Produits directs et semi-directs de groupes

1 Suites exactes, extensions

Dans ce paragraphe, on présente des notations et conventions d'usage courant et pratique dans l'étude de la théorie des groupes.

Soient $G_0, G_1, \dots, G_n$ des groupes, et pour tout $i \in \{1, \dots, n\}$, un morphisme $f_i : G_{i-1} \longrightarrow G_i$. On dit que

$$G_0 \xrightarrow{f_1} G_1 \xrightarrow{f_2} \cdots \xrightarrow{f_{n-1}} G_{n-1} \xrightarrow{f_n} G_n$$

est une *suite exacte* si pour tout $i \in \{1, \dots, n-1\}$, $\operatorname{Im} f_i = \operatorname{Ker} f_{i+1}$.

Un abus traditionnel consiste à noter 1 le groupe $\{1\}$ réduit à un élément. (Ou éventuellement 0 si on utilise la notation additive, dans le cas de groupes abéliens.) Puis, pour un groupe G quelconque, on désigne par $1 \longrightarrow G$ (respectivement $G \longrightarrow 1$) l'unique[1] morphisme de $\{1\}$ dans G (respectivement de G sur $\{1\}$). Il est très facile de vérifier qu'un morphisme de groupes $f : G \longrightarrow G'$ est injectif (respectivement surjectif) si et seulement si la suite $1 \longrightarrow G \xrightarrow{f} G'$ (respectivement $G \xrightarrow{f} G' \longrightarrow 1$) est une suite exacte.

De même que l'on ne nomme pas les morphismes entre 1 et un groupe G, il est courant de ne pas attribuer de nom à un morphisme canonique, comme l'injection canonique d'un sous-groupe dans un groupe, ou la surjection canonique d'un groupe sur un de ses groupes quotients. Ainsi, si N est un sous-groupe normal de G, on a la suite exacte

$$1 \longrightarrow N \longrightarrow G \longrightarrow G/N \longrightarrow 1.$$

Si $f : G \longrightarrow G'$ est un morphisme de groupe, on a de même la suite exacte

$$1 \longrightarrow \operatorname{Ker} f \longrightarrow G \xrightarrow{f} \operatorname{Im} f \longrightarrow 1.$$

Il est donc courant de rencontrer des suites exactes de la forme

$$1 \longrightarrow N \xrightarrow{f} G \xrightarrow{g} H \longrightarrow 1.$$

On dit dans ce cas que le groupe G est une *extension* de N par H (ou, suivant les auteurs, de H par N...Mais attention, cette notion d'extension n'est pas symétrique !).

Exercice 1.1 *Soient N, G et H trois groupes. Prouver l'équivalence entre*

1. *G est une extension de N par H,*
2. *il existe un sous-groupe normal $\bar{N}$ de G, isomorphe à N, et tel que le groupe quotient $G/\bar{N}$ soit isomorphe à H.*

Étant donnés deux groupes N et H, il est en général difficile de trouver toutes les extensions possibles de N par H. La suite est consacrée à l'étude de cas particuliers élémentaires d'extension : les produits directs et semi-directs.

[1] pourquoi unique ?

2 Produits directs et semi-directs

2.1 Produit direct de deux groupes

Soient N et H deux groupes. Le *produit direct des groupes N et H* est le produit cartésien de N et de H muni de la loi définie par

$$(n,h)(n',h') \stackrel{\text{déf}}{=} (nn',hh').$$

Il est très facile de vérifier que ce produit direct, noté $N \times H$, est un groupe. Vérifions que c'est une extension de N par H. Il existe un morphisme surjectif naturel de $N \times H$ sur H, qui est la projection $p_H : (n,h) \longmapsto h$. Le noyau de p_H est le sous-groupe $\bar{N}$ formé des éléments de la forme $(n,1)$. En écrivant i l'injection de N dans $N \times H$ définie par $i(n) \stackrel{\text{déf}}{=} (n,1)$, on a donc la suite exacte

$$1 \longrightarrow N \xrightarrow{i} N \times H \xrightarrow{p_H} H \longrightarrow 1.$$

