupe de G engendré par x_1, isomorphe à $\mathbb{Z}/n_1\mathbb{Z}$. D'après la proposition 2.8, il admet un supplémentaire K_1. Si $K_1 \neq \{1\}$, on recommence en remplaçant G par K_1 et en partant d'un élément x_2 d'ordre maximal n_2 dans K_1. Après un nombre fini r d'étapes, on a $K_r = \{1\}$. Alors $G = \bigoplus_{1 \leqslant i \leqslant r} H_i$. De plus, n_{i+1} divise n_i pour tout $i \leqslant r-1$, donc en posant $d_i = n_{r+1-i}$, on obtient la décomposition de G de l'énoncé.

Unicité. Soient $\mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_r\mathbb{Z}$ et $\mathbb{Z}/d'_1\mathbb{Z} \oplus \mathbb{Z}/d'_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d'_q\mathbb{Z}$ deux décompositions de G conformes à l'énoncé. Il est clair que l'exposant de G est égal à d_r et à d'_q. Donc $d_r = d'_q$, donc les supplémentaires $\mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_{r-1}\mathbb{Z}$ et $\mathbb{Z}/d'_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_{q-1}\mathbb{Z}$ de $\mathbb{Z}/d_r\mathbb{Z}$ et $\mathbb{Z}/d'_q\mathbb{Z}$ sont isomorphes, et l'on peut recommencer à comparer leurs exposants. Ainsi $r = q$ et $d_i = d'_i$ pour tout i. □

Tout un vocabulaire est associé à ce type de décomposition.

Définition 2.10 (A propos de la classification des groupes abéliens finis)**.**

- la *décomposition canonique de G* est la décomposition faite à la proposition 2.9 ;
- les *facteurs invariants de G* sont les entiers d_i ;
- les *diviseurs élémentaires de G* sont les $d_{i,j}$ où pour tout $i \leqslant r$, si $d_i = \prod_j p_j^{\alpha_j}$, $d_{i,j} = p_j^{\alpha_j}$;
- la *composante p-primaire de G* est le p-Sylow de G.
- le *type de G* est la liste croissante des diviseurs élémentaires $d_{i,j}$ écrits chacun autant de fois qu'ils apparaissent dans les différents facteurs invariants
- la *décomposition totale de G* la somme directe des $\mathbb{Z}/d_{i,j}\mathbb{Z}$ pour tous i, j écrite dans l'ordre croissant des$d_{i,j}$, où les $d_{i,j}$ sont les diviseurs élémentaires.

Exemple. Le groupe abélien de type (2, 2, 3, 5, 8, 9) est le groupe abélien d'ordre 4320 dont la décomposition canonique est $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/360\mathbb{Z}$. Sa composante 2-primaire est $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.

La classification des groupes abéliens est rendue particulièrement efficace grâce au lemme suivant :

Lemme 2.11 (Calcul du type d'un groupe abélien et de sa décomposition canonique)**.**

(i) Etant donné un groupe G abélien donné sous la forme

$$G \cong \mathbb{Z}/\ell_1\mathbb{Z} \oplus \mathbb{Z}/\ell_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/\ell_r\mathbb{Z},$$

on retrouve le type du groupe en réécrivant avec répétition pour tout i les puissances des facteurs premiers des ℓ_i élevés à la puissance à laquelle ils interviennent dans ℓ_i.

(ii) Deux groupes abéliens finis sont isomorphes si et seulement s'ils sont de même type.

(iii) Etant donné le type d'un groupe abélien fini, on peut reconstruire la liste des facteurs invariants en procédant ainsi : d_r sera le plus grand produit obtenu en choisissant de multiplier entre eux des diviseurs élémentaires premiers entre eux deux à

deux, on raye de la liste des diviseurs élémentaires ceux que l'on vient d'utiliser et on recommence avec ceux qui restent pour définir de la même façon d_{r-1}, et ainsi de suite jusqu'à ce que la liste soit épuisée.

Démonstration. Il est facile de vérifier qu'il existe :
- un *algorithme de déconstruction* permettant de passer à l'aide du lemme chinois de la donnée d'un groupe sous forme de somme directe de groupes cycliques à la donnée de ce groupe sous forme de somme directe de p-groupes cycliques,
- et un *algorithme de construction* permettant de passer à l'aide du lemme chinois de la donnée d'un groupe sous forme de somme directe de p-groupes à la décomposition canonique de ce groupe.

On montre que l'algorithme de construction envoie deux données différentes de groupes sous forme de somme directe de p-groupes sur deux décompositions canoniques différentes. Par unicité de cette dernière pour une classe d'isomorphie de groupes, il vient que la donnée sous forme de somme directe de p-groupes est unique (à l'ordre des facteurs près) et coïncide donc avec la décomposition totale de ce groupe. Ceci prouve le (ii).

Par unicité de la donnée d'un groupe sous forme de somme directe de p-groupes, il vient que l'algorithme de déconstruction mène à la décomposition totale du groupe. Ceci prouve le (i).

Enfin, sachant que la donnée d'un groupe sous forme de somme directe de p-groupes est unique et correspond à la décomposition totale, et puisque l'algorithme de construction mène à la décomposition canonique, le (iii) est prouvé. □

Exemple. Les groupes $G_1 = \mathbb{Z}/36\mathbb{Z} \oplus \mathbb{Z}/45\mathbb{Z} \oplus \mathbb{Z}/60\mathbb{Z}$ et $G_2 = \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/108\mathbb{Z} \oplus \mathbb{Z}/180\mathbb{Z}$ sont-ils isomorphes ? Calculons leurs types. Celui de G_1 est $(2, 2, 3, 4, 5, 5, 9, 9)$, tandis que celui de G_1 est $(4, 4, 5, 5, 9, 27)$. Puisque les deux types sont différentes, ces deux types sont différents. Leurs représentations canoniques sont $G_1 \cong \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/90\mathbb{Z} \oplus \mathbb{Z}/180\mathbb{Z}$ et $G_2 \cong \mathbb{Z}/180\mathbb{Z} \oplus \mathbb{Z}/540\mathbb{Z}$.

3 Produits semi-directs

3.1 Rappels sur les sous-groupes distingués

Définition 3.1 (Sous-groupes distingués, caractéristiques, groupes simples)**.**
Un sous-groupe H de G est dit *distingué dans* G (ou *sous-groupe normal de* G) si $gHg^{-1} = H$ pour tout $g \in G$, autrement dit, s'il est stable par les automorphismes intérieurs[8] de G. On notera alors :

$$H \triangleleft G.$$

Si un sous-groupe H est stable par tous les automorphismes de G, il est dit *caractéristique*. Un groupe dont les seuls sous-groupes distingués sont lui-même et $\{1\}$ est dit *simple*.

[8] Un automorphisme de G est dit *intérieur* s'il est une conjugaison par un élément de G. Un automorphisme qui n'est pas intérieur est dit *extérieur*.

Remarques.

1. Les assertions suivantes sont équivalentes :
(i) pour tout $g \in G$, $gHg^{-1} \subset H$,
(ii) pour tout $g \in G$, $gHg^{-1} = H$,
(iii) pour tout $g \in G$, $gH = Hg$.

2. Par contre, pour un g donné, $gHg^{-1} \subset H$ n'implique pas $gHg^{-1} = H$. Considérons par exemple le groupe :

$$G = \langle\, a,\, b \,|\, abab^{-1} = bab^{-1}a \,\rangle$$

et pour tout $k \in \mathbb{Z}$, soit le sous-groupe :

$$H_k = \langle\, b^n a b^{-n} \;;\; n \geqslant k \,\rangle_G$$

On a bien sûr l'égalité $b^\ell H_k b^{-\ell} = H_{k+\ell}$, mais $b^k a b^{-k}$ n'appartient pas à H_{k+1} (ce n'est pas tout à fait évident), donc l'inclusion de H_{k+1} dans H_k est stricte, et on a :

$$bH_kb^{-1} \subsetneq H_k, \text{ et } b^{-1}H_kb \not\subset H_k$$

Les sous-groupes H_k ne sont donc pas distingués dans G.

3. Si $K \lhd H \lhd G$, on n'a pas pour autant $K \lhd G$. En effet, considérons le groupe[9] :

$$G = \langle\, a,\, b,\, x \mid a^2 = b^2 = x^2 = 1,\; ab = ba,\; ax = xb,\; xa = bx \,\rangle.$$

Les deux sous-groupes $K = \langle\, a \,\rangle_G$ et $H = \langle\, a,\, b \,\rangle_G$ fournissent un contre-exemple. Par contre, si K est un sous-groupe caractéristique d'un groupe H, lui-même sous-groupe distingué de G, alors il est facile de voir que K est distingué dans G.

Exemples de sous-groupes distingués

0. Tout noyau d'un morphisme partant de G est un sous-groupe distingué de G.

1. Tout sous-groupe d'un groupe abélien est distingué. La réciproque est fausse. Considérons par exemple le groupe quaternionique $\mathbb{H}_8$ (cf. définition 5.1). Tous ses sous-groupes sont distingués, alors que $\mathbb{H}_8$ n'est pas abélien.

2. Le centre de tout groupe est distingué.

3. Dès qu'un groupe contient un unique p-Sylow, il est distingué (cf. chapitre 4).

4. Tout sous-groupe d'indice[10] 2 est distingué. En effet, si H est un tel sous-groupe de G, soit x un élément de $G \smallsetminus H$. Les classes d'équivalence à gauche selon le sous-groupe H (i.e. les orbites sous l'action de H par multiplication à gauche sur G) sont H et xH, les classes d'équivalence à droite selon le sous-groupe H sont H et Hx. Puisque les classes d'équivalence forment une partition de G, xH doit être égal à Hx. Ceci étant vrai pour tout $x \in G \smallsetminus H$, on en déduit que H est distingué.

5. Ce fait se généralise si G est fini. Soit G un groupe fini et H un sous-groupe de G d'indice p où p est le plus petit facteur premier de $|G|$. Alors H est distingué dans G. C'est le théorème de Frobenius (cf. proposition 6.2).

[9] Il s'agit du produit semi-direct (cf. définition 3.11) de $(\mathbb{Z}/2\mathbb{Z})^2$ par $\mathbb{Z}/2\mathbb{Z}$ où l'action de $1 \in \mathbb{Z}/2\mathbb{Z}$ sur $(\mathbb{Z}/2\mathbb{Z})^2$ consiste à échanger les deux sous-groupes $\mathbb{Z}/2\mathbb{Z} \times \{0\}$ et $\{0\} \times \mathbb{Z}/2\mathbb{Z}$. Ce groupe est isomorphe à $\mathcal{D}_4$, le groupe diédral d'ordre 4 (cf. définition 3.9).

[10] L'indice d'un sous-groupe H de G, noté $[G : H]$, est le cardinal de G/H. Si G est fini, on a l'égalité $[G : H] = |G|/|H|$.

6. Par contre, un sous-groupe d'indice 3 d'un groupe G peut ne pas être distingué si G est infini ou si 2 divise $|G|$. Par exemple, le sous-groupe H de $\mathfrak{S}_3$ engendré par une transposition (disons $H = \langle(12)\rangle$) n'est pas distingué. En effet, les classes à gauche selon H ne coïncident pas avec les classes à droite selon H.

7. On montrera, cf. proposition 5.7, que dans le cas des p-groupes, les sous-groupes maximaux sont d'indice p et sont donc distingués.

Exemples de sous-groupes caractéristiques

1. Pour tout groupe G, Le centre $\mathcal{Z}_G$, le groupe dérivé $[G, G]$ et le sous-groupe de Frattini $\Phi(G)$ (cf. définition 5.18) sont des sous-groupes caractéristiques. Les sous-groupes $C_n(G)$ de la suite centrale descendante en sont également. Il existe d'autres exemples de sous-groupes caractéristiques pouvant être associés à tout groupe. Connaître de tels sous-groupes est précieux, car étant invariants par automorphismes, ils sont d'une grande aide dans la classification des groupes.

2. Tous les sous-groupes d'un groupe cyclique sont caractéristiques, puisque pour tout diviseur d de n, le groupe $\mathbb{Z}/n\mathbb{Z}$ ne possède qu'un seul sous-groupe de cardinal d. Rappelons que pour autant, $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ n'est pas trivial (cf. paragraphe 3.5).

3. L'exemple diamétralement opposé est le cas de $(\mathbb{Z}/p\mathbb{Z})^k$ et plus généralement de tout espace vectoriel. Dans un espace vectoriel, les sous-groupes propres sont les sous-espaces propres, et ceux-ci ne sont jamais caractéristiques.

4. Le groupe $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ ne contient que de ses sous-groupes caractéristiques si et seulement si m et n sont premiers entre eux, car dans ce cas, et seulement dans ce cas-là,

$$\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) \cong \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z}) \times \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$$

Dans $\mathbb{Z}/dm\mathbb{Z} \times \mathbb{Z}/dn\mathbb{Z}$, il existe par exemple un automorphisme envoyant $(1, 0)$ sur $(1, n)$ et $(0, 1)$ sur $(0, 1)$, et ne préservant pas le sous-groupe $\mathbb{Z}/dm\mathbb{Z} \times \{0\}$.

5. Les groupes symétriques $\mathfrak{S}_n$ ont peu d'automorphismes extérieurs (ils n'en ont aucun à l'exception de $\mathfrak{S}_6$), par conséquent, le sous-groupe $\mathfrak{A}_n$ qui est distingué est aussi caractéristique.

6. Un autre exemple de groupe caractéristique est donné par la proposition 3.2 ci-dessous.

7. Dans les exemples ci-dessus (à l'exception peut-être de ceux donnés en 0.), les sous-groupes considérés sont caractéristiques parce qu'ils sont les seuls à posséder leur cardinal. Or on peut tout à fait avoir deux sous-groupes caractéristiques isomorphes. Par exemple, prenons

$$G = \mathfrak{S}_4 \times V_4.$$

où V_4 est le groupe $(\mathbb{Z}/2\mathbb{Z})^2$. Soit H le sous groupe de $\mathfrak{S}_4$ des double-transpositions (produits de deux transpositions à supports disjoints), c'est un sous-groupe caractéristique de $\mathfrak{S}_4$. Les sous-groupes $K_1 = H \times \{0_{V_4}\}$ et $K_2 = \{1_{\mathfrak{S}_3}\} \times V_4$ sont tous deux isomorphes, et constituent deux sous-groupes caractéristiques de G. C'est clair pour K_2 puisque c'est le centre de G. Pour K_1, il faut voir qu'une transposition par un automorphisme peut être envoyée sur le produit d'une transposition et d'un élément central, mais les transpositions étant deux à deux conjuguées, elles sont alors toutes envoyées sur le produit d'une transposition et du même élément central. Puisque les éléments centraux sont d'ordre 2,

les double-transpositions sont envoyées sur les double-transpositions. Donc K_1 est caractéristique[11].

Proposition 3.2 (Un exemple de sous-groupes caractéristiques)**.**
Tout p-Sylow distingué est caractéristique. Plus généralement, soit H un sous-groupe distingué d'un groupe G fini tel que $|H| \wedge |G/H| = 1$, alors H est un sous-groupe caractéristique.

Démonstration. Soit $m = |H|$. Nous affirmons que H est le seul sous-groupe d'ordre m de G. Par conséquent, tout automorphisme de G ne peut envoyer H que sur lui-même. Montrons l'affirmation. Soit K un sous-groupe de G de cardinal m. Soient $i : K \to G$ l'inclusion, $p : G \to G/H$ le passage au quotient et $\varphi = p \circ i$ la composition. Puisque l'image de φ doit diviser $|G/H|$, le morphisme φ doit être trivial. Le noyau de φ est $K \cap H$ et puisque φ est trivial, $K \cap H = K$. D'après l'égalité des cardinaux, il vient $K = H$. □

Définition 3.3 (Produit, quotient et complément)**.**
Soit G un groupe et N un sous-groupe distingué. Alors,

- $G/N = \{gN,\, g \in N\}$ l'ensemble des classes à gauche selon le sous-groupe N est naturellement muni d'une loi de groupe issue de celle de G : c'est la seule qui fasse de l'application de passage au quotient un morphisme de groupes.
- $NH = \{nh,\, n \in N,\, h \in H\}$ est un sous-groupe de G pour tout sous-groupe H de G. Si $NH = G$ et $H \neq G$, le sous-groupe H est appelé un *complément partiel de N dans G*. Si $N \cap H = \{1_G\}$ et $NH = G$, alors H est appelé un *complément de N dans G*.

Proposition 3.4 (Produit et quotient par un sous-groupe distingué)**.**

(1) Soient N un sous-groupe distingué de G et H un sous-groupe de G. Alors l'ensemble NH est égal à l'ensemble HN et constitue un sous-groupe de G. Si H aussi est distingué, alors le groupe NH est un sous-groupe distingué de G.

(2) Les assertions suivantes sont équivalentes :

(i) N est distingué dans G,

(ii) N est le noyau d'un morphisme de groupes,

(iii) l'ensemble G/N est muni d'une structure de groupe qui fait de la projection $\pi : G \to G/N$ un morphisme de groupes.

[11] Cependant il existe un groupe G' contenant G dans lequel un automorphisme intérieur échange K_1 sur K_2. C'est un fait général dû à G.Higman, B.Neumann et H.Neumann (1949) : étant donnés un groupe $G = \langle S|R\rangle$ et deux sous-groupes H et K isomorphes par un isomorphisme $\alpha : H \to K$, soit $G' = \langle\, S, t \,|\, R, tht = \alpha(h), \forall h \in H \,\rangle$. Alors, (ce n'est pas du tout évident) G est (canoniquement) inclus dans G' et $tHt^{-1} = K$. C'est une généralisation du produit semi-direct par $\mathbb{Z}$ lorsque α est un automorphisme extérieur de G.

Démonstration. La partie (2) de la proposition est bien connue. Concentrons-nous sur le partie (1). Remarquons qu'en notant $\varphi_h(n) = hnh^{-1}$, on a avec des notations évidentes :

$$\underbrace{h_1n_1\,h_2n_2\,h_3n_3...}_{\text{produit dans } NH} = \underbrace{\varphi_{h_1}(n_1)\,\varphi_{h_1h_2}(n_2)\,\varphi_{h_1h_2h_3}(n_3)...}_{\text{dans } N}\underbrace{h_1h_2h_3...}_{\text{dans } H}.$$

Ainsi $HN = NH$ et NH est stable par multiplication. Il est stable par passage à l'inverse, puisque si $nh \in NH$, alors $(nh)^{-1} \in HN$. Enfin, si H est à son tour distingué, alors pour tout $g \in G$, $gNHg^{-1} = gNg^{-1}gHg^{-1} = NH$. □

Exemples.

1. Pour un exemple où intervient le produit NH, voir la proposition 3.5 ci-dessous.
2. En général, les produits du type NH sont intéressants lorsque $N \cap H$ est réduit à l'élément neutre. Dans ce cas, les exemples sont légions et constituent ce qu'on appelle un *produit semi-direct de N par H* auquel est consacré le paragraphe 3.2 suivant.
3. Voir également le lemme 4.7 et la proposition 4.8, traitant le cas de groupes où deux (respectivement tous les) sous-groupes de Sylow sont distingués.

On redonne sans démonstration les théorèmes classiques suivants.

Proposition 3.5 (Théorèmes d'isomorphisme)**.**

Premier théorème d'isomorphisme. *Soit φ un morphisme de groupes G vers G'. Alors le morphisme induit de $G/\mathrm{Ker}\,(\varphi) \to \mathrm{Im}\,(\varphi)$ est un isomorphisme.*

Deuxième théorème d'isomorphisme. *Soit N et H deux sous-groupes de G tels que N est distingué dans G. Alors $N \cap H$ est distingué dans H et l'inclusion $H \to NH$ induit par passage au quotient l'isomorphisme $\frac{H}{H\cap N} \to \frac{NH}{N}$.*

Troisième théorème d'isomorphisme. *Soit N et M deux sous-groupes distingués de G, M étant inclus dans N. Alors N/M est distingué dans G/M et le morphisme quotient $\frac{G/M}{N/M}$ est isomorphe à G/N.* □

3.2 Produit semi-direct interne

La définition du produit semi-direct est motivée par la proposition suivante.

Proposition 3.6 (Sous-groupes distingués admettant un complément)**.**
Soient N un sous-groupe distingué de G admettant un complément H. Autrement dit, N et H sont deux sous-groupes tels que :

(i) $N \triangleleft G$,
(ii) $N \cap H = \{1_G\}$,
(iii) G *et* $N \times H$ *sont en bijection.*

Alors la bijection $\varphi : N \times H \to G$, $(n, h) \mapsto nh$ devient un isomorphisme de groupe si et seulement si on munit $N \times H$ de la loi $(n, h)(n', h') = (nhn'h^{-1}, hh')$.

Démonstration. Avec la condition (i), NH est un groupe, tandis qu'avec les conditions (ii) et (iii), l'ensemble G et son sous-ensemble NH sont de même cardinal, donc sont égaux. En effet, $nh = n'h'$ implique $n'^{-1}n = h'h^{-1}$, donc $n = n'$ et $h = h'$. Pour que φ soit un groupe, il faut que $(n, h).(n', h') = \varphi^{-1}(nhn'h')$. Mais $nhn'h' = nhn'h^{-1}hh'$, or $nhn'h^{-1}$ appartient à N car N est distingué, donc $\varphi^{-1}(nhn'h') = (nhn'h^{-1}, hh')$. Donc pour que φ soit un isomorphisme de groupe, il faut munir NH de la loi $(n, h)(n', h') = (nhn'h^{-1}, hh')$. Réciproquement, si on munit NH d'une telle loi, alors on vérifie que :

(a) cette loi est associative,
(b) $(1_N, 1_H)$ est l'élément neutre,
(c) l'inverse de (n, h) est $(h^{-1}nh, h^{-1})$
(d) φ transforme cette loi en la loi de G devenant ainsi un morphisme de groupes, donc un isomorphisme. □

Définition 3.7 (Produit semi-direct (interne) de deux sous-groupes)**.**
Deux sous-groupes H et N de G vérifiant

(i) $N \lhd G$,
(ii) $N \cap H = \{1_G\}$,
(iii) G et $N \times H$ sont en bijection.

sont dits en *produit semi-direct*. On écrit alors[12] $G = N \rtimes H$. Si l'on paramètre G par $N \times H$, la loi de G devient :

$$(n, h)(n', h') = (nhn'h^{-1}, hh').$$

Le sous-groupe H agit sur N par conjugaison dans G. Par un abus de langage, on pourrait écrire $\mathrm{Int}(G) \subset \mathrm{Aut}(N)$. Le morphisme structurel de cette action est noté Ad :

$$\mathrm{Ad} : \begin{array}{ccc} H & \longrightarrow & \mathrm{Aut}(N) \\ h & \longmapsto & \mathrm{Ad}_h : n \mapsto hnh^{-1} \end{array} .$$

Remarquons que sous les conditions (i) et (ii), la condition (iii) est équivalente à chacune des conditions suivantes :

(iii-a) $G/N \cong H$,
(iii-b) $G = NH$,
(iii-c) $|G| = |N|.|H|$, à supposer que G est fini.

Proposition 3.8 (Produits directs parmi les produits semi-directs)**.**
Soient N et H deux sous-groupes d'un groupe G. On suppose que N est distingué dans G avec $N \lhd G$. Les assertions suivantes sont équivalentes.

(i) le produit semi-direct $N \rtimes H$ est direct[13] *;*
(ii) l'action par conjugaison induite de H sur N est triviale ;
(iii) $[N, H] = \{1_G\}$ (cf. [14]*) ;*
(iv) H est distingué dans G.

[12] Remarquer que les triangles inclus dans les symboles des expressions $N \lhd G$ et $N \rtimes H$ vont dans le même sens.

[13] Dans ce cas-là, on dit aussi que le produit semi-direct est *trivial*.

[14] Le sous-groupe $[N, H]$ de G est le sous-groupe engendré par les éléments $nhn^{-1}h^{-1}$ avec $n \in N$ et $h \in H$.

Démonstration. Les implications $(i) \Leftrightarrow (ii) \Leftrightarrow (iii)$ et $(i) \Rightarrow (iv)$ sont immédiates. Prouvons l'implication $(iv) \Rightarrow (i)$. Pour cela, étudions le commutateur $[n,h] = nhn^{-1}h^{-1}$. Il vient $n(hn^{-1})h^{-1}) \in N$ mais $(nhn^{-1})h^{-1} \in H$. Or $N \cap H = \{1_G\}$, donc $[n,h] = 1$. □

Remarque. Attention cependant, un produit semi-direct non trivial peut être isomorphe à un produit direct, cf. l'exemple donné au début du paragraphe 3.4.

Passons aux exemples.

Exemples.

- $\mathfrak{S}_n = \mathfrak{A}_n \rtimes \langle\tau\rangle$ où τ est une transposition (ou un produit impair de transpositions à supports disjoints). On peut le voir rapidement en remarquant que :
  - $\mathfrak{A}_n = \mathrm{Ker}\,(\varepsilon)$, donc $\mathfrak{A}_n \lhd \mathfrak{S}_n$,
  - $\varepsilon(\tau) = -1$, donc $\mathfrak{A}_n \cap \langle\tau\rangle = \{1_{\mathfrak{S}_n}\}$,
  - $\mathfrak{S}_n/\mathfrak{A}_n \cong \mathbb{Z}/2\mathbb{Z} \cong \langle\tau\rangle$,

  où ε est la signature.
- $\mathcal{O}(n,\mathbb{R}) = \mathcal{SO}(n,\mathbb{R}) \rtimes \langle\gamma\rangle$ où γ est une réflexion (symétrie dont le noyau est un hyperplan). On peut le voir rapidement en remarquant que :
  - $\mathcal{SO}(n,\mathbb{R}) = \mathrm{Ker}\,(\det)$, donc $\mathcal{SO}(n,\mathbb{R}) \lhd \mathcal{O}(n,\mathbb{R})$,
  - $\det(r) = -1$, donc $\mathcal{SO}(n,\mathbb{R}) \cap \langle r\rangle = \{1_{\mathcal{O}(n,\mathbb{R})}\}$,
  - $\mathcal{O}(n,\mathbb{R})/\mathcal{SO}(n,\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z} \cong \langle r\rangle$,

  où det est le déterminant.
- $\mathcal{GL}(n,\Bbbk) = \mathcal{SL}(n,\Bbbk) \rtimes \mathrm{Dil}$ où $\Bbbk$ est un corps différent de $\mathbb{F}^2$ et Dil est l'ensemble des matrices diagonales n'ayant que des 1 sur la diagonale excepté le premier élément diagonal qui est un élément quelconque de $\Bbbk^*$. On peut le voir rapidement en remarquant que :
  - $\mathcal{GL}(n,\Bbbk) = \mathrm{Ker}\,(\det)$, donc $\mathcal{SL}(n,\Bbbk) \lhd \mathcal{GL}(n,\Bbbk)$,
  - $\{\det(d),\ d \in \mathrm{Dil} \smallsetminus \{\mathrm{Id}_{\Bbbk^n}\}\} \in \Bbbk^* \smallsetminus \{1_\Bbbk\}$, donc $\mathcal{SL}(n,\Bbbk) \cap \langle d\rangle = \{\mathrm{Id}_{\Bbbk^n}\}$,
  - $\mathcal{GL}(n,\Bbbk)/\mathcal{SL}(n,\Bbbk) \cong \Bbbk^* \cong \mathrm{Dil}$,

  où det est le déterminant.
- Voir aussi $\mathcal{D}_n \subset \mathcal{O}(2,\mathbb{R})$, le groupe diédral, cf. définition 3.9 ci-dessous.

Définition 3.9 (Le groupe diédral $\mathcal{D}_n$)**.**
Le groupe diédral $\mathcal{D}_n$ est le groupe des déplacements du plan préservant un polyèdre régulier à n côtés centré en l'origine de $\mathbb{R}^2$ et ayant un sommet en $(1,0)$. Soient Rot_n le sous-groupe de $\mathcal{D}_n$ d'ordre n engendré par la rotation centrée en l'origine d'angle $2\pi/n$ et S le sous-groupe de $\mathcal{D}_n$ d'ordre 2 engendré par la réflexion γ d'axe horizontal. En voyant $\mathcal{D}_n$ plongé dans $\mathcal{O}(2,\mathbb{R})$, cela revient à poser :

$$\begin{cases} \mathrm{Rot}_n = \{R_\theta,\ \theta \in \frac{2\pi}{n}\mathbb{Z}\} & \text{où} \quad R_\theta = \left(\begin{smallmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{smallmatrix}\right), \\ S = \{\mathrm{Id}_{\mathbb{R}^2},\ \gamma\} & \text{où} \quad \tau = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right). \end{cases}$$

Le groupe $\mathcal{D}_n$ contient n rotations et n symétries (dont les axes passent par les sommets ou les milieux des arêtes du polyèdre). Or Rot_n contient n rotations et $\gamma\mathrm{Rot}_n$ contient n transformations du plan de déterminant -1, donc contient les n symétries. De plus $\mathrm{Rot}_n \cap S = \{\mathrm{Id}_{\mathbb{R}^2}\}$. Enfin, $\gamma.\mathrm{Rot}_n.\gamma = \mathrm{Rot}_n$ puisque :

$$\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} = \begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix} = \begin{pmatrix}\cos(-\theta) & -\sin(-\theta)\\ \sin(-\theta) & \cos(-\theta)\end{pmatrix}.$$

Donc Rot_n est distingué dans $\mathcal{D}_n$. Donc :

$$\mathcal{D}_n = \mathrm{Rot}_n \rtimes \langle\gamma\rangle,$$

et l'action est donnée par la relation

$$\gamma R_\theta \gamma = R_{(-\theta)},$$

donc ce groupe n'est commutatif que si $\sigma = \sigma^{-1}$, donc que si $n = 2$. Remarquons qu'en remplaçant Rot_n par $\mathcal{SO}(2, \mathbb{R})$, on retrouve le produit semi-direct donné ci-dessus : $\mathcal{SO}(2, \mathbb{R}) = \mathcal{SO}(2, \mathbb{R}) \rtimes \langle\gamma\rangle$.

Un dernier exemple :

Proposition 3.10 (Sous-groupes de Sylow dans des produits semi-directs)**.**
Soit un groupe G de cardinal $p^\alpha m$ où p est un nombre premier ne divisant pas m, soient N un sous-groupe distingué de G d'ordre m et P un sous-groupe de cardinal p^α. Alors

$$G = N \rtimes P.$$

Démonstration. En effet, N est distingué, $N \cap P = \{1_G\}$ (conséquence du théorème de Lagrange appliqué aux éléments de $N \cap P$), et $|NP| = |G|$. □

3.3 Produit semi-direct externe

On cherche à étendre la notion de produit semi-direct interne à deux groupes « étrangers l'un à l'autre », i.e. qui ne soient pas forcément plongé dans un même troisième dans un même troisième. De la même, le produit direct interne a donné lieu au produit direct externe et la somme directe interne a donné lieu à la somme directe externe.

Pour étendre cette notion de produit semi-direct, souvenons-nous que la loi dans $N \rtimes H$ est donnée par la formule

$$(n, h).(n', h') = (nhn'h^{-1}, hh') = (n\varphi_h(n'), hh')$$

où φ appartient à $\mathrm{Hom}(H, \mathrm{Int}(G))$ en associant à tout élément $h \in H$ la conjugaison par h dans G. Cette conjugaison par h est un automorphisme intérieur dans G qui stabilise N et qui du point de vue de N est un automorphisme quelconque (éventuellement extérieur). Ainsi, φ peut être vu comme un morphisme de $\mathrm{Hom}(H, \mathrm{Aut}(N))$.

Définition 3.11 (Produit semi-direct (externe) de deux groupes)**.**
Soit N et H deux groupes. Soit φ, un morphisme de H dans $\mathrm{Aut}(N) : h \mapsto \varphi_h$. Le produit semi-direct de N par H via le morphisme φ et noté $N \rtimes_\varphi H$ est le groupe d'ensemble sous-jacent $N \times H$ et de loi

$$(n,\, h).(n',\, h') = (n\,\varphi_h(n),\, hh'), \qquad (*)$$

que l'on gagnera à mémoriser sous la forme :

$$(1,\, h).(n,\, 1).(1,\, h)^{-1} = (\varphi_h(n),\, 1). \qquad (**)$$

Remarques.

1. Il faudrait vérifier que la loi ainsi définie est bien une loi de groupe. Commençons par remarquer que l'élément neutre est $(1_N,\, 1_H)$, et que l'inverse de $(n,\, h)$ est

$$\big(\varphi_{h^{-1}}(n^{-1}),\, h^{-1}\big).$$

Le calcul est facile, à condition de se souvenir que ${\varphi_h}^{-1} = \varphi_{h^{-1}}$, car $\varphi \in \mathrm{Hom}(H,\, \mathrm{Aut}(N))$. Il reste à voir que la loi est associative, cf. remarque suivante.

