Suites exactes et produits de groupes

Ce document prolonge celui sur les ensembles quotients.
On y présente une méthode pour « casser » (ou « dévisser ») un groupe en plus petits groupes dont l'étude est moins difficile.
Pour cela, on réalise une première approche sur les espaces vectoriels dont la manipulation est plus intuitive, avant d'appliquer cette méthode aux groupes.

Prérequis : Espaces quotients et diagrammes commutatifs tels qu'introduits dans le document sur les espaces quotients.
Notions élémentaires sur les espaces vectoriels et espaces affines, applications linéaires en dimension finie, théorème du rang, projecteurs.

Notation : Dans tout ce document $E \approx F$ indique que E et F sont isomorphes (pour la structure considérée : espace vectoriel ou groupe).

Avertissement : *Comme pour les documents précédents, on cherche à découvrir les notions à partir d'analogies et par l'intuition. Le chemin est donc long avant d'accéder aux définitions et théorèmes finaux. Ainsi, tout ce chapitre tient en seulement deux pages dans le célèbre* Cours d'Algèbre *de D. Perrin.*

Ce cours est loin d'être parfait et je suis ouvert aux commentaires (constructifs).

1 Exemple de l'espace vectoriel

A Nouvelle interprétation du théorème du rang en algèbre linéaire

Nous revisitons ici la preuve du théorème du rang déjà vue en algèbre linéaire et nons montrerons qu'elle procède de la même idée que les quotients de groupes.

On considère donc deux espaces vectoriels E et F, avec E de dimension finie, et $f \in \mathscr{L}(E, F)$.
On sait que toute application linéaire de $\mathscr{L}(E, F)$ est un morphisme[1] entre les groupes E et F et on peut donc s'intéresser au diagramme commutatif :

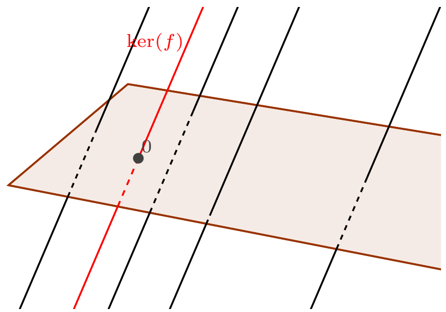
$$\begin{tikzcd} E \arrow[r, "f"] \arrow[d, "s"'] & F \\ E/\ker(f) \arrow[r, "\widetilde{f}"'] & \operatorname{Im}(f) \arrow[u, "i"'] \end{tikzcd}$$

$\widetilde{f}$ est un isomorphisme de groupes.
Mais $E/\ker(f)$ qui est un groupe, peut aussi hériter d'une structure d'espace vectoriel (sur le même corps que E), $E/\ker(f)$ est alors un espace vectoriel isomorphe à $\operatorname{Im}(f)$.

Contrairement aux groupes finis, la notion intéressante ici n'est plus le cardinal mais la dimension et nous allons donc la déterminer pour $E/\ker(f)$.

On remarque que quotienter E par $\ker(f)$ revient à identifier deux objets dont la différence est dans le noyau. Ainsi les classes d'équivalences sont simplement les sous-espaces affines dirigés par le noyau.

Prenons l'exemple d'un noyau de dimension 1.
Les classes d'équivalence de $E/\ker(f)$ sont exactement les droites affines parallèles au noyau.



Chacune de ces droites représente un élément de $\operatorname{Im}(f)$. On décide donc de désigner chaque droite à l'aide d'un unique représentant. Pour cela, on choisit un hyperplan H

1. On rappelle que pour un espace vectoriel E, $(E, +)$ est un groupe. Si $f \in \mathscr{L}(E, F)$, alors pour tous $x, y \in E$, $f(x + y) = f(x) + f(y)$: c'est un morphisme de groupes.

supplémentaire à $\ker(f)$, qui coupe chaque droite en un unique point. Ce point fait alors office de représentant unique pour la droite :

$$\text{on peut identifier } E/\ker(f) \text{ et } H.$$

Cette identification revient à considérer p, la projection sur H parallèlement à $\ker(f)$. Elle décrit parfaitement la relation d'équivalence car

$$\forall (x,\, y) \in E^2,\, x - y \in \ker(f) \iff p(x) = p(y).$$

Bien évidemment, ce procédé n'est pas valable que pour les droites, mais quelle que soit la dimension de $\ker(f)$.

$E/\ker(f)$ et H sont alors isomorphes et donc de même dimension.
On trouve ainsi $\mathrm{rg}\,(f) = \dim\,(E/\ker(f)) = \dim(H)$.
Or $H \oplus \ker(f) = E$, donc par égalité des dimensions, on obtient le **théorème du rang** :

$$\mathrm{rg}\,(f) + \dim\,(\ker(f)) = \dim(E).$$

En résumé : La factorisation de l'application linéaire conduit à la même preuve que celle du chapitre sur les applications linéaires : à travers l'espace quotient, on choisit un supplémentaire H du noyau et on décompose ensuite chaque vecteur de manière unique sur cette somme directe $\ker(f) \oplus H$.