En fait, N et H jouent ici des rôles symétriques ; la projection p_N sur la première coordonnée est aussi un morphisme de $N \times H$ sur N, dont le noyau est $\bar{H} \stackrel{\text{déf}}{=} \{(1,h)\ /\ h \in H\}$. En particulier, le produit direct de N et H possède deux sous-groupes normaux $\bar{N}$ et $\bar{H}$, respectivement isomorphes à N et H. Cette symétrie n'est plus valable en général dans le cas du produit semi-direct.

2.2 Produit semi-direct de deux groupes

On considère toujours deux groupes N et H, et on se donne de plus un morphisme $\varphi : h \longmapsto \varphi_h$ de H dans le groupe $\mathrm{Aut}(N)$ des automorphismes de N. On munit cette fois le produit cartésien de N et de H de la loi de composition interne définie à partir de φ par

$$(n,h)(n',h') \stackrel{\text{déf}}{=} (n\varphi_h(n'),hh').$$

On obtient à nouveau un groupe [...], noté $N \rtimes_\varphi H$ (ou plus fréquemment, de manière abusive : $N \rtimes H$), et appelé *produit semi-direct de N par H (relativement à φ)*. Comme dans le cas du produit direct, $\bar{N} \stackrel{\text{déf}}{=} \{(n,1)\ /\ n \in N\}$ et $\bar{H} \stackrel{\text{déf}}{=} \{(1,h)\ /\ h \in H\}$ sont des sous-groupes de $N \rtimes_\varphi H$, respectivement isomorphes à N et H. La projection p_H est toujours un morphisme de groupe de noyau $\bar{N}$, qui est donc même un sous-groupe normal. On a encore la suite exacte

$$1 \longrightarrow N \xrightarrow{i} N \rtimes_\varphi H \xrightarrow{p_H} H \longrightarrow 1.$$

En revanche, la projection p_N n'est plus un morphisme de groupe dès que φ_h n'est pas constamment égal à l'identité sur N [...]. $\bar{H}$ n'a plus cette fois de raison d'être un sous-groupe normal. Notons toutefois que le produit direct est un cas particulier de produit semi-direct : justement celui où φ_h est toujours l'identité sur N.

Si on appelle G le produit semi-direct $N \rtimes_\varphi H$, la suite exacte ci-dessus permet de dire que G est une extension de N par H. De plus, cette extension possède une propriété importante : il existe ici un sous-groupe $\bar{H}$ de G, isomorphe à H, et tel que la restricion à $\bar{H}$ de la surjection canonique $\pi : G \longrightarrow G/\bar{N}$ soit un isomorphisme entre $\bar{H}$ et $G/\bar{N}$. Un tel sous-groupe $\bar{H}$ s'appelle un *relèvement* du groupe quotient $G/\bar{N}$. Il revient au même de dire qu'il existe une *section* de π, c'est-à-dire un morphisme $s : G/\bar{N} \longrightarrow G$ tel que $\pi \circ s = \mathrm{Id}_{G/\bar{N}}$ [...]. On dit dans ce cas que l'extension est *scindée*.

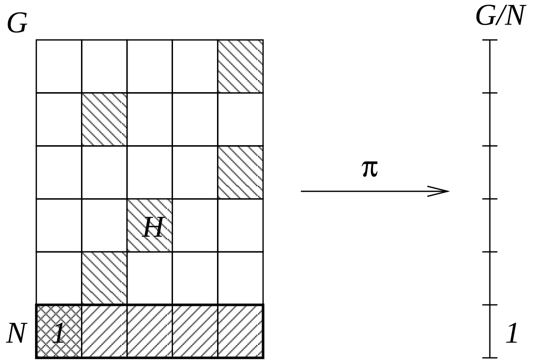
2.3 Décomposition d'un groupe en produit semi-direct

Étant donné un groupe G à étudier, il peut être très intéressant de voir G comme un produit semi-direct de deux de ses sous-groupes non triviaux : l'étude de G peut alors se ramener à celle de deux groupes strictement plus petits.