2. Si φ n'est qu'une application de H dans $\mathfrak{S}(N)$, ce qui suffit après tout pour constituer une action de H sur N, on retrouve que la loi (*) fait de $N \rtimes_\varphi H$ un groupe si et seulement si φ est en fait un *morphisme* de H *à valeurs dans* $\mathrm{Aut}(N)$. En effet, en étudiant l'associativité de la loi dans $N \rtimes_\varphi H$, on obtient :

$$\begin{array}{rcl} \big((n,\, h)(n',\, h')\big)\,(n'',\, h'') & = & (n\,\varphi_h(n')\,\varphi_{hh'}(n''),\, hh'h'')\ , \\ (n,\, h)\,\big((n',\, h')(n'',\, h'')\big) & = & (n\,\varphi_h(n'\,\varphi_{h'}(n'')),\, hh'h'')\ . \end{array}$$

d'où l'on tire l'égalité suivante, vraie pour tous $n', n'' \in N$, $h, h' \in H$:

$$\varphi_h(n')\varphi_{hh'}(n'') = \varphi_h(n'\varphi_{h'}(n''))$$

En posant $h' = 1_H$, on obtient l'égalité suivante,

$$\varphi_h(n')\,\varphi_h(n'') = \varphi_h(n'n''),$$

autrement dit, φ est bien à valeur dans $\mathrm{Aut}(N)$. Et, en posant $n' = 1_N$, on a :

$$\varphi_h(\varphi_{h'}(n'')) = \varphi_{hh'}(n''),$$

autrement dit, φ est bien un morphisme.

3. Le produit semi-direct interne ne fait intervenir que des automorphismes intérieurs du groupe G, et la notation $G = N \rtimes H$ n'est pas ambigüe une fois que l'on connaît les sous-groupes N et H. Par contre, le produit semi-direct externe de deux groupes N et H est une construction à partir d'un morphisme $\varphi \in \mathrm{Hom}(H,\, \mathrm{Aut}(N))$ bien particulier qui doit apparaître dans l'écriture $N \rtimes_\varphi H$. Il arrive qu'on l'omette cependant lorsqu'on considère qu'il n'y a pas d'ambiguïté. Ce cas arrive par exemple lorsqu'on a démontré que pour ces deux groupes N et H, tous les morphismes non triviaux de $\mathrm{Hom}(H,\, \mathrm{Aut}(N))$ se déduisent les uns des autres par la formule

$$(\varphi_2)_h(n) = \alpha^{-1}(\varphi_1)_{\beta(h)}\alpha(n).$$

où $\alpha \in \mathrm{Aut}(N)$ et $\beta \in \mathrm{Aut}(H)$, comme nous allons le voir au paragraphe suivant. Dans ce cas, $N \rtimes H$ désigne toujours un produit semi-direct non trivial (i.e. il est construit à partir d'un morphisme non trivial). Mais attention, cette situation n'est absolument pas générale.

4. On voit par l'égalité (**) que l'automorphisme φ_h qui est éventuellement extérieur dans $\mathrm{Aut}(N)$ apparaît comme un automorphisme intérieur dans $N \rtimes_\varphi H$. On reviendra sur ce point après avoir énoncé la proposition 3.12 établissant le lien entre les deux produits semi-directs (interne et externe).

Proposition 3.12 (Rapport entre les deux notions de produit semi-direct)**.**
Soient N et H deux groupes, φ un morphisme de H dans $\mathrm{Aut}(N)$*. Soit $G = N \rtimes_\varphi H$. Soient $\bar{N} = \{(n, 1)\ ;\ n \in N\}$ et $\bar{H} = \{(1, h)\ ;\ h \in H\}$ les images de H et N dans G. Alors G est le produit semi-direct interne de $\bar{N}$ par $\bar{H}$. Ainsi :*

(i) $\bar{N} \triangleleft G$, $\bar{N} \cap \bar{H} = \{1_G\}$, *et* $\bar{N}\bar{H} = G$;
(ii) $\bar{H}$ *agit sur* $\bar{N}$ *par conjugaison dans* G ;
(iii) on a un isomorphisme de groupes Φ : $\begin{array}{ccc} N \rtimes_\varphi H & \longrightarrow & \bar{N} \rtimes \bar{H} \\ (n,\, h) & \longmapsto & \bar{n}.\bar{h} \end{array}$. □

Remarques. Le produit semi-direct externe est donc une construction « à rebours » du produit semi-direct interne par laquelle des automorphismes (éventuellement extérieurs) deviennent intérieurs :

- Si G est le produit semi-direct interne de N par H, alors H agit sur N via les automorphismes intérieurs de G.
- A l'inverse, prenons H et N deux groupes, et φ, un morphisme de H dans $\mathrm{Aut}(N)$, le produit semi-direct externe $N \rtimes H$ rend tous ces automorphismes intérieurs, puisque φ_h coïncide avec Ad_h, la restriction dans N de la conjugaison par h dans $N \rtimes H$.

Ainsi, pour tout automorphisme ψ d'un groupe G, il existe un « sur-groupe » G' contenant G comme sous-groupe distingué tel que ψ coïncide avec la restriction à G d'un automorphisme intérieur.

Exemples.

- Il existe un unique morphisme non trivial de $\mathbb{Z}/2\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$, consistant à envoyer l'élément 1 de $\mathbb{Z}/2\mathbb{Z}$ sur l'unique involution de $\mathbb{Z}/n\mathbb{Z}$ envoyant k sur $-k$. Le produit semi-direct $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ qui en résulte est isomorphe au groupe diédral $\mathcal{D}_n$.
- Soit $\vec{E}$ un espace vectoriel et $\mathrm{Aut}(\vec{E})$ le groupes des bijections de $\vec{E}$ préservant l'addition. Considérons l'inclusion $\varphi : \mathcal{GL}(\vec{E}) \to \mathrm{Aut}(\vec{E})$. Elle permet de construire le produit semi-direct **externe** :
$$\vec{E} \rtimes_\varphi \mathcal{GL}(\vec{E}). \tag{1}$$
Maintenant, soit E un espace affine d'espace directeur $\vec{E}$. Soit $\mathcal{GA}(E)$ le groupe des transformations affines de E, soit $\mathcal{T}(E)$ le sous-groupe des translations et $\mathcal{GA}_O(E)$ le sous-groupes des transformations affines fixant le point O. Soit enfin le morphisme $\ell : \mathcal{GA}(E) \to \mathcal{GL}(\vec{E})$, $f \mapsto \vec{f}$, où $\vec{f}$ est la partie linéaire de f. On a le produit semi-direct **interne** :
$$\mathcal{GA}(E) = \mathcal{T}(E) \rtimes \mathcal{GA}_O(E). \tag{2}$$
On peut le voir rapidement en remarquant que :
  - $\mathcal{T}(E) = \mathrm{Ker}\,(\ell)$, donc $\mathcal{T}(E) \triangleleft \mathcal{GA}(E)$,
  - $\ell(\mathcal{GA}_0(E) \setminus \{\mathrm{Id}_E\}) = \mathcal{GL}(\overrightarrow{E}) \setminus \{\mathrm{Id}_{\vec{E}}\}$, donc $\mathcal{T}(E) \cap \mathcal{GA}_O(E) = \{\mathrm{Id}_E\}$,
  - $\mathcal{GA}_0(E)/\mathcal{T}(E) \cong \mathcal{GL}(\vec{E}) \cong \mathcal{GA}_0(E)$.

Ces deux produits semi-directs (1) et (2), externe et interne respectivement, décrivent deux points de vue différent d'une même situation, et on a un isomorphisme Φ entre ces deux groupes qui préserve la structure de produit semi-direct (cf. paragraphe 3.4). En effet, posons :
$\tau : \vec{E} \to \mathcal{GA}(E)$, $\vec{u} \mapsto t_{\vec{u}}$, où $t_{\vec{u}}$ est la translation par $\vec{u}$,
$s : \mathcal{GL}(\vec{E}) \to \mathcal{GA}(E)$, $\vec{f} \mapsto f_O$ (l'application affine de partie linéaire $\vec{f}$ fixant O).
$\Phi : \vec{E} \rtimes_\varphi \mathcal{GL}(\vec{E}) \to \mathcal{GA}(E)$, $(\vec{u}, \vec{f}) \mapsto \tau(\vec{u}) \circ s(\vec{f}) = t_{\vec{u}} \circ f_O$.

On a alors le diagramme suivant, en affirmant que le sous-diagramme réduit aux flèches pleines est commutatif, tandis que s vérifie $\ell s = \mathrm{Id}$. On verra au chapitre 7 que l'existence du morphisme s est intimement lié au fait qu'on a un produit semi-direct.

$$\begin{array}{ccccc} \mathcal{T}(E) & \xrightarrow[incl.]{} & \mathcal{GA}(E) & \underset{\ell}{\overset{s}{\leftrightarrows}} & \mathcal{GL}(\vec{E}) \\ \uparrow{\scriptstyle \tau} & & \uparrow{\scriptstyle \Phi} & & \uparrow{\scriptstyle =} \\ \vec{E} & \xrightarrow[can.]{} & \vec{E} \rtimes_\varphi \mathcal{GL}(\vec{E}) & \xrightarrow[can.]{} & \mathcal{GL}(\vec{E}) \end{array}$$

En conclusion, on a montré que :

$$\mathcal{GA}(E) \cong \vec{E} \rtimes \mathcal{GL}(\vec{E}).$$

Le fait que Φ préserve la structure de produit semi-direct (cf. paragraphe suivant) vient du fait que $\Phi(\vec{u}, \vec{f}) = \tau(\vec{u}) \circ s(\vec{u})$.

- Pour d'autres exemples, cf. paragraphe 3.6.

3.4 Structures de produits semi-directs

Il est naturel de se demander si deux produits semi-directs externes munis de deux actions différentes définissent le même groupe à isomorphismes près. C'est une question difficile, mais il existe un cas simple (il y en a d'autres, comme on le verra au paragraphe 7.2) où l'on sait répondre : lorsqu'on peut passer d'un premier produit semi-direct de N par H à un second par des automorphismes de N et de H (comme dans l'exemple ci-dessus entre $\mathcal{GA}(E)$ et $\vec{E} \rtimes \mathcal{GL}(\vec{E})$). Formalisons ce cas.

Définition 3.13 (Structure de produit semi-direct)**.**
La *structure de produit semi-direct* d'un produit semi-direct externe consiste en la donnée :
(i) de deux groupes N et H,
(ii) d'un morphisme $\varphi \in \mathrm{Hom}(N, \mathrm{Aut}(N))$,
que l'on résumera en disant : « Soit $N \rtimes_\varphi H$ une structure de produit semi-direct externe. »
La *structure de produit semi-direct* d'un produit semi-direct interne consiste en la donnée :
(i) d'un groupe G,
(ii) d'un sous-groupe H et d'un sous-groupe distingué N tels que $G = N \rtimes H$,
(iii) de deux injections $i : N \to G$ et $s : H \to G$,
que l'on résumera en disant : « Soit $N \xrightarrow{i} G \xleftarrow{s} H$ une structure de produit semi-direct interne. ».
Une structure de produit semi-direct $N \xrightarrow{i} G \xleftarrow{s} H$ (respectivement $N \rtimes_\varphi H$) est dite *triviale* si :

$$G = i(N) \times s(H)$$

(resp. si φ est le morphisme trivial).

Remarque. Les deux notions sont identiques, seul le point de vue change. Les injections i et s incluses dans la donné du produit semi-direct interne sont les injections canoniques

$i : \begin{array}{ccc} N & \longrightarrow & G \\ n & \longmapsto & (n, 1_H) \end{array}$ et $s : \begin{array}{ccc} N & \longrightarrow & G \\ n & \longmapsto & (1_N, H) \end{array}$ dans le produit semi-direct externe. Le morphisme φ inclus dans la donnée du produit semi-direct externe est le morphisme $\widetilde{\mathrm{Ad}}_s : \begin{array}{ccc} H & \longrightarrow & \mathrm{Aut}(N) \\ h & \longmapsto & \{n \mapsto i^{-1}(hi(n)h^{-1})\} \end{array}$ dans le produit semi-direct interne.

Définition 3.14 (Similitude de structures de produits semi-directs)**.**
Soient deux structures de produit semi-direct interne $N \xrightarrow{i} G \xleftarrow{s} H$ et $N' \xrightarrow{i'} G' \xleftarrow{s'} H'$. Ces deux structures seront dites *semblables* s'il existe trois isomorphismes $\alpha : N' \to N$, $\Phi : G' \to G$, $\beta : H' \to H$, tels que

$$\begin{cases} \Phi\, i' &= i\, \alpha, \\ \Phi\, s' &= s\, \beta, \end{cases}$$

autrement dit tels que le diagramme ci-dessous commute.

$$\begin{array}{ccccc} N & \xrightarrow{i} & G & \xleftarrow{s} & H \\ \uparrow{\scriptstyle \alpha} & & \uparrow{\scriptstyle \Phi} & & \uparrow{\scriptstyle \beta} \\ N' & \xrightarrow{i'} & G' & \xleftarrow{s'} & H' \end{array}$$

Un tel isomorphisme Φ sera appelé une *similitude de structures de produit semi-direct.*

Remarque. La donné des morphismes α et β ou celle de Φ sont équivalentes.

Lemme 3.15 (Actions de produits semi-directs de structures semblables)**.**
Soient deux structures de produits semi-directs semblables comme sur le diagramme ci-dessous.

$$\begin{array}{ccccc} M & \xrightarrow{i} & M \rtimes_\psi K & \xleftarrow{s} & K \\ \uparrow{\scriptstyle \alpha} & & \uparrow{\scriptstyle \Phi} & & \uparrow{\scriptstyle \beta} \\ N & \xrightarrow{i'} & N \rtimes_\varphi H & \xleftarrow{s'} & H \end{array}$$

Alors pour tous $n \in N$, $h \in H$, on a :

$$\varphi_h(n) = \alpha^{-1}\, \psi_{\beta(h)}\, \alpha\, (n).$$

ce qui traduit simplement le fait que le diagramme suivant commute :

$$\begin{array}{ccc} K & \xrightarrow{\psi} & \mathrm{Aut}(M) \\ \uparrow{\scriptstyle \beta} & & \uparrow{\scriptstyle \mathrm{Ad}_\alpha} \\ H & \xrightarrow{\varphi} & \mathrm{Aut}(N) \end{array}$$

où Ad_α *est le morphisme de* $\mathrm{Aut}(N)$ *dans* $\mathrm{Aut}(M)$ *qui envoie un automorphisme* f *sur* $\alpha f \alpha^{-1}$*.*

Démonstration. Partons de l'égalité $(**)$ de la définition 3.11. Pour tout $n \in N$ et tout $h \in H$, on a :

$$\begin{aligned}
\psi_{\beta(h)}\alpha(n) &= (1, \beta(h))\,(1, \alpha(n))\,(1, \beta(h))^{-1} \\
&= \Phi\big((1,h)\big)\,\Phi\big((1,n)\big)\,\Phi\big((1,h)\big)^{-1} \\
&= \Phi\big(\,(1,h)\,(1,n)\,(1,h)^{-1}\,\big) \\
&= \Phi\big(\,(\,\varphi_h(n),\,1)\,\big) \\
&= \alpha\varphi_h(n).
\end{aligned}$$

□

Proposition 3.16 (Premier critère de similitudes de structure de produit semi-direct)**.** *Soient* $\varphi^1,\ \varphi^2 \in \mathrm{Hom}(H,\, \mathrm{Aut}(N))$ *et* $\gamma \in \mathrm{Aut}(H)$ *tels que*

$$\varphi^2 = \varphi^1 \circ \gamma.$$

Alors les structures de produit semi-direct $N \rtimes_{\varphi_1} H$ *et* $N \rtimes_{\varphi_2} H$ *sont équivalentes (donc les groupes résultant sont isomorphes).*

Démonstration. Il suffit de poser $\alpha = \mathrm{Id}_N$, $\beta = \gamma \in \mathrm{Aut}(H)$ et

$$\Phi\ :\ \begin{array}{ccc} N \rtimes_{\varphi^2} H & \longrightarrow & N \rtimes_{\varphi^1} H \\ (n,\, h) & \longmapsto & (n,\, \gamma(h)) \end{array},$$

et d'appliquer la définition 3.14. □

Exemples.

- Les groupes non abéliens du type $\mathbb{R} \rtimes \mathbb{R}$ sont tous isomorphes (cf. paragraphe 3.6).
- L'étude des groupes non abéliens du type $\mathbb{R}^2 \rtimes \mathbb{R}$ (cf. paragraphe 3.6).
- Les groupes $G = \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ où p et q sont premiers avec p divise $q-1$. Pour un tel couple p, q, il n'existe qu'un seul produit semi-direct non trivial (cf. proposition 6.4).
- Soit $V_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Les groupes du type $V_4 \rtimes \mathbb{Z}/3\mathbb{Z}$ non abéliens sont tous isomorphes. De même des groupes du type $\mathbb{Z}/3\mathbb{Z} \rtimes V_4$ non abéliens (cf. proposition 6.7).
- Voir l'étude des groupes d'ordre p^3 (cf. proposition 6.9).

Proposition 3.17 (Deuxième critère de similitude de structure de produit semi-direct)**.** *Soient* $\varphi^1,\ \varphi^2 \in \mathrm{Hom}(H,\, \mathrm{Aut}(N))$ *et* $\gamma \in \mathrm{Aut}(N)$ *tels que pour tout* $h \in H$*, on ait*

$$\varphi^2{}_h = \gamma^{-1} \circ \varphi^1{}_h \circ \gamma.$$

Alors les produits semi-directs $N \rtimes_{\varphi_1} H$ *et* $N \rtimes_{\varphi_2} H$ *sont équivalents (donc les groupes résultant sont isomorphes).*

Démonstration. Il suffit de poser $\alpha = \gamma$, $\beta = \mathrm{Id}_H \in \mathrm{Aut}(H)$ et

$$\Phi\ :\ \begin{array}{ccc} N \rtimes_{\varphi^2} H & \longrightarrow & N \rtimes_{\varphi^1} H \\ (n,\, h) & \longmapsto & (\gamma(n),\, h) \end{array},$$

et d'appliquer la définition 3.14. □

Exemples.

- Voir le lemme 3.19 ci-dessous à propos de $\mathfrak{S}_3 \rtimes \mathbb{Z}/2\mathbb{Z}$.
- Voir l'étude des groupes de la forme $\mathbb{R}^2 \rtimes \mathbb{R}$ au paragraphe 3.6.
- Pour tout p, les groupes non abéliens de la forme $\big(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}\big) \rtimes \mathbb{Z}/p\mathbb{Z}$ sont tous isomorphes cf. proposition 6.9.

Proposition 3.18 (Structure de produit direct parmi les structures de produits semi-directs)**.**
Soit $N \xrightarrow{i} G \xleftarrow{s} H$ une structure de produit semi-direct. Les assertions suivantes sont équivalentes :

(i) la structure de produit semi-direct $N \xrightarrow{i} G \xrightarrow{s} H$ est triviale ;
(ii) $[i(N),\, s(H)] = 1_G$;
(iii) les structures $N \xrightarrow{i} G \xrightarrow{s} H$ et $N \xrightarrow{can.} N \times H \xrightarrow{can.} H$ sont semblables. □

Attention ! Deux produits semi-directs peuvent ne pas être équivalents, alors qu'ils définissent deux groupes isomorphes. Voici un exemple.

Lemme 3.19 (Un exemple contre-intuitif)**.**
Tout produit semi-direct non trivial $\mathfrak{S}_3 \rtimes \mathbb{Z}/2\mathbb{Z}$ est isomorphe au produit direct $\mathfrak{S}_3 \times \mathbb{Z}/2\mathbb{Z}$! Mais bien entendu, ces deux structures de produit (semi)-direct ne sont pas les semblables.

Démonstration.
0°) Tout d'abord, on voit grâce au deuxième critère s'équivalence qu'il n'existe qu'un seul produit semi-direct non trivial $\mathfrak{S}_3 \rtimes \mathbb{Z}/2\mathbb{Z}$, décrit par un morphisme $\mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathfrak{S}_3)$ envoyant 1 sur la conjugaison par une transposition de $\mathfrak{S}_3$. En effet, deux tels morphismes $\varphi_1 = \mathrm{Ad}_{\tau_1}$ et $\varphi_2 = \mathrm{Ad}_{\tau_2}$ sont conjugués au but par un automorphisme Φ de $\mathfrak{S}_3$ envoyant la deuxième transposition τ_2 sur la première τ_1 :

$$\Phi\varphi_2\Phi^{-1} = \Phi\mathrm{Ad}_{\tau_2}\Phi^{-1} = \mathrm{Ad}_{\Phi(\tau_2)} = \mathrm{Ad}_{\tau_1} = \varphi_1.$$

1°) Montrons le lemme. Soit $G = \mathfrak{S}_3 \times \mathbb{Z}/2\mathbb{Z}$, soit N l'image de $\mathfrak{S}_3$ dans G et τ un élément d'ordre 2 dans N. Soit H l'image de $\mathbb{Z}/2\mathbb{Z}$ dans G et j l'élément d'ordre 2 de H. On a :

$$G = N \times H.$$

Considérons maintenant K, le sous-groupe de G engendré par $j\tau$. Le sous-groupe K est d'ordre 2, mais n'est pas central, puisque τ lui-même n'est pas central alors que j l'est. Puisque N est distingué dans G et que $N \cap K = \{1_G\}$, on a :

$$G = N \rtimes K,$$

et ce produit semi-direct n'est pas trivial.

2°) Montrons que ces deux structures de produit (semi)-direct ne sont pas semblables. Une similitude de structures de produit semi-direct enverrait $(1,\, H) \subset N \times H$ sur $(1,\, K) \subset N \rtimes K$, or $(1,\, H)$ est un sous-groupe central, tandis que $(1,\, K)$ n'en est pas un !

3°) L'isomorphisme $\Phi \;:\; \mathfrak{S}_3 \times \mathbb{Z}/2\mathbb{Z} \to \mathfrak{S}_3 \rtimes \mathbb{Z}/2\mathbb{Z}$ est donné par :

$$\Phi(\sigma,\, 0) = (\sigma, 0) \qquad \text{et} \qquad \Phi(\sigma,\, 1) = (\sigma\tau, 1),$$

où σ est un élément quelconque de $\mathfrak{S}_3$ et τ est l'unique transposition de $\mathfrak{S}_3$ telle que les conjugaisons par $(1, 1)$ et par $(\tau,\, 0)$ dans $\mathfrak{S}_3 \rtimes \mathbb{Z}/2\mathbb{Z}$ coïncident. □

Remarques.

1. On verra plus tard (cf. proposition 7.15) que ce lemme découle en fait simplement du fait que tous les automorphismes de $\mathfrak{S}_3$ sont intérieurs.

2. On verra plus tard (cf. proposition 7.22) une condition suffisante pour qu'au contraire, deux produits semi-directs soient isomorphes seulement s'ils possèdent la même structure équivalente.

3.5 Quelques groupes d'automorphismes élémentaires

Puisqu'identifier un produit semi-direct $N \rtimes H$ exige de connaître l'action de H sur N, donc son morphisme structurel de H dans $\mathrm{Aut}(N)$, rappelons sans démonstration quelques résultats classiques sur les groupes d'automorphismes les plus élémentaires.

Le groupe d'automorphismes $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$**.** On a un premier isomorphisme $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^*$ traduisant le fait que tout automorphisme de $\mathbb{Z}/n\mathbb{Z}$ est la multiplication dans $\mathbb{Z}/n\mathbb{Z}$ par un inversible. Rappelons que l'ensemble des inversibles de $\mathbb{Z}/n\mathbb{Z}$ est noté $(\mathbb{Z}/n\mathbb{Z})^*$, contient $\varphi(n)$ éléments où φ est l'indicatrice d'Euler, et constitue un groupe multiplicatif.

Le groupe d'automorphismes $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$**.** Soit p un nombre premier. Comme le groupe multiplicatif d'un corps fini est cyclique et puisque $\varphi(p) = p - 1$, on a $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$. Soit a un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$ (on en compte $\varphi(p-1)$). L'isomorphisme $\mathbb{Z}/(p-1)\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})^*$ n'est pas canonique : il dépend de a et peut être vu comme une fonction exponentielle de base a. Voici un exemple avec $(\mathbb{Z}/11\mathbb{Z})^*$ et 2 pour choix de générateur :

$$\begin{array}{ccc} \mathbb{Z}/10\mathbb{Z} & \xrightarrow{\exp_2} & (\mathbb{Z}/11\mathbb{Z})^* \\ 0 & \mapsto & 1 \\ 1 & \mapsto & 2 \\ 2 & \mapsto & 4 \\ 3 & \mapsto & 8 \\ 4 & \mapsto & 5 \\ 5 & \mapsto & -1 = 10 \\ 6 & \mapsto & -2 = 9 \\ 7 & \mapsto & -4 = 7 \\ 8 & \mapsto & -8 = 3 \\ 9 & \mapsto & -5 = 6 \end{array}$$

et on vérifie par exemple que :

$$10 = \exp_2(5) = \exp_2(2+3) = \exp_2(2)\exp_2(3) = 4 \times 8.$$

Le groupe d'automorphisme $\mathrm{Aut}(G \times H)$**.** Lorsque G et H sont deux groupes d'ordres premiers entre eux, on a

$$\mathrm{Aut}(G \times H) \cong \mathrm{Aut}(G) \times \mathrm{Aut}(H),$$

car un automorphisme doit envoyer un élément sur un élément de même ordre. Lorsque $G = \mathbb{Z}/p\mathbb{Z}$ et $H = \mathbb{Z}/q\mathbb{Z}$ avec p et q deux nombres premiers distincts, on utilise conjointement à ceci l'isomorphisme provenant du lemme chinois :

$$\begin{array}{ccc} \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} & \xrightarrow{\Phi} & \mathbb{Z}/pq\mathbb{Z} \\ (a,\, b) & \to & qa + pb \\ (q^{-1}m\,,\ p^{-1}m) & \leftarrow & m \end{array}$$

où q^{-1} est l'inverse de q dans $\mathbb{Z}/p\mathbb{Z}$, p^{-1} est l'inverse de p dans $\mathbb{Z}/q\mathbb{Z}$, et les entiers sont vus modulo k quand ils sont dans $\mathbb{Z}/k\mathbb{Z}$.

Voici un exemple :

Le groupe d'automorphismes de $\mathbb{Z}/133\mathbb{Z}$. Remarquons que $133 = 19 \times 7$. Par ce qui précède, on a

$$\mathrm{Aut}(\mathbb{Z}/133\mathbb{Z}) \cong \mathrm{Aut}(\mathbb{Z}/7\mathbb{Z}) \times \mathrm{Aut}(\mathbb{Z}/19\mathbb{Z}) \cong (\mathbb{Z}/7\mathbb{Z})^* \times (\mathbb{Z}/19\mathbb{Z})^* \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$$

Explicitons ces isomorphismes.

$$\begin{array}{ccc} \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/19\mathbb{Z} & \xrightarrow{\Phi} & \mathbb{Z}/133\mathbb{Z} \\ (a,\, b) & \to & 19a + 7b \\ (3m\,,\ 11m) & \leftarrow & m \end{array}$$

car $3 = 19^{-1}$ dans $(\mathbb{Z}/7\mathbb{Z})^*$, et $11 = 7^{-1}$ dans $(\mathbb{Z}/19\mathbb{Z})^*$. Ainsi, $(3,\, 11) \mapsto 1$.

Pour expliciter un isomorphisme de $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$ dans $(\mathbb{Z}/7\mathbb{Z})^* \times (\mathbb{Z}/19\mathbb{Z})^*$, il faut trouver un générateur de $(\mathbb{Z}/7\mathbb{Z})^*$, par exemple 3, et un générateur de $(\mathbb{Z}/19\mathbb{Z})^*$, par exemple 2. Alors l'isomorphisme est le suivant :

$$\begin{array}{ccccc} \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z} & \to & (\mathbb{Z}/7\mathbb{Z})^* \times (\mathbb{Z}/19\mathbb{Z})^* & \to & \dots \\ (k,\, \ell) & \mapsto & (\,3^k,\ 2^\ell\,) & \mapsto & \dots \end{array}$$

$$\begin{array}{ccccc} \dots & \to & \mathrm{Aut}(\mathbb{Z}/7\mathbb{Z}) \times \mathrm{Aut}(\mathbb{Z}/19\mathbb{Z}) & \to & \mathrm{Aut}(\mathbb{Z}/133\mathbb{Z}) \\ \dots & \mapsto & \{(a,\, b) \mapsto (3^k a,\, 2^\ell b)\} & \mapsto & \left\{ \begin{array}{ccc} 19a + 7b & \mapsto & 19 \times 3^k a + 7 \times 2^\ell b \\ m & \mapsto & (57 \times 3^k + 77 \times 2^\ell)m \end{array} \right\} \end{array}$$

Autres groupes d'automorphismes connus. Soit p un nombre premier[15].

$$\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^n) = \mathcal{GL}(n,\, \mathbb{F}_p),$$
$$\mathrm{Aut}(V_4) = \mathcal{GL}(2,\, \mathbb{F}_2) \cong \mathfrak{S}_3,$$
$$\mathrm{Aut}(\mathfrak{S}_3) = \mathrm{Int}(\mathfrak{S}_3) \cong \mathfrak{S}_3.$$

L'égalité $\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^n) = \mathcal{GL}(n,\, \mathbb{F}_p)$ vient de ce que tout morphisme d'un tel groupe est nécessairement $\mathbb{F}_p$-linéaire (puisque l'itération de l'addition doit être préservée). L'isomorphisme $\mathrm{Aut}(V_4) \cong \mathfrak{S}_3$ vient de ce que $\mathrm{Aut}(V_4)$ agit sur les trois éléments non triviaux de V_4, et le morphisme structurel $\mathrm{Aut}(V_4) \to \mathfrak{S}_3$ qui en résulte est un isomorphisme. Enfin, montrons l'isomorphisme $\mathrm{Aut}(\mathfrak{S}_3) = \mathrm{Int}(\mathfrak{S}_3)$. Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_3)$. Alors φ envoie les transpositions sur des éléments d'ordre deux, donc des transpositions, et envoie deux transpositions distinctes sur deux transpositions distinctes. Il existe un automorphisme intérieur ϕ ayant la même action que φ sur les transpositions. Donc la composée $\varphi \circ \psi^{-1}$

[15]Les symboles $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{F}_p$ désignes les mêmes ensembles, mais on réserve le symbole $\mathbb{Z}/p\mathbb{Z}$ lorsqu'on considère le groupe, et $\mathbb{F}_p$ lorsqu'on considère le corps.

fixe chaque transposition. Puisque ces dernières engendrent $\mathfrak{S}_3$, l'automorphisme $\varphi \circ \psi^{-1}$ est trivial, donc φ est intérieur.

3.6 Exemples de produits semi-directs externes

Les deux premiers exemples que nous donnons échappent au cadre des groupes finis, mais la proximité des résultats avec la situation de certains groupes finis valait d'être présentée. Dans les deux cas, la fonction exponentielle joue un rôle important. [16]

1°) Le produit semi-direct $\mathbb{R} \rtimes \mathbb{R}$.

Soit $\varphi : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathrm{Aut}(\mathbb{R}) \\ t & \longmapsto & \{\varphi_t \ : \ x \mapsto \varphi_t(x) = f(t)x\} \end{array}$ un morphisme continu[17]. Cela impose que f soit continue et que :

$$\begin{cases} f(t+s) = f(t)f(s), \\ f(0) = 1. \end{cases} \qquad (*)$$

On montre alors qu'il existe $\lambda \in \mathbb{R}$ tel que $f(t) = \exp(\lambda t)$ pour tout $t \in \mathbb{R}$. On a alors dans $G \cong \mathbb{R} \rtimes_\lambda \mathbb{R}$:

$$(x,\, t) +_\lambda (x',\, t') = (x + e^{\lambda t}x',\, t + t').$$

Or étant données deux actions non triviales de $\mathbb{R}$ dans $\mathrm{Aut}(\mathbb{R})$ décrites par φ^λ et φ^μ, soit $\alpha \ : \ \mathbb{R} \to \mathbb{R}$, $t \mapsto \frac{\mu}{\lambda}t$. Alors il est clair que $\varphi^\mu = \varphi^\lambda \circ \alpha$. Autrement dit, il existe un unique groupe à isomorphisme près, provenant du produit semi-direct non trivial $\mathbb{R} \rtimes \mathbb{R}$.

2°) Les produits semi-directs $\mathbb{R}^2 \rtimes \mathbb{R}$.

