4. Le langage des suites exactes

Le langage des *suites exactes* est commode pour exprimer le genre de phénomènes observés ci-dessus pour $n \leqslant 4$, et plus généralement les dévissages.

DÉFINITION 4.1. *Une suite de $n \geqslant 2$ morphismes de groupes*

$$G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} \cdots \xrightarrow{f_n} G_{n+1},$$

est dite exacte, si on a $\operatorname{Im} f_i = \ker f_{i+1}$ *pour* $i = 1, \ldots, n-1$.

Par exemple, dire que $1 \to G \xrightarrow{f} G'$ est exacte signifie donc $\{1\} = \ker f$, *i.e.* que le morphisme f est injectif : on ne précise par le morphisme $1 \to G$, nécessairement trivial. De même, $G \xrightarrow{f} G' \to 1$ est exacte si, et seulement si, f est surjective.

DÉFINITION 4.2. *Une suite exacte de la forme* $1 \to H \xrightarrow{i} G \xrightarrow{\pi} K \to 1$ *s'appelle une suite exacte courte (en abrégé,* s.e.c.*).*

L'exactitude d'une telle suite signifie donc que le morphisme i est injectif, que π est surjectif, et que l'on a $\ker \pi = \operatorname{Im} i$. Comme nous le verrons, les exemples de suites exactes courtes abondent :

EXEMPLE 4.3. *(i) Pour tout entier $n \geqslant 2$ on a une s.e.c.*

$$1 \to \mathrm{A}_n \xrightarrow{i} \mathrm{S}_n \xrightarrow{\varepsilon} \{\pm 1\} \to 1,$$

où i désigne encore l'inclusion naturelle et ε la signature.

(ii) Pour tout k-espace vectoriel V avec $1 \leqslant \dim V < \infty$ on a une s.e.c.

$$1 \to \mathrm{SL}(V) \xrightarrow{i} \mathrm{GL}(V) \xrightarrow{\det} k^\times \to 1.$$

(iii) Pour tout sous-groupe distingué H d'un groupe G on a une s.e.c. naturelle

$$1 \to H \xrightarrow{i} G \xrightarrow{\pi} G/H \to 1,$$

où i est le morphisme d'inclusion et π la projection canonique.

La proposition facile suivante fait le lien entre dévissage et suite exacte courte.

PROPOSITION 4.4. *Soient H, G, K trois groupes. Il est équivalent de se donner :*

(i) une suite exacte $1 \to H \xrightarrow{i} G \xrightarrow{\pi} K \to 1$,

(ii) un sous-groupe distingué $H' \subset G$ et des isomorphismes $i' : H \xrightarrow{\sim} H'$ et $\pi' : G/H' \xrightarrow{\sim} K$.

DÉMONSTRATION — Soit $1 \to H \xrightarrow{i} G \xrightarrow{\pi} K \to 1$ une suite exacte. Alors $H' := \operatorname{Im} i$ est un sous-groupe de G. On a aussi $H' = \ker \pi$ par exactitude "au milieu", et donc H' est distingué dans G. Le morphisme injectif i induit un isomorphisme $i' : H \xrightarrow{\sim} H'$, et par le premier théorème d'isomorphisme, le morphisme surjectif π induit un isomorphisme $\pi' : G/H' \to K$.

Réciproquement, soient (H', i', π') comme dans le (ii). On pose $i : H \to G$, $h \mapsto i'(h)$, et on note $\pi : G \to K$ la composée de la projection canonique $G \to G/H'$ et de l'isomorphisme $\pi' : G/H' \to K$. Par construction, i est un morphisme injectif,

π est un morphisme surjectif, et on a $\ker \pi = H' = \operatorname{Im} i$. Ainsi, la suite $1 \to H \xrightarrow{i} G \xrightarrow{\pi} K \to 1$ est exacte. Cela conclut car il est clair que les deux constructions $(i, \pi) \leftrightarrow (H', i', \pi')$ sont inverses l'une de l'autre. □