Pour qu'une telle décomposition soit possible, il est nécessaire que G ne soit pas simple : il doit admettre au moins un sous-groupe normal non trivial N. On dispose alors de la suite exacte canonique

$$1 \longrightarrow N \longrightarrow G \longrightarrow G/N \longrightarrow 1.$$

Supposons de plus que G/N admette un relèvement, c'est-à-dire un sous-groupe H de G tel que la restriction à H de la surjection canonique π de G sur G/N soit un isomorphisme. On en déduit que $N \cap H = \{1\}$ (puisqu'il n'y a qu'un élément de H se projetant sur le neutre de G/N), et que $G = NH = \{nh \;/\; n \in N,\, h \in H\}$. En effet, si on prend $g \in G$, il existe par hypothèse un $h \in H$ tel que $\pi(g) = \pi(h)$, c'est-à-dire $gN = hN$ ($= Nh$ car N est normal dans G). En particulier il existe $n \in N$ tel que $g = nh$.



Le fait que G se décompose alors en un produit semi-direct $N \rtimes H$ se déduit alors de la proposition suivante.

Proposition 2.1 *Supposons qu'un groupe G admette deux sous-groupes N et H vérifiant*

1. $N \lhd G$,
2. $N \cap H = \{1\}$,
3. $G = NH$.

Alors il existe un morphisme $\varphi \;:\; h \longmapsto \varphi_h$ de H dans $\mathrm{Aut}(N)$ tel que G soit isomorphe au produit semi-direct $N \rtimes_\varphi H$.

Preuve — Sous ces hypothèses, remarquons que tout $g \in G$ s'écrit *de manière unique* sous la forme nh avec $n \in N$ et $h \in H$. En effet, supposons $nh = n'h'$, avec n, n' dans N et h, h' dans H. Alors $n'^{-1}n = h'h^{-1} \in N \cap H$, d'où $n = n'$ et $h = h'$ puisque $N \cap H = \{1\}$. G est donc déjà en bijection avec le produit cartésien (ensembliste) $N \times H$. Puis, le produit de deux éléments de G, nh et $n'h'$, s'écrit

$$(nh)(n'h') \;=\; n(hn'h^{-1})(hh') \;=\; (n\varphi_h(n'))(hh'),$$

où pour tout h, φ_h est la restriction à N de l'automorphisme intérieur $g \longmapsto hgh^{-1}$. On a bien $\varphi_h(n') \in N$ car $N \lhd G$. Et $h \longmapsto \varphi_h$ est bien un morphisme de H dans $\mathrm{Aut}(N)$. ❏

Exemple. Dans le groupe symétrique $\mathbf{S}_n$, la signature ε fournit la suite exacte

$$1 \longrightarrow \mathbf{A}_n \longrightarrow \mathbf{S}_n \xrightarrow{\varepsilon} \{-1,1\} \longrightarrow 1.$$

Pour trouver un relèvement de $\{-1,1\}$, il suffit de prendre le sous-groupe engendré par une transposition quelconque. On en déduit que $\mathbf{S}_n$ est isomorphe à un produit semi-direct $\mathbf{A}_n \rtimes \{-1,1\}$.

Exercice 2.1 *Montrer de même que le groupe diédral D_n (groupe des isométries du plan euclidien laissant invariant un polygone régulier à n côtés) est isomorphe à un produit semi-direct $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.*

Le résultat présenté dans l'exercice qui suit peut être très utile lorsqu'il s'agit de décomposer un groupe *fini* en un produit semi-direct.