Soit $\varphi : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathrm{Aut}(\mathbb{R}^2) \\ t & \longmapsto & \{\varphi_t \ : \ X \mapsto \varphi_t(X) = F(t)X\} \end{array}$ un morphisme, où $X = \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$ est un vecteur de $\mathbb{R}^2$, φ_t appartient à $\mathrm{Aut}(\mathbb{R}^2)$ et est décrit par $F(t)$, une matrice de $\mathcal{GL}(2,\, \mathbb{R})$. Cela impose que :

$$\begin{cases} F(t+s) = F(t)F(s), \\ F(0) = \mathrm{Id}\,. \end{cases} \qquad (**)$$

On distingué alors trois cas, selon que $F(1)$ est diagonalisable à valeurs propres réelles, non diagonalisable avec deux valeurs propres réelles identiques, ou deux valeurs propres complexes conjuguées.

Examinons le cas où $F(1)$ est diagonalisable à valeurs propres réelles. Puisque $\mathbb{R}$ est abélien, les matrices $\big(F(t)\big)_{t\in\mathbb{R}}$ sont codiagonalisables. Il existe donc $P \in \mathcal{GL}(2,\, \mathbb{R})$ et deux fonctions de $\mathbb{R}$ dans $\mathbb{R}$ f et g telles que $F(t) = P\left(\begin{smallmatrix} f(t) & 0 \\ 0 & g(t) \end{smallmatrix}\right)P^{-1}$. Les groupes obtenus

[16] L'un des produits semi-directs $\mathbb{R}^2 \rtimes \mathbb{R}$ « modèle » l'espace SOL, qui est l'un des huit *modèles géométriques de Thurston*, correspondants aux huit géométries possibles des variétés de dimension 3 (grand théorème de géométrisation des variétés de dimension 3, dû à Grigori Perelman, apportant enfin une réponse affirmative à la conjecture de Poincaré).

[17] Du pur point de vue de la théorie des groupes $\mathbb{R}$ est mal défini. Il faut ajouter de la topologie et il est naturel alors d'exiger des morphismes considérés qu'ils respectent cette structure addtitionnelle. Si on préfère rester dans la pure théorie des groupes, on peut considérer les produits semi-directs $\mathbb{Q} \rtimes \mathbb{Q}$, ce qui reviendra au même.

par les actions $t \mapsto F(t)$ et $t \mapsto P^{-1}F(t)P$ sont isomorphes d'après la proposition 3.17, donc on peut supposer que $F(t)$ est diagonale pour tout t. Les fonctions f et g jouant les rôles de coefficients diagonaux vérifient alors les conditions $(*)$ décrites au 1°) , et s'expriment donc comme des exponentielles : il existe deux réels λ et μ tels que pour tout (x, y, t), $(x', y', t') \in \mathbb{R}^2 \rtimes \mathbb{R}$:

$$(x,\, y,\, t) +_\lambda (x',\, y',\, t') = (x + e^{\lambda t}x',\, y + e^{\mu t}y',\, t + t').$$

Deux groupes provenant de deux tels produits semi-directs caractérisés par $(\lambda,\, \mu)$ pour l'un, et $(\lambda',\, \mu')$ pour l'autre, sont isomorphes s'il existe $r \in \mathbb{R}^*$ tel que $(\lambda',\, \mu') = (r\lambda,\, r\mu)$. Par ailleurs, une conjugaison permet de ramener $(\lambda,\, \mu)$ sur (μ, λ). On peut alors réduire l'étude à trois cas :

(a) $\lambda = \mu = 0 : G = \mathbb{R}^3$;
(b) $\lambda = 1$ et $\mu = 0 : G \cong (\mathbb{R} \rtimes \mathbb{R}) \rtimes \mathbb{R}$;
(c) $\lambda = 1$ et $\mu \in \mathbb{R}^*$: contrairement aux cas précédents, le centre du groupe est réduit à $\{(0, 0, 0)\}$.

Arrivé à ce stade, il est difficile de montrer que pour différentes valeurs de μ dans le cas c, on obtient différentes classes d'isomorphie. Une technique envisageable serait de montrer que partant d'un tel groupe, on peut retrouver la structure de produit semi-direct, et en déduire que deux tels groupes sont isomorphes seulement s'ils ont la même structure de produit semi-direct. or ils n'ont pas la même.

3°) Le produit semi-direct $\mathbb{Z}/q\mathbb{Z} \rtimes_\lambda \mathbb{Z}/p\mathbb{Z}$.
Soient p et q deux nombres premiers tels que p divise $q - 1$. Par exemple $q = 11$ et $p = 5$. Suivons le diagramme 1.

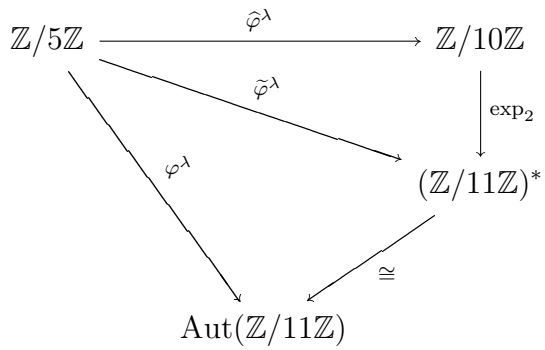


Diagramme 1 –

Le morphisme $\widehat{\varphi}$ est caractérisé par $\lambda \in 2\mathbb{Z}/10\mathbb{Z}$. On le notera $\widehat{\varphi}^\lambda$ de sorte que $\widehat{\varphi}^\lambda(k) = \lambda k$. Puis $\widetilde{\varphi}^\lambda(k) = \exp_2(\lambda k)$ et enfin : $\varphi^\lambda(k)$ est le morphisme $\ell \mapsto \exp_2(\lambda k)\ell$. Ainsi, pour tous couples (x, y), $(x', y') \in \mathbb{Z}/11\mathbb{Z} \rtimes_\lambda \mathbb{Z}/5\mathbb{Z}$, on a :

$$(x, y) +_\lambda (x', y') = (x + e^{\lambda y}x',\, y + y').$$

On pourrait également écrire :

$$(x, y) +_\lambda (x', y') = (x + k^y x',\, y + y').$$

où $k = \exp^\lambda$ est un élément de $(\mathbb{Z}/11\mathbb{Z})^*$ d'ordre 5. Remarquons que pour deux éléments $\lambda,\, \mu \in 2\mathbb{Z}/10\mathbb{Z}$, on a $\widehat{\varphi}^\lambda = \widehat{\varphi}^\mu\alpha$ où α est la multiplication dans $\mathbb{Z}/10\mathbb{Z}$ par l'élément $\lambda^{-1}\mu$

de $\mathbb{Z}/10\mathbb{Z}$. Donc ces structures de produit semi-direct sont semblables et tous ces produits semi-directs sont isomorphes.

4°) Les produits semi-directs $\mathbb{Z}/133\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$ (avec $133 = 19 \times 7$).
Choisissons l'exponentielle de base 2 comme isomorphisme $\mathbb{Z}/18\mathbb{Z} \to (\mathbb{Z}/19\mathbb{Z})^*$, de sorte que si $k \in \{0, 6, 12\}$ dans $\mathbb{Z}/18\mathbb{Z}$, on ait $\exp_2(k) \in \{1, 7, 11\}$ dans $(\mathbb{Z}/19\mathbb{Z})^*$. Choisissons l'exponentielle de base 3 comme isomorphisme $\mathbb{Z}/6\mathbb{Z} \to (\mathbb{Z}/7\mathbb{Z})^*$, de sorte que si $k \in \{0, 2, 4\}$ dans $\mathbb{Z}/6\mathbb{Z}$, on ait $\exp_2(k) \in \{1, 2, 4\}$ dans $(\mathbb{Z}/7\mathbb{Z})^*$. Suivons le diagramme 2.

- Soient $\lambda \in \{0, 6, 12\} \subset \mathbb{Z}/18\mathbb{Z}$ et $\mu \in \{0, 2, 4\} \subset \mathbb{Z}/6\mathbb{Z}$.
- Soit $\widehat{\varphi}^{\lambda,\mu} \ : \ \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, $1 \mapsto (\lambda,\ \mu)$.
- Soient $\Lambda(t) = \exp_2(\lambda t)$ et $\mathcal{M}(t) = \exp_3(\mu t)$.
- Soit $\widetilde{\varphi}^{\lambda,\mu} \ : \ \mathbb{Z}/3\mathbb{Z} \to (\mathbb{Z}/19\mathbb{Z})^* \times (\mathbb{Z}/7\mathbb{Z})^*$, $t \mapsto (\Lambda(t),\ M(t))$.
- Soit $\varphi^{\lambda,\mu} \ : \ \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/19\mathbb{Z}) \times \mathrm{Aut}(\mathbb{Z}/7\mathbb{Z})$, $t \mapsto \{(x, y) \mapsto (\Lambda(t)x, M(t)y)\}$.
- Soit $m(t) = 77\Lambda(t) + 57M(t)$.
- Soit $\psi_m \ : \ \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/133\mathbb{Z})$, $t \mapsto \{z \mapsto m(t)z\}$.

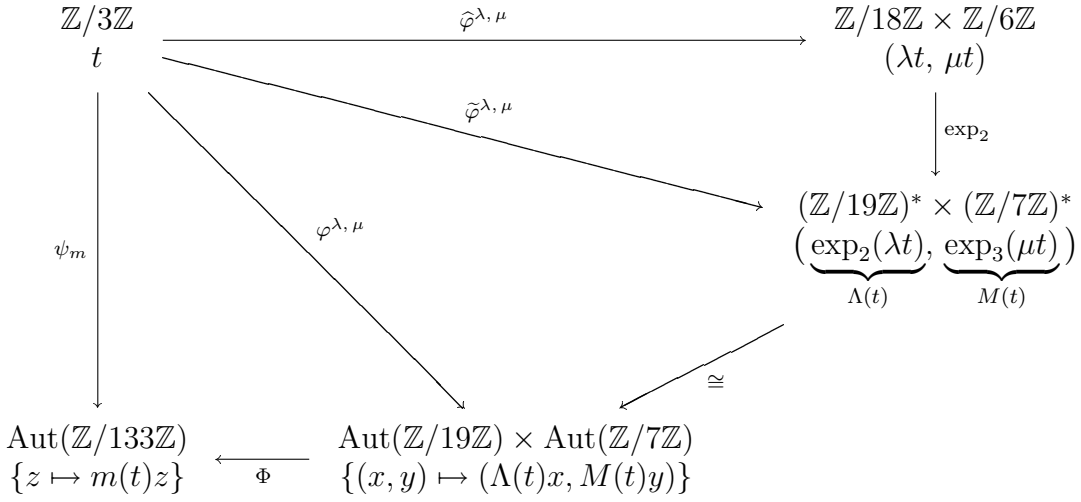


Diagramme 2 –

Les valeurs de $m(t)$ sont données dans le tableau 1.

		μt	0	2	4
		$M(t)$	1	2	4
λt	$\Lambda(t)$				
0	1		1	58	39
6	7		64	121	102
12	11		106	30	11

Tableau 1 – Valeur de $m(t)$ en fonction de λ, μ et t.

Pour tous triplets (x, y, t), (x', y', t') dans $(\mathbb{Z}/19\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}) \rtimes_\lambda \mathbb{Z}/3\mathbb{Z}$, on a :

$$(x, y, t) +_{\lambda,\mu} (x', y') = (x + \exp_2(\lambda t)x',\ y + \exp_3(\mu t)y',\ t + t') \qquad (***)$$

et pour tous couples (z,t), (z',t') dans $(\mathbb{Z}/133\mathbb{Z}) \rtimes_\lambda \mathbb{Z}/3\mathbb{Z}$, on a :

$$(z,t) +_m (z',t') = (z + m(t)z',\, t + t').$$

Considérons $\widehat{\varphi}^{\lambda,\mu}$. Soit $\alpha \in \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$ la multiplication par -1. Alors $\widehat{\varphi}^{2\lambda,2\mu} = \widehat{\varphi}^{\lambda,\mu} \circ \alpha$, donc d'après le premier critère d'isomorphie des groupes obtenus par produits semi-directs, les couples $(\lambda,\, \mu)$ et $(2\lambda,\, 2\mu)$ induisent deux structures de produit semi-direct sembalbles. Soit G le groupe $\mathbb{Z}/133\mathbb{Z} \rtimes_\varphi^{\lambda,\,\mu} \mathbb{Z}/3\mathbb{Z}$. On a au plus cinq classes d'isomorphie possible pour le groupe G en fonction de λ et μ :

(a) si $(\lambda,\mu) = (0,0)$, alors $G \cong \mathbb{Z}/399\mathbb{Z}$,
(b) si $(\lambda,\mu) = (0,2)$, alors $G \cong \big(\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}\big) \times \mathbb{Z}/19\mathbb{Z}$,
(c) si $(\lambda,\mu) = (6,0)$, alors $G \cong \big(\mathbb{Z}/19\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}\big) \times \mathbb{Z}/7\mathbb{Z}$,
(d) si $(\lambda,\mu) = (6,2)$, alors $G \cong \mathbb{Z}/133\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$ où $\varphi(1) = \{z \mapsto 11z\}$,
(e) si $(\lambda,\mu) = (12,2)$, alors $G \cong \mathbb{Z}/133\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$ où $\varphi(1) = \{z \mapsto 30z\}$.

Le cas (a) est le seul où G est abélien. Le cas (b) est le seul où tous les éléments d'ordre 19 sont centraux, mais certains éléments d'ordre 7 ne le sont pas. Dans le cas (c), la situation est inversée. Dans les cas (d) et (e) il existe à la fois des éléments d'ordre 7 et 19 qui ne soient pas centraux. On montrera au paragraphe 7.4 que les cas (d) et (e) mènent à deux classes d'isomorphie de G distinctes.

4 Théorèmes de Sylow

Dans ce paragraphe, on va tenter de retrouver pour les groupes finis ce qu'on a établi pour les groupes abéliens finis (théorème de Cauchy, théorèmes de Sylow, existence de sous-groupes particuliers).

4.1 Les trois théorèmes

Proposition 4.1 (Théorème de Cauchy)**.**
Soient G un groupe d'ordre n et p un nombre premier qui divise n. Alors, il existe un élément dans G d'ordre p.

Démonstration. On donne deux méthodes, toutes deux utilisant l'équation aux classes.

Première méthode, en utilisant une action astucieuse de $\mathbb{Z}/p\mathbb{Z}$: preuve directe.
Soit F le sous-ensemble de l'ensemble E des fonction de $\mathbb{Z}/p\mathbb{Z}$ dans G suivant :

$$F = \{f \in E \mid \prod_{k\in\mathbb{Z}/p\mathbb{Z}} f(k) = 1_G\}.$$

Remarquons que $|F| = |G|^{p-1}$. On fait agir $\mathbb{Z}/p\mathbb{Z}$ sur F en posant $k.f(\ell) = f(\ell + k)$ pour tous $f \in F$, et $k, \ell \in \mathbb{Z}/p\mathbb{Z}$. Remarquons que f est un point fixe sous l'action de $\mathbb{Z}/p\mathbb{Z}$ si et seulement si f est constante et prend pour valeur un élément de G dont la puissance p-ème vaut 1_G. Soit f_0 la fonction constante sur 1_G. S'il existe une autre fonction constante dans F que f_0, on aura trouvé un élément d'ordre p dans G, précisément la valeur que

prend cette fonction. Lorsque f n'est pas constante, l'orbite de f contient p éléments. Considérons l'équation aux classes sous l'action de $\mathbb{Z}/p\mathbb{Z}$:

$$|F| = |F^G| + \sum_{f \in F''} |\mathrm{Orb}_{\mathbb{Z}/p\mathbb{Z}}(f)|,$$

où F'' est une transversale de $F \setminus F^G$. On vient de voir que p divisait $|F|$ et divisait $|\mathrm{Orb}(f)|$ pour toute f non constante, donc en particulier pour toute f dans F''. Ainsi p doit diviser $|F^G|$. Or cet ensemble n'est pas vide puisqu'il contient f_0. Il doit donc contenir au moins p fonctions constantes, donc f_0 n'est pas la seule fonction constante. □

Deuxième méthode, en utilisant l'action par conjugaison de G sur lui-même : preuve par récurrence, en utilisant le théorème de Cauchy dans le cas abélien.
On raisonne par récurrence sur $k = \frac{|G|}{p}$. Le résultat est vrai pour $|G| = p$. Soit G un groupe d'ordre kp avec $k \geqslant 2$. On suppose le résultat vrai pour tout groupe d'ordre ℓp avec $\ell < k$. Partons de l'équation aux classes associée à l'action de G par conjugaison sur lui-même :

$$|G| = |\mathcal{Z}_G| + \sum_{g \in G''} \frac{|G|}{|\mathrm{Stab}_G(g)|}, \tag{1}$$

où G est une transversale de $G \setminus \mathcal{Z}_G$. Ceci étant, deux cas de figure se présentent.

Premier cas de figure . Si pour tout $g \in G''$, p ne divise pas $\mathrm{Stab}_G(g)$, alors p divise $\frac{|G|}{|\mathrm{Stab}_G(g)|}$, donc p divise $\sum_{g \in G''} \frac{|G|}{|\mathrm{Stab}_G(g)|}$. Or p divise aussi $|G|$, donc d'après (1), p doit diviser le centre $\mathcal{Z}_G$. Le théorème de Cauchy abélien appliqué au centre permet de conclure.

Deuxième cas de figure . S'il existe $g \in G''$ tel que p divise $|\mathrm{Stab}_G(g)|$. Par ailleurs, on a $|\mathrm{Stab}_G(g)| < |G|$ puisque g, appartenant à G'', n'est pas central. On peut donc appliquer l'hypothèse de récurrence à $\mathrm{Stab}_G(g)$. Cela achève la preuve. □

Passons aux théorèmes de Sylow.

Théorème 4.2 (Premier théorème de Sylow, 1872)**.**
Soit G un groupe d'ordre $p^\alpha m$ où p est premier et ne divise pas m. Alors il existe un sous-groupe de G d'ordre p^α.

Démonstration par l'action de G par conjugaison sur lui-même.
La démonstration commence comme la deuxième que nous avons proposé pour le théorème de Cauchy. On raisonne par récurrence sur $k = \frac{|G|}{p}$. Le résultat est vrai pour $|G| = p$. Soit G un groupe d'ordre $p^\alpha m$ avec $m \wedge p = 1$ et $p^\alpha m > p$. On suppose le résultat vrai pour tout groupe d'ordre strictement inférieur à $|G|$. Partons de l'équation aux classes associée à l'action de G par conjugaison sur lui-même :

$$|G| = |\mathcal{Z}_G| + \sum_{g \in G''} \frac{|G|}{|\mathrm{Stab}_G(g)|},$$

où G est une transversale de $G \setminus \mathcal{Z}_G$. Ceci étant, deux cas de figure se présentent.

Premier cas de figure. S'il existe $g \in G''$ tel que p^α divise $\mathrm{Stab}_G(g)$, alors d'après l'hypothèse de récurrence, $\mathrm{Stab}_G(g)$ contient p-Sylow, qui sera également un p-Sylow de G.

Deuxième cas de figure. Si pour tout $g \in G''$, p^α ne divise pas $|\mathrm{Stab}_G(g)|$, alors p divise $\sum_{g \in G''} \frac{|G|}{|\mathrm{Stab}_G(g)|}$ et donc p divise $|\mathcal{Z}_G|$. Prenons H un sous-groupe cyclique d'ordre p inclus dans $|\mathcal{Z}_G|$ (possible car H est abélien). On applique l'hypothèse de récurrence au groupe G/H (H est central donc distingué). Soit $\bar{K}$ un p-Sylow de G/H, donc d'ordre $p^{\alpha-1}$. Soit $\pi : G \to G/H$ le morphisme de passage au quotient et soit $K = \pi^{-1}(K)$. Alors K est d'ordre p^α. □

Dans la démonstration, au lieu de chercher les groupes d'ordre p^α, on aurait pu chercher les groupes d'ordre p^β, $1 \leqslant \beta \leqslant \alpha$ et montrer ainsi :

Proposition 4.3 (Premier théorème de Sylow étendu)**.**
Soit G un groupe d'ordre $p^\beta m$ où p est premier et m est quelconque (éventuellement multiple de p). Alors il existe un sous-groupe de G d'ordre p^β. □

Théorème 4.4 (Deuxième théorème de Sylow, 1872)**.**
(i) Tout p-sous-groupe est inclus dans un p-Sylow.
(ii) Les p-Sylow sont conjugués.

Démonstration. La partie (ii) découle de (i). Prouvons la partie (i). Soit H un p-groupe dans G et S un p-Sylow de G. On va montrer qu'il existe $g \in G$ tel que $gHg^{-1} \subset S$. On va utiliser (EC3), en faisant agir H par multiplication à gauche sur l'ensemble $E = G/S = \{gS,\, g \in G\}$. On a

$$|E| \equiv |E^H| \mod p,$$

mais $|E| = |G/S|$ est premier avec p, puisque S est un p-Sylow. Donc il existe $g_0 \in G$ tel que $g_0 S \in E^H$, autrement dit tel que pour tout h, $hg_0S = g_0S$. Donc $hg_0 \in g_0S$ pour tout $h \in H$, donc $H \subset g_0 S g_0^{-1}$. □

En réadaptant la preuve de ce dernier théorème, on peut trouver une preuve élégante des deux premiers théorèmes de Sylow à la fois, à partir de la proposition suivante.

Proposition 4.5 (p-Sylow des sous-groupes)**.**
Soit G un groupe, S un p-Sylow de G et H un sous-groupe de G. Alors, il existe $g \in G$ tel que $gSg^{-1} \cap H$ soit un p-Sylow de H.

Démonstration. Reprenons la preuve du théorème 4.4. Soit S un p-Sylow de G et E l'ensemble quotient G/S. A nouveau, on fait opérer H par multiplication à gauche sur les classes de E. Soit E' une section de E sous l'action de H. La partition en orbites donne :

$$|E| = \sum_{g \in G'} |\mathrm{Orb}_H(gS)| = \sum_{gS \in E'} \frac{|H|}{|gSg^{-1} \cap H|}.$$

Si $gSg^{-1} \cap H$ n'est jamais un p-Sylow de H, alors p divise $\sum_{gS \in (G/H)'} \frac{|H|}{|gSg^{-1} \cap H|}$, donc p divise G/S. Mais ceci contredit le fait que S est un p-Sylow de G. □

Démonstrations alternatives des premiers théorèmes de Sylow.

Preuve du premier théorème de Sylow : existence des p-Sylow.

Soit G un groupe et p un diviseur de $|G| = n$. On plonge d'abord G dans $\mathfrak{S}_n$ (par Cayley), puis on plonge $\mathfrak{S}_n$ dans $\mathcal{GL}_n(\mathbb{F}_p)$ de la manière classique, à savoir que $\sigma \in \mathfrak{S}_n$ s'envoie sur l'endomorphisme u_σ défini dans la base canonique par $u_\sigma(ei) = e_{\sigma(i)}$. Finalement, on a réalisé G comme un sous-groupe de $(\mathcal{GL}_n(\mathbb{F}_p), \circ)$. Or $\mathcal{GL}_n(\mathbb{F}_p)$ est d'ordre $(p^n-1)(p^n-p)(p^n-p^2)\dots(p^n-p^{n-1})$, et $\mathcal{T}_{n,p}$, le sous-groupe des matrices triangulaires supérieures à coefficients diagonaux égaux à 1, est d'ordre $p \times p^2 \times \cdots \times p^{n-1}$. Donc $\mathcal{T}_{n,p}$ est un p-Sylow de $\mathcal{GL}_n(\mathbb{F}_p)$. Donc d'après la proposition 4.5, G possède lui aussi un p-Sylow. □

Preuve du deuxième théorème de Sylow : Tout p-sous-groupe est inclus dans un p-Sylow, lesquels sont tous conjugués.

Si H est un p-sous-groupe et S un p-Sylow de G, il existe $g \in G$ tel que $gSg^{-1} \cap H$ soit un p-Sylow de H. Mais comme H est un p-groupe, on a $gSg^{-1} \cap H = H$, donc H est inclus dans gSg^{-1} qui est un Sylow. Si de plus H est lui-même un p-Sylow de G, on a exactement $H = gSg^{-1}$. □

Théorème 4.6 (Troisième théorème de Sylow, 1872)**.**
Soit G un groupe d'ordre $p^\alpha m$ avec $\alpha \geqslant 1$ et $m \wedge p = 1$. Soit n_p le nombre de p-Sylow.

(i) $n_p \mid m$.

(ii) $n_p| \equiv 1 \mod p$.

Démonstration.

(i) Soit S un p-Sylow de G et $\mathcal{S}y\ell_p(G)$ l'ensemble des p-Sylow de G. D'après le point (ii) du théorème 4.6, l'action de G par conjugaison sur $\mathcal{S}y\ell_p(G)$ est transitive, donc $\mathcal{S}y\ell_p(G) = \mathrm{Orb}_G(S)$. Or $\mathrm{Stab}_G(S) = \mathrm{Norm}_G(S)$, donc $|\mathcal{S}y\ell_p(G)| = \frac{|G|}{|\mathrm{Norm}_G(S)|}$. Or $|S|$ divise $|\mathrm{Norm}_G(S)|$ (Lagrange), donc $|\mathcal{S}y\ell_p(G)|$ divise $\frac{|G|}{|S|}$ qui est égal à m.

(ii) On va utiliser (EC3), en faisant agir un p-Sylow S par conjugaison sur $E = \mathcal{S}y\ell_p(G)$ et obtenir $|E| \equiv |E^S| \mod p$. Il reste à montrer que $|E^S| = 1$. Pour tout p-Sylow T appartenant à E^S, on a $sTs^{-1} = T$ pour tout $s \in S$. Donc S est inclus dans $\mathrm{Norm}_G(T)$. Dans le groupe $\mathrm{Norm}_G(T)$, S et T sont conjugués d'après le théorème 4.4, mais par définition de $\mathrm{Norm}_G(T)$, T est distingué dans $\mathrm{Norm}_G(T)$. Donc $T = S$. Donc $E^S = \{S\}$. □

Remarque. Considérons l'action de G par conjugaison sur $\mathcal{S}y\ell_p(G)$. Soit $S \in \mathcal{S}y\ell_p(G)$. On notera que :

- l'action est transitive : $\mathrm{Orb}_G(S) = \mathcal{S}y\ell_p(G)$,
- $\mathrm{Stab}_G(S) = \mathrm{Norm}_G(S)$,
- le seul p-Sylow de $\mathrm{Norm}_G(S)$ est S.

4.2 Premières applications

Exemples théoriques d'utilisation des théorèmes de Sylow.

1. Prouver qu'un groupe n'est pas simple (en démontrant qu'un p-Sylow est distingué grâce au troisième théorème de Sylow).
2. Compter le nombre de sous-groupes d'un ordre donné (en particulier le nombre de p-Sylow). S'il n'y en a qu'un, il est caractéristique.
3. Montrer qu'un groupe est un produit semi-direct en exhibant un complément (généralement un p-Sylow) d'un sous-groupe distingué.
4. Montrer que des sous-groupes, ou simplement des éléments d'un certain ordre, sont conjugués.
5. Prouver qu'il existe ou non des éléments d'un certain ordre.
6. Amorcer la classification des groupes finis et dans certains, pouvoir conclure. Les théorèmes de Sylow et une bonne connaissance des produits semi-directs permettent de classer assez facilement de nombreux groupes (i.e. de déterminer le nombre de classes d'isomorphie en fonction de l'ordre).

Nous allons illustrer cela dans les exemples ci-dessous. Les numéros se correspondent.

Exemples pratiques d'utilisation des théorèmes de Sylow.

1.a. Les groupes d'ordre 63 et 255 ne sont pas simples. En effet :
- le 7-Sylow d'un groupe d'ordre 63 est distingué, car $n_7|9$ et $n_7 \equiv 1 \mod 7$;
- le 17-Sylow d'un groupe d'ordre 255 est distingué, car $n_{17}|15$ et $n_{17} \equiv 1 \mod 17$.

1.b. Les groupes d'ordre 56 ne sont pas simples. Il s'agit d'un cas plus subtil que les précédents, car on n'a pas directement $n_7 = 1$ ou $n_2 = 1$. Cependant, on peut montrer que $n_7 \neq 1$ et $n_2 \neq 1$ sont contradictoires. Ainsi, si $n_7 \neq 1$, alors $n_7 = 8$. Les éléments de ces huit 7-Sylow sont deux à deux distincts sinon deux de ces 7-Sylow seraient confondus. On compte donc 48 éléments d'ordre 7. Or $56 - 48 = 8$, donc il n'y a alors qu'un seul 8-Sylow, qui est donc distingué.

2. Soient G et G' deux groupes d'ordre 63, et N et N' leurs 7-Sylow respectifs. Alors tout isomorphisme de G dans G' envoie N sur un sous-groupe d'ordre 7, donc un 7-Sylow, donc N' puisque G' ne possède qu'un seul 7-Sylow, comme on l'a vu précédemment pour tout groupe d'ordre 63. La classification des groupes d'ordre 399 par exemple utilise un tel argument (cf. proposition 6.11).

3. Soit G un groupe d'ordre 63. Alors c'est un produit semi-direct. En effet, soit N un 7-Sylow. On a vu que N était distingué. Par le premier théorème de Sylow, il existe un 3-Sylow H. Ce 3-Sylow est nécessairement un complément de N, car $N \cap H = \{1\}$ en raison du théorème de Lagrange et $NH = G$ pour une raison de cardinal.

4. Soit A et B deux matrices de $\mathcal{GL}(2, \mathbb{F}_p)$ d'ordre p. Alors A est conjuguée à une puissance de B. En effet, $\mathcal{GL}(2, \mathbb{F}_p)$ contient $(p^2 - 1)(p^2 - p)$ éléments, donc les p-Sylow contiennent p éléments et sont donc monogènes. Puisqu'ils sont conjugués, le résultat s'en déduit.

5. Sans rien connaître du groupe $\mathbb{Z}/7\mathbb{Z} \rtimes (\mathbb{Z}/3\mathbb{Z})^2$, nous pouvons déduire des théorèmes de Sylow qu'il ne contient pas d'éléments d'ordre 9 (cf. [18]). En effet, le groupe

[18] Attention : un tel groupe pourrait fort bien a priori contenir des éléments d'ordre 9 et d'ordre 7, sans en contenir d'ordre 63, comme c'est le cas par exemple de $\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/9\mathbb{Z}$.

$\mathbb{Z}/7\mathbb{Z} \rtimes (\mathbb{Z}/3\mathbb{Z})^2$ contient une copie de $(\mathbb{Z}/3\mathbb{Z})^2$ qui est un 3-Sylow. Or tous les 3-Sylow sont conjugués, donc $\mathbb{Z}/7\mathbb{Z} \rtimes (\mathbb{Z}/3\mathbb{Z})^2$ ne peut pas contenir de copie de $\mathbb{Z}/9\mathbb{Z}$ qui serait un 2-Sylow non conjugué à $(\mathbb{Z}/3\mathbb{Z})^2$.

6. Soit G un sous-groupe d'ordre 63. Nous avons vu qu'il était un produit semi-direct de N d'ordre 7 par H d'ordre 9. Deux cas sont à considérer, selon que $H = \mathbb{Z}/9\mathbb{Z}$ ou $H = (\mathbb{Z}/3\mathbb{Z})^2$. Traitons le cas $(\mathbb{Z}/3\mathbb{Z})^2$ (le cas $\mathbb{Z}/9\mathbb{Z}$ se traite de la même manière).

   Il faut déterminer l'action $\varphi : H \to \mathrm{Aut}(N)$. Ces morphismes peuvent être repérés par des formes linéaires de ${\mathbb{F}_3}^2$. Les formes linéaires non nulles peuvent être obtenues les unes des autres par multiplication par un élément de $\mathrm{Aut}(H) = \mathcal{GL}(2, \mathbb{F}_3)$, donc les structures de produit semi-direct associées sont semblables. Les groupes G obtenus par ce produit semi-direct sont isomorphes à $(\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}) \times \mathbb{Z}/3\mathbb{Z}$ (où l'action n'est pas triviale).

   En traitant le cas $H = \mathbb{Z}/9\mathbb{Z}$, on aurait également trouvé un groupe non abélien $\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/9\mathbb{Z}$. Ces deux groupes sont-ils les mêmes ? Non, car $\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/9\mathbb{Z}$ contient un élément d'ordre 9, tandis que $(\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}) \times \mathbb{Z}/3\mathbb{Z}$ n'en contient pas, comme on l'a vu précédemment. Ainsi il existe quatre classes d'isomorphie de groupes d'ordre 63 :
   - $\mathbb{Z}/63\mathbb{Z}$,
   - $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/21\mathbb{Z}$,
   - $\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/9\mathbb{Z}$,
   - $(\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}) \times \mathbb{Z}/3\mathbb{Z}$.

Voici deux exemples supplémentaires où les théorèmes de Sylow peuvent aider à la classification des groupes.