B Connaître E par la somme directe

Ici, nous inversons la perspective : l'objet qu'on souhaite étudier n'est plus l'application f mais l'espace E lui-même. On sait que :

$$E = \ker(f) \oplus H.$$

Ainsi, la connaissance de $\ker(f)$ et de H permet de reconstituer E.

$$E = \{x + h,\, (x,\, h) \in \ker(f) \times H\}\,.$$

L'étude de $\ker(f)$ et H, qui sont des espaces de plus petites dimensions, donne E par somme directe. On a « cassé » E en deux sous-espaces.

Un isomorphisme :
La décomposition précédente se traduit par l'isomorphisme

$$\varphi\,:\, \left\{ \begin{array}{ccc} \ker(f) \times H & \to & E \\ (x,\, h) & \mapsto & x + h. \end{array} \right.$$

Remarque : φ est bien une application linéaire.
En effet, pour tous $(x,\, h),\, (x',\, h') \in \ker(f) \times H$, et pour tout $\lambda \in \mathbf{K}$:
$\varphi\,((x,\, h) + \lambda(x',\, h)) = \varphi(x + \lambda x',\, h + \lambda h') = x + \lambda x' + h + \lambda h' = \varphi(x,\, h) + \lambda\varphi(x',\, h')$.
L'injectivité vient de l'unicité de la décomposition sur la somme directe, et la surjectivité de l'existence d'une telle décomposition.

Sortir de E :
Ce qui est fait n'est pas encore satisfaisant. En effet, si on ne connaît pas E, alors il y a peu de chances que l'on connaisse ses sous-espaces vectoriels $\ker(f)$ et H.
L'idée est donc de retrouver E à partir d'espaces vectoriels « extérieurs ».
Pour cela, on remplace H par $\mathrm{Im}\,(f) = F'$ qui lui est isomorphe et on crée un isomorphisme entre $\ker(f)$ et un autre espace :

$$\phi\;:N \to \ker(f).$$

Ainsi, on pourra écrire plus simplement

$$E \approx N \times F'.$$

Comme ϕ n'est pas très pratique à manipuler en l'état, on complète son espace d'arrivée ce qui donne $i\;:N \to E$ qui reste injective, mais n'est plus surjective en général. On conserve $i(N) = \ker(f)$.
On obtient :

$$N \xrightarrow{\;i\;} E \xrightarrow{\;f\;} F'$$

avec

1. i injective,
2. $\mathrm{Im}\,(i) = \ker(f)$,
3. f surjective.

On appelle cela une *suite exacte* (courte).
Cette suite donne une « décomposition » de E en produit de deux espaces vectoriels plus simples.

Cette notion de *suite exacte* est très efficace et mérite qu'on s'y attarde.

C Suite exacte

Définition 1.1 *(Suite exacte)*

Soient $E_1,\, E_2,\, \cdots,\, E_n$ des espaces vectoriels et $\forall i \in [\![1,\, n-1]\!],\, f_i \in \mathscr{L}\,(E_i,\, E_{i+1})$.
La suite

$$E_1 \xrightarrow{f_1} E_2 \xrightarrow{f_2} E_3 \xrightarrow{f_3} \cdots\cdots \xrightarrow{f_{n-2}} E_{n-1} \xrightarrow{f_{n-1}} E_n$$

est **exacte** si

$$\forall i \in [\![1,\, n-2]\!],\, \mathrm{Im}\,(f_i) = \ker\,(f_{i+1})\,.$$

C'est-à-dire si l'image de chaque application linéaire est égale au noyau de celle qui suit.

Exemple *(Application injective)*

Pour écrire qu'une application est injective, il suffit d'indiquer que son noyau est réduit à $\{0\}$.
On fait donc précéder l'application d'une autre dont on sait que l'image est nécessairement $\{0\}$:

$$\{0\} \xrightarrow{i_1} E \xrightarrow{f} F.$$

Exemple *(Application surjective)*

Pour écrire qu'une application est surjective, on la fait suivre d'une application dont le noyau est l'espace tout entier : l'application nulle.
On écrit

$$E \xrightarrow{f} F \xrightarrow{s_2} \{0\}.$$

Exemple *(Suite exacte courte)*

Pour reprendre l'exemple de la partie précédente, on obtient la suite exacte *courte* :

$$\{0\} \longrightarrow N \xrightarrow{i} E \xrightarrow{f} F \longrightarrow \{0\}.$$

L'injectivité de i et la surjectivité de f sont codées par les flèches.

2 Décomposer un groupe en produit direct

Nous allons faire la même chose avec les groupes.

Notations :
Nous utiliserons la notation multiplicative ; l'élément neutre est donc 1.
Dans les suites exactes, on notera[2] abusivement 1 au lieu de $\{1\}$ pour le singleton correspondant.