C'est toujours plus précis de nommer les morphismes apparaissant dans une suite exacte. On omet parfois de le faire, soit pour ceux qui sont naturels (inclusion canonique d'un sous-groupe, projection canonique...), soit parce que cela ne présente pas d'intérêt particulier pour notre propos, ou encore quand les morphismes utilisés sont le fruit d'un choix que l'on ne veut pas préciser (comme les choix, arbitraires, d'isomorphisme $S_{\mathscr{P}} \simeq S_3$ et $\ker f \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ plus haut). Dans ce langage, et par la Proposition 4.4, les dévissages de S_3, S_4 et A_4 étudiés en Section 3 s'écrivent :

Corollaire 4.5. *Il existe des suites exactes :*

(i) $1 \to \mathbb{Z}/3\mathbb{Z} \to S_3 \to \mathbb{Z}/2\mathbb{Z} \to 1$,
(ii) $1 \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to S_4 \to S_3 \to 1$,
(iii) $1 \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to A_4 \to \mathbb{Z}/3\mathbb{Z} \to 1$.

Bien noter en revanche que le morphisme $S_5 \to S_6$ étudié au chapitre précédent ne s'insère pas dans une suite exacte courte : il n'est pas surjectif et son image n'est (comme on le verra !) pas distinguée dans S_6.

Exemple 4.6. (*Groupe diédral*) Soit $n \geqslant 3$. Le groupe diédral D_{2n} est le sous-groupe de S_n engendré par le n-cycle $c = (1\ 2\ \ldots\ n)$ et l'élément τ défini par $\tau(i) = n + 1 - i$ pour $i = 1, \ldots, n$. On a les relations $\tau^2 = 1$ et $\tau c \tau^{-1} = (n\ n-1\ \ldots\ 2\ 1) = c^{-1}$. Le sous-groupe $C = \langle c \rangle$ de D_{2n}, cyclique d'ordre n, est donc distingué. Il ne contient pas τ (car $\tau c \tau^{-1} = c^{-1} \neq c$ pour $n > 2$), et on a donc $D_{2n} = C\langle \tau \rangle$ puis

$$D_{2n} = C \coprod C\tau \text{ et } |D_{2n}| = 2n.$$

Par exemple, on a $D_6 = S_3$ (plus petit groupe diédral), et D_8 est un 2-Sylow de S_4. On a $C \simeq \mathbb{Z}/n\mathbb{Z}$ et donc (Proposition 4.4) une s.e.c.

$$1 \to \mathbb{Z}/n\mathbb{Z} \to D_{2n} \to \mathbb{Z}/2\mathbb{Z} \to 1.$$

Le groupe D_{2n} n'est pas commutatif, en particulier il n'est pas isomorphe à $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Comme nous le verrons, il s'identifie naturellement au groupe des isométries d'un polygone régulier du plan à n côtés.

Définition 4.7. *Si G, H et K sont des groupes donnés, on dira que G est extension de K par H s'il existe une suite exacte courte $1 \to H \to G \to K \to 1$* [9]. *On appelle aussi extension de K par H la donnée d'une telle suite.*

Ainsi, S_4 est une extension de S_3 par le groupe de Klein, et D_{2n} est une extension de $\mathbb{Z}/2\mathbb{Z}$ par $\mathbb{Z}/n\mathbb{Z}$.

5. Le dévissage de S_n

Les résultats suivants étaient connus de Galois, mais les premières démonstrations semblent dues à Jordan.

9. Bien noter l'ordre de K et H dans cette terminologie Bourbakiste.

THÉORÈME 5.1. *Les seuls sous-groupes distingués de* S_n *sont* $\{1\}$, A_n, S_n, *ainsi que* K_4 *dans le cas particulier* $n = 4$.