Lemme 4.7 (Groupe ayant un unique p-Sylow et un unique q-Sylow)**.**
Si un groupe fini G possède un unique p-Sylow P et un unique q-Sylow Q où p et q sont deux entiers premiers quelconques, alors

(i) P et Q sont en somme directe dans G,

(ii) tout élément de G dont l'ordre est du type $p^\alpha q^\beta$ est dans $P \times Q$.

(iii) $P \times Q$ est le seul sous-groupe de G d'ordre $|P||Q|$, en particulier, $P \times Q$ est caractéristique (donc distingué),

Démonstration.

(i) Puisque P est distingué dans G, PQ est un groupe et P est distingué dans PQ. De même, Q est distingué dans PQ. Comme en plus $P \cap Q = \{1_G\}$ (car leurs ordres sont premiers entre eux), il vient que PQ est un produit semi-direct, et même direct puisque P et Q sont tous les deux distingués.

(ii) Soit x dans G d'ordre $p^\alpha q^\beta$. Alors l'élément $y = x^{p^\alpha}$ appartient à Q. De même l'élément $z = x^{q^\beta}$ appartient à P. Or il existe deux entiers u et v tels que $up^\alpha + vq^\beta = 1$, donc x appartient à $\langle y, z \rangle$, donc $x \in P \times Q$.

(iii) Soit H un sous-groupe d'ordre $|P||Q|$. Alors tous ses éléments vérifient les hypothèses du (ii), donc appartiennent à $P \times Q$. Finalement, $H = P \times Q$. □

Un cas particulier assez fréquent, puisqu'il concerne tous les groupes nilpotents[19].

Proposition 4.8 (Groupe n'ayant qu'un seul p-Sylow pour tout p)**.**
Si un groupe fini G possède un seul p-Sylow pour tout diviseur premier p de $|G|$, alors G est produit direct de ses p-Sylow.

Démonstration. Soit $S_1, \ldots, S_r$ les p-Sylow de G. Soit $K = S_2 S_3 \ldots S_r$. Alors les deux sous-groupes S_1 et K sont distingués dans G. De plus, $S_1 \cap K = \{1_G\}$ à cause du théorème de Lagrange. Enfin, pour des raison de cardinal, $S_1 K = G$. Donc G est un produit semi-direct de S_1 par K, donc un produit direct puisque K aussi est distingué dans G. En appliquant à nouveau ce fait à K, on montre ainsi que G est produit direct de ses p-Sylow. □

Remarque. Puisqu'il existe des p-groupes de tous ordres divisant $|G|$, d'après la proposition 4.3, on obtient la réciproque du théorème de Lagrange pour ce type de groupes (cf. proposition 5.15).

5 Groupes nilpotents et p-groupes

Les théorèmes de Sylow proposent d'étudier les groupes en examinant leurs p-sous-groupes maximaux. Cela motive l'étude des p-groupes. Cependant, bien qu'ils jouent un rôle essentiel dans la classification des groupes, nous arrêterons notre classification à l'ordre 15 (justement freiné par l'étude des groupes d'ordre 16) et les résultats présentés sont donc indépendants de la suite, en dehors de la proposition 5.4 selon laquelle tout groupe d'ordre p ou p^2 est abélien.

Le premier réflexe à avoir est de se demander si cette étude des p-groupe est nécessaire, autrement dit s'il existe vraiment des p-groupes non abéliens. Malheureusement, oui ! Voici deux exemples.

Définition 5.1 (Le groupe quaternionique[20] $\mathbb{H}_8$)**.**
Le groupe qui admet la présentation

$$\langle\, a,\, b \mid a^2 = b^2 = (ab)^2,\, a^4 = 1 \,\rangle$$

est appelé le *groupe quaternionique* et est souvent noté $\mathbb{H}_8$. C'est un groupe d'ordre 8 dont les éléments sont traditionnellement notés ± 1, $\pm i$, $\pm j$, $\pm k$, de sorte que $ij = k$, $i^2 = j^2 = k^2 = -1$, et $(-1)^2 = 1$. Ce groupe n'est pas commutatif, puisque $ij = -ji$. En effet, $ijij = k^2 = -1$, donc $i^2 jij^2 = -ij$, donc $ji = -ij$.

[19] Cf définition 5.8 et théorème 5.14.

[20] découvert par Hamilton en 1843. Une plaque commémorative à Dublin raconte qu'il grava lui-même sur un pont sa découverte : $i^2 = j^2 = k^2 = ijk = -1$.

Définition 5.2 (Le groupe $\mathcal{T}_{n,p}$)**.**
Pour tout p premier, soit $\mathcal{T}_{n,p}$ le groupe multiplicatif des matrices triangulaires supérieures à coefficients dans $\mathbb{F}_p$ et à coefficients diagonaux égaux à 1. Aucun de ces groupes n'est commutatif, dès que $n \geqslant 3$. Par exemple considérons le groupe

$$\mathcal{T}_{3,p} = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \in \mathcal{GL}(3, \mathbb{F}_p),\ x, y, z \in \mathbb{F}_p \right\}.$$

Alors en posant $a = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ et $b = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, on a $ab = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$, tandis que $ba = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$. Attention, ce groupe est isomorphe à $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ lorsque $p = 2$, et à $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/p\mathbb{Z}$ lorsque $p \geqslant 3$.

Dès que l'on entre dans le monde des groupes non-commutatifs, les actions de groupes sont des outils très efficaces. Rappelons que pour toute action d'un p-groupe sur un ensemble, l'équation aux classes implique :

$$|E| \equiv |E^G| \pmod{p}. \qquad (EC3)$$

5.1 Sous-groupes distingués dans les p-groupes

Le premier sous-groupe distingué auquel on s'intéresse est le centre.

Proposition 5.3 (Théorème de Burnside)**.** *Le centre d'un p-groupe non trivial n'est jamais trivial.*

Démonstration. C'est un corollaire de l'équation aux classes appliquée à l'action de G sur lui-même par conjugaison. Les points fixes de G par cette action sont les éléments du centre $\mathcal{Z}_G$ de G, donc on a d'après (EC3) :

$$|G| \equiv |\mathcal{Z}_G| \pmod{p}.$$

Or $\mathcal{Z}_G$ n'est pas vide (puisque 1_G y appartient), donc $\mathcal{Z}_G$ est de cardinal au moins p. □

Au passage, on déduit de cette dernière proposition que les p-groupes sont nilpotents, cf. paragraphe 5.2. On déduit également la proposition suivante :

Proposition 5.4 (Petits p-groupes)**.**
Tout p-groupe d'ordre p ou p^2 est abélien.

Démonstration. Soit G un groupe d'ordre p. D'après le théorème de Lagrange, il existe un élément d'ordre p, donc G est cyclique.

Considérons maintenant le cas d'un groupe G d'ordre p^2. D'après la proposition 5.3, le centre d'un p-groupe de cardinal p^2 n'est pas trivial. Il est donc de cardinal p ou p^2. S'il est de cardinal p, soit x un élément dans $G \setminus \mathcal{Z}_G$. Alors le stabilisateur $\mathrm{Stab}_G(x)$ sous l'action de G par conjugaison sur lui-même contient au moins x et $\mathcal{Z}_G$, et est donc de cardinal au moins $p + 1$. Comme $\mathrm{Stab}_G(x)$ est un sous-groupe de G, p doit diviser $\mathrm{Stab}_G(x)$, donc $\mathrm{Stab}_G(x)$ est de cardinal p^2, donc $\mathrm{Stab}_G(x) = G$, donc x est central.

C'est une contradiction. Donc le centre de G est de cardinal p^2, donc G est abélien. □

Remarque. Dans cette démonstration, après avoir utilisé le théorème de Burnside, on aurait aussi bien pu conclure en utilisant le lemme 6.1 (cf. chapitre suivant) selon lequel si le quotient d'un groupe par son centre est monogène, alors ce groupes abélien.

Proposition 5.5 (Réciproque du théorème de Lagrange pour les p-groupes)**.**
Soit G un groupe d'ordre p^α. Pour tout $\beta \leqslant \alpha$, G contient un sous-groupe distingué d'ordre p^β.

Démonstration. Par récurrence sur α. Lorsque $\alpha = 0$, le résultat est trivial. Soit $\alpha \geqslant 1$. On suppose que le résultat est vrai pour tout entier strictement inférieur à α. Soit G un groupe d'ordre p^α. Soit $\beta < \alpha$. Cherchons un sous-groupe distingué H de G d'ordre p^β.

- *Obtention d'un sous-groupe central d'ordre p.* Le centre de G est un p-groupe abélien non trivial d'après la proposition 5.3, donc (théorème de Cauchy abélien) il contient un élément d'ordre p. Notons W le sous-groupe de G engendré par cet élément.
- *Obtention d'un sous-groupe d'ordre p^β.* Puisque W est central, il est distingué et le quotient G/W est un p-groupe de cardinal $p^{\alpha-1}$. On peut lui appliquer l'hypothèse de récurrence. Il existe un sous-groupe distingué $\bar{H}$ de G/W d'ordre $p^{\beta-1}$. Soit $\pi : G \to G/W$ le morphisme de passage au quotient. Alors le sous-groupe K de G égal à $\pi^{-1}(H)$ est d'ordre p^β. Vérifions que K est distingué. Pour tous $k \in K$, $g \in G$, on a $\pi(gkg^{-1}) \in H$ car H et distingué dans G/W, donc $gkg^{-1} \in HW = K$, donc K est distingué. □

La proposition suivante nous sera utile pour établir le théorème de Frattini (cf. paragraphe 5.3.

Définition 5.6 (Sous-groupe maximal)**.**
Un sous-groupe M de G est dit *maximal* si c'est un sous-groupe propre (i.e. différent de G) tel que M et G soient les seuls sous-groupes de G contenant M.

Proposition 5.7 (Sous-groupes maximaux d'un p-groupe)**.**
Tout sous-groupe maximal d'un p-groupe d'ordre p^α est d'ordre $p^{\alpha-1}$ et est distingué.

Démonstration. Montrons d'abord que M est distingué. Soit M un sous-groupe maximal. On considère l'action de G par conjugaison sur l'ensemble E des sous-groupes maximaux. On a la partition :

$$E = E^G \underset{M \in E''}{\cup} \mathrm{Orb}_G(M) \qquad (*)$$

où E'' est la transversale de $E \smallsetminus E^G$ sous l'action de G. Les éléments de E^G sont les sous-groupes maximaux distingués. On va montrer par l'absurde que E'' doit être vide, autrement dit que $E = E^G$. Supposons qu'il existe $M \in E''$. L'orbite de M est $\mathrm{Orb}_G(M) = \frac{|G|}{\mathrm{Stab}_G(M)}$, elle n'est pas de cardinal 1 (puisque $M \in E''$), donc p divise son

cardinal. Considérons l'action de M par conjugaison sur $\mathrm{Orb}_G(M)$. L'équation aux classes correspondante donne :

$$|\mathrm{Orb}_G(M)| \equiv |(\mathrm{Orb}_G(M))^M| \mod p. \qquad (**)$$

Or M appartient à $\mathrm{Orb}_G(M))^M$ (puisque tout élément de M agit trivialement par conjugaison sur M). D'après $(**)$, il existe un sous-groupe N de $(\mathrm{Orb}_G(M))^M$ distinct de M. Alors tout élément de M et de N agit trivialement par conjugaison sur N, donc $\langle M, N\rangle$ agit trivialement par conjugaison sur N. Or $\langle M, N\rangle = G$, donc N est distingué dans G. Mais N appartient à $\mathrm{Orb}_G(M)$, donc N est conjugué à M donc $N = M$: absurde ! Donc tout sous-groupe maximal d'un p-groupe est distingué.

Calculons l'ordre d'un sous-groupe maximal. Soit M un tel sous-groupe d'ordre p^β. Montrons $\beta = \alpha - 1$. Si ce n'était pas le cas, G/M serait un p-groupe d'ordre au moins p^2 et contiendrait un sous-groupe $\bar{H}$ d'ordre p. Alors, l'image réciproque de $\bar{H}$ dans G serait un sous-groupe d'ordre $p^{\beta+1}$ contenant M, ce qui contredirait le fait que M soit maximal. □

Remarque. Par le théorème de Frobenius (cf. proposition 6.2), dont la démonstration est plus simple que celle-ci, on sait qu'un sous-groupe d'ordre $p^{\alpha-1}$ est distingué. La force de cette proposition est donc le calcul de l'ordre des sous-groupes maximaux, ou, ce qui revient au même, de montrer que tout sous-groupe d'un groupe d'ordre p^α est inclus dans un sous-groupe d'ordre $p^\alpha - 1$.

5.2 Groupes nilpotents et p-groupes

Les groupes nilpotents[21] forment une famille importante de groupe, plus faciles que les autres à étudier puisque comme nous allons le voir, de même qu'un groupe abélien, un p-groupe est somme directe de ses p-Sylow. C'est ce que nous nous proposons de démontrer dans ce paragraphe. La méthode consiste à examiner (cf. argument de Frattini ci-dessous), les normalisateurs des p-Sylow et montrer que dans le cas des groupes nilpotents, ces normalisateurs sont le groupe tout entier, autrement dit les p-Sylow sont distingués.

Définition 5.8 (Groupe nilpotent)**.**
Rappelons que pour deux sous-groupes H et K de G, on note $[H, K]$ la clôture normale dans G de l'ensemble des éléments $hkh^{-1}k^{-1}$ où $h \in H$ et $k \in K$.

La *suite centrale descente* $(C_n(G))_{n\in\mathbb{N}}$ d'un groupe G est définie ainsi : $C_0(G) = G$ et pour tout $n \geqslant 1$, $C_n(G) = [G, C_{n-1}(G)]$.

Un groupe G est dit *nilpotent* s'il existe un entier m tel que $C_m(G) = \{1_G\}$. Le plus petit indice m satisfaisant cette condition est appelé l'*indice de nilpotence de* G.

Proposition 5.9. *Les p-groupes sont nilpotents.*

[21] Tous les groupes nilpotents sont résolubles. Ils constituent un premier exemple de groupes résolubles non nécessairement abéliens. Cependant, il existe comme $\mathfrak{S}_3$ des groupes résolubles, mais non nilpotents.

Démonstration. Soit G un p-groupe d'ordre p^α. On montre par récurrence sur α que G est nilpotent. Lorsque $\alpha = 0$, c'est évident. Soit $\alpha > 1$. On suppose le résultat vrai pour tout entier strictement inférieur à $\alpha \geqslant 0$ et on veut le démontrer pour α. Le centre $\mathcal{Z}_G$ de G n'est pas trivial, donc le groupe quotient $G/\mathcal{Z}_G$ est un p-groupe d'ordre strictement inférieur p^α, donc un groupe nilpotent d'après l'hypothèse de récurrence. Soit $\pi : G \to G/\mathcal{Z}_G$ le morphisme de passage au quotient. On a $\pi(G) = G/\mathcal{Z}_G$, donc pour tout n, on a $\pi(C_n(G)) = C_n(\pi(G)) = C_n(G/\mathcal{Z}_G)$. Or, puisque $G/\mathcal{Z}_G$ est nilpotent, il existe un entier m tel que $C_m(G/\mathcal{Z}_G) = \{1\}$. Donc pour cet entier m, on a $C_m(G) \subset \mathcal{Z}_G$. Alors $C_{m+1}(G) = [G, C_m(G)] \subset [G, \mathcal{Z}_G] = \{1\}$, par définition du centre. Ainsi G lui-même est nilpotent. □

Corollaire 5.10. *Tout produit direct de p-groupes est nilpotent.*

Démonstration. Cela découle de la proposition précédente et du fait que si A et B et A' et B' sont deux sous-groupes respectifs, alors $[A \times B, A' \times B'] \subset [A, A'] \times [B, B']$.

Proposition 5.11 (Croissance des normalisateurs)**.**
Soit G un groupe nilpotent. Alors tout sous-groupe propre H de G est strictement contenu dans son normalisateur $\mathrm{Norm}_G(H)$.

Démonstration. Il est clair par récurrence que $C_i(G)$ est distingué dans G. Soit H un sous-groupe de G et pour tout i, soit $H_i = HC_i(G)$. Vérifions que H_{i+1} est distingué dans H_i, autrement dit que H_{i+1} est normalisé par H (c'est évident) et par $C_i(G)$ (ce que nous allons démontrer). Soient h un élément de H_{i+1} et g un élément de $C_i(G)$. On a :

$$ghg^{-1} = ghg^{-1}h^{-1}h \in [G, C_i(G)]H_{i+1} = C_{i+1}(G)H_{i+1} = H_{i+1},$$

d'où $ghg^{-1} \in H_i + 1$. Ainsi, il existe une suite :

$$G = H_1 \supset H_2 \supset \cdots \supset H_n = H \qquad (*)$$

vérifiant $H_{i+1} \lhd H_i$ et $H_n = H$. On peut supposer que $H_n \subsetneq H_{n-1}$. Or on a $\mathrm{Norm}_G(H) \supset H_{n-1}$, puisque $H = H_n \lhd H_{n-1}$. Ce qu'il fallait démontrer. □

Remarque. En fait, cette propriété caractérise les groupes nilpotents.

Lemme 5.12 (Argument de Frattini)**.**
Soit G un groupe, H un sous-groupe distingué, et S un p-Sylow de H. Alors $G = \mathrm{Norm}_G(S)H$.

Démonstration. Soit $g \in G$. Le sous-groupe gSg^{-1} de G est inclus dans H puisque H est distingué, et par ailleurs, c'est un p-Sylow de H, donc gSg^{-1} est conjugué à H dans H, d'après le deuxième théorème de Sylow. Ainsi, il existe $h \in H$ tel que $hgSg^{-1}h^{-1} = S$. Alors $hg \in \mathrm{Norm}_G(S)$, donc $g \in H\mathrm{Norm}_G(S)$. Ceci étant vrai pour tout $g \in G$, on a $G = H\mathrm{Norm}_G(S)$, puis en utilisant le fait que H est distingué, $G = \mathrm{Norm}_G(S)H$. □

Lemme 5.13 (Normalisateur d'un p-Sylow)**.**
Soit G un groupe et S un p-Sylow de G. Alors $\mathrm{Norm}_G(\mathrm{Norm}_G(S)) = \mathrm{Norm}_G(S)$.

Démonstration. Appliquons l'argument de Frattini au groupe $\mathrm{Norm}_G(\mathrm{Norm}_G(S))$ dont $\mathrm{Norm}_G(S)$ est un sous-groupe normal et S un p-Sylow de $\mathrm{Norm}_G(S)$. On obtient que $\mathrm{Norm}_G(\mathrm{Norm}_G(S)) = \mathrm{Norm}_G(S)\mathrm{Norm}_G(S)$. Mais $\mathrm{Norm}_G(S)\mathrm{Norm}_G(S) = \mathrm{Norm}_G(S)$, d'où le résultat. □

Théorème 5.14 (Structure des groupes nilpotents)**.**
Un groupe nilpotent est produit direct de ses p-Sylow.

Démonstration. Soit G un groupe nilpotent d'ordre n et p un diviseur premier de n. Soit S un p-Sylow de G. D'après le lemme 5.13, on a $\mathrm{Norm}_G(S)\mathrm{Norm}_G(S) = \mathrm{Norm}_G(S)$. Or d'après la proposition 5.11, le seul sous-groupe H de G vérifiant $\mathrm{Norm}_G(H) = H$ est G lui-même, donc en appliquant ceci à $\mathrm{Norm}_G(S)$, on voit que $\mathrm{Norm}_G(S) = G$, autrement dit, S est distingué dans G. Ceci étant vrai pour tout p premier diviseur de n, on peut appliquer la proposition 4.8. Ainsi G est somme directe de ses p-Sylow. □

Remarques.

1. Moralement, les groupes finis nilpotents sont « presque » des p-groupes. Par exemple, on savait que les p-groupes admettaient des sous-groupes distingués de tous ordres (cf. proposition 5.5). C'est aussi le cas des groupes nilpotents (cf. proposition 5.15).

2. Ce théorème 5.14 donne une condition nécessaire très forte pour un groupe d'être nilpotent. Par exemple, $\mathfrak{S}_3$ est le produit semi-direct non trivial de $\mathbb{Z}/3\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$ et n'est donc un produit direct de ses sous-groupes de Sylow. Par conséquent, $\mathfrak{S}_3$ n'est pas nilpotent. En effet, $C_1(\mathfrak{S}_3) = [\mathfrak{S}_3, \mathfrak{S}_3] = \langle \sigma, \rangle$, où σ est un 3-cycle. Puis $C_2(\mathfrak{S}_3) = [\mathfrak{S}_3, \mathfrak{A}_3] = \mathfrak{A}_3$ car $\sigma\tau\sigma^{-1}\tau = \sigma^{-1}$, où τ est une transposition. Ainsi, pour tout n, $C_n(\mathfrak{S}_3) = \mathfrak{S}_3$, donc $\mathfrak{S}_3$ n'est pas nilpotent.

Proposition 5.15 (Réciproque du théorème de Lagrange pour les groupes nilpotents)**.**
Un groupe est nilpotent si et seulement s'il admet des sous-groupes distingués de tous ordres.

Démonstration. Montrons le sens direct. Soit $n = \prod_{1 \leqslant i \leqslant r} {p_i}^{\alpha_i}$ l'ordre de G et $m = \prod_{1 \leqslant i \leqslant r} {p_i}^{\beta_i}$ un diviseur de n. D'après le théorème 5.14, il existe r sous-groupes H_i de G d'ordre respectivement ${p_i}^{\alpha_i}$ tels que $G = \bigoplus_{1 \leqslant i \leqslant r} H_i$. Or tout groupe H_i contient un sous-groupe distingué K_i d'ordre ${p_i}^{\beta_i}$ d'après la proposition 5.5. Alors, le sous-groupe $N = \bigoplus_{1 \leqslant i \leqslant r} K_i$ de G est d'ordre m, et est distingué puisque c'est le produit de sous-groupes distingués.

Montrons la réciproque. Si un groupe admet des sous-groupes distingués de tous ordre, chacun de ses sous-groupes de Sylow sont distingués. Alors on peut appliquer la proposition 4.8. Ainsi un tel groupe est produit direct de ses sous-groupes de Sylow. Donc il est nilpotent d'après le théorème 5.14. □

5.3 Théorème de Frattini

Beaucoup de sous-groupes particuliers ont été inventés pour faciliter l'étude des groupes (groupe de Fitting, socle, cosocle, etc.). Nous présentons l'un d'eux, le sous-groupe de Frattini, conçu pour l'étude des p-groupes, dont la définition peut être immédiatement élargie à tous les groupes finis (et même aux groupes infinis).

Définition 5.16 (Eléments mous d'un groupe)**.**
Un élément d'un groupe est dit *mou*[22] si pour toute partie $S \subset G$ telle que S et cet élément engendrent le groupe, S engendre le groupe.

Exemple. L'élément neutre est toujours un élément mou. Par exemple, $\mathbb{Z}$ ne contient aucun élément mou autre que 0, puisque pour tout $m \in \mathbb{Z}$, on peut choisir n premier à m et différent de ± 1. Alors m et n engendrent $\mathbb{Z}$, mais n tout seul n'engendre pas $\mathbb{Z}$.

Proposition 5.17.
(i) L'ensemble Φ des éléments mous d'un groupe est un sous-groupe,
(ii) Φ est même un sous-groupe caractéristique,
(iii) Φ est l'intersection de tous les sous-groupes maximaux[23]*.*

Démonstration.
(i) Soit Φ l'ensemble des éléments mous d'un groupe G. Il est clair que $1_G \in \Phi$, et que Φ est stable par passage à l'inverse. Si g et h sont deux éléments de Φ, alors pour tout sous-ensemble S tel que $\langle gh, , S\rangle = G$, on a bien sûr $\langle g, h, S\rangle = G$. Or m est mou, donc $\langle h, S\rangle = G$, or h est mou donc $\langle S\rangle = G$. Ceci prouve que Φ est un groupe.

(ii) Soit φ un automorphisme de G et g un élément de G. S'il existe un sous-ensemble S de G tel que $\langle \varphi(g), S\rangle = G$, alors $\langle g, \varphi^{-1}(S)\rangle = \varphi^{-1}(G) = G$. Ainsi, l'image d'un élément mou par un automorphisme est un élément mou. Donc Φ est stable par tout automorphisme.

(iii) Montrons que Φ est inclus dans tout sous-groupe maximal M. Supposons qu'il existe un sous-groupe maximal M de G ne contenant pas Φ. Soit alors $g \in \Phi \setminus M$. Alors on a $M \subsetneq \langle g, M\rangle \subset G$. La deuxième inclusion doit être stricte car g est mou, mais elle doit être une égalité car M était maximal, d'où une contradiction.

Montrons que Φ contient l'intersection de tous les sous-groupes maximaux. Supposons qu'il existe g appartenant à l'intersection de tous les sous-groupes maximaux mais n'appartenant pas à Φ. Soit S inclus dans G tel que $\langle S\rangle \neq G$ et $\langle g, S\rangle = G$. Soit M un sous-groupe maximal contenant S. Par définition de g, g appartient à M, donc M contient $\langle g, S\rangle$ et doit être égal à G : absurde ! □

Définition 5.18 (Sous-groupe de Frattini)**.**
Le sous-groupe de tous les éléments mous d'un groupe G est appelé le *sous-groupe de Frattini* et est noté $\Phi(G)$.

[22] En anglais, un élément mou est appelé *non-generating element*, ce qui décrit bien la situation.
[23] Cf. définition 5.6.

Exemples.

- Un élément $\bar{k}$ de $G = \mathbb{Z}/p^n\mathbb{Z}$ est mou si et seulement si $k \wedge p = 1$. Donc $\Phi(G)$ est le groupe engendré par $\bar{p}$, isomorphe à $\mathbb{Z}/p^{n-1}\mathbb{Z}$.
- Soit G_1 et G_2 deux groupes finis, et $G = G_1 \times G_2$. Alors $\Phi(G) = \Phi(G_1) \times \Phi(G_2)$.
- Soit $n = \prod p_i^{\alpha_i}$, les p_i étant premiers deux à deux distincts. Alors $\Phi(\mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/m\mathbb{Z}$ où $m = \prod p_i^{\alpha_i - 1}$.

Lemme 5.19 (Existence de compléments partiels)**.**

(i) Soit $\{x_i\}_{1 \leqslant i \leqslant n}$ des éléments d'un groupe G. Si $\langle \Phi(G),\, x_i \,|\, 1 \leqslant i \leqslant n \rangle = G$, alors $\langle x_i \,|\, 1 \leqslant i \leqslant n \rangle = G$.

(ii) Soit H un sous-groupe de G tel que $\Phi(G)H = G$. Alors $H = G$.

(iii) Plus généralement, un sous-groupe H de G distingué possède un complément partiel si et seulement si H n'est pas inclus dans $\Phi(G)$.

Démonstration.

(i) Montrons la contraposée. Soit $H = \langle x_i \,|\, 1 \leqslant i \leqslant n \rangle$ que l'on suppose différent de G et M un sous-groupe maximal contenant H. Alors $\langle \Phi(G),\, x_i \,|\, 1 \leqslant i \leqslant n \rangle$ est contenu dans M puisque $\Phi(G)$ est lui aussi inclus dans M. Donc $\langle \Phi(G),\, x_i \,|\, 1 \leqslant i \leqslant n \rangle$ est différent de G.

(ii) Il suffit d'appliquer (i) aux éléments h_i de H.

(iii) Si un sous-groupe H distingué dans G est inclus dans $\Phi(G)$, il ne peut admettre de complément partiel, sinon $\Phi(G)$ en contiendrait un, ce qui contredirait (ii).

Réciproquement, si un sous-groupe H distingué dans G n'est pas inclus dans $\Phi(G)$, il existe un sous-groupe maximal K de G tel que $\langle H,\, K \rangle$ engendre G. Or $\langle H,\, K \rangle = HK$. donc K est un complément partiel de H. □

Théorème 5.20 (Théorème de Frattini)**.**

Le quotient d'un p-groupe par le sous-groupe de Frattini est un $\mathbb{F}_p$-espace vectoriel.

Démonstration. Soit G un p-groupe et $\Phi(G)$ son sous-groupe de Frattini. Montrons que $G/\Phi(G)$ est commutatif. Tout sous groupe maximal M est d'ordre $p^{\alpha-1}$ d'après la proposition 5.7, donc $G/M \cong \mathbb{Z}/p\mathbb{Z}$ et est commutatif, donc $[G,\, G] \subset M$. Par conséquent, $[G,\, G] \subset \Phi(G)$, donc $G/\Phi(G)$ est commutatif.

Montrons maintenant que tous les éléments de $G/\Phi(G)$ sont d'ordre p. Si ce n'était pas le cas, on aurait l'existence d'un élément $\bar{y}$ d'ordre p^2 dans $G/\Phi(G)$ (puisque $G/\Phi(G)$ est commutatif). Soit y dans G d'image $\bar{y}$ dans $G/\Phi(G)$. Puisque $\bar{y}^p$ n'est pas dans $G/\Phi(G)$, y^p n'est pas mou, donc il existe M, un sous-groupe maximal de G, ne contenant pas y^p. Il ne contient pas y non plus. Alors l'image $\tilde{y}$ de y dans G/M est d'ordre au moins p^2, donc M est d'ordre au plus $p^{\alpha-2}$, ce qui contredit le fait que M soit maximal d'après la proposition 5.7. Ainsi tous les éléments de $G/\Phi(G)$ sont d'ordre p.

Finalement, $G/\Phi(G)$ est un groupe abélien dont tous les éléments sont d'ordre p. □

Remarque. On peut montrer en fait que $\Phi(G)$ est le plus petit sous-groupe de G tel que $G/\Phi(G)$ soit un espace vectoriel. L'espace vectoriel engendré est donc le plus gros parmi ceux obtenus en quotientant G.

Définition 5.21 (Espace de Frattini)**.**
L'*espace de Frattini* d'un p-groupe G est le $\mathbb{F}_p$-espace vectoriel $G/\Phi(G)$.

Proposition 5.22 (Espaces de Frattini de petite dimension)**.**
Soit G un p-groupe. L'espace de Frattini n'est jamais de dimension 0. Il est de dimension 1 si et seulement si G est cyclique.

Démonstration. Puisque $\Phi(G)$ est contenu dans tout sous-groupe maximal, $\Phi(G)$ est strictement contenu dans G, donc $G/\Phi(G)$ n'est pas de dimension 0. Si $G/\Phi(G)$ est de dimension 1, soit $x \in G$ tel que l'élément $x\Phi(G)$ de $G/\Phi(G)$ engendre $G/\Phi(G)$. Alors $\langle \Phi(G), x\rangle = G$, donc d'après le lemme 5.19, $\langle x\rangle = G$. □

Exemples.

1. L'espace de Frattini d'un groupe abélien G de type $(p^{\alpha_1}, p^{\alpha_2}, \ldots, p^{\alpha_r})$ est $(\mathbb{F}_p)^r$.
2. Pour le groupe quaternionique, $\Phi(\mathbb{H}_8) = \{\pm 1\}$ donc $\mathbb{H}_8/\Phi(\mathbb{H}_8) \cong (\mathbb{F}_2)^2$.
3. Plus généralement, soit G un groupe non abélien d'ordre p^3 (p premier). Nous allons montrer que :

$$\Phi(G) = \mathbb{Z}_G \cong \mathbb{Z}/p\mathbb{Z} \quad \text{et} \quad G/\Phi(G) = {\mathbb{F}_p}^2.$$

Le centre de G n'est pas trivial par le théorème de Burnside. Par ailleurs, $G/\mathcal{Z}_G$ n'est pas cyclique, sinon G serait abélien par le lemme 6.1. Donc $G/\mathcal{Z}_G \cong (\mathbb{Z}/p\mathbb{Z})^2$ et contient p^2 éléments, et $\mathcal{Z}_G \cong \mathbb{Z}/p\mathbb{Z}$. Soit M un sous-groupe maximal de G. Si $\mathcal{Z}_G \cap M = \{1\}$, alors G est un produit direct (car $\mathcal{Z}_G$ est central) de deux groupes abéliens, donc G est abélien : absurde ! Donc le centre est inclus dans tout sous-groupe maximal, d'où :

$$\mathcal{Z}_G \subset \Phi(G).$$

Alors selon le cardinal de $\Phi(G)$, $G/\Phi(G)$ est isomorphe à $(\mathbb{F}_p)^2$, $\mathbb{F}_p$ ou 1_G. Mais les deux derniers cas sont interdits par la proposition 5.22, donc $G/\Phi(G) \cong (\mathbb{F}_p)^2$, donc $\Phi(G) = \mathbb{Z}_G$.

En fait, on peut prouver la proposition suivante, que l'on ne démontrera pas ici.

Proposition 5.23. *Le sous-groupe de Frattini d'un p-groupe G est égal à $G^p[G, G]$ où $G^p = \langle g^p,\ g \in G\rangle$, et est inclus dans le centre $\mathcal{Z}_G$.*

6 Classification des groupes de petit cardinal

6.1 Deux résultats utiles

En plus du théorème de Burnside (cf. proposition 5.3 : « Le centre d'un p-groupe n'est pas trivial. »), fondamental pour l'étude des p-groupes, voici deux résultats tout aussi utiles.