Exercice 2.2 *Soit G un groupe fini d'ordre mn, où m et n sont deux entiers premiers entre eux, et soit $N \lhd G$, avec $|N| = n$. Prouver qu'un sous-groupe H de G est un relèvement de G/N si et seulement si H est d'ordre m.*

Voyons aussi un contre-exemple prouvant qu'une extension n'est pas toujours un produit semi-direct. Le groupe des quaternions $\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ ne possède que des sous-groupes normaux [...]. Si N est un sous-groupe de $\mathbb{H}_8$, on a donc toujours la suite exacte

$$1 \longrightarrow N \longrightarrow \mathbb{H}_8 \longrightarrow \mathbb{H}_8/N \longrightarrow 1,$$

autrement dit $\mathbb{H}_8$ est une extension de n'importe lequel de ses sous-groupes N par le groupe quotient $\mathbb{H}_8/N$. Mais si N est un sous-groupe non trivial (donc d'ordre 2 ou 4), le groupe quotient $\mathbb{H}_8/N$ n'admet jamais de relèvement. En effet, si N est d'ordre 2 (c'est-à-dire si $N = \{1, -1\}$), $\mathbb{H}_8/N$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ [...]. Or, $\mathbb{H}_8$ n'a pas de sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ [...]. Le groupe quotient ne peut donc pas avoir de relèvement dans ce cas. De même, si N est d'ordre 4, N contient forcément -1, et le quotient $\mathbb{H}_8/N$ qui est d'ordre 2 ne peut avoir de relèvement puisque le seul élément d'ordre 2 est dans N.

Attention ! Il se peut que l'on ait écrit un groupe G comme l'extension d'un de ses sous-groupes normaux N par le groupe quotient G/N, et que G/N n'admette pas de relèvement ; *cela ne veut pas dire qu'il est impossible d'écrire G comme un produit semi-direct.* Peut-être qu'un autre sous-groupe normal N' (qui éventuellement est isomorphe à N) va donner, lui, une extension scindée et permettra de voir G comme un produit (semi-)direct...Pour illustrer ceci, prenons $G = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, et N le sous-groupe d'ordre 2 engendré par $(2,0)$. Alors G/N est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, et n'admet pas de relèvement [...]. Cependant, il est évident que G s'écrit comme un produit (semi-)direct de $\mathbb{Z}/2\mathbb{Z}$ par un autre groupe.

2.4 Quand un produit semi-direct est-il direct ?

Proposition 2.2 *Soient deux groupes N et H, φ un morphisme de H dans $\mathrm{Aut}(N)$, et G le produit semi-direct $N \rtimes_\varphi H$. On note $\bar{N}$ (respectivement $\bar{H}$) le sous-groupe de G constitué des éléments de la forme $(n,1)$, $n \in N$ (respectivement $(1,h)$, $h \in H$). Les propriétés suivantes sont équivalentes.*

1. *La loi de G est celle du produit direct de N et H,*

2. *φ est trivial, autrement dit $\varphi_h = \mathrm{Id}_N$ pour tout $h \in H$,*
3. *$\bar{H} \lhd G$,*
4. *les éléments de $\bar{N}$ commutent avec ceux de $\bar{H}$.*

Preuve — Laissée en exercice...

Une conséquence immédiate : si un groupe *abélien* est un produit semi-direct, c'est en fait un produit direct. En application, l'exercice qui suit présente un exemple bien classique de produit direct.

Exercice 2.3 (Lemme chinois) *Soient m et n deux entiers strictement positifs. Montrer que le groupe additif $\mathbb{Z}/mn\mathbb{Z}$ admet un unique sous-groupe N d'ordre n, et un unique sous-groupe H d'ordre m. À quelle condition H est-il un relèvement du groupe quotient $(\mathbb{Z}/mn\mathbb{Z})/N$? En déduire que $\mathbb{Z}/mn\mathbb{Z}$ est isomorphe au produit direct $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ si et seulement si m et n sont premiers entre eux.*

Mais on tire aussi de la proposition 2.2 un résultat plus fin : si un groupe G possède un sous-groupe normal N tel que G/N admette un relèvement H, avec de plus N ou H inclus dans le centralisateur de G, alors G s'identifie en fait au produit direct $N \times H$.