DÉMONSTRATION — On a déjà vu que les sous-groupes de l'énoncé sont distingués. Soit H un sous-groupe distingué non trivial de S_n. Notons que si H contient une transposition, alors H contient toutes les transpositions (elles sont conjuguées) et on a donc $H = \mathrm{S}_n$ (elles sont génératrices). De plus, pour $h \in H$ et $\sigma \in \mathrm{S}_n$ observons

$$[h, \sigma] := h\sigma h^{-1}\sigma^{-1} = (h\sigma h^{-1})\sigma^{-1} = h(\sigma h^{-1}\sigma^{-1}).$$

La dernière écriture, et $H \lhd \mathrm{S}_n$, montrent $[h, \sigma] \in H$. La seconde écriture montre *e.g.*

$$[h, (i\,j)] = (h(i)\,h(j))(i\,j)^{-1} \in H, \quad \forall 1 \leqslant i < j \leqslant n.$$

Ainsi, on a trouvé un élément de H dont le support est dans $\{i, j, h(i), h(j)\}$ (technique dite de *réduction du support*).

Supposons d'abord que H contienne un élément h possédant un cycle de longueur $\geqslant 3$ dans sa décomposition en cycles. Écrivant ce cycle $(i\,j\,k\,\ldots)$, on a alors

$$[h, (i\,j)] = (j\,k)(i\,j) = (i\,k\,j) \in H.$$

Comme les 3-cycles sont conjugués dans S_n pour $n \geqslant 3$, on a donc $H \supset \mathrm{A}_n$, puis $H = \mathrm{A}_n$ ou $H = \mathrm{S}_n$.

On peut donc supposer que tous les éléments non triviaux de H sont des produits de $\geqslant 2$ transpositions à supports disjoints, et en particulier $n \geqslant 4$. Dans le cas $n = 4$, ce sont nécessairement des doubles transpositions, et comme ces dernieres sont conjuguées dans S_4, on constate $H = \mathrm{K}_4$. On peut donc supposer $n \geqslant 5$. Écrivons $h = (i\,j)(k\,l)$... (décomposition en cycles). On en déduit que H contient la double transposition $[h, (i\,k)] = (j\,l)(i\,k)$, et donc toutes les doubles transpositions par conjugaison. Il contient donc $(j\,l)(i\,m)$ pour tout entier m distinct de i, j, k et l (il en existe car $n \geqslant 5$). Mais alors H contient le 3-cycle $(j\,l)(i\,k)(j\,l)(i\,m) = (i\,m\,k)$, qui n'est pas produit de transpositions à supports disjoints. □

On a déjà vu $\mathrm{A}_1 = \mathrm{A}_2 = \{1\}$, $\mathrm{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$ et que le groupe A_4 n'est pas simple. Nous laissons au lecteur le soin de montrer que les sous-groupes distingués de A_4 sont $1, \mathrm{K}_4$ et A_4. La situation est radicalement différente pour $n \geqslant 5$.

THÉORÈME 5.2. *Le groupe* A_n *est simple (non abélien) pour* $n \geqslant 5$.

Bien noter que ce résultat ne se déduit pas immédiatement du précédent, car si on a $K \lhd H$ et $H \lhd G$ il n'est pas vrai en général que l'on a $K \lhd G$ (voir l'Exercice 4.11). On s'en sort toutefois par une approche est similaire à celle de la preuve du théorème ci-dessus.

DÉMONSTRATION — Soit $H \subset \mathrm{A}_n$ distingué avec $H \neq 1$ et $n \geqslant 5$. On va montrer $H = \mathrm{A}_n$. Il suffit de voir que H contient un 3-cycle car ces derniers sont conjugués dans A_n et l'engendrent pour $n \geqslant 5$ (Propositions 2.15 et 2.17). Fixons $h \in H - \{1\}$.

Supposons d'abord $n = 5$. En considérant les décompositions en cycles possibles, on constate que h est soit un 3-cycle, soit une double-transposition, soit un 5-cycle. Si h est un 3-cycle, on a gagné. Si h est une double-transposition $(a\,b)(c\,d)$, H contient aussi $[h, (c\,d\,e)] = (c\,e\,d)(c\,d\,e)^{-1} = (c\,e\,d)^2 = (c\,d\,e)$: encore gagné. Enfin si h est

un 5-cycle $(a\,b\,c\,d\,e)$, H contient aussi $[h,(c\,d\,e)] = (d\,e\,a)\,(c\,d\,e)^{-1} = (a\,d\,c)$, ce qui conclut.