Lemme 6.1 (Groupes dont le quotient par le centre est monogène)**.**
Un groupe dont le quotient par son centre est monogène est abélien.

Démonstration. Soit G un tel groupe, $\mathcal{Z}_G$ sont centre, et x un élément tel que $x\mathcal{Z}_G$ engendre $G/\mathcal{Z}_G$. Soient alors deux éléments de ce groupe g_1 et g_2. Il existe $z_1, z_2 \in \mathcal{Z}_G$ et $k_1, k_2 \in \mathbb{Z}$ tels que $g_1 = x^{k_1} z_1$ et $g_2 = x^{k_2} z_2$. Clairement, g_1 et g_2 commutent. □

Proposition 6.2 (Théorème de Frobenius, 1895)**.**
Soit G un groupe d'ordre n et soit p le plus petit diviseur premier de n. Alors tout sous-groupe d'indice p est distingué[24]*.*

Démonstration. Soit H un sous-groupe d'indice p que l'on fait agir par multiplication à gauche sur $E = G/H$. Remarquons que l'action est triviale si et seulement si pour tout $g \in G$, on a $HgH = gH$, donc si et seulement si H est distingué. Soit E'' une transversale de $E \setminus E^H$. Alors, l'équation aux classes s'écrit :

$$|E| = |E^H| + \sum_{gH \in E''} \mathrm{Orb}_H(gH).$$

Or $|E| = p$ par hypothèse, donc chaque orbite qui n'est pas réduite à un point contient p éléments. Puisqu'il existe au moins une orbite réduite à un point, celle de H, elles sont toutes réduites à un point. Donc l'action est triviale et H est distingué dans G. □

Remarques.

1. Ce résultat est absolument fondamental ! Grâce à lui, il est facile de percevoir presque tout groupe (attention, pas les groupes simples !) comme une extension de groupes plus petits. En effet, dès qu'un groupe G possède un sous-groupe N du bon indice, on sait que N doit être distingué. Connaissant alors N et G/N, on peut espérer retrouver le groupe G. Tous les espoirs de classification complète des groupes reposent sur de telles extensions !

2. Ce résultat est redondant avec le troisième théorème de Sylow dans le cas des groupes d'ordre $p^\alpha q$ où q est un nombre premier strictement inférieur à p. En effet, dans ce cas, le nombre n_p de p Sylow vérifie $n_p \equiv 1 \mod p$ et $n_p | q$, ce qui montre que $n_p = 1$, donc d'après le deuxième théorème de Sylow, le p-Sylow (qui est un sous-groupe d'indice q) est distingué.

6.2 Classification des groupes d'ordre $n \leqslant 15$

On notera V_4 le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, appelé *groupe de Klein.*

Amorce de la classification :

- pour tout p premier, il existe un unique groupe $\mathbb{Z}/p\mathbb{Z}$,
- tout groupe d'ordre p^2 est abélien (cf. proposition 5.4),
- on connaît quelques groupes non abéliens :

[24] Lorsque $p = 2$, la preuve peut être simplifiée, cf. l'exemple 4 page 14 et s'entend même aux groupes d'ordre infini.

- $n = 6$: $\mathfrak{S}_3$, $\mathcal{D}_3$, $\mathcal{GL}(2, \mathbb{F}_2)$.
- $n = 8$: $\mathcal{D}_4$, $\mathbb{H}_8$, $\mathcal{T}_{3,2}$ (cf. définition 5.2),
- $n = 10$: $\mathcal{D}_5$,
- $n = 12$: $\mathcal{D}_6$, $\mathfrak{A}_4$,
- $n = 14$: $\mathcal{D}_7$.

Proposition 6.3 (Groupes d'ordre 6)**.**
Les groupes non abéliens d'ordre 6 sont isomorphes à $\mathfrak{S}_3$

Démonstration. Soit σ un élément d'ordre 3 et τ un élément d'ordre 2. Si $\tau\sigma\tau = \sigma$, le groupe est abélien ; si $\tau\sigma\tau = \sigma^2$, on retrouve la table de multiplication de $\mathfrak{S}_3$. □

Proposition 6.4 (Groupes d'ordre pq)**.**
Soient p et q deux entiers distincts avec $p < q$. Il existe une ou deux classes d'isomorphie de groupes d'ordre pq, selon que p divise $q - 1$ ou non :
- $\mathbb{Z}/pq\mathbb{Z}$,
- $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$, *seulement si p divise $q - 1$.*

Lorsque $p = 2$, $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ est le groupe diédral $\mathcal{D}_q$.

Démonstration. Soit p le plus petit facteur de G. Alors le q-Sylow Q est distingué d'après le théorème de Frobenius (proposition 6.2). On peut le voir aussi en invoquant le troisième théorème de Sylow : $n_q \equiv 1 \mod q$ et $n_q | p$, où n_q est le nombre de q-Sylow. Notons P un p-Sylow. Alors, on a $Q \lhd G$, $Q \cap P = \{1_G\}$ et $|QP| = |G|$, donc G est le produit semi-direct de Q par P. Examinons l'action de P sur Q via son morphisme structurel $\varphi : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/q - 1\mathbb{Z}$. Différents cas se produisent.
- Si $p = 2$, il existe une unique action non triviale donnée par $\varphi(\bar{1}) = \frac{q-1}{2}$ et le groupe associé est le groupe diédral $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \cong \mathcal{D}_q$. Il n'est pas commutatif et est donc distinct de $\mathbb{Z}/2q\mathbb{Z}$.
- Si p ne divise pas $q - 1$, il n'existe pas d'action non triviale et tous les groupes d'ordre pq où p ne divise pas q est abélien.
- Si p divise $q - 1$, il existe différentes actions, toutes de la forme $\varphi_k(\bar{1}) = k^{\frac{q-1}{p}}$ où $k \in \{1, \ldots, p - 1\}$. Or $\varphi_k = \varphi_1 \circ \gamma_k$, où γ_k est la multiplication par k dans $\mathbb{Z}/p\mathbb{Z}$. C'est un automorphisme, donc toutes ces actions produisent des produits semi-directs isomorphes. Le groupe associé n'est pas commutatif, donc il n'est pas isomorphe à $\mathbb{Z}/pq\mathbb{Z}$. □

Remarque. On a vu au paragraphe 3.6 que dans le cas des produits semi-directs non triviaux des groupes d'ordre pq, l'action de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathbb{Z}/q\mathbb{Z}$ est décrite par un morphisme $\varphi : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$, $t \mapsto \{x \mapsto k^t x\}$ où k est un élément de $(\mathbb{Z}/q\mathbb{Z})^*$ d'ordre p.

Lemme 6.5. *Le groupe $\mathbb{H}_8$ n'est pas un produit semi-direct.*

Démonstration. Supposons qu'il existe deux sous-groupes N et H de $\mathbb{H}_8$ tels que $\mathbb{H}_8 = N \rtimes H$.

– Si $|N| = 4$, alors $H = \{1, h\}$ où h est d'ordre 2 dans $\mathbb{H}_8$, donc $h = -1$, mais -1 appartient déjà à $|N|$, puisque -1 est le carré de tout $x \in \mathbb{H}_8 \setminus \{\pm 1\}$. Donc $H \cap N \neq \{1\}$: c'est absurde.
– Si $|N| = 2$, puisque H est central, le produit serait direct. Alors $\mathbb{H}_8$ serait le produit direct de deux groupes abéliens, donc serait abélien : c'est absurde. □

Proposition 6.6 (Groupes d'ordre 8)**.**
Il existe deux classes d'isomorphie de groupes non abéliens d'ordre 8 :
- $\mathcal{D}_4 \cong \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \cong V_4 \rtimes \mathbb{Z}/2\mathbb{Z} \cong \mathcal{T}_{3,2}$ *(cf. définition 5.2),*
- $\mathbb{H}_8$.

Démonstration. Soit G un groupe non abélien d'ordre 8. Rappelons qu'un groupe dont tous les éléments sont d'ordre 2 est abélien. Donc G contient des éléments d'ordre 4. Soit i un élément d'ordre 4 et H le sous-groupe engendré par i. Puisque c'est un sous-groupe d'indice 2, il est distingué. Distinguons les cas selon qu'il existe ou non un élément d'ordre 2 dans $G \setminus H$.

– S'il existe un élément d'ordre 2 dans $G \setminus H$, alors la suite exacte
$$1 \to H \to G \to G/H \to 1$$
est scindée, donc G est un produit semi-direct de H par $\mathbb{Z}/2\mathbb{Z}$. Un tel produit semi-direct est caractérisé par une action de $\mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$. Il existe un unique tel morphisme non trivial, donc on obtient un unique produit semi-direct non abélien.
– S'il n'existe pas d'élément d'ordre 2 dans $G \setminus H$, alors $G \setminus H$ consiste en quatre éléments d'ordre 4 (précisons qu'il ne peut pas contenir d'élément d'ordre 8, sinon$G$ serait abélien cyclique). Appelons j l'un d'eux. Notons 1, i, $i^2 = -1$ et $i^3 = -i$ les quatre éléments de H. Les éléments de G sont
$$\{1, i, -1, -i, j, ij, -j, -ij\}.$$
Puisque -1 est le seul élément d'ordre 2, il est central et $i^2 = j^2 = (ij)^2 = -1$. Puisque $ijij = -1 = i^2$, on a $jij = i$, donc $jij^{-1} = -i$. Ainsi, on a reconstitué la table d'opération de $\mathbb{H}_8$. Or on sait que $\mathbb{H}_8$ n'est pas un produit semi-direct, donc il n'est pas isomorphe à $\mathcal{D}_4$.

Les groupes $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ et $V_4 \rtimes \mathbb{Z}/2\mathbb{Z}$ étant des produits semi-directs, ils ne sont pas isomorphes à $\mathbb{H}_8$ d'après le lemme 6.5. Le groupe $\mathcal{T}_{3,2}$ contient plusieurs éléments d'ordre 2, donc n'est pas isomorphe à $\mathbb{H}_8$. □

Proposition 6.7 (Groupes d'ordre 12)**.**
Il existe trois classes d'isomorphie de groupes non abéliens d'ordre 12 :
- $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$,
- $\mathcal{D}_6 \cong \mathbb{Z}/3\mathbb{Z} \rtimes V_4 \cong \mathcal{D}_3 \times \mathbb{Z}/2\mathbb{Z} \cong \mathcal{D}_3 \rtimes \mathbb{Z}/2\mathbb{Z}$,
- $\mathfrak{A}_4 \cong V_4 \rtimes \mathbb{Z}/3\mathbb{Z}$.

Démonstration. Soit G un groupe d'ordre 12 et soit n_3 le nombre de 3-Sylow. Il doit diviser 4 et doit vérifier $n_3 \equiv 1 \mod 3$, donc $n_3 \in \{1, 4\}$.

Si $n_3 = 4$, alors on compte 8 éléments d'ordre 3. Il en reste donc 4 pour former le 4-Sylow qui est donc distingué. Appelons-le N. Soit K un 3-Sylow. Puisque par ailleurs $N \cap K = \{1_G\}$, le groupe G est le produit semi-direct de N par K, décrit par un morphisme φ de $K = \mathbb{Z}/3\mathbb{Z}$ dans $\mathrm{Aut}(N)$. Deux cas se présentent : $N = \mathbb{Z}/4\mathbb{Z}$ ou bien $N = V_4$.

- Si $N = \mathbb{Z}/4\mathbb{Z}$, alors $\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ et φ va de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathbb{Z}/2\mathbb{Z}$, donc est trivial, donc le produit est direct et correspond à un groupe abélien.
- Si $N = V_4$, alors $\mathrm{Aut}(V_4) \cong \mathfrak{S}_3$ et φ va de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathfrak{S}_3$, donc associe 1 à un 3-cycle ou à son carré. Notons φ_1 et φ_2 ces deux morphismes. Soit $\gamma : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$, $1 \mapsto -1$. Il vient $\varphi_2 = \varphi_1 \circ \gamma$ et par conséquent, les deux structures de produit semi-direct sont semblables et décrivent le même groupe $V_4 \rtimes \mathbb{Z}/3\mathbb{Z}$ à isomorphisme près.

Si $n_3 = 1$, soit N le 3-Sylow distingué et soit H le groupe d'ordre 4 : $\mathbb{Z}/4\mathbb{Z}$ ou V_4. Le produit semi-direct $N \rtimes H$ est décrit par un morphisme φ de H dans $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$. Etudions les deux cas.

- Si $H = \mathbb{Z}/4\mathbb{Z}$, alors il existe un unique morphisme non trivial de $\mathbb{Z}/4\mathbb{Z}$ dans $\mathbb{Z}/2\mathbb{Z}$, correspondant au produit semi-direct $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$.
- Si $H = V_4$, alors φ est un morphisme de V_4 dans $\mathbb{Z}/2\mathbb{Z}$, autrement dit une $\mathbb{F}_2$-forme linéaire de ${\mathbb{F}_2}^2$. Il en existe trois non triviales, décrite par les matrices en ligne : $[\varphi_1] = (0,1)$, $[\varphi_2] = (1,0)$, $[\varphi_3] = (1,1)$. Cependant, il existe $\gamma \in \mathrm{Aut}[V_4] = \mathcal{GL}(2, \mathbb{F}_2)$ tel que $\varphi_2 = \varphi_1 \circ \gamma$ pour $[\gamma] = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ et $\varphi_3 = \varphi_1 \circ \gamma$ pour $[\gamma] = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$. Ainsi les trois produits semi-directs sont isomorphes. On note $\mathbb{Z}/3\mathbb{Z} \rtimes V_4$ le groupe associé.

Faisons le bilan. Nous avons trouvé trois groupes : $V_4 \rtimes \mathbb{Z}/3\mathbb{Z}$ qui possède quatre 3-Sylow, et $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z} \rtimes V_4$ qui possèdent tous deux un seul 3-Sylow. Pour départager $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z} \rtimes V_4$, remarquons que l'un possède un élément d'ordre 4 et l'autre pas. On a donc exactement trois groupes non abéliens d'ordre 12 différents à isomorphisme près.

Le groupe $\mathfrak{A}_4$ possède un sous-groupe distingué isomorphe à V_4, le sous-groupe des double-transpositions (produit de deux transpositions à supports disjoints). Donc $\mathfrak{A}_4 \cong V_4 \cong \mathbb{Z}/3\mathbb{Z}$. Le groupe $\mathcal{D}_6 = \mathbb{Z}/6\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ possède un sous-groupe d'ordre 3 distingué, mais aucun élément d'ordre 4, donc $\mathcal{D}_6 \cong \mathbb{Z}/3\mathbb{Z} \rtimes V_4$. Les groupes $\mathfrak{S}_3 \times \mathbb{Z}/2\mathbb{Z}$ et $\mathfrak{S}_3 \rtimes \mathbb{Z}/2\mathbb{Z}$ ne possèdent qu'un seul 3-Sylow et aucun élément d'ordre 4, et sont donc isomorphes à $\mathbb{Z}/3\mathbb{Z} \rtimes V_4$. Ceci achève la classification des groupes non abéliens d'ordre 12. □

Théorème 6.8 (Classification des groupes d'ordre $n \leqslant 15$)**.**

n	*groupes abéliens*	*groupes non abéliens*	*total*
2	$\mathbb{Z}/2\mathbb{Z}$	-	*1*
3	$\mathbb{Z}/3\mathbb{Z}$	-	*1*
4	$\mathbb{Z}/4\mathbb{Z}, \quad V_4$	-	*1*
5	$\mathbb{Z}/5\mathbb{Z}$	-	*1*
6	$\mathbb{Z}/6\mathbb{Z}$	$\mathfrak{S}_3 \cong \mathcal{D}_3 \cong \mathcal{GL}(2, \mathbb{F}_2)$	*2*
7	$\mathbb{Z}/7\mathbb{Z}$	-	*1*
8	$\mathbb{Z}/8\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \quad (\mathbb{Z}/2\mathbb{Z})^3$	$\mathcal{D}_4 \cong V_4 \rtimes \mathbb{Z}/2\mathbb{Z} \cong \mathcal{T}_{3,2}$, $\quad \mathbb{H}_8$	*5*
9	$\mathbb{Z}/9\mathbb{Z}, \quad (\mathbb{Z}/3\mathbb{Z})^2$	-	*2*
10	$\mathbb{Z}/10\mathbb{Z}$	$\mathcal{D}_5$	*2*
11	$\mathbb{Z}/11\mathbb{Z}$	-	*1*
12	$\mathbb{Z}/12\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z} \rtimes V_4 \cong \mathfrak{S}_3 \times \mathbb{Z}/2\mathbb{Z} \cong \mathcal{D}_6$, $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}, \quad V_4 \rtimes \mathbb{Z}/3\mathbb{Z} \cong \mathfrak{A}_4$	*5*
13	$\mathbb{Z}/13\mathbb{Z}$	-	*1*
14	$\mathbb{Z}/14\mathbb{Z}$	$\mathcal{D}_7$	*2*
15	$\mathbb{Z}/15\mathbb{Z}$	-	*1*

où $\mathcal{T}_{3,2}$ est le groupe introduit à la définition 5.2.

6.3 Etude de quelques groupes de plus gros cardinal

Proposition 6.9 (Groupes d'ordre p^3)**.**
Il existe deux classes d'isomorphie de groupes d'ordre p^3 ($p \geqslant 3$ premier) :

- $\mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$
- $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/p\mathbb{Z}$

Le groupe[25] $\mathcal{T}_{3,p}$ est isomorphe[26] à $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/p\mathbb{Z}$.

Idée de la démonstration. Soit G un groupe d'ordre p^3. S'il existe un élément d'ordre p^3 le groupe est abélien. En de hors de ce cas, tous les éléments non triviaux sont d'ordre p ou p^2.

Premier cas : si tous les éléments sont d'ordre p, soit N un sous-groupe d'indice p. Il est distingué d'après le théorème de Frobenius (cf. proposition 6.2), et nécessairement, $N \cong (\mathbb{Z}/p\mathbb{Z})^2$. N'importe quel élément du complémentaire de N engendre un sous-groupe H d'ordre p dont l'intersection avec N est $\{1_G\}$, donc G est le produit semi-direct de N par H. L'action sous-jacente est décrite par un morphisme φ de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^2) = \mathcal{GL}(2, \mathbb{F}[p])$ qui envoie $\bar{1}$ sur un isomorphisme de $(\mathbb{F}_p)^2$ d'ordre p. Soient φ_1 et φ_2 deux tels morphismes. Puisque $\mathcal{GL}(2, \mathbb{F}[p])$ est d'ordre $(p^2-1)(p^2-p) = p(p-1)^2(p+1)$, les sous-groupes d'ordre p sont les p-Sylow deux à deux conjugués. Donc $\varphi_1(1)$ est conjugué à $\varphi_2(k)$ pour un certain $k \in (\mathbb{Z}/p\mathbb{Z})^*$. Soit α la multiplication par k dans $\mathbb{Z}/p\mathbb{Z}$. Alors $\varphi_1 \circ \alpha(1)$ est conjugué à $\varphi_2(1)$ par un élément $P \in \mathcal{GL}(2, \mathbb{F}[p])$, donc pour tout $k \in \mathbb{Z}/p\mathbb{Z}$, on a $\varphi_1(k) \circ \alpha = P \circ \varphi_2(k) \circ P^{-1}$. Donc les deux actions décrivent deux produits semi-directs

[25] Cf. définition 5.2.

[26] Attention, ce résultat est faux lorsque $p = 2$.

isomorphes. Autrement dit, cette étude donne lieu à un unique groupe $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/p\mathbb{Z}$ à isomorphisme près.

Deuxième cas : il existe un élément d'ordre p^2 que l'on note x. Soit N le sous-groupe engendré par x, distingué dans G d'après le théorème de Frobenius. On admet[27] alors qu'il existe y dans $G \setminus N$ d'ordre p. On a alors un produit semi-direct $\mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$, décrit par un morphisme de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathbb{Z}/(p(p-1))\mathbb{Z}$. Soient φ_1 et φ_2 deux tels morphismes : $\varphi_1(1) = k_1(p-1)$ et $\varphi_2(1) = k_2(p-1)$, avec k_1 et k_2 premiers à p. Soit $\alpha : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, $1 \mapsto {k_1}^{-1}k_2$, où ${k_1}^{-1}$ est l'inverse de k_1 dans $\mathbb{Z}/p\mathbb{Z}$. Alors $\alpha \in \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ vérifie $\varphi_1 \circ \alpha = \varphi_2$. On a donc un unique produit semi-direct $\mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ à isomorphisme près.

Les deux groupes obtenus ne sont pas isomorphes puisqu'il n'existe pas d'éléments d'ordre p^2 dans le premier. Le groupe $\mathcal{T}_{3,p}$ ne contient pas de matrice d'ordre p^2, donc $\mathcal{T}_{3,p}$ est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/p\mathbb{Z}$. □

Proposition 6.10 (Groupes d'ordre $255 = 3 \times 5 \times 17$)**.**
Tout sous-groupe d'ordre 255 est cyclique.

Démonstration. D'après les théorèmes de Sylow, on compte :
- nombre de 17-Sylow : 1, distingué ;
- nombre de 5-Sylow : 1 ou 51, mais alors 204 éléments d'ordre 5 ;
- nombre de 3-Sylow : 1 ou 85, mais alors 170 éléments d'ordre 3.

Soit N le 17-Sylow et H un 5-Sylow. Alors NH est un sous-groupe d'indice 5 dans G qui est donc distingué. Puisque les 5-Sylow sont conjugués, leurs éléments restent dans NH qui est de cardinal 85. Donc il ne peut pas y avoir 204 éléments d'ordre 5. Donc le 5-Sylow est distingué d'après le théorème de Frobenius (cf. proposition 6.2). Alors G est un produit semi-direct de $\mathbb{Z}/85\mathbb{Z}$ par $\mathbb{Z}/3\mathbb{Z}$. L'action associée est décrite par un morphisme de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/85\mathbb{Z}) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$, mais un tel morphisme est trivial. Donc le produit est direct et G est abélien, donc cyclique. □

Remarque. En fait, on peut prouver que tout groupe de cardinal n est abélien si et seulement si $n \wedge \varphi(n) = 1$. Ici, $\varphi(255) = 16 \times 4 \times 2$ et est premier à 255.

Proposition 6.11 (Groupes d'ordre $399 = 3 \times 7 \times 19$)**.**
Il existe cinq classes d'isomorphie de groupes d'ordre 399 :
- $\mathbb{Z}/399\mathbb{Z}$,
- $\big(\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}\big) \times \mathbb{Z}/19\mathbb{Z}$,
- $\big(\mathbb{Z}/19\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}\big) \times \mathbb{Z}/7\mathbb{Z}$,
- $\mathbb{Z}/133\mathbb{Z} \rtimes_{\varphi_1} \mathbb{Z}/3\mathbb{Z}$ *où* $\varphi_1(1)$ *est la multiplication par 11 dans* $\mathbb{Z}/133\mathbb{Z}$,
- $\mathbb{Z}/133\mathbb{Z} \rtimes_{\varphi_2} \mathbb{Z}/3\mathbb{Z}$ *où* $\varphi_2(1)$ *est la multiplication par 30 dans* $\mathbb{Z}/133\mathbb{Z}$.

[27] La preuve de ce fait consiste à considérer un élément $y \in G \setminus N$ d'ordre p^2 et à montrer en une demi-page qu'il existe un entier k tel que yx^k soit d'ordre p dans G : un tel k doit être solution d'une équation dans $\mathbb{Z}/p^2\mathbb{Z}$ et on vérifie qu'il existe effectivement des solutions. Cela prend une demi-page de calculs compliqués et astucieux.

Démonstration. Un tel groupe possède un seul 19-Sylow N d'après le troisième théorème de Sylow. Les 7-Sylow sont a priori au nombre de 1 ou 57. Soit H un 7-Sylow. On va montrer par deux méthodes différentes que H est le seul 7-Sylow.

Première tentative Considérons le groupe NH dans G. C'est un produit semi-direct car N est distingué dans G donc dans NH et car $N \cap H = \{1\}$ à cause des ordres des éléments de N et H. Or un tel produit semi-direct est déterminé par une action de H dans dans $\mathrm{Aut}(N)$, mais en raison des cardinaux, de tels morphismes sont triviaux et NH est un produit direct. Malheureusement, cela ne permet pas de conclure.

Première méthode. Le groupe NH est un sous-groupe d'indice 3, donc un sous-groupe distingué dans G. Pour tout $g \in G$, $gHg^{-1} \subset gNHg^{-1} = NH$, donc $gHg^{-1} \subset HN$. Or si les 7-Sylow sont au nombre de 57, on compte 57×6 éléments d'ordre 7 distincts, inclus dans HN d'ordre 17×7 : absurde. Donc G ne contient qu'un seul 7-Sylow.

Deuxième méthode. S'il existait effectivement 57 7-Sylow H_i avec $1 \leqslant i \leqslant 57$, il existerait également 57 groupes NH_i d'ordre $7 \times 19 = 133$. Vérifions que deux éléments x_i et x_j d'ordre 133 (car on a vu que $NH = N \times H$), l'un dans NH_i, l'autre dans NH_j avec i et j différents, sont nécessairement différents. Elevés à la puissance 19, x_i^{19} est dans H_i et x_j^{19} est dans H_j, or $|H_i \cap H_j| \in \{1, 7\}$, donc $H_i \cap H_j = \{1_G\}$, donc x_i^{19} et x_j^{19} sont différents, donc x_i et x_j étaient différents. Or dans chaque NH_i, on compte $\phi(133) = 6 \times 18$ éléments d'ordre 133, donc on compte au total $57 \times 6 \times 18$ éléments d'ordre 133, ce qui est absurde. On a donc qu'un seul 7-Sylow.

D'après le lemme 4.7, il vient que N et H sont en somme directe. Soit $K = NH = N \times H$. Alors $K = \mathbb{Z}/133\mathbb{Z}$ est le seul groupe de G de cet ordre. Pour terminer l'étude, il reste à examiner les produit semi directs

$$\mathbb{Z}/133\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}.$$

Ces produits semi-directs ont été étudiés pour une large part à la fin du paragraphe 3.6, et l'étude sera achevée à la fin du paragraphe 7.4. □

Proposition 6.12 (Groupe d'ordre $147 = 3 \times 7^2$)**.**
Il existe cinq classes d'isomorphie de groupes d'ordre 147 :

- $\mathbb{Z}/147\mathbb{Z}$,
- $(\mathbb{Z}/7\mathbb{Z})^2 \times \mathbb{Z}/3\mathbb{Z}$,
- $\mathbb{Z}/49\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$,
- $(\mathbb{Z}/7\mathbb{Z})^2 \rtimes_{\varphi_1} \mathbb{Z}/3\mathbb{Z}$, *avec* $\varphi_1(1) = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right) \in \mathrm{Aut}({\mathbb{F}_7}^2)$,
- $(\mathbb{Z}/7\mathbb{Z})^2 \rtimes_{\varphi_2} \mathbb{Z}/3\mathbb{Z}$, *avec* $\varphi_2(1) = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 4 \end{smallmatrix}\right) \in \mathrm{Aut}({\mathbb{F}_7}^2)$.

Démonstration. Soit G un groupe d'ordre 49. On montre facilement qu'il n'y a qu'un seul 7-Sylow d'ordre 49 que l'on appelle N. Puisque l'intersection de N avec un 3-Sylow H est réduite à 1_G, on en déduit que $NH = G$, et ainsi G est un produit semi-direct de N par H.

On écarte le cas où G est abélien. Si $N = \mathbb{Z}/49\mathbb{Z}$, tous les morphismes de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/49\mathbb{Z}) \cong \mathbb{Z}/42\mathbb{Z}$ se déduisent les uns des autres par composition à la source par un automorphisme de $\mathbb{Z}/3\mathbb{Z}$. Donc dans ce cas, il n'existe qu'un seul produit semi-direct $\mathbb{Z}/49\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$.

Intéressons-nous au cas où $N = (\mathbb{Z}/7\mathbb{Z})^2$. Alors le produit semi-direct est déterminé par un morphisme

$$\varphi \ : \ \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(\mathbb{F}_7{}^2) \cong \mathcal{GL}(2, \mathbb{F}_7).$$

Le groupe $\mathcal{GL}(2, \mathbb{F}_7)$ est d'ordre $(7^2-1)(7^2-7) = 2^5 \times 3^2 \times 7$. Alors le groupe engendré par les matrices $A = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ et $B = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)$ est un 3-Sylow de $\mathcal{GL}(2, \mathbb{F}_7)$. Notons le H. Puisque tous les 3-Sylow de $\mathcal{GL}(2, \mathbb{F}_7)$ sont conjugués, on peut se ramener (d'après le deuxième critère de similitude de structures de produit semi-direct) à des morphismes φ de $\mathbb{Z}/3\mathbb{Z}$ dans H. Supposons qu'il existe un isomorphisme de G_1 vers G_2. Cet isomorphisme préserve l'unique 7-Sylow de chaque groupe. Alors, d'après la proposition 7.22, un tel isomorphisme est une similitude de structures de produit semi-direct. Déterminons le nombre de classes de similitude. Par composition par un automorphisme de $\mathbb{Z}/3\mathbb{Z}$, on peut se ramener aux morphismes φ de $\mathbb{Z}/3\mathbb{Z}$ dans H tel que $\varphi(1)$ soit de déterminant 1 ou 2 (application du premier critère), et dont la première valeur propre est « supérieure » ou égale à la seconde (application du deuxième critère). On obtient ainsi trois classes de similitude de structures de produit semi-direct (rappelons que nous avons écarté le cas abélien) caractérisés par $\varphi(1)$:

$$\varphi(1) \in \left\{ \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right), \ \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right), \ \left(\begin{smallmatrix} 4 & 0 \\ 0 & 2 \end{smallmatrix}\right) \right\}$$

Le premier cas correspond à la classe d'isomorphie de $(\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}) \times \mathbb{Z}/7\mathbb{Z}$. Le morphisme φ_2 correspond à $(\mathbb{Z}/7\mathbb{Z})^2 \rtimes \mathbb{Z}/3\mathbb{Z}$ avec une action isotrope. Le morphisme φ_2 correspond à $(\mathbb{Z}/7\mathbb{Z})^2 \rtimes \mathbb{Z}/3\mathbb{Z}$ avec une action non-isotrope. □

7 Extension de groupes : généralités

7.1 Suites exactes scindées et produits semi-directs

Définition 7.1 (Suites exactes, abéliennes, centrales, scindées)**.**

- Soient N, G et H trois groupes, $i \ : \ N \to G$ et $\pi \ : \ G \to H$ deux morphismes. On dira que la suite

  $$N \xrightarrow{i} G \xrightarrow{\pi} H$$

  est *exacte en* G si et seulement si $\mathrm{Im}\,(i) = \mathrm{Ker}\,(\pi)$. Par conséquent, dire que la suite

  $$1 \xrightarrow{\varepsilon} N \xrightarrow{i} G$$

  est exacte en N, où 1 est le groupe trivial[28], revient à dire que $\mathrm{Ker}\,(i) = \mathrm{Im}\,(\varepsilon) = 1$, donc que i est injectif. Et dire que la suite

  $$G \xrightarrow{\pi} H \xrightarrow{\varepsilon} 1$$

  est exacte en H revient à dire que $\mathrm{Im}\,(\pi) = \mathrm{Ker}\,(\varepsilon) = H$, donc que π est surjective.
- Dire que la suite

  $$1 \to N \xrightarrow{i} G \xrightarrow{\pi} H \to 1. \qquad (*)$$

  est *exacte* revient à dire qu'elle est exacte en N, G et H, et donc $G/N \cong H$.

[28]Le symbole 1 est remplacé par 0 lorsqu'on adopte la notation additive. Les morphismes qui arrivent à 1 ou qui partent de 1 ne sont jamais précisés, puisqu'ils sont triviaux.

- Une *extension de H par N* est la donnée d'un groupe G et de deux morphismes $i : N \to G$ et $\pi : G \to H$ tels que la suite $(*)$ soit exacte.
- L'extension est dite *abélienne* (resp. *centrale*) si N est abélien (resp. si $i(N)$ est central).
- S'il existe un morphisme $s : H \to G$ tel que $\pi \circ s = \mathrm{Id}_H$, on dira que la suite est *scindée à droite* ou simplement *scindée*. Un tel morphisme s est appelé une *section de π*. S'il existe un morphisme $\alpha : G \to N$ tel que $\alpha \circ i = \mathrm{Id}_N$, on dira que la suite est *scindée à gauche*. Un tel morphisme α est appelé une *anti-section de i*.
- L'extension donné par la suite exacte $(*)$ sera dite *triviale* si G est isomorphe à $N \times H$.