Exemple. Le groupe spécial orthogonal $SO(3,\mathbb{R})$ est un sous-groupe normal du groupe orthogonal $O(3,\mathbb{R})$, puisque c'est le noyau de det : $O(3,\mathbb{R}) \longrightarrow \{-1,1\}$. Il est facile de trouver un relèvement du groupe quotient (qui ici s'identifie à $\{-1,1\}$) contenu dans le centralisateur : il suffit de prendre $H = \{-\mathrm{Id}_{\mathbb{R}^3}, \mathrm{Id}_{\mathbb{R}^3}\}$. Le groupe $O(n,\mathbb{R})$ est donc isomorphe au produit direct $SO(3,\mathbb{R}) \times \{-1,1\}$. Cette démonstration se généralise clairement à $O(2n+1,\mathbb{R})$, mais le résultat n'est plus vrai en dimension paire. Ainsi dans $O(2,\mathbb{R})$, il est toujours possible de trouver un relèvement du groupe quotient $O(2,\mathbb{R})/SO(2,\mathbb{R})$ en prenant le sous-groupe H engendré par une réflexion quelconque. Mais un tel relèvement ne donnera jamais un produit direct car une réflexion ne commute jamais avec toutes les rotations [...].

Exercice 2.4 *On note $\mathbb{U}$ le groupe multiplicatif des complexes de module 1. Soit $n \geq 2$. Montrer qu'il n'existe pas de sous-groupe H de $\mathbb{U}$ tel que $z \longmapsto z^n$ soit un isomorphisme de H sur $\mathbb{U}$.*

En déduire que $\mathbb{U}$ n'est pas isomorphe à un produit semi-direct d'un groupe cyclique de cardinal supérieur ou égal à deux avec un autre de ses sous-groupes.

En déduire aussi que pour $n \geq 2$, $GL(n,\mathbb{C})$ n'est pas produit direct de $SL(n,\mathbb{C})$ avec un autre de ses sous-groupes.

Attention ! Un produit semi-direct non trivial de deux groupes N et H peut parfois être isomorphe au produit *direct* de N par H, comme on le voit sur l'exemple suivant : prenons $G \overset{\text{déf}}{=} \mathbf{S}_3 \times \mathbb{Z}/2\mathbb{Z}$, et soit N le sous-groupe des éléments de la forme $(\sigma, 0)$, $\sigma \in \mathbf{S}_3$. Alors N est un sous-groupe normal de G, et le quotient G/N isomorphe à $\mathbb{Z}/2\mathbb{Z}$ admet un relèvement évident : le sous-groupe $H_1 \overset{\text{déf}}{=} \{(\mathrm{Id},0),(\mathrm{Id},1)\}$ (qui donne G comme produit direct). Mais on peut aussi trouver un autre relèvement de G/N, en prenant une transposition τ, et en considérant le sous-groupe $H_2 \overset{\text{déf}}{=} \{(\tau,1),(\mathrm{Id},0)\}$. Cette fois, il n'y a plus commutation des éléments de H_2 avec ceux de N, et donc G est aussi isomorphe à un produit semi-direct non trivial de N par H_2 (autrement dit de $\mathbf{S}_3$ par $\mathbb{Z}/2\mathbb{Z}$).

Exercice 2.5 *Les produits semi-directs présentés comme exemples au paragraphe précédent* ($\mathbf{S}_n \simeq \mathbf{A}_n \rtimes \{-1, 1\}$ *et* $D_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$) *peuvent-ils être des produits directs ?*

Références

[1] Alain BOUVIER et Denis RICHARD. *Groupes – observation, théorie, pratique.* Hermann, 1994.

[2] Josette CALAIS. *Éléments de Théorie des Groupes.* Puf, 1998.

[3] Daniel PERRIN. *Cours d'Algèbre.* Ellipses, 1996.