Considérons maintenant le cas général. Fixons $\tau = (a\,b\,c)$ un 3-cycle, et regardons

$$[h,(a\,b\,c)] = (h(a)\,h(b)\,h(c))\,(a\,c\,b) \in H$$

Vérifions qu'on peut choisir τ tel que $[h,(a\,b\,c)] \neq 1$. Comme $h \neq 1$, il existe a tel que $h(a) \neq a$, et on peut donc poser $b = h(a)$, puis choisir $c \notin \{a, b, h(b)\}$ car $n \geqslant 4$. Dans ce cas $[h,(a\,b\,c)]$ envoie c sur $h(b) \neq c$, ce que l'on voulait. D'autre part, le support de $s := [h,(a\,b\,c)]$ est inclus dans $\{a, b, c, h(b), h(c)\}$ qui a $\leqslant 5$ éléments. On peut donc voir s comme une permutation paire (non triviale) d'un sous-ensemble C à 5 éléments de $\{1,\dots,n\}$, et fixant le complémentaire C' de C. Le sous-groupe G de A_n fixant C' est isomorphe à A_5. De plus, $H \cap G$ est trivialement distingué dans G, car $H \lhd \mathrm{A}_n$, et il contient l'élément $s \neq 1$. D'après le cas $n = 5$ on a donc $H \cap G = G$, *i.e.* $G \subset H$, et donc H contient tous les 3-cycles de support dans C. □

Un exemple de corollaire à ces résultats est le suivant. Il montre par exemple que l'action exotique de S_5 sur $\{1,\dots,6\}$ est automatiquement fidèle.

COROLLAIRE 5.3. *(i) Pour $n \neq 4$, toute action de A_n est fidèle ou triviale.*

(ii) Une action transitive de S_n sur un ensemble à $m > 2$ éléments est fidèle, sauf peut-être si $n = 4$ et $m = 3$ ou 6.

DÉMONSTRATION — Le (i) vaut pour tout groupe simple (ou trivial) : le noyau d'une action d'un tel groupe G est un sous-groupe distingué, c'est donc soit $\{1\}$ (action fidèle), soit G (action triviale).

Pour le (ii), supposons que $G := \mathrm{S}_n$ agit transitivement sur X avec $|X| = m$. Soit $x \in X$; on a $|\mathrm{O}_x| = m$ (action transitive) et donc $|G_x| = |\mathrm{S}_n|/m < n!/2$ (orbite-stabilisateur). Mais le noyau de l'action de G sur X est un sous-groupe distingué $K \subset \mathrm{S}_n$ inclus dans G_x, et donc de cardinal $< n!/2$. Par le Théorème 5.1 on a donc soit $K = \{1\}$, soit $n = 4$, $K = \mathrm{K}_4$ et par Lagrange $4 = |K|$ divise $4!/m = |G_x|$, *i.e.* $m \mid 6$. □

REMARQUE 5.4. En utilisant un morphisme surjectif $\mathrm{S}_4 \to \mathrm{S}_3$ on construit aisément des actions transitives de S_4 de noyau K_4 sur des ensembles à 3 ou 6 éléments. Le morphisme surjectif $\mathrm{S}_n \to \mathrm{S}_2$ (signature !) construit aussi une action transitive de S_n sur $\{1,2\}$ pour tout $n \geqslant 2$, de noyau A_n.

6. Commutateurs et groupes dérivés

La notion de *commutateur* a joué un rôle important dans les démonstrations ci-dessus. Discutons-les plus généralement. Si $x, y \in G$, on appelle commutateur du couple (x, y) l'élément [10]

$$[x, y] = xyx^{-1}y^{-1}.$$

On a donc $[x, y] = 1$ si et seulement si $xy = yx$. Si A et B sont deux parties de G, on note $[A, B]$ le sous-groupe de G engendré par les $[a, b]$ avec $a \in A$ et $b \in B$.

DÉFINITION 6.1. *Le groupe dérivé d'un groupe G est le sous-groupe $\mathrm{D}(G) := [G, G]$ engendré par les $[x, y]$ avec $x, y \in G$.*

10. Certains auteurs le définissent plutôt comme $x^{-1}y^{-1}xy$. Cela n'a que peu d'incidence.

On a évidement $\mathrm{D}(G) = \{1\}$ si, et seulement si, G est abélien.