Définition 7.2 (Extensions équivalentes)**.**
Deux extensions $N \xrightarrow{i} G \xrightarrow{\pi} H$ et $N \xrightarrow{i'} G' \xrightarrow{\pi'} H$ seront dites *faiblement équivalentes* s'il existe trois isomorphismes α, Φ et β tels que le diagramme suivant soit commutatif.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & N & \xrightarrow{i} & G & \xrightarrow{\pi} & H & \longrightarrow & 1 \\
 & & \uparrow{\scriptstyle \alpha} & & \uparrow{\scriptstyle \Phi} & & \uparrow{\scriptstyle \beta} & & \\
1 & \longrightarrow & N & \xrightarrow[i']{} & G' & \xrightarrow[\pi']{} & H & \longrightarrow & 1
\end{array}$$

Un tel isomorphisme Φ est appelé une *équivalence faible d'extensions*.

Deux extensions $N \xrightarrow{i} G \xrightarrow{\pi} H$ et $N \xrightarrow{i'} G' \xrightarrow{\pi'} H$ seront dites *fortement équivalentes* ou simplement *équivalentes* s'il existe un morphisme Φ (le caractère bijectif est imposé par les deux suites exactes et la commutativité du diagramme[29]) tel que le diagramme suivant soit commutatif.

$$\begin{array}{ccccccc}
 & & & & G & & & & \\
 & & & \nearrow^{i''} & \uparrow & \searrow^{\pi} & & & \\
1 & \longrightarrow & N & & \Phi & & H & \longrightarrow & 1 \\
 & & & \searrow_{i'} & \downarrow & \nearrow_{\pi''} & & & \\
 & & & & G' & & & &
\end{array}$$

Un tel isomorphisme Φ est appelé une *équivalence d'extensions*.

Remarque. Il n'y a pas de différences profondes entre équivalences fortes et faibles, mais parce qu'elles sont plus simples à manipuler, nous utiliseront essentiellement des équivalences fortes.

[29] Ce résultat est parfois connu sous le nom de « lemme des cinq ».

Lemme 7.3 (Caractérisation des équivalences faibles d'extensions parmi les isomorphismes)**.**
Soient $N \xrightarrow{i} G \xrightarrow{\pi} H$ *et* $N \xrightarrow{i'} G' \xrightarrow{\pi'} H$ *deux extensions et* $\Phi : G' \to G$ *un isomorphisme de groupes. Les propositions suivantes sont équivalentes :*

(i) Φ *est une équivalence faible d'extensions,*

(ii) il existe $\alpha \in \mathrm{Aut}(N)$ *tel que* $\Phi\, i' = i\alpha$,

(iii) il existe $\beta \in \mathrm{Aut}(H)$ *tel que* $\pi\Phi = \beta\pi'$.

Démonstration. Par définition, (i) est équivalent à la réunion de (ii) et (iii). Il nous suffit donc de montrer que (ii) et (iii) sont équivalents.

Montrons (ii) $\Rightarrow$ *(iii).* Si $\Phi\, i' = i\alpha$, alors $\pi\Phi\, i' = \pi\, i\alpha = 0$, donc $\mathrm{Im}\,(i') \subset \mathrm{Ker}\,(\pi\Phi)$. Or $\mathrm{Im}\,(i') = \mathrm{Ker}\,(\pi')$ et $\mathrm{Ker}\,(\pi\Phi) = \Phi^{-1}(\mathrm{Ker}\,(\pi))$. Donc :

$$\mathrm{Ker}\,(\pi') \subset \Phi^{-1}(\mathrm{Ker}\,(\pi)).$$

En partant de $i'\alpha^{-1} = \Phi^{-1}i$ et en procédant de même, on aurait montré l'inclusion réciproque. Donc :

$$\mathrm{Ker}\,(\pi') = \Phi^{-1}(\mathrm{Ker}\,(\pi)).$$

Or on a deux isomorphismes induits par π et π' allant respectivement de $G/\mathrm{Ker}\,(\pi)$ dans H et de $G'/\mathrm{Ker}\,(\pi')$ dans H. L'égalité ci-dessus dit seulement que Φ passe au quotient et induit un isomorphisme de $G/\mathrm{Ker}\,(\pi)$ dans $G'/\mathrm{Ker}\,(\pi')$. Donc il existe un automorphisme β de H (obtenu comme la composée des trois précédents) tel que $\pi\Phi = \beta\pi'$.

Montrons (iii) $\Rightarrow$ *(ii).* Si $\pi\Phi = \beta\pi'$, alors $\pi\Phi\, i' = \beta\, i\alpha = 0$, donc $\mathrm{Im}\,(\Phi\, i') \subset \mathrm{Ker}\,(\pi)$. Or $\mathrm{Ker}\,(\pi) = \mathrm{Im}\,(i)$ et $\mathrm{Im}\,(\Phi\, i') = \Phi(\mathrm{Im}\,(i'))$. Donc :

$$\mathrm{Im}\,(i) \subset \Phi(\mathrm{Im}\,(i')).$$

En partant de $\beta^{-1}\pi = \pi'\Phi^{-1}$ et en procédant de même, on aurait montré l'inclusion réciproque. Donc :

$$\mathrm{Im}\,(i) = \Phi(\mathrm{Im}\,(i')).$$

Or on a deux isomorphismes induits par i et i' allant respectivement de N dans $\mathrm{Im}\,(i')$ et de N dans $\mathrm{Im}\,(i')$. D'après l'égalité, Φ induit un isomorphisme de $\mathrm{Im}\,(i')$ dans $\mathrm{Im}\,(i)$. Donc il existe un automorphisme α de N (obtenu comme la composée des trois précédents) tel que $\Phi i' = i\alpha$. □

Corollaire 7.4 (Caractérisation des équivalences fortes d'extensions parmi les isomorphismes)**.**
Soient $N \xrightarrow{i} G \xrightarrow{\pi} H$ *et* $N \xrightarrow{i'} G' \xrightarrow{\pi'} H$ *deux extensions et* $\Phi : G' \to G$ *un isomorphisme de groupes. Les propositions suivantes sont équivalentes :*

(i) Φ *est une équivalence faible d'extensions,*

(ii) $\Phi\, i' = i$,

(iii) $\pi\Phi = \pi'$. □

Lemme 7.5 (Propriétés des extensions invariantes par équivalence)**.**
Dans le diagramme de la définition 7.2 ci-dessus traduisant une équivalence d'extensions,

(i) le morphisme π admet une section si et seulement si π' en admet une ;
(ii) de même, i admet une anti-section si et seulement si i' en admet une ;
(iii) enfin, l'une des deux extensions est centrale si et seulement si l'autre l'est.

Démonstration.
(i) Soit s une section de π. Alors Φs est une section de π' puisque pour tout $h \in H$, on a :

$$\pi' \Phi s(h) = \pi s(h) = h.$$

(ii) De même, si α est une anti-section de i, alors $\alpha \circ \Phi^{-1}$ est une anti-section de i' puisque pour tout $n \in N$, on a :

$$\alpha \Phi^{-1} i'(n) = \alpha i(n) = n.$$

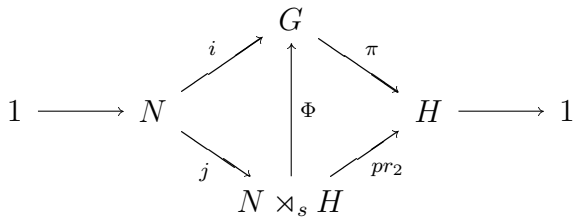
(iii) Si $i(N)$ est central dans G, alors $\Phi i(N)$ est central dans $\Phi(G) = G'$, donc $i'(N)$ est central dans G'. □

Proposition 7.6 (Caractérisation du produit semi-direct)**.**
Soit l'extension $(*)$ suivante : $1 \to N \xrightarrow{i} G \xrightarrow{\pi} H \to 1$.

(i) Si l'extension $(*)$ est scindée par une section s de π, alors :
- *on a une action de H sur N de morphisme structurel*
$$\widetilde{\mathrm{Ad}}_s : \begin{array}{ccc} H & \longrightarrow & \mathrm{Aut}(N) \\ h & \longmapsto & \{\, n \mapsto i^{-1}(s(h)i(n)s(h)^{-1}) \,\} \end{array} ;$$
- *cette action permet de définir un produit semi-direct $N \rtimes_s H$;*
- *les extensions $(*)$ et $N \xrightarrow{can.} N \rtimes_s H \xrightarrow{can.} H$ sont équivalentes.*

(ii) Réciproquement, s'il existe $\varphi \in \mathrm{Hom}(H, \mathrm{Aut}(N))$ tel que les extensions $(*)$ et $N \xrightarrow{can.} N \rtimes_\varphi H \xrightarrow{can.} H$ sont équivalentes, alors l'extension $(*)$ est scindée.

Démonstration. La partie (ii) est une application directe du lemme 7.5. Concentrons-nous sur la partie (i). Puisque N est un noyau, N est distingué, donc les automorphismes intérieurs de G stabilisent N et par restriction définissent des automorphismes de N. Ainsi, Ad_s induit par restriction un morphisme de H dans $\mathrm{Aut}(N)$. On construit alors le diagramme suivant



où :
- $N \rtimes_s H$ est le produit semi-direct induit par Ad_s,
- $j : N \to N \rtimes_s H$, $n \mapsto (n, 1_H)$ est un morphisme injectif,
- $pr_2 : N \rtimes_s H \to H$, $(n, h) \mapsto h$ est un morphisme surjectif,
- $\Phi : N \rtimes H \to G$, $(n, h) \mapsto i(n)s(h)$ est un morphisme,
- les deux « lignes » sont exactes.

Le diagramme est commutatif puisque $\Phi \circ j = i$ et

$$\pi \circ \Phi(n,h) = \pi(i(n)s(h)) = \pi \circ s(h) = h = pr_2(n,h).$$

L'application α : $\begin{array}{ccc} G & \longrightarrow & N \\ g & \longmapsto & i^{-1}\big(g\big(s\circ\pi(g)\big)^{-1}\big) \end{array}$ vérifie $\alpha \circ i(n) = n$ pour $n \in N$. Mieux :

$$\begin{aligned} \alpha\big(i(n)s(h)\big) &= i^{-1}\big(i(n)s(h).\big(s\circ\pi(i(n)s(h))\big)^{-1}\big) \\ &= i^{-1}\big(i(n)s(h)\big(s\pi s(h)\big)\big)^{-1} \\ &= n. \end{aligned}$$

Remarquons que α n'est pas un morphisme : pour tous $n, n' \in N$ et $h, h' \in H$, on a :

$$\begin{aligned} \alpha(i(n)s(h)i(n')s(h')) &= \alpha(i(n)s(h)i(n')s(h^{-1}hh')) \\ &= \alpha(i(n)i(\mathrm{Ad}_{s(h)}(n'))s(hh')) \\ &= n\mathrm{Ad}_{s(h)}(n'). \end{aligned}$$

Pour tout $g \in G$, posons Ψ : $\begin{array}{ccc} G & \longrightarrow & N \rtimes_s H \\ g & \longmapsto & (\alpha(g),\, \pi(g)) \end{array}$.

Alors, pour tous $n \in N$ et $h \in H$, on a $\Psi(i(n)s(h)) = (n,h)$. Donc Ψ est une application réciproque de Φ, donc c'est le morphisme réciproque de Φ et Φ est un isomorphisme. On peut aussi voir directement que Ψ est un morphisme, puisque pour tous $n, n' \in N$ et $h, h' \in H$, on a :

$$\begin{aligned} \Psi(i(n)s(h)i(n')s(h')) &= (n\mathrm{Ad}_{s(h)}(n'),\, hh') \\ &= (n,\, h)(n',\, h') \\ &= \Psi(i(n)s(h))\Psi(i(n')s(h')). \end{aligned}$$

□

Remarques.

1. On voit que l'existence d'une section s de π n'implique pas l'existence d'une anti-section de i, puisque c'est α dans la dernière démonstration qui aurait dû jouer ce rôle, mais α n'était pas un morphisme. D'après le lemme suivant, α est un morphisme si et seulement si $G = N \times H$.

2. Dans la partie (ii), le fait que G soit isomorphe à $N \rtimes_\varphi H$ ne suffit pas pour que l'extension soit scindée : il faut en outre qu'on ait une equivalence d'extensions entre G et $N \rtimes_\varphi H$. Voici un exemple.

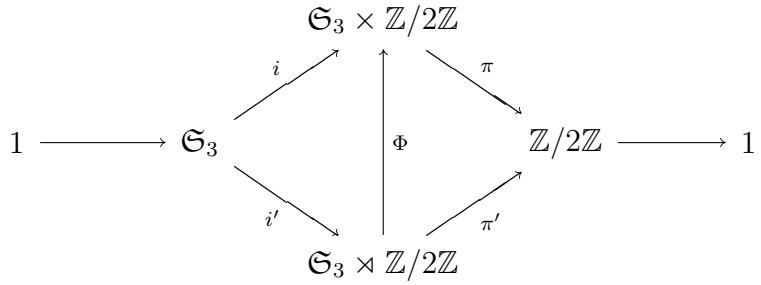
Le centre $\mathcal{Z}(\mathcal{T}_{3,p})$ du groupe $\mathcal{T}_{3,p}$ n'est pas trivial car $\mathcal{T}_{3,p}$ est un p-groupe, mais ne peut pas être d'ordre p^2, car le quotient serait cyclique, donc le groupe serait abélien d'après le lemme 6.1. Donc $\mathcal{Z}(\mathcal{T}_{3,p})$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Le quotient de $\mathcal{T}_{3,p}$ par son centre est $(\mathbb{Z}/p\mathbb{Z})^2$, puisque les éléments non triviaux de $\mathcal{T}_{3,p}$ sont d'ordre p. Donc $\mathcal{T}_{3,p}$ une extension centrale de $(\mathbb{Z}/p\mathbb{Z})^2$ par $\mathbb{Z}/p\mathbb{Z}$. Soit $G = \mathcal{T}_{3,p} \times \mathbb{Z}/p\mathbb{Z}$. Alors G est l'extension centrale suivante :

$$1 \to (\mathbb{Z}/p\mathbb{Z})^2 \to G \to (\mathbb{Z}/p\mathbb{Z})^2 \to 1.$$

Si cette extension était scindée, puisqu'elle est centrale, le groupe G serait abélien. Pourtant, $\mathcal{T}_{3,p}$ est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/p\mathbb{Z}$, donc le groupe G est isomorphe à $\big((\mathbb{Z}/p\mathbb{Z})^2 \times \mathbb{Z}/p\mathbb{Z}\big) \times \mathbb{Z}/p\mathbb{Z}$, lui-même isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes (\mathbb{Z}/p\mathbb{Z})^2$.

Finalement, G est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes (\mathbb{Z}/p\mathbb{Z})^2$, mais l'extension centrale G considérée au début n'est pas équivalente à l'extension scindée $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes (\mathbb{Z}/p\mathbb{Z})^2$.

3. Si deux structures de produits semi-directs les mêmes, alors les extensions associées sont équivalentes. La réciproque est fausse. Appuyons-nous sur l'exemple du lemme 3.19. On a une équivalence d'extensions :



où les morphismes i, i', π et π' sont les morphismes canoniques et où Φ est donné par :

$$\Phi(\sigma,\, 0) = (\sigma, 0) \text{ et } \Phi(\sigma,\, 1) = (\sigma\tau, 1)$$

pour tout $\sigma \in \mathfrak{S}_3$, où τ est l'unique transposition de $\mathfrak{S}_3$ telle que les conjugaisons par $(1, 1)$ et par $(\tau,\, 0)$ dans $\mathfrak{S}_3 \rtimes \mathbb{Z}/2\mathbb{Z}$ coïncident. La proposition suivante précise ce qu'il manque à une équivalence d'extensions pour devenir une similitude de structures de produit semi-direct.

Proposition 7.7 (Caractérisation des similitudes de structure de produit semi-direct parmi les équivalences d'extensions)**.**
Soient $N \xrightarrow{i} G \xrightarrow{\pi} H$ et $N \xrightarrow{i'} G' \xrightarrow{\pi'} H$ deux extensions scindées par deux sections respectivement s et s', et soit Φ une équivalences d'extensions de G' vers G. Alors les assertions suivantes sont équivalentes :

(i) Φ est une similitude de structures de produit semi-direct,

(ii) $s = \Phi s'$ (à un automorphisme de H près).

Démonstration. Puisque Φ est une équivalence d'extensions, elle vérifie $\Phi\, i' = i$ (à un automorphisme de N près) d'après le lemme 7.4. Alors précisément, la condition manquante pour être une similitude de structures de produit semi-direct est la condition (ii). □

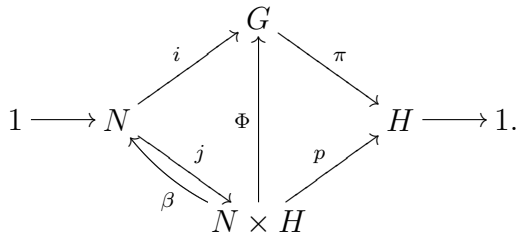
Proposition 7.8 (Caractérisation des extensions triviales)**.**
Les extensions $N \xrightarrow{i} G \xrightarrow{\pi} H$ et $N \xrightarrow{can.} N \times H \xrightarrow{can.} H$ sont équivalentes si et seulement si la suite exacte

$$1 \to N \xrightarrow{i} G \xrightarrow{\pi} H \to 1$$

est scindée à gauche (i.e. il existe une anti-section α de i).

Démonstration.

Montrons le sens direct. On part de l'équivalence d'extensions suivante où j et p sont les morphismes canoniques.



Puisque j admet une anti-section β évidente, d'après le lemme 7.5, il existe une anti-section α de i définie par $\alpha = \beta\Phi^{-1}$.

Montrons le sens retour. Partons d'une anti-section α de i, dans la suite exacte (*). Soit $g \in \mathrm{Ker}\,(\alpha)$ et $n \in N$ tel que $i(n) = g$. Alors $n = \alpha i(n) = \alpha(g) = 1_N$, donc

$$\mathrm{Ker}\,(\alpha) \cap \mathrm{Im}\,(i) = \{1_G\},$$

donc $\mathrm{Ker}\,(\alpha) \cap \mathrm{Ker}\,(\pi) = \{1_G\}$. Donc π restreint à $\mathrm{Ker}\,(\alpha)$ est un isomorphisme. Vérifions que cet isomorphisme est surjectif sur H. Pour tout $h \in H$, il existe $g \in G$ tel que $\pi(g) = h$. Alors $\pi(g.i\alpha(g)^{-1}) = \pi(g)\pi i(\alpha(g)^{-1}) = \pi(g) = h$. Par ailleurs, $\alpha(g.i\alpha(g)^{-1}) = \alpha(g)\alpha i\alpha(g)^{-1} = 1_N$. Finalement, $\mathrm{Im}\,(\pi) \subset \pi(\mathrm{Ker}\,(\alpha))$. Ainsi, la restriction de π à $\mathrm{Ker}\,(\alpha)$ possède un inverse que l'on appelle s, qui est une section de π, et qui vérifie :

$$\mathrm{Im}\,(s) = \mathrm{Ker}\,(\alpha).$$

Alors G est le produit semi-direct interne $i(N) \rtimes s(H)$, et puisque $s(H)$ est un noyau, $s(H)$ est distingué dans G, donc G est le produit direct interne $i(N) \times s(H)$. □

Exemples.

1. Pour tout groupe G, notons $\mathcal{Z}_G$ son centre et $\mathrm{Int}(G)$ le groupe d'automorphismes intérieurs de G. Alors on a la suite exacte centrale où i est l'inclusion et Ad envoie un élément g sur la conjugaison par g :

$$1 \to \mathcal{Z}_G \xrightarrow{i} G \xrightarrow{\mathrm{Ad}} \mathrm{Int}(G) \to 1.$$

Puisque la suite exacte est centrale, elle n'est scindée que si G est le produit direct de son centre par un sous-groupe, d'après la proposition 7.8.

2. Attention, même si l'extension $N \hookrightarrow G \twoheadrightarrow H$ n'est pas scindée, G peut être malgré tout un produit semi-direct. Voici un exemple.

Soient G et H le groupe et le sous-groupe suivants.

$$G = \langle\, x,\, y \mid xy = yx, x^4 = 1, y^2 = 1 \,\rangle \;\cong\; \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$
$$N = \langle x^2, y \rangle_G \;\cong\; \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \;\triangleleft\; G.$$

On a la suite exacte :

$$1 \to \underbrace{N}_{(\mathbb{Z}/2\mathbb{Z})^2} \to \underbrace{G}_{\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}} \to \underbrace{G/N}_{\mathbb{Z}/2\mathbb{Z}} \to 1. \qquad (*)$$

Le groupe G est une extension de H par N. Pourtant, G n'est pas un produit semi-direct de N par G/N. En effet, s'il l'était, puisque $N \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, on aurait $G \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$. Puisque G est commutatif, le produit serait direct et finalement, G serait isomorphe à $(\mathbb{Z}/2\mathbb{Z})^3$.

7.2 Extensions de H par N et $\mathrm{Hom}(H, \mathrm{Out}(N))$

Définition 7.9.
Notons :
- $E(H, N)$ l'ensemble des extensions de H par N,
- $E_s(H, N)$ l'ensemble des extensions scindées de H par N,
- $\mathcal{E}(H, N)$ l'ensemble des classes d'équivalences des extensions de H par N,
- $\mathcal{E}_s(H, N)$ l'ensemble des classes d'équivalences des extensions de H par N.

Définition 7.10 (Groupe d'automorphismes extérieurs)**.**
Etant donné un groupe G, on note $\mathrm{Aut}(G)$ le groupe de ses automorphismes et $\mathrm{Int}(G)$ le groupe de ses automorphismes intérieurs. Remarquons que $\mathrm{Int}(G)$ est distingué dans $\mathrm{Aut}(G)$. Le groupe quotient est noté $\mathrm{Out}(G)$ et est appelé *le groupe des automorphismes extérieurs*. Par ailleurs, un automorphisme de $\mathrm{Aut}(G)$ est dit *extérieur* s'il n'est pas intérieur.

Exemples.
1. Par exemple, pour tout $n \neq 6$, $\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n)$, donc $\mathrm{Out}(\mathfrak{S}_n) = \{1\}$. Pour $n = 6$, on a $\mathrm{Out}(\mathfrak{S}_6) = \mathbb{Z}/2\mathbb{Z}$. Les automorphismes extérieurs de $\mathfrak{S}_6$ envoient les transpositions sur des produits de trois transpositions à support disjoint. Précisons que certains de ces automorphismes extérieurs sont des involutions. Autrement dit, $\mathrm{Out}(\mathfrak{S}_6)$ se relève dans $\mathrm{Aut}(\mathfrak{S}_6)$.

2. A l'inverse, dans un groupe abélien A, $\mathrm{Int}(A) = \{1\}$, donc $\mathrm{Aut}(A) = \mathrm{Out}(A)$: tous les automorphismes sont extérieurs.

Remarques.
1. On a une suite exacte faisant intervenir $\mathrm{Out}(G)$:
$$1 \to \mathcal{Z}_G \xrightarrow{incl.} G \xrightarrow{\mathrm{Ad}} \mathrm{Aut}(G) \xrightarrow{quot.} \mathrm{Out}(G) \to 1$$
dans laquelle toutes les flèches sont canoniques (l'inclusion, la conjugaison par un élément, le passage au quotient). Cette suite exacte provient de deux suites courtes exactes :
$$1 \to \mathcal{Z}_G \xrightarrow{incl.} G \xrightarrow{\mathrm{Ad}} \mathrm{Int}(G) \to 1,$$
$$1 \to \mathrm{Int}(G) \xrightarrow{incl.} \mathrm{Aut}(G) \xrightarrow{quot.} \mathrm{Out}(G) \to 1.$$
En général, aucune de ces deux suites exactes n'est scindée.

2. Remarquons que l'on a un morphisme canonique de $\mathrm{Hom}(H, \mathrm{Aut}(G))$ dans $\mathrm{Hom}(H, \mathrm{Out}(G))$ de noyau $\mathrm{Hom}(H, \mathrm{Int}(G))$, donc on a un morphisme injectif canonique :
$$\frac{\mathrm{Hom}(H, \mathrm{Aut}(G))}{\mathrm{Hom}(H, \mathrm{Int}(G))} \hookrightarrow \mathrm{Hom}(H, \mathrm{Out}(G)).$$
S'il existe une section du morphisme $\mathrm{Aut}(G) \to \mathrm{Out}(G)$, alors le morphisme ci-dessus est un isomorphisme. Mais s'il n'en existe pas, ce morphisme n'est pas toujours surjectif (prendre $H \cong \mathrm{Out}(G)$).

Définition 7.11 (Pseudo-sections)**.**
Etant donnée la suite exacte,

$$1 \to N \xrightarrow{i} G \xrightarrow{\pi} H \to 1, \qquad (*)$$

une pseudo-section de π est une application ensembliste $\tilde{s} \ : \ H \to G$, $h \mapsto \tilde{h}$ telle que $\pi(\tilde{h}) = h$, i.e. $\pi \circ s = \mathrm{Id}_H$.

Définition 7.12 (Extensions et morphismes d'action extérieure)**.**
Il existe une application canonique :

$$\theta \ : \ E(H,\, N) \to \mathrm{Hom}(H,\, \mathrm{Out}(N))$$

définie ainsi. A toute extension $N \xrightarrow{i} G \xrightarrow{\pi} H$, on associe le morphisme :

$$\widetilde{\mathrm{Ad}} \ : \ \begin{array}{ccc} G & \longrightarrow & \mathrm{Aut}(N) \\ g & \longmapsto & \widetilde{\mathrm{Ad}}_g \ : \ n \mapsto i^{-1}(gi(n)g^{-1}) \end{array} .$$

Soit $pr \ : \ \mathrm{Aut}(N) \to \mathrm{Out}(N)$ le morphisme canonique. La composition $pr\,\widetilde{\mathrm{Ad}}$ passe au quotient sous $i(N)$ et induit via π un morphisme $\widehat{\mathrm{Ad}}$ de G dans $\mathrm{Out}(N)$. L'application $\widetilde{\mathrm{Ad}}$ est la seule qui fait commuter le diagramme suivant :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \xrightarrow{i} & G & \xrightarrow{\pi} & H & \longrightarrow & 1 \\ & & \Big\downarrow{\scriptstyle =} & & \Big\downarrow{\scriptstyle \widetilde{\mathrm{Ad}}} & & \Big\downarrow{\scriptstyle \widehat{\mathrm{Ad}}} & & \\ & & N & \xrightarrow[\mathrm{Ad}]{} & \mathrm{Aut}(N) & \xrightarrow[pr]{} & \mathrm{Out}(N) & \longrightarrow & 1 \end{array}$$

Le morphisme θ associe à l'extension $N \xrightarrow{i} G \xrightarrow{\pi} H$ le morphisme $\widehat{\mathrm{Ad}}$. On dira que $\widehat{\mathrm{Ad}}$ est **le morphisme d'action extérieure** de l'extension.

Remarques.

1. L'application θ envoie toute extension scindée par une section s sur Ad_s, conformément à la proposition 7.6. Dans ce cas, θ est surjective, puisque toujours d'après la proposition 7.6, $E_s(H,\, N)$ est en bijection canonique avec $\mathrm{Hom}(H,\, \mathrm{Aut}(N))$. Dans la proposition suivante, on calcule le noyau de la restriction de θ à $E_s(H,\, N)$.

2. Le fait que la seconde ligne ne soit pas exacte à gauche, en raison du centre éventuellement non trivial de G, est un sérieux problème à la classification des extensions éventuellement non scindées. Cela dit, lorsque le centre de G est trivial, les choses se passent bien comme on le verra au paragraphe suivant.

Proposition 7.13 (Extensions scindées équivalentes et $\mathrm{Hom}(H,\, \mathrm{Out}(N))$)**.**
Soient $N \to N \rtimes_\varphi H \to H$ et $N \to N \rtimes_\psi H \to H$ deux extensions scindées. Elles sont équivalentes si et seulement si :

$$\psi^{-1}\varphi \in \mathrm{Hom}(H,\, \mathrm{Int}(N)).$$

Démonstration. Considérons deux extensions de H par N, toutes deux scindées, dont les actions respectives sont données par deux morphismes φ et ϕ de H dans $\mathrm{Aut}(N)$, et coïncidant dans $\mathrm{Out}(N)$. Alors, pour tout $h \in H$, soit un élément $n_h \in N$ tel que

$$\psi_h = \mathrm{Ad}_{n_h} \circ \varphi_h.$$

Puisque ψ, Ad et φ sont des morphismes, il doit exister une relation entre n_h, $n_{h'}$ et $n_{hh'}$. D'une part on a $\psi_{hh'} = \mathrm{Ad}_{n_{hh'}} \psi_{hh'}$, d'autre part on a :

$$\begin{aligned} \psi_{hh'} &= \psi_h \psi_{h'} \\ &= \mathrm{Ad}_{n_h} \varphi_h \mathrm{Ad}_{n_{h'}} \varphi_{h'} \\ &= \mathrm{Ad}_{n_h} \mathrm{Ad}_{\varphi_h(n_{h'})} \varphi_h \varphi_{h'} \\ &= \mathrm{Ad}_{n_h \varphi_h(n_{h'})} \varphi_{hh'}, \end{aligned}$$

d'où :

$$n_{hh'} = n_h \, \varphi_h(n_{h'}).$$

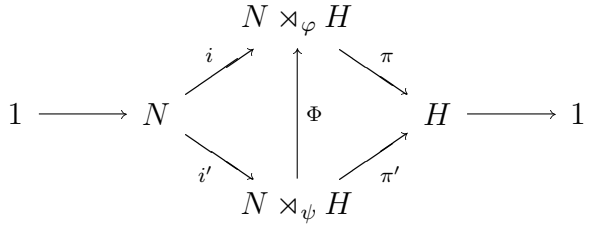
Ceci étant, posons

$$\Phi : \begin{array}{ccc} N \rtimes_\phi H & \longrightarrow & N \rtimes_\varphi H \\ (n,\, h) & \longmapsto & (n n_h,\, h) \end{array},$$

et vérifions que Φ ainsi défini est bien un morphisme :

$$\begin{aligned} \Phi(n,\, h)\, \Phi(n',\, h') &= (n\, n_h,\, h), (n'\, n_{h'},\, h') \\ &= \big(n\, n_h \varphi_h(n'\, n_{h'}),\, hh'\big) \\ &= \big(n\, n_h \varphi_h(n') \varphi_h(n_{h'}),\, hh'\big) \\ &= \big(n\, \psi_h(n') n_h \varphi_h(n_{h'}),\, hh'\big) \\ &= \big(n\, \psi_h(n') n_{hh'}),\, hh'\big) \\ &= \Phi\big(n\, \psi_h(n')),\, hh'\big) \\ &= \Phi\big((n\, h)\, (n',\, h')\big). \end{aligned}$$

Par ailleurs, il est clair que le diagramme suivant commute.



Ainsi, les deux extensions sont équivalentes.

Réciproquement, partons de deux extensions scindées $N \rtimes_\varphi H$ et $N \rtimes_\psi H$ équivalentes, comme sur le diagramme ci-dessus. Appelons s la section de π telle que $\mathrm{Ad}_s = \varphi$, et s' la section de π' telle que $\mathrm{Ad}_{s'} = \psi$. Soit $n \in N$ et $h \in H$. Alors,

$$\psi_{h^{-1}} \varphi_h(s) \;=\; i'^{-1}\big(\, s'(h^{-1}) i' i^{-1}\big(\, s(h) i(n) s(h^{-1})\,\big) s'(h)\,\big).$$

Or $s(h) i(n) s(h^{-1}) \in i(N)$, or $i' i^{-1}$ coïncide avec Φ^{-1} sur $i(N)$, donc on obtient :

$$\begin{aligned} \big(\psi_h\big)^{-1} \varphi_h(n) &= \psi_{h^{-1}} \varphi_h(n) \\ &= i'^{-1}\big(\, s'(h^{-1}) \Phi^{-1}\big(\, s(h) i(n) s(h^{-1})\,\big) s'(h)\,\big) \\ &= i'^{-1}\big(\, s'(h^{-1}) \Phi^{-1} s(h) \Phi^{-1} i(n) \Phi^{-1} s(h^{-1}) s'(h)\,\big) \\ &= i'^{-1}\big(\, s'(h^{-1}) \Phi^{-1} s(h) i'(n) \Phi^{-1} s(h^{-1}) s'(h)\,\big) \\ &= i'^{-1}\big(\, g i'(n) g^{-1}\,\big) \end{aligned} .$$

où :

$$g = s'(h^{-1}) \Phi^{-1} s(h).$$

Il s'agit de montrer que l'élément g de $N \rtimes_\psi H$ appartient en fait à $i'(N)$. Or on tire des relations $\pi s = \mathrm{Id}_H$ et $\pi\Phi = \pi'$ l'égalité :

$$\pi'\Phi^{-1}s = \mathrm{Id}_H$$

donc :

$$\begin{aligned} \pi'(g) &= \pi'\big(s'(h^{-1})\Phi^{-1}s(h)\big) \\ &= \pi's'(h^{-1})\,\pi'\Phi^{-1}s(h) \\ &= \underbrace{\pi's'(h^{-1})}_{h^{-1}}\,h \;=\; 1_H. \end{aligned}$$

Finalement, $\pi'(g) = 1_H$, donc $g \in i'(N)$, donc $\psi_{h^{-1}}\varphi_h(n)$ est une conjugaison dans N de n. Donc $\psi^{-1}\varphi$ est un morphisme de H dans $\mathrm{Int}(N)$. □

Récapitulons les résultats de ce paragraphe (définition 7.12 et proposition 7.15).

Théorème 7.14 (Liens entre $\mathcal{E}_s(H,\,N)$ et $\mathrm{Hom}(H,\,\mathrm{Out}(N))$, cas général)**.**
On a le diagramme commutatif suivant,

$$\begin{array}{ccc} \mathcal{E}(H,\,N) & \xrightarrow{\;\Theta\;} & \mathrm{Hom}(H,\,\mathrm{Out}(N)) \\ \uparrow{\scriptstyle incl.} & & \uparrow{\scriptstyle can.} \\ \mathcal{E}_s(H,\,N) & \xrightarrow{\;\approx\;} & \dfrac{\mathrm{Hom}(H,\,\mathrm{Aut}(G))}{\mathrm{Hom}(H,\,\mathrm{Int}(G))} \end{array}$$

où Θ est l'application induite par θ (cf. définition 7.12). □

Corollaire 7.15 (Produits semi-directs isomorphes à des produits triviaux)**.**

(i) Si $\mathrm{Hom}(H,\,\mathrm{Out}(N))$ *est trivial, tout produit semi-direct de N par H est isomorphe au produit direct de N par H.*

(ii) Un produit semi-direct $N \rtimes_\varphi H$ est trivial si et seulement si $\varphi \in \mathrm{Hom}(H,\,\mathrm{Int}(N))$.

□

Exemples.

1. Ceci éclaire d'un jour nouveau le lemme 3.19 dans lequel on montrait que tout produit semi-direct de $\mathfrak{S}_3$ par $\mathbb{Z}/2\mathbb{Z}$ formait une extension équivalente au produit direct de $\mathfrak{S}_3$ par $\mathbb{Z}/2\mathbb{Z}$. Cela venait tout simplement du fait que $\mathrm{Out}(\mathfrak{S}_3) = \{1\}$.

2. De façon générale, tout produit semi-direct de $\mathfrak{S}_n$, $n \neq 6$, par un groupe est isomorphe au produit direct de $\mathfrak{S}_n$ par ce groupe. Dans le cas $n = 6$, il existe un unique produit semi-direct $\mathfrak{S}_6 \rtimes \mathbb{Z}/2\mathbb{Z}$ non isomorphe à $\mathfrak{S}_6 \times \mathbb{Z}/2\mathbb{Z}$, car il existe dans $\mathrm{Aut}(\mathfrak{S}_6)$ une involution extérieure (autrement dit, $\mathrm{Out}(\mathfrak{S}_6)$ se relève dans $\mathrm{Aut}(\mathfrak{S}_6)$). C'est un groupe qui n'a pas de centre, et tel que l'action de $(1,1)$ par conjugaison dans ce groupe envoie les transpositions de $\mathfrak{S}_6 \times \{0\}$ sur les produits de trois transpositions à supports disjoints.

7.3 Extensions de H par N où N est de centre trivial.

Proposition 7.16 (Extensions par des groupes de centres triviaux, 1)**.**
Soit N un groupe dont le centre est trivial. L'application $\theta : E(G, N) \to \mathrm{Hom}(G, \mathrm{Out}(N))$ induit la bijection

$$\Theta : \mathcal{E}(G, N) \xrightarrow{\approx} \mathrm{Hom}(G, \mathrm{Out}(N)).$$

Le lemme suivant nous sera utile pour la preuve de la proposition 7.16.

Lemme 7.17 (Tiré en arrière d'une extension)**.**
Soit $N \xrightarrow{i} G \xrightarrow{\pi} H$ une extension et α un morphisme d'un groupe H' dans H. Alors, il existe une extension $N \to G' \to H'$ rendant le diagramme suivant commutatif, et l'ensemble de toutes ces extensions constitue une classe d'équivalence d'extensions de H' par N.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \xrightarrow{i} & G & \xrightarrow{\pi} & H & \longrightarrow & 1 \\ & & \| & & \uparrow & & \uparrow{\scriptstyle \alpha} & & \\ 1 & \longrightarrow & N & \longrightarrow & G' & \longrightarrow & H' & \longrightarrow & 1 \end{array}$$

Une telle extension $N \to G' \to H'$ sera appelée un tiré en arrière de G via α.

Démonstration. Soit G' le produit de G et H' fibré par H via π et α, i.g. :

$$G' = G \times_G G' = \big\{(g, h') \in G \times H' \mid \pi(g) = \alpha(h')\big\},$$

muni de la loi :

$$(g_1, h'_1)(g_2, h'_2) = (g_1 g_2, h'_1 h'_2).$$

Soient alors :

$$\pi' : \begin{array}{ccc} G' & \longrightarrow & H' \\ (g, h') & \longmapsto & h' \end{array}, \quad i' : \begin{array}{ccc} N & \longrightarrow & G' \\ n & \longmapsto & (i(n), 1_H) \end{array}, \quad \beta : \begin{array}{ccc} G' & \longrightarrow & G \\ (g, h') & \longmapsto & g \end{array}.$$

On vérifie l'exactitude en G' :

$$\begin{array}{rcl} \mathrm{Ker}\,(\pi') & = & \big\{(g, h') \,|\, h' = 1\big\} \\ & = & \big\{(g, 1_{H'}) \,|\, \pi(g) = 1_H\big\} \\ & = & \big\{(g, 1_{H'}) \,|\, \exists n \in N,\, g = i(n)\big\} \\ & = & i'(N) \end{array}.$$

Il est alors facile de voir que le diagramme suivant est commutatif.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \xrightarrow{i} & G & \xrightarrow{\pi} & H & \longrightarrow & 1 \\ & & \| & & \uparrow{\scriptstyle \beta} & & \uparrow{\scriptstyle \alpha} & & \\ 1 & \longrightarrow & N & \xrightarrow[i']{} & G' & \xrightarrow[\pi']{} & H' & \longrightarrow & 1 \end{array}$$

Vérifions que deux telles extensions $N \to G' \to H'$ et $N \to G'' \to H'$ sont équivalentes. On vérifie facilement que tout élément g' de G' est déterminé par le couple

$(\beta(g'), \pi'(g'))$. D'où l'isomorphisme Φ de G'' vers G' prouvant que deux telles extensions sont équivalentes.

Enfin, vérifions que si deux extensions $N \to G' \to H'$ et $N \to G'' \to H'$ sont équivalentes et si $N \to G' \to H'$ est un tiré en arrière de $N \to G \to H$ via α, alors $N \to G'' \to H'$ est un tiré en arrière via α. C'est immédiat par le diagramme commutatif ci-dessous.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & N & \xrightarrow{i} & G & \xrightarrow{\pi} & H & \longrightarrow & 1 \\
 & & \| & & \uparrow{\scriptstyle \beta} & & \uparrow{\scriptstyle \alpha} & & \\
1 & \longrightarrow & N & \longrightarrow & G' & \longrightarrow & H' & \longrightarrow & 1 \\
 & & \| & & \uparrow{\scriptstyle \Phi} & & \uparrow{\scriptstyle =} & & \\
1 & \longrightarrow & N & \longrightarrow & G'' & \longrightarrow & H' & \longrightarrow & 1
\end{array}$$

□

Démonstration de la proposition 7.16.
Nous allons démontrer que l'application $\theta : E(G, N) \to \mathrm{Hom}(G, \mathrm{Out}(N))$ (cf. la définition 7.12) est surjective lorsque N est de centre trivial, puis que deux extensions ont la même image si et seulement si elles sont équivalentes.

Soit $\alpha \in \mathrm{Hom}(G, \mathrm{Out}(N))$. On complète le diagramme suivant par un tiré en arrière de $\mathrm{Aut}(N)$ via α, comme dans le lemme 7.17.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & N & \xrightarrow{\mathrm{Ad}} & \mathrm{Aut}(N) & \xrightarrow{pr} & \mathrm{Out}(N) & \longrightarrow & 1 \\
 & & \| & & & & \uparrow{\scriptstyle \alpha} & & \\
 & & N & & & & H & &
\end{array}$$

ce qui montre que θ est surjective, car en complétant le diagramme ci-dessus, on obtient le diagramme ci-dessous, dans lequel nous allons montrer que α est bien l'action extérieure de l'extension ainsi obtenue de H par N.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & N & \xrightarrow{\mathrm{Ad}} & \mathrm{Aut}(N) & \xrightarrow{pr} & \mathrm{Out}(N) & \longrightarrow & 1 \\
 & & \| & & \uparrow{\scriptstyle \beta} & & \uparrow{\scriptstyle \alpha} & & \\
1 & \longrightarrow & N & \xrightarrow[i]{} & G & \xrightarrow[\pi]{} & H & \longrightarrow & 1
\end{array}$$

Soit $g \in G$. Par définition du produit fibré, il existe $\varphi \in \mathrm{Aut}(N)$ et $h \in H$, tel que g s'écrit sous la forme (φ, h) où $pr\varphi = \alpha(h)$. Rappelons également que par construction de β, on a $\beta(g) = \varphi$, et par construction de i, on a $i(n) = (\mathrm{Ad}_n, 1)$ pour tout $n \in N$. Montrons que $\beta = \widetilde{\mathrm{Ad}}$. Pour tout $n \in N$,

$$gi(n)g^{-1} = (\varphi, h)(\mathrm{Ad}_n, 1)(\varphi^{-1}, h^{-1}) = (\mathrm{Ad}_{\varphi(n)}, 1) = i(\varphi(n)).$$

Donc $\varphi = \widetilde{\mathrm{Ad}}_g$, or $\beta(g) = \varphi$, donc $\beta = \widetilde{\mathrm{Ad}}$. Or, par définition, $\widehat{\mathrm{Ad}}$ est le morphisme qui joue le rôle de α dans le diagramme ci-dessus lorsque $\beta = \widetilde{\mathrm{Ad}}$, donc on a montré que $\alpha = \widehat{\mathrm{Ad}}$. Autrement dit, α est bien le morphisme d'action extérieure de l'extension obtenue.

Réciproquement, toute extension $N \to G \to H$ de morphisme d'action extérieure α fait commuter le diagramme suivant, par définition.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \xrightarrow{i} & G & \xrightarrow{\pi} & H & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle \widetilde{\mathrm{Ad}}} & & \downarrow{\scriptstyle \widehat{\mathrm{Ad}}} & & \\ & & N & \xrightarrow[\mathrm{Ad}]{} & \mathrm{Aut}(N) & \xrightarrow[pr]{} & \mathrm{Out}(N) & \longrightarrow & 1 \end{array}$$

Or puisque N est de centre trivial, la suite du bas est elle aussi une suite exacte. Donc l'extension $N \to G \to H$ peut être vu comme un tiré en arrière de l'extension $N \to \mathrm{Aut}(N) \to \mathrm{Out}(N)$ par α. Or d'après le lemme 7.17, l'ensemble des tirés en arrière constitue une classe d'équivalence d'extension. Ceci achève la démonstration de la proposition 7.16. □

En rassemblant les résultats des propositions 7.15 et 7.16, on obtient le résultat suivant.

Théorème 7.18 (Liens entre $\mathcal{E}_s(H,\, N)$ et $\mathrm{Hom}(H,\, \mathrm{Out}(N))$, cas où $\mathcal{Z}_N = \{1\}$)**.**
On a le diagramme commutatif suivant,

$$\begin{array}{ccc} \mathcal{E}(H,\, N) & \xrightarrow[\Theta]{\approx} & \mathrm{Hom}(H,\, \mathrm{Out}(N)) \\ {\scriptstyle incl.}\uparrow & & \uparrow{\scriptstyle incl.} \\ \mathcal{E}_s(H,\, N) & \xrightarrow{\approx} & \dfrac{\mathrm{Hom}(H,\, \mathrm{Aut}(G))}{\mathrm{Hom}(H,\, \mathrm{Int}(G))} \end{array}$$

où Θ est l'application induite par θ (cf. définition 7.12). □

Remarques.

1. On avait vu avec la proposition 7.15 que les extensions scindées d'un groupe par un groupe symétrique étaient toujours équivalentes (en tant qu'extensions) à des produits directs (sauf dans le cas du groupe $\mathfrak{S}_6$). Avec la proposition 7.16, on voit que toutes les extensions, même a priori non scindées d'un groupe par un groupe symétrique sont équivalentes (en tant qu'extensions) à des produits directs.

2. Dans le cas où G est un groupe dont le centre n'est pas trivial, on ne peut plus appliquer le lemme 7.17. Et pour cause : dans certains cas, un morphisme de $\mathrm{Hom}(G,\, \mathrm{Out}(N))$ ne correspond à aucune extension, tandis que dans d'autres cas, un morphisme de $\mathrm{Hom}(G,\, \mathrm{Out}(N))$ peut correspondre à plusieurs classes d'équivalence d'extensions. On verra au chapitre 8 que la cohomologie des groupes en degré un et deux répond à des problèmes d'extension des groupes. Le problème d'existence ou non d'extensions correspondant à un morphisme de $\mathrm{Hom}(G,\, \mathrm{Out}(N))$ est liée à la cohomologie en degré 3 (en fait, de telles extensions existent si et seulement si un l'image d'un cocycle dépendant du morphisme choisi est nulle dans $H^3(G,\, \mathcal{Z}_N)$).

7.4 Extensions de H par A où A est abélien

On considère la suite exacte $(*)$ suivante où A est un groupe abélien noté additivement. En revanche, G et H sont des groupes quelconques notés multiplicativement.

$$0 \to A \xrightarrow{i} G \xrightarrow{\pi} H \to 1, \qquad (*)$$

La situation ici est radicalement opposée à celle du paragraphe précédent, puisque dans ce cas-là, on cherchait les extensions par des groupes de centres triviaux, alors qu'ici, nous allons nous intéresser aux les extensions par des groupes abéliens (donc des groupes dont le centre est eux-mêmes). Alors $\mathrm{Hom}(H, \mathrm{Out}(A))$ se ramène à $\mathrm{Hom}(H, \mathrm{Aut}(A))$.

Rappelons qu'au paragraphe 7.2, nous avons associé à toute extension de H par N un morphisme H dans $\mathrm{Out}(N)$ que nous avons appelé le *morphisme d'action extérieure* (cf. définition 7.12). Lorsque N est abélien, il n'y a plus lieu de quotienter par $\mathrm{Int}(A)$, donc ce morphisme s'exprime plus simplement. De plus, l'adjectif « extérieur » n'a plus lieu d'être, puisque ce morphisme devient effectivement le morphisme structurel d'une action de H sur A canoniquement associé à l'extension considérée. Nous posons donc la définition suivante.

Définition 7.19 (Morphismes d'action d'une extension abélienne)**.**

- Etant donnée une extension abélienne,
$$0 \to A \xrightarrow{i} G \xrightarrow{\pi} H \to 1. \qquad (*)$$
l'*action extérieure* (cf. définition 7.12) est une action bien définie de H sur A que l'on appellera l'**action canonique** de l'extension $(*)$.
- On appellera **morphisme d'action** de cette extension le morphisme φ suivant
$$\varphi : \begin{array}{ccc} H & \longrightarrow & \mathrm{Aut}(N) \\ h & \longmapsto & \{\, n \mapsto i^{-1}(\tilde{h} i(n) \tilde{h}^{-1}) \,\} \end{array}$$
où $\tilde{h}$ est un élément de G tel que $\pi(\tilde{h}) = h$, qui n'est rien d'autre que le morphisme structurel de l'action canonique. C'est également l'image de l'extension $(*)$ par le morphisme $\theta : E(H, A) \to \mathrm{Hom}(H, \mathrm{Aut}(A))$ (cf. définition 7.12).

Remarque. Le morphisme d'action de l'extension $A \xrightarrow{i} A \rtimes_\varphi H \xrightarrow{\pi} H$ où i et π sont les morphismes canoniques coïncide avec φ. Par contre, si i et π ne sont plus les morphismes canoniques, il n'y a plus égalité entre φ et le morphisme d'action (cependant, il existe une relation simple permettant de passer de l'un à l'autre, cf. proposition 7.22).

Proposition 7.20 (Extensions abéliennes et morphismes d'action)**.**

(i) L'application $\theta : E(H, A) \to \mathrm{Hom}(H, \mathrm{Aut}(A))$ est surjective.

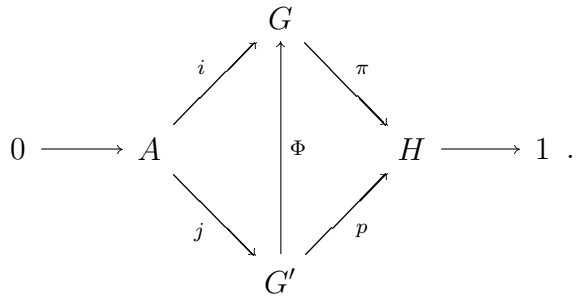
(ii) Deux extensions équivalentes ont le même morphisme d'action.

(iii) L'extension suivante de morphisme d'action φ
$$0 \to A \xrightarrow{i} G \xrightarrow{\pi} H \to 1$$
est scindée si et seulement si elle est équivalente à l'extension
$$0 \to A \xrightarrow{can.} A \rtimes_\varphi H \xrightarrow{can.} H \to 1.$$

Démonstration.

(i) Le morphisme d'action de l'extension $A \xrightarrow{can.} A \rtimes_\varphi H \xrightarrow{can.} H$ coïncide avec φ, donc θ est surjective.

(ii) Partons d'une équivalence d'extensions :



Soit $\varphi : H \to \mathrm{Aut}(A)$ le morphisme structurel de l'action canonique via G et $\varphi' : H \to \mathrm{Aut}(A)$ celui de l'action canonique via G'. On va montrer qu'elles coïncident. Soit

$$h \in H \mapsto \tilde{h} \in G$$

une pseudo-section de π. Alors,

$$h \in H \mapsto \Phi^{-1}(\tilde{h}) \in G'$$

est une pseudo-section de p, et pour tout $h \in H$ et tout $a \in A$, on a :

$$\begin{aligned} {\varphi'}_h(a) &= j^{-1}\big(\Phi^{-1}(\tilde{h})j(a)\Phi^{-1}(\tilde{h})^{-1}\big) \\ &= i^{-1}\Phi\big(\Phi^{-1}(\tilde{h})\Phi^{-1}i(a)\Phi^{-1}(\tilde{h}^{-1})\big) \\ &= i^{-1}\big(\tilde{h}i(a)\tilde{h}^{-1}\big) \\ &= \varphi_h(a) \end{aligned}$$

(iii) C'est une conséquence directe de la partie (ii) et de la proposition 7.6. □

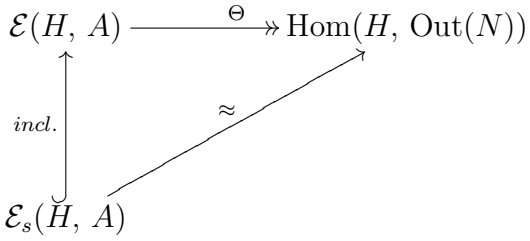
Remarques.

1. Deux extensions abéliennes de H par A équivalentes définissent une même action de H sur A. Changer les pseudo-sections (ou les sections quand il y en a) ne modifie pas cette action. Par contre, changer l'extension elle-même en conservant E, mais en changeant i ou π par exemple modifie l'action de H sur A.

2. Deux extensions abéliennes de H par A équivalentes définissent une même action de H sur A. Réciproquement, partant d'une action donnée de H dans A, les extensions dont l'action canonique coïncide avec cette action sont-elles toutes équivalentes ?
   - dans le cas des extensions scindées, la réponse est oui, d'après la partie (iii),
   - dans le cas général, la réponse est non (cf. l'exemple ci-dessous),
   - au paragraphe 8.3, on verra que ces classes d'équivalences sont en bijection avec $H^2(H, A)$ (cf. définition au paragraphe 8.1, puis théorème 8.3).

3. Attention, lorsque les extensions ne sont pas abéliennes, deux extensions équivalentes peuvent donner lieu à deux actions différentes de H sur A. Par exemple, les extensions $\mathfrak{S}_3 \rtimes \mathbb{Z}/2\mathbb{Z}$ et $\mathfrak{S}_3 \times \mathbb{Z}/2\mathbb{Z}$ sont équivalentes, comme on l'a vue. Or l'action de $\mathbb{Z}/2\mathbb{Z}$ sur $\mathfrak{S}_3$ est non triviale dans un cas, triviale dans l'autre.

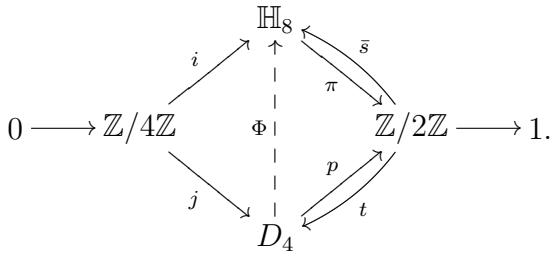
Théorème 7.21 (Liens entre $\mathcal{E}_s(H,\, A)$ et $\mathrm{Hom}(H,\, \mathrm{Out}(A))$, avec A abélien)**.**
On a le diagramme commutatif suivant,



où Θ est l'application induite par θ (cf. définition 7.12). □

Exemple.

Voici un exemple de deux extensions abéliennes de même action canonique, mais non équivalentes :



où $\bar{s}$ est une pseudo-section et t est une section, induisant toute deux la même action non triviale de $\mathbb{Z}/2\mathbb{Z}$ sur $\mathbb{Z}/4\mathbb{Z}$. Un tel morphisme Φ faisant commuter le diagramme n'existe pas.

Voici le détail. Le sous-groupe $A = \langle\, i\rangle$ de $\mathbb{H}_8$ est distingué. Notons $H = \{\bar{1},\, \bar{j}\}$ le quotient $\mathbb{H}_8/A$, et π le morphisme $\mathbb{H}_8 \to H$ envoyant les éléments de A sur $\bar{1}$, et les éléments de $\{\pm j,\, \pm k\}$ sur $\bar{j}$. Soit $\tilde{s} \;:\; H \to \mathbb{H}_8$ une pseudo-section telle que $\tilde{s}(\bar{1}) = 1$ et $\tilde{s}(\bar{j}) = j$. On a la suite exacte :

$$1 \longrightarrow A \xrightarrow{i_1} \mathbb{H}_8 \underset{\tilde{s}}{\overset{\pi}{\rightleftarrows}} H \longrightarrow 1.$$

La pseudo-section $\tilde{s}$ permet de définir l'action canonique de H sur A. Elle est décrite par un morphisme $\varphi \;:\; H \to \mathrm{Aut}(A)$ envoyant $\bar{1}$ sur l'identité, et $\bar{j}$ sur l'involution de A qui fixe 1 et -1, et qui échange i et $-i$. Choisir une autre pseudo-section aurait produit la même action. Mais il n'existe pas de vraie section de H dans $\mathbb{H}_8$, puisque $\{\pm j,\, \pm k\}$ ne contient pas d'éléments d'ordre 2. Le groupe $\mathbb{H}_8$ n'est donc pas pas isomorphe à $A \rtimes_\varphi H$. En effet, $A \rtimes_\varphi H$ est isomorphe au groupe diédral $\mathcal{D}_4$ qui possède quatre éléments d'ordre 2, contrairement à $\mathbb{H}_8$.

Corollaire 7.22 (Distinguer deux produits semi-directs)**.**
Soient H un groupe, A un groupe abélien, φ_1 et φ_2 deux morphismes de H dans $\mathrm{Aut}(A)$*. Si les groupes $G_1 = A \rtimes_{\varphi_1} H$ et $G_2 = A \rtimes_{\varphi_2} H$ sont isomorphes par un isomorphisme Φ qui envoie $i_1(A)$ sur $i_2(A)$, alors il existe $\beta \in \mathrm{Aut}(H)$ et $\alpha \in \mathrm{Aut}(A)$ tels que pour tout $h \in H$, on ait :*

$$(\varphi_2)_h = \alpha^{-1}(\varphi_1)_{\beta(h)}\alpha,$$

Autrement dit, les deux produits semi-directs sont de structures semblables.

Démonstration. Partons des deux extensions de l'énoncé et appelons-les E_1 et E_2 :

- E_1 : $\quad A \xrightarrow{i_1} G_1 \xrightarrow{\pi_1} H$,
- E_2 : $\quad A \xrightarrow{i_2} G_2 \xrightarrow{\pi_2} H$.

Soit $\Phi \in \mathrm{Isom}(G_2, G_1)$ tel que $\Phi i_1(A) = i_2(A)$. Alors, il existe $\alpha \in \mathrm{Aut}(N)$ tel que :

$$i_1\,\alpha \;=\; \Phi\, i_2$$

D'après le lemme 7.4, cette dernière égalité implique l'existence de $\beta \in \mathrm{Aut}(H)$ tel que :

$$\beta\,\pi_2 \;=\; \pi_1\,\Phi$$

On se donne également l'extension intermédiaire suivante que l'on appelle F.

- F : $\quad A \xrightarrow{i} G_2 \xrightarrow{\pi} H$ avec $i = i_2\alpha^{-1}$ et $\beta\pi_2 = \pi$.

Grâce aux quatre égalités précédentes, le diagramme suivant est commutatif.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & A & \xrightarrow{i_1} & G_1 & \xrightarrow{\pi_1} & H & \longrightarrow & 1 \\
 & & \uparrow{\scriptstyle =} & & \uparrow{\scriptstyle \Phi} & & \uparrow{\scriptstyle =} & & \\
1 & \longrightarrow & A & \xrightarrow[i]{} & G_2 & \xrightarrow[\pi]{} & H & \longrightarrow & 1 \\
 & & \uparrow{\scriptstyle \alpha} & & \uparrow{\scriptstyle =} & & \uparrow{\scriptstyle \beta} & & \\
1 & \longrightarrow & A & \xrightarrow[i_2]{} & G_2 & \xrightarrow[\pi_2]{} & H & \longrightarrow & 1
\end{array}$$

Alors les extensions E_1 et F sont équivalentes, donc $\theta(F) = \theta(E_1) = \varphi_1$. Soit s une section de π. Alors $s\beta$ est une section de π_2 car $\beta\pi_2 s = \pi\, s = \mathrm{Id}_H$. Or A est abélien, donc le morphisme d'action associé à une extension scindée ne dépend pas de la section. En appliquant ce fait aux extensions F et E_2, on trouve :

$$\begin{aligned}
(\varphi_1)_h(n) &= i^{-1}(s(h)i(n)s(h)^{-1}) \\
(\varphi_2)_h(n) &= {i_2}^{-1}(s\beta(h)\, i_2(n)\, s\beta(h)^{-1}) \\
&= \alpha^{-1}i^{-1}(s\beta(h)\, i\,\alpha(n)\, s\beta(h)^{-1}) \\
&= \alpha^{-1}\,(\varphi_1)_{\beta(h)}\,\alpha\,(n).
\end{aligned}$$

Le corollaire est ainsi démontré. □

Exemple. Au paragraphe 3.6, on on classé tous les produits semi-directs du type $\mathbb{Z}/133\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$. Il ne nous restait plus qu'à décider si les deux groupes

$$G_1 = \mathbb{Z}/133\mathbb{Z} \rtimes_{\varphi_1} \mathbb{Z}/3\mathbb{Z} \text{ où } \varphi(1) = \{z \mapsto 11z\},$$
$$G_2 = \mathbb{Z}/133\mathbb{Z} \rtimes_{\varphi_2} \mathbb{Z}/3\mathbb{Z} \text{ où } \varphi(1) = \{z \mapsto 30z\},$$

sont isomorphes ou non. S'il existe un isomorphisme $\Phi : G_1 \to G_2$, il devrait envoyer le sous-groupe normal $\mathbb{Z}/133\mathbb{Z}$ de G_1 sur le sous-groupe normal $\mathbb{Z}/133\mathbb{Z}$ de G_2, car on a vu lors de la démonstration de la proposition 6.11 que G_1 et G_2 ne possédaient qu'un seul sous-groupe d'ordre 19 et qu'un seul sous-groupe d'ordre 7, donc qu'un seul sous-groupe d'ordre 133. Alors, d'après la proposition 7.22, ces deux extensions devraient être équivalentes. Or elles ne le sont pas puisqu'on ne peut pas passer de l'action φ_1 à l'action φ_2 par une combinaison des deux critères d'équivalence. En effet, rappelons que $\mathrm{Aut}(\mathbb{Z}/133\mathbb{Z})$ est isomorphe à $\mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, et que par cet isomorphisme, φ_1 et φ_2 sont les morphismes suivants :

$$\varphi_1 : \begin{array}{ccc} \mathbb{Z}/3\mathbb{Z} & \longrightarrow & \mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \\ 1 & \longmapsto & (6,2) \end{array} \qquad \text{et} \qquad \varphi_2 : \begin{array}{ccc} \mathbb{Z}/3\mathbb{Z} & \longrightarrow & \mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \\ 1 & \longmapsto & (12,2) \end{array}.$$

Or il n'existe pas d'éléments $\alpha \in \mathbb{Z}/3\mathbb{Z}$ et $\beta \in \mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ tels que

$$\beta\varphi_1(\alpha)\beta^{-1} = \varphi_2(1),$$

car $\mathbb{Z}/18\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ est abélien, donc la conjugaison est sans effet, et multiplier par α envoie éventuellement $(6,2)$ sur $(12,4)$, mais en aucun cas sur $(12,2)$.

8 Extensions de groupes et cohomologie de groupes

8.1 Cohomologie de groupes

G-modules (libres), l'anneau $\mathbb{Z}[G]$.
Soit G un groupe. Un G-module est la donnée d'un groupe abélien A et d'une action de G sur A. Soit $\mathbb{Z}[G]$ le groupe additif des polynômes dont les indéterminées sont les éléments de G,

$$\mathbb{Z}[G] = \Big\{ \sum_{1\leqslant i\leqslant n} k_i g_i, \quad n \in \mathbb{N},\ k_i \in \mathbb{Z},\ g_i \in G \Big\}.$$

Le groupe $\mathbb{Z}[G]$ est un G-module via l'action évidente :

$$g.\sum_{1\leqslant i\leqslant n} k_i g_i = \sum_{1\leqslant i\leqslant n} k_i (g g_i).$$

La multiplication entre indéterminées issue du produit dans G fait du groupe $\mathbb{Z}[G]$ un anneau. Un G-module est en fait un module sur l'anneau $\mathbb{Z}[G]$. Un morphisme de G-modules est un morphisme de groupes qui « commute à l'action de G », autrement dit, un morphisme de groupe f tel que $f(g.x) = g.f(x)$.

Un G-module M est dit *libre* si l'action de $\mathbb{Z}[G]$ sur M est libre. Il est équivalent de demander que M soit une somme directe de sous-groupes isomorphes à $\mathbb{Z}[G]$.

Résolution libre de G-modules sur $\mathbb{Z}$.
Une *résolution libre F de G-modules sur $\mathbb{Z}$* est une suite exacte longue de la forme

$$\ldots \xrightarrow{\partial_3} F_2 \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\varepsilon} \mathbb{Z},$$

où les F_i sont des G-modules libres, où F_0 est un G-module libre de rang 1 (donc isomorphe à $\mathbb{Z}[G]$), où $\mathbb{Z}$ est vu comme un G-module (non libre) via l'action triviale, et où toutes les flèches sont des morphismes de G-modules. Avec ces conditions, la flèche ε est forcément le morphisme suivant appelé *augmentation* :

$$\varepsilon(\sum_{1\leqslant i\leqslant n} k_i g_i) = \sum_{1\leqslant i\leqslant n} k_i.$$

Un exemple est fondamental : la résolution standard.