A Suite exacte courte et produit direct de groupes

Définition 2.1 *(Extension)*

Soit G un groupe (multiplicatif).
On considère la suite exacte courte de morphismes

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{f} Q \longrightarrow 1.$$

On dit que G est une **extension** de N par Q.

Nous verrons à l'aide des produits directs et semi-directs comment traduire concrètement cette extension dans de nombreux cas.

2. Cette notation se conforme à l'usage.

Remarque : Certains auteurs disent que G est une extension « de N par Q », et d'autres « de Q par N ».

Donnons également la définition du produit direct de deux groupes. C'est la même qu'avec les espaces vectoriels, mais on utilise ici la notation multiplicative.

Définition 2.2 *(Produit direct)*

Soient $(G_1, \star_1)$ et $(G_2, \star_2)$ deux groupes.
On définit alors le produit direct $(G_1 \times G_2, \star)$ avec la loi :

$$\forall (g_1, g_2) \in G_1 \times G_2, \forall (g_1', g_2') \in G_1 \times G_2,$$
$$(g_1, g_2) \star (g_1', g_2') = (g_1 \star_1 g_1', g_2 \star_2 g_2').$$

On vérifie aisément que $(G_1 \times G_2, \star)$ est un groupe.
Dans la suite, toutes les lois seront notées de la même façon par $g_1 g_2$ ou $g_1.g_2$ selon ce qui est le plus lisible.

B Présentation de la démarche

Notre but est de « dévisser » un groupe G en produit direct de deux groupes.
Dans un premier temps, on cherche des **conditions suffisantes**.

En nous inspirant de ce qui a été fait avec les espaces vectoriels, nous proposons trois approches de difficulté croissante :

1. On écrit G comme produit direct de deux sous-groupes par analogie avec les espaces vectoriels supplémentaires.
   Contrairement aux espaces vectoriels on a besoin de certaines hypothèses sur G car on ne suppose plus la commutativité de la loi de groupe.

2. On décompose ensuite G à l'aide d'un projecteur (dont il faudra trouver une bonne définition).

3. Enfin on utilise une suite exacte courte pour écrire G comme produit direct de groupes externes.

Nous montrerons enfin que ces trois propriétés sont équivalentes et qu'elles sont **nécessaires** pour dévisser un groupe en produit direct.

En conclusion :
Nous aurons des conditions nécessaires et suffisantes pour qu'un groupe se dévisse en produit direct.
Comme ces propriétés ne sont pas toujours vérifiées, la partie suivante les affaiblira un peu pour obtenir la notion de produit semi-direct.

C Produit direct interne

On cherche l'analogue de la somme directe pour reconstruire G à partir de ses propres sous-groupes.
On part donc d'un sous-groupe $K \subset G$ et on lui cherche un **complément** (l'équivalent du supplémentaire pour les espaces vectoriels).

On considère H tel que

1. $H \cap K = \{1\}$,
2. $KH = \{kh,\, k \in K,\, h \in H\} = G$.

Sous réserve de l'existence de tels sous-groupes $K\&H$, on définit

$$\varphi : \left\{ \begin{array}{ccc} K \times H & \to & G \\ (k,\, h) & \mapsto & kh. \end{array} \right.$$

Vérifions s'il s'agit d'un morphisme de groupes.
Soient $(k_1,\, h_1)$ et $(k_2,\, h_2)$ deux éléments de $K \times H$.
D'une part : $\varphi\left((k_1,\, h_1).(k_2,\, h_2) \right) = \varphi\left(k_1k_2,\, h_1h_2\right) = k_1k_2h_1h_2$.
D'autre part : $\varphi\left(k_1,\, h_1\right) . \varphi\left(k_2,\, h_2\right) = k_1h_1k_2h_2$.
Si le groupe est commutatif, on a l'égalité, mais sinon il n'y a aucune raison.

Voyons à quelles conditions φ est un morphisme : $\forall (k_1,\, h_1),\, (k_2,\, h_2) \in K \times H$,

$$\begin{aligned} \varphi\left((k_1,\, h_1).(k_2,\, h_2)\right) = \varphi\left(k_1,\, h_1\right).\varphi\left(k_2,\, h_2\right) &\iff k_1k_2h_1h_2 = k_1h_1k_2h_2 \\ &\iff k_2h_1 = h_1k_2. \end{aligned}$$

Ainsi, il est nécessaire et suffisant que les éléments de H commutent avec ceux de K.

En supposant cette condition vérifiée, montrons que φ est un isomorphisme.

Injectivité : $\forall (k,\, h) \in \ker(\varphi)$, $\varphi(k,\, h) = 1$ donc $kh = 1$ donc $k = h^{-1}$.
Ainsi $k \in K \cap H = \{1\}$, donc $k = 1$ et $h^{-1} = k = 1$
ce qui prouve que $\ker(\varphi) \subset \{(1,\, 1)\}$. L'autre inclusion est évidente, donc φ est injective.
La *surjectivité* est donnée par l'hypothèse $KH = G$.

On obtient donc le théorème :

Propriété 2.3

Soit G un groupe. Si K et