Remarque 6.2. ⚠ Les commutateurs ne forment pas un sous-groupe en général, d'où la nécessité de considérer le sous-groupe engendré dans la définition de $\mathrm{D}(G)$. Par exemple, Guralnick a montré [11] que le plus petit groupe fini G pour lequel $\mathrm{D}(G)$ n'est pas constitué de commutateurs est d'ordre 96.

Exemple 6.3. Si $\sigma \in G$ est conjugué dans G à son carré, alors σ est un commutateur. En effet, on a $\sigma^2 = \tau\sigma\tau^{-1}$, et donc $\sigma = [\sigma^{-1}, \tau]$ (voir l'Exercice 4.28 pour une généralisation). Comme le carré d'un 3-cycle est un 3-cycle, et que les 3-cycles sont conjugués dans S_n pour tout n, et même dans A_n pour $n \geqslant 5$, on en déduit que les 3-cycles sont des commutateurs de S_n, et même des commutateurs de A_n pour $n \geqslant 5$.

L'observation suivante est aussi importante que triviale.

Fait 6.4. *Si $f : G \to G'$ est un morphisme de groupes, on a pour tout $x, y \in G$ $f([x, y]) = [f(x), f(y)]$, et donc $f(\mathrm{D}(G)) \subset \mathrm{D}(G')$, avec égalité si f est surjective*

Par exemple, on a $\mathrm{D}(H) \subset \mathrm{D}(G)$ pour H sous-groupe de G. Un sous-groupe C d'un groupe G est dit *caractéristique* si on a $\alpha(C) \subset C$ pour tout $\alpha \in \mathrm{Aut}(G)$. On a alors $\alpha(C) = C$ pour tout $\alpha \in \mathrm{Aut}(G)$ (considérer α^{-1}) et aussi $C \lhd G$ (prendre pour α un automorphisme intérieur).

Corollaire 6.5. *$\mathrm{D}(G)$ est un sous-groupe caractéristique de G.*

Démonstration — C'est le fait ci-dessus appliqué à un automorphisme de G. □

Corollaire 6.6. *Soit G un groupe.*

(i) Tout morphisme $f : G \to G'$ avec G' abélien vérifie $\mathrm{D}(G) \subset \ker f$.

(ii) Pour $H \lhd G$, alors G/H est abélien si, et seulement si, H contient $\mathrm{D}(G)$.

Démonstration — Pour le (i), on a $f([x, y]) = [f(x), f(y)] = 1$ pour tout $x, y \in G$, donc $\mathrm{D}(G) \subset \ker f$. Pour le (ii), on constate $[xH, yH] = [x, y]H$. C'est aussi la relation $\pi([x, y]) = [\pi(x), \pi(y)]$ pour $\pi : G \to G/H$. Ainsi, xH et yH commutent dans G/H si, et seulement si, on a $[x, y] \in H$. □

D'après le (ii) ci-dessus, $\mathrm{D}(G)$ est le plus petit sous-groupe distingué de G de quotient abélien. Le groupe quotient $G_{\mathrm{ab}} := G/\mathrm{D}(G)$ s'appelle l'*abélianisé* G. C'est le plus grand quotient abélien de G. Terminons par une étude des groupes dérivés successifs de S_n.

Proposition 6.7. *Soit $n \geqslant 1$ un entier. On a*

(i) $\mathrm{D}(\mathrm{S}_n) = \mathrm{A}_n$,

(ii) $\mathrm{D}(\mathrm{A}_n) = \mathrm{A}_n$ pour $n \geqslant 5$,

(iii) $\mathrm{D}(\mathrm{A}_4) = \mathrm{K}_4$ et $\mathrm{D}(\mathrm{A}_n) = \{1\}$ pour $n \leqslant 3$.

11. Robert Guralnick, *Commutators and commutator subgroups*, Adv. in Math. 45, 319–330 (1982)

Démonstration — En [12] considérant la signature, on constate $\mathrm{D}(\mathrm{S}_n) \subset \mathrm{A}_n$. Ces deux groupes sont triviaux pour $n \leqslant 2$, donc on suppose définitivement $n \geqslant 3$. Comme les 3-cycles engendrent A_n, l'Exemple 6.3 montre les point (i) et (ii).