La résolution standard de G-modules sur $\mathbb{Z}$.
Pour tout $i \geqslant 0$, soit G^i l'ensemble des i-uplets, notés entre crochets [.], d'éléments de G. Ainsi G^0 est réduit à l'élément $[\,]$, G^1 est en bijection avec G, G^2 est en bijection avec $G \times G$, etc. Pour tout $i \geqslant 0$, on note $\widetilde{G}_i$ le G-module libre de base G^i. Ainsi

$$\begin{aligned}
\widetilde{G}_0 &= \mathbb{Z}[G][\,] = \Big\{ \sum_{1\leqslant i\leqslant n} k_i g_i[\,], \quad n\in\mathbb{N},\ k_i\in\mathbb{Z},\ g_i\in G \Big\},\\
\widetilde{G}_1 &= \bigoplus_{g\in G} \mathbb{Z}[G][g],\\
\widetilde{G}_2 &= \bigoplus_{(g,h)\in G^2} \mathbb{Z}[G][g,h],
\end{aligned}$$

etc. Un morphisme de G-modules de $\widetilde{G}_i$ dans un G-module A est déterminé par une application ensembliste de G^i dans A. On définit différents morphismes de G-modules entre les $\widetilde{G}_i$, que l'on définit à partir de fonctions ensemblistes sur les G^i. Soit $d_k : \widetilde{G}_n \to \widetilde{G}_{n-1}$ défini pour tout $k\in\mathbb{N}$ par :

$$\left\{\begin{array}{lcl}
d_0([g_1,g_2,\ldots,g_i,\ldots,g_n]) &=& [g_2,g_3,\ldots,g_n]\\
d_1([g_1,g_2,\ldots,g_i,\ldots,g_n]) &=& [g_1g_2,g_3,\ldots,g_n]\\
d_i([g_1,g_2,\ldots,g_i,\ldots,g_n]) &=& [g_1,\ldots,g_{i-1},g_ig_{i+1},g_{i+2},\ldots,g_n]\\
d_n([g_1,g_2,\ldots,g_i,\ldots,g_n]) &=& [g_1,\ldots,g_{n-1}]
\end{array}\right.$$

Soit $\partial_i : \widetilde{G}_i \to \widetilde{G}_{i-1}$ défini pour tout $i\in\mathbb{N}^*$ par :

$$\left\{\begin{array}{l}
\partial_1([g]) = g[\,]-[\,]\\
\partial_2([g,h]) = g[h]-[gh]+[g]\\
\partial_3([g,h,k]) = g[h,k]-[gh,k]+[g,hk]-[g,h]\\
\partial_n([g_1,g_2,\ldots,g_i,\ldots,g_n]) = \sum_{i=0}^{n}(-1)^i d_i([g_1,g_2,\ldots,g_i,\ldots,g_n])
\end{array}\right.$$

Soit $\varepsilon : \widetilde{G}_0 \to \mathbb{Z}$ défini par :

$$\varepsilon\Big(\sum_{1\leqslant i\leqslant n} k_i g_i[\,]\Big) = \sum_{1\leqslant i\leqslant n} k_i$$

Alors la suite suivante

$$\ldots \xrightarrow{\partial_3} F_2 \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z}$$

est une résolution de G-modules libres sur $\mathbb{Z}$ appelée *la résolution standard* et notée ici $\widetilde{G}$. Il est facile mais laborieux de vérifier par le calcul que $\partial^{i-1}\partial^i = 0$ pour tout $i\in\mathbb{N}^*$ et $\varepsilon\partial^1 = 0$, il est un peu plus difficile de prouver directement que réciproquement $\mathrm{Ker}\,(\partial^{i-1}) \subset \mathrm{Im}\,(\partial^i)$, mais il existe dans les deux cas des techniques plus élégantes.

Complexe de cochaîne et cohomologie.
Soit A un G-module et F une résultion libre de G-modules sur $\mathbb{Z}$. On appelle *complexe de cochaîne associé à la résolution F de G-modules libres sur $\mathbb{Z}$ à coefficient dans A* la donnée pour tout $i\in\mathbb{N}$ de

- $C^i(F,\,A) = \mathrm{Hom}_G(F_i,\,A)$, le groupe additif des morphismes de G-modules de F_i dans A,
- $\delta^i : C^i(F,\,A) \to C^{i+1}(F,\,A)$ le morphisme de G-modules tel que pour tout $f\in C^i(F,\,A)$ et tout $x\in F_{i+1}$,

$$\delta^i(f)(x) = f\partial_{i+1}(x)$$

On a ainsi une suite :

$$C^0(F,\,A) \xrightarrow{\delta^0} C^1(F,\,A) \xrightarrow{\delta^1} C^2(F,\,A) \xrightarrow{\delta^2} C^3(F,\,A) \xrightarrow{\delta^3} \ldots$$

qui vérifie pour tout $i\in\mathbb{N}$:

$$\delta^{i+1}\delta^i = 0,$$

car cette composition fait intervenir $\partial_{i+1}\partial_{i+2}$ qui est l'application nulle. Par contre, ce n'est plus une suite exacte. On définit alors pour tout $i \in \mathbb{N}$:

$$\begin{array}{ll} C^i(F,\, A) = \mathrm{Hom}_G(F_i,\, A), & \text{les éléments de } C^i(F,\, A) \text{ sont appelés les } \textit{cochaînes}, \\ Z^i(F,\, A) = \mathrm{Ker}\,(\delta^i), & \text{les éléments de } Z^i(F,\, A) \text{ sont appelés les } \textit{cocyles}, \\ \left.\begin{array}{l} B^0(F,\, A) = \{0\}, \\ B^{i+1}(F,\, A) = \mathrm{Im}\,(\delta^i), \end{array}\right\} & \text{les éléments de } B^i(F,\, A) \text{ sont appelés les } \textit{cobords}, \\ H^i(G, A) = \dfrac{Z^i(F,\, A)}{B^i(F,\, A)}. & \text{appelé } \textit{i-ème groupe de cohomologie de } G \textit{ à coefficients dans } A. \end{array}$$

En fait, les cochaînes, cocyles et cobords dépendent de la résolution choisie, mais on peut démontrer par une succession de lemmes sur les diagrammes de suites exactes que le groupe $H^i(G, A)$ est indépendant de la résolution choisie dès que les G-modules F_i qui la composent sont libres[30].

Exemple. Prenons la résolution standard $\widetilde{G}$, et A un G-module quelconque. L'ensemble $C^0(\widetilde{G},\, A)$ des cochaînes d'indice 0 est l'ensemble des morphismes de G-modules de $\widetilde{G}_0$ dans A. Ces morphismes sont caractérisés par les applications de G^0 dans A, donc par le choix d'un élément de A :

$$C^0(\widetilde{G},\, A) \cong A$$

Les cobords de degré zéro sont des morphismes f tels que pour tout $x \in \widetilde{G}_1$, on ait $\big(\delta^0(f)\big)(x) = 0$, autrement dit $f(\partial_1(x)) = 0$. Lorsque $x = [g]$, on obtient $f(g[\,] - [\,]) = 0$, donc $gf([\,]) = f([\,])$. Par ailleurs, $B^0(\widetilde{G},\, A) = \{[\,] \mapsto 0_A\}$. Donc, en notant A^G les éléments de A invariants par G, on a :

$$H^0(G,\, A) \cong Z^0(\widetilde{G},\, A) \cong A^G.$$

Le groupe des dérivations $\mathcal{D}\mathrm{er}(G,\, A)$ et des dérivations principales $\mathcal{P}(G,\, A)$. Soit A un G-module. On appelle *dérivation de G dans A* toute application f de G dans A telle que[31] :

$$f(gh) = f(g) + g.f(h)$$

pour tous $g, h \in G$. Le groupe additif des dérivations est noté $\mathcal{D}\mathrm{er}(G,\, A)$. Ses éléments sont des applications f de G^1 dans A vérifiant :

$$g.f([h]) - f([gh]) + f([g]) = f(\partial_2([g, h])) = \big(\delta^1(f)\big)([g, h]) = 0,$$

autrement dit, on a un isomorphisme[32] entre $\mathcal{D}\mathrm{er}(G,\, A)$ et de $Z^1(\widetilde{G},\, A)$. On appelle *dérivation principale de G dans A* toute application f de G dans A telle qu'il existe un élément $a \in A$ tel que pour tout $g \in G$, on ait :

$$f(g) = g.a - a.$$

Le groupe additif des dérivations principales est noté $\mathcal{P}(G,\, A)$. Remarquons qu'on a :

[30] En fait, demander que les G-modules soient *projectifs* suffit. Tout module libre est projectif, mais la réciproque est fausse.

[31] Reprenons la formule $f(gh) = f(g)+g.f(h)$ convenons d'une action triviale à droite de G sur A. Alors on peut réécrire la formule ainsi : $f(gh) = f(g).h + g.f(h)$, et l'on retrouve la dérivation d'un produit de fonctions, d'où le nom de dérivation.

[32] Il ne s'agit pas d'une égalité, car les éléments de $\mathcal{D}\mathrm{er}(G,\, A)$ vont de G dans A tandis que les éléments de $Z^1(\widetilde{G},\, A)$ vont de $\widetilde{G}$ dans A. Pour passer des premiers aux seconds, il faut linéariser par $\mathbb{Z}[G]$.

$$f(gh) = (gh).a - a = (g.a - a) + g.(h.a - a) = f(g) + gf(h),$$

d'où l'on déduit que $\mathcal{P}(G,\, A) \subset \mathcal{D}\mathrm{er}(G,\, A)$. Les éléments de $\mathcal{P}(G,\, A)$ sont des applications f de G^1 dans A telles qu'il existe $a \in A$ vérifiant

$$f([g]) = g.a - a = f'(g[\,] - [\,]) = f'(\partial_1([g])) = \big(\delta_0(f')\big)([g]),$$

où $f' \,:\, G^0 \to A$ envoie $[\,]$ sur a. Donc $\mathcal{P}(G,\, A) \cong B^1(\widetilde{G},\, A)$. Finalement,

$$H^1(G,\, A) = \frac{\mathcal{D}\mathrm{er}(G,\, A)}{\mathcal{P}(G,\, A)}.$$

Si l'action de G sur A est triviale, les dérivations sont en fait les morphismes de G dans le groupe A et les dérivations principales sont réduites au morphisme trivial de G dans A. Ainsi :

$$\text{si l'action de } G \text{ sur } A \text{ est triviale, alors } H^1(G,\, A) = \mathrm{Hom}_{\mathbb{Z}}(G,\, A).$$

Remarque. On voit sur ces deux exemples (le calcul de $H_0(G,\, A)$ et le calcul de $H_1(G,\, A)$) que les groupes d'homologie ne dépendent pas seulement de G et du groupe A, mais également de **la structure de G-module sur A**.

8.2 Classification des sections des extensions abéliennes scindées par le $H^1(G,\, A)$

On considère la suite exacte suivante où A est un groupe abélien :

$$0 \to A \xrightarrow{\;i\;} E \xrightarrow{\;\pi\;} G \to 1. \tag{1}$$

Soit

$$\varphi \,:\, \begin{array}{ccc} G & \longrightarrow & \mathrm{Aut}(A) \\ g & \longmapsto & \mathrm{Ad}_{\tilde{g}} \,:\, a \mapsto i^{-1}(\tilde{g} i(a) \tilde{g}^{-1}) \end{array}$$

le morphisme d'action associée à l'extension (1), où $g \mapsto \tilde{g}$ est une pseudo-section de π. On note

$$ga = \varphi_g(a)$$

cette action. De plus, on suppose que

$$E \cong A \rtimes_{\varphi} G,$$

de sorte que l'extension soit scindée.

Problème. On cherche alors quelles sont les sections de π (rappelons que puisque A est abélien, le produit semi-direct à équivalence d'extension près ne dépend pas de la section, mais que de φ). A l'évidence, partant d'une section $s \,:\, G \to E$, et d'un élément e de E, le morphisme $s' \,:\, G \to E$ défini par $s'(g) = es(g)e^{-1}$ est encore une section si $\pi \circ s' = \mathrm{Id}_G$, autrement dit si $\pi(e)g\pi(e^{-1}) = g$. Donc pour que s' soit aussi une section de π, il faut et il suffit que :

$$\pi(e) \in \mathcal{Z}_G.$$

Cette condition est évidemment vérifiée si $e \in i(A)$ (elle n'y est cependant pas équivalente, sinon tous les produits semi-directs entre groupes abéliens seraient triviaux). On pose alors la définition :

Définition 8.1 (Sections A-conjuguées)**.**
Deux sections s et s' seront dites *A-conjuguées* s'il existe $a \in A$ telles que pour tout $g \in G$, on ait :

$$s'(g) = i(a)s(g)i(a)^{-1}.$$

Le problème consiste alors à décrire l'ensemble des sections de la suite (1) à A-conjugaisons près. La réponse est donnée par $H_1(G,\, A)$...

Théorème 8.2 (Classes de A-conjugaisons des sections de $A \rtimes G \to G$ et $H^1(G,\, A)$.)**.**
Soient A un groupe abélien, G un groupe, et $\varphi : G \to \mathrm{Aut}(A)$ un morphisme de groupes. Les classes de A-conjugaison de sections de l'extension suivante

$$0 \to A \xrightarrow{i} A \rtimes_\varphi G \xrightarrow{\pi} G \to 1$$

sont en bijection avec $H^1(G,\, {}_\varphi A)$ où ${}_\varphi A$ est le G-module dont le groupe sous-jacent est A et l'action par G est donnée par le morphisme φ.

Démonstration. Partons d'une section s de G. Puisque $\pi \circ s = \mathrm{Id}_G$, il existe une unique application $d : G \to G$ telle que :

$$s : \begin{array}{ccc} G & \longrightarrow & A \rtimes G \\ g & \longmapsto & (dg,\, g) \end{array}.$$

Alors : $$s(g)s(h) = (dg,\, g)(dh,\, h) = (dg + gdh,\, gh),$$
or : $$s(gh) = (d(gh),\, gh),$$
donc : $$d(gh) = d(g) + gd(h),$$
donc : $$d \in \mathcal{D}\mathrm{er}(G,\, A).$$

Partons maintenant de deux sections A-conjuguées s_1 et s_2 associées aux dérivations d_1 et d_2. Il existe $a \in A$ tel que pour tout $g \in G$, on ait :

$$\begin{array}{rcl} s_1(g) & = & i(a)s_2(g)i(a)^{-1} \\ & = & (a,\, 1_G)(d_2 g,\, g)(-a,\, 1_G) \\ & = & (a + d_2 g - ga,\, g). \end{array}$$

Autrement dit, on a :

$$d_1(g) = d_2(g) - (ga - a),$$

donc les sections d_1 et d_2 sont égales à une dérivation principale près. Ainsi, l'ensemble des sections à A-conjugaison près sont en bijection avec :

$$\tfrac{\mathcal{D}\mathrm{er}(G,\, A)}{\mathcal{P}(G,\, A)} \cong H^1(G,\, A).$$

□

Remarque . Dans le cas où le produit est direct, les sections sont en bijection avec $\mathrm{Hom}(G,\, A)$ par l'application suivante.

$$\begin{array}{ccc} \mathrm{Hom}(G,\, A) & \to & \{\text{Sections de } \pi\} \\ f & \mapsto & s : g \in G \mapsto (f(g), g) \in A \times G \end{array}$$

Or une section n'est pas modifiée par A-conjugaison puisque A est abélien. Ainsi, lorsque E est isomorphe au produit direct de A par G, par le théorème 8.2 on retrouve le calcul du H^1 dans le cas particulier où l'action de G sur A est triviale :

$$H^1(G,\, A) \cong \mathrm{Hom}_{\mathbb{Z}}(G,\, A), \text{ lorsque l'action de } G \text{ sur } A \text{ est triviale.}$$

8.3 Classification des extensions abéliennes par le $H^2(G,\, A)$

Etant donnée une extension abélienne :

$$0 \to A \xrightarrow{i} E \xrightarrow{\pi} G \to 1, \tag{1}$$

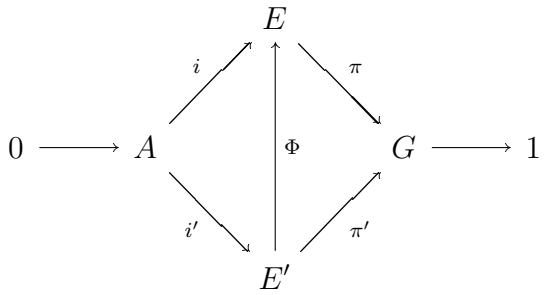
soit φ le morphisme d'action associé à cette application. Partant d'une pseudo-section $h \mapsto \tilde{h}$ le morphisme d'action est :

$$\varphi \ : \ \begin{array}{ccc} G & \longrightarrow & \mathrm{Aut}(A) \\ g & \longmapsto & \mathrm{Ad}_{\tilde{g}} \ : \ a \mapsto i^{-1}(\tilde{g} i(a) \tilde{g}^{-1}) \end{array} .$$

Problème. Réciproquement, étant donnés un groupe abélien A, un groupe G et une action de G sur A caractérisée par un morphisme structurel

$$\varphi \ : \ \begin{array}{ccc} G & \longrightarrow & \mathrm{Aut}(A) \\ g & \longmapsto & \{a \mapsto ga\} \end{array} ,$$

on cherche à décrire l'ensemble des classes d'équivalence extensions de G par A de morphisme d'action φ. Rappelons que deux extensions $G \to E \to A$ et $G \to E' \to A$ sont équivalentes s'il existe un isomorphisme $\Phi \ : \ E' \to E$ tel que le diagramme ci-dessous commute,



et que sous ces conditions, les morphismes d'action des deux extensions coïncident d'après la proposition 7.20. Rappelons enfin qu'il existe exactement une classe d'équivalence d'extensions **scindées** de G par A ayant φ pour morphisme d'action, mais qu'il peut n'exister aucune ou exister plusieurs classes d'équivalence d'extensions **non scindées** de G par A ayant φ pour morphisme d'action.

Théorème 8.3 (Classification des extensions abéliennes par $H^2(G,\, A)$)**.**
Soient un groupe abélien A, un groupe G, et une action de G sur A donnée par un morphisme $\varphi \ : \ G \to \mathrm{Aut}(A)$ faisant de A un G-module. Soit $\mathcal{E}(G,\, A, \varphi)$ l'ensemble des classes d'équivalence d'extensions de G par A de morphisme d'action φ. Alors, on a[33] *:*

$$\mathcal{E}(G,\, A, \varphi) \cong H^2(G,\, {}_{\varphi}A)$$

Démonstration.

0°) Partons d'une extension de G par A de morphisme d'action φ :

$$0 \to A \xrightarrow{i} E \xrightarrow{\pi} G \to 1. \tag{0}$$

Soit s une pseudo-section de G dans E telle que

[33] On note ${}_{\varphi}A$ pour rappeler que $H^2(G,\, {}_{\varphi}A)$ est la cohomologie de G à coefficients dans A où A est vu comme G-module via l'action induite par φ.

$$s(1_G) = 1_E. \tag{1}$$

On note $ga = \varphi_g(a)$ de sorte que :

$$s(g)i(a) = i(ga)s(g). \tag{2}$$

Si s est un morphisme (autrement dit, si s est une section), alors l'extension E est équivalente à l'extension $A \rtimes_\varphi G$ d'après la proposition 7.20. Ainsi les sections induisent toutes un même élément de $\mathcal{E}(G, A)$.

1°) Supposons que s ne soit pas une section. On va construire une équivalence d'extensions entre E et une extension de référence construite à partir de s. Pour cela, on définit une application $f : G \times G \to A$ exprimant de combien l'écart entre s et ce que devrait être s si s était un morphisme :

$$f : \begin{array}{ccc} G \times G & \longrightarrow & A \\ (g,\, h) & \longmapsto & i^{-1}\big(s(g)s(h)s(gh)^{-1}\big) \end{array}. \tag{3}$$

Remarquons que (1) implique :

$$f(g,\, 1) = f(1,\, g) = 0. \tag{4}$$

Montrons que l'on peut retrouver l'extension (0) (à équivalence près) à partir de A, G, φ et f. En effet, puisque $s(G)$ est une transversale de E sous l'action de A, on a la bijection :

$$\Psi : \begin{array}{ccc} A \times G & \longrightarrow & E \\ (a,\, g) & \longmapsto & i(a)s(g) \end{array}.$$

On va créer une loi sur $A \times E$ qui fasse de $A \times E$ un groupe et de Ψ un isomorphisme de groupes. En utilisant (2), on voit que :

$$\begin{array}{rcl} i(a)s(g)i(b)s(h) & = & i(a)i(gb)s(g)s(h) \\ & = & i(a+gb)s(g)s(h)s(gh)^{-1}s(gh) \\ & = & i(a+gb)i(f(g,h))s(gh) \\ & = & i(a+gb+f(g,h))s(gh). \end{array}$$

Soit E_f le groupe obtenu en munissant $A \times G$ de la loi de groupes :

$$(a, g)(b, h) = (a + gb + f(g, h),\, gh)). \tag{5}$$

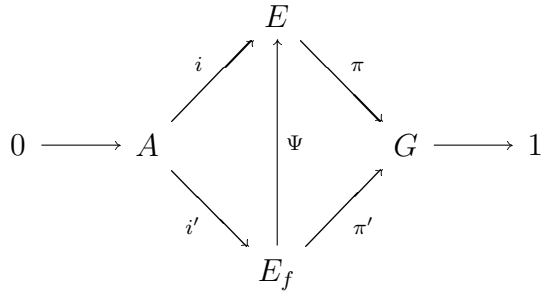
Le groupe E_f ressemble ainsi à un produit semi-direct perturbé par f. La bijection Ψ vérifie :

$$\Psi\big((a, g)\big)\Psi\big((b, h)\big) = \Psi\big((a + gb + f(g, h),\, gh)\big) = \Psi\big((a, g)(b, h)\big)$$

et est bien un morphisme de groupes de E_f vers E. Soient alors :

$$i' : \begin{array}{ccc} A & \longrightarrow & E_f \\ a & \longmapsto & (a, 1) \end{array} \qquad \text{et} \qquad \pi' : \begin{array}{ccc} E_f & \longrightarrow & G \\ (a, g) & \longmapsto & g \end{array}. \tag{6}$$

On obtient l'équivalence d'extensions suivante qui montre qu'avec A, G, φ et f, on a pu reconstruire à équivalence près l'extension (0).



(7)

2°) Si l'on part d'une application $f : G \times G \to A$ arbitraire satisfaisant (3) et (4), on pourrait tenter de reconstruire le groupe E_f, mais la loi donnée par (5) ne serait pas associative en général. En définissant le produit par (5) et en calculant $\big((a,g)(b,h)\big)(c,k)$ et $(a,g)\big((b,h)(c,k)\big)$, on constate que l'associativité a lieu si et seulement si f satisfait[34] :

$$f(g,h) + f(gh,k) = gf(h,k) + f(g,hk). \tag{8}$$

pour tout $g,h,k \in G$. Avec (7), la loi donnée par (5) est bien une loi de groupes. En effet, on vérifie que $(0,1)$ est bien l'élément neutre, et que (a,g) possède un unique inverse $(-g^{-1}a - g^{-1}f(g,g^{-1}),\ g^{-1})$, en remarquant que d'après (8), g^{-1} commute avec $f(g,g^{-1})$. De plus, on vérifie également que les applications données par (6) sont encore des morphismes, et qu'on obtient encore une équivalence d'extensions (7).

Remarquons que l'égalité (8) s'écrit également :

$$\big(\delta^2(f)\big)([g,h,k]) = 0,$$

Donc pour pouvoir construire le groupe E_f, il faut et il suffit de partir d'un cocycle $f \in \mathcal{Z}^2(\widetilde{G},\, A)$ satisfaisant en outre (4).

3°) Montrons que si l'on change la pseudo-section s pour une autre pseudo-section s' sans changer l'extension E dans (0), cela revient à ajouter un cobord au cocycle f, puisque $\pi s'(g) = \pi s(g)$ et $s'(1_G) = 1_E$ entraîne l'existence d'une application $c : G \to A$ telle que

$$\begin{cases} s'(g) = i(c(g))s(g) \\ c(1_G) = 0_A \end{cases}. \tag{9}$$

Or l'application $f' : G \times G \to A$ doit être un cocycle, donc :

$$\begin{aligned}
i(f'(g,h)) &= s'(g)s'(h)s'(gh)^{-1} \\
&= i(c(g))s(g)\, i(c(h))s(h)\, s'(gh)^{-1} \\
&= i(c(g))i(gc(h))s(g)s(h)\, s'(gh)^{-1} \\
&= i\big(c(g) + gc(h) + f(g,h) - c(gh) + c(gh)\big)s(gh)\, s'(gh)^{-1} \\
&= i\big(c(g) + gc(h) + f(g,h) - c(gh)\big)\, i(c(gh))s(gh)s'(gh)^{-1} \\
&= i\big(c(g) + gc(h) + f(g,h) - c(gh)\big) \\
&= i\big(f(g,h) + \delta^1(c)([g,h])\big).
\end{aligned}$$

Donc $f' = f + \delta^1(c)$ où c est une cochaîne de degré 1 vérifiant $c(1_G) = 0_A$. Notons $\widetilde{G}^*$ les cochaînes qui envoient $[1_G, \ldots, 1_G]$ sur 0_A. Il découle de cette étude que les classes

[34] En anglais, une telle fonction f s'appelle *a factor set*.

d'équivalence d'extensions de G par A de morphisme d'action φ sont en bijection avec $H^2(G,\, A)$, puisque :

$$\mathcal{E}(G,\, A,\, \varphi) = \frac{Z^2(\widetilde{G}^*,\, {}_\varphi A)}{B^2(\widetilde{G}^*,\, {}_\varphi A)} = H^2(G,\, {}_\varphi A).$$

□

Corollaire 8.4 (Existence de compléments)**.**
Soit E un groupe fini d'ordre mn avec $m \wedge n = 1$ tel que E contienne un sous-groupe distingué abélien A d'ordre m. Alors E contient des sous-groupes d'ordre n et deux tels sous-groupes sont conjugués.

Démonstration. On va utiliser sans démonstration le fait que si $|A| \wedge |G| = 1$, alors $H^2(G,\, A) = 0$ pour tout $n \geqslant 0$.

Soit $G = E/A$. Considérons l'extension

$$0 \to A \xrightarrow{i} E \xrightarrow{\pi} G \to 1. \qquad (*)$$

Le fait que $|A| \wedge |G| = 1$ implique que $H^2(G,\, A) = 0$. Donc $\mathcal{E}(G,\, A)$ ne contient qu'un seul élément. Donc l'extension $(*)$ est scindée. Cela prouve l'existence d'un sous-groupe d'ordre n dans E.

Supposons qu'on ait deux sous-groupes H et H' de E d'ordre n. Puisque n et m sont premiers entre eux, ce sont des compléments de A. Donc il existe deux sections s et s' de G dans E telles que $s(G) = H$ et $s(G') = H'$. Le fait que $|A| \wedge |G| = 1$ implique que $H^1(G,\, A) = 0$. Donc toutes les sections de G dans E sont A-équivalentes. Par conséquent, il existe $a \in A$ tel que $H' = aHa^{-1}$. □

A Un peu d'histoire des mathématiques : les théorèmes de Burnside

William Burnside est un mathématicien anglais (1852 - 1927) dont les nombreux travaux (plus de 150 articles !) ont porté essentiellement sur les groupes finis. La théorie des groupes finis pris son essor à la fin du XIXème siècle à la suite de N.Abel, E.Galois, J.Liouville, A.Cauchy, L.Sylow grâce notamment à H.Weber, G.Frobenius et W.Burnside. W.Burnside a donné son nom à de nombreux résultats dont les suivants :

Le lemme de Burnside (qui serait en fait dû à Cauchy) :
*S*i G agit sur un ensemble X, alors on a l'égalité :

$$|X/G| = \frac{1}{|G|}\sum_{g\in G}|X^g|$$

où X^g est l'ensemble des points de x de X fixés par g. La démonstration consiste simplement à exprimer la somme en l'indexant par les éléments de X et en faisant intervenir le stabilisateur $\mathrm{Stab}_G(x)$.

Un théorème de Burnside sur le centre des p-groupes.
Le centre d'un p-groupe n'est pas trivial. Cf. proposition 5.3.

Un théorème de Burnside sur les p-Sylow.
Soit G un groupe fini, S un p-Sylow. Si S est contenu dans le centre de son normalisateur, alors il existe un sous-groupe distingué N de G tel que G/N est isomorphe à S. Comme première application, cela permet par exemple de classifier les groupes d'ordre 60, ce qui est difficile, par exemple $\mathcal{A}_5$ qui est simple en fait partie, ou de trouver tous les entiers n (comme 7, 15, 255, etc.) tels qu'il n'existe qu'un seul groupe d'ordre n (donc un groupe cyclique).

Un théorème de Burnside sur les groupes d'ordre $p^\alpha q^\beta$.
Soient p et q deux entiers premiers distincts. Tout groupe d'ordre $p^\alpha q^\beta$ est résoluble. En particulier, l'ordre de tout groupe simple non cyclique contient au moins trois facteurs premiers distincts. Ce théorème est l'un des succès de la théorie des représentations (on parle aussi de caractères) appliquée à la théorie des groupes finis, une approche due à Frobenius.

Les conjectures de Burnside.
Les conjectures qu'il a formulées influencent encore aujourd'hui la recherche en théorie des groupes. On les détaille ci-dessous.

- *La première conjecture de Burnside (1902)*, dont certains énoncés dérivés restent encore aujourd'hui des questions ouvertes.
- « Le théorème de Burnside » (1905) qui apporte une réponse partielle positive à la première conjecture.
- La deuxième conjecture de Burnside (1906), résolue depuis, et devenue le théorème de Feit-Thomson.

A.1 Première conjecture de Burnside (1902)

Problème général de Burnside (1902) :

Un groupe finiment engendré dont les éléments sont tous d'ordre fini est-il fini ?

Au début du XXème siècle, les résultats que l'on connaissait tendait vers une réponse positive. Intuitivement, si un groupe ressemble à un groupe fini du point de vue de ses éléments, est-il vraiment fini ? Posée de façon aussi générale, la réponse est négative, et le premier contre-exemple a été trouvé en 1964 par Golod et Shafarevich.

Problème affaibli de Burnside :

Un groupe finiment engendré et d'exposant fini est-il fini ?

Problème restreint de Burnside (1930) :

Le nombre de groupes finis engendré par m éléments et d'exposant r est-il fini ?

Cette question est « plus simple » que la précédente. Cela dépend bien sûr de m et r. Il est facile de voir que pour tout m, si $r = 2$, alors $G \cong (\mathbb{Z}/2\mathbb{Z})^m$, donc dans ce cas, la réponse est affirmative. En effet, étant donné deux éléments a et b, le fait que $a^2 = b^2 = (ab)^2 = 1$ montre en particulier que $aabb = abab$, d'où $ab = ba$, et le groupe est commutatif. En 1994, Zelmanov obtint la Médaille Fields en répondant à cette question par l'affirmative : le nombre de tels groupes est toujours fini. Actuellement, On sait connaît des bornes en fonction de m pour tout $m \in \mathbb{N}^*$ seulement lorsque $r \in \{2, 3, 4, 6\}$.

Théorème de Burnside (1905) :

Tout sous-groupe du groupe linéaire d'un espace vectoriel de dimension finie et d'exposant fini est d'ordre fini.

A.2 Deuxième conjecture de Burnside (1906)

Théorème A.1 (Feit-Thomson, 1962)**.**
Tout groupe fini d'ordre impair est résoluble.

Démonstration. L'une des plus compliquées des mathématiques qui valut la médaille Fields à Thomson. □

En corollaire immédiat vient le résultat suivant, fondamental dans la recherche des groupes simples.

Corollaire A.2 (Vers la classification des groupes simples)**.**
Tout groupe simple non cyclique est d'ordre pair. □

Bibliographie

D. Guin : *Algèbre, tome 1, groupes et anneaux*, Belin, 1997.

Ce livre est destinée aux étudiants en licence découvrant les groupes. Il est très bien fait, reste simple et abordable.

X. Gourdon, *Algèbre*, Ellipses, 1997.

Rappels de cours et théorèmes démontrés de niveau Classe Préparatoire aux Grandes Ecoles. De nombreux exercices corrigés permettent d'aller plus loin.

D. Perrin : *Cours d'algèbre*, Ellipses, 1996.

Le premier chapitre sur les groupes finis est très riche et de rédaction concise. Il est conseillé au lecteur d'avoir déjà rencontré les principales notions présentées pour profiter pleinement de ce cours.

S. Francinou, H. Gianella : *Exercices de mathématiques pour l'agrégation, Algèbre 1*, Masson 1994.

Ce recueil est une mine d'exercices.

P. Ortiz : *Exercices d'algèbre*, Ellipses, 2004.

Contient une large partie de la correction des exercices suggérés par le *Cours d'algèbre* de D. Perrin, en évitant toutefois les redondances avec ceux déjà traîtés dans le libre d'exercices de Francinou et Gianella.

D. Gorenstein : *Finite groups*, Harper and Row, New York. 1968.

Bible de la théorie des groupes finis de 500 pages.

S. Lang : *Algebra, third edition*, Addison Wesley, 1999.

Bible de l'algèbre de 900 pages.

K.S. Brown : *Cohomology of groups*, Graduate texts in Mathematics, **87**, Springer-Verlag, New York, 1982.

Livre sur la cohomologie des groupes, s'adressant à de futurs chercheurs, exigeant peu de pré-requis, et pourtant très approfondi. Attention, la rédaction est très concise et l'ouvrage peut paraître difficile en première lecture.