Pour le cas restant $n = 4$ on a $\mathrm{D}(\mathrm{A}_4) \subset \mathrm{K}_4$ en considérant un morphisme $\mathrm{A}_4 \to \mathrm{A}_3$ de noyau K_4. On a l'égalité en observant, pour a, b, c, d distincts, l'égalité $[(a\,b\,c), (a\,b\,d)] = (b\,c\,d)(a\,b\,d)^{-1} = (a\,b)(c\,d)$. □

Remarque 6.8. Ore a démontré dans cet article [13] que tout élément de A_n est un commutateur de deux éléments de S_n, et que pour $n \geqslant 5$ tout élément de A_n est un commutateur de deux éléments de A_n.

Pour $n \geqslant 0$ on pose $\mathrm{D}^0(G) = G$ et on définit récursivement, pour $n > 1$,

$$\mathrm{D}^n(G) = \mathrm{D}(\mathrm{D}^{n-1}(G)).$$

C'est une suite décroissante (au sens large) de sous-groupes caractéristiques de G.

Définition 6.9. *Un groupe G est dit résoluble s'il existe un entier $n \geqslant 0$ tel que $\mathrm{D}^n(G) = \{1\}$. Le plus petit tel n est alors appelé classe (de résolubilité) de G.*

Les groupes abéliens sont trivialement résolubles de classe $\leqslant 1$. D'après la Proposition 6.7, on a :

Corollaire 6.10. *Le groupe S_n (resp. A_n) est résoluble, si et seulement si, on a $n \leqslant 4$.*

Ce résultat est particulièrement significatif du point de vue de la théorie de Galois (voir le Complément en Section 9). La Proposition 6.7 montre aussi que S_3 et S_4 sont résolubles de classe 2 et 3 respectivement. De même, D_{2n} est résoluble de classe 2 pour $n \geqslant 3$. La propriété d'être résoluble est stable par passage au sous-groupe, au quotient et par extension :

Proposition 6.11. *Soient G un groupe et H un sous-groupe distingué de G. Alors G est résoluble si, et seulement si, les groupes H et G/H le sont. En outre, si G, H, K sont résolubles de classes n, a, b respectivement, alors $a, b \leqslant n$ et $n \leqslant a + b$.*

Démonstration — Pour tout $j \geqslant 0$, on a $\mathrm{D}^j(H) \subset \mathrm{D}^j(G)$, et si $\pi : G \to G/H$ est la projection canonique, on a aussi $\pi(\mathrm{D}^j(G)) = \mathrm{D}^j(G/H)$ par le Fait 6.4. Ainsi, si $\mathrm{D}^n(G) = \{1\}$ pour un certain $n \geqslant 1$ on a $\mathrm{D}^n(H) = \{1\} = \mathrm{D}^n(G/H)$. Si réciproquement $\mathrm{D}^a(H) = \{1\}$ et $\mathrm{D}^b(G/H) = 1$ pour certains $a, b \geqslant 1$. On a alors $\pi(\mathrm{D}^b(G)) = \{1\}$, donc $\mathrm{D}^b(G) \subset H$, puis $\mathrm{D}^{a+b}(G) \subset \mathrm{D}^a(H) = \{1\}$, et donc $\mathrm{D}^{a+b}(G) = \{1\}$. □

Remarque 6.12.
(i) On peut montrer que *le plus petit groupe simple non abélien est* A_5. On en déduit par récurrence sur le cardinal du groupe que *tout groupe d'ordre < 60 est résoluble*, d'après la Proposition 6.11.
(ii) Burnside a démontré que *tout groupe d'ordre $p^a q^b$, avec p, q premiers, est résoluble*. Nous reviendrons sur ce résultat à la fin du cours.

12. Un argument massue serait d'utiliser la simplicité de A_n pour $n \geqslant 5$.
13. O. Ore, *Some remarks on commutators*, Proc. A. M. S. Vol. 2, 307–314 (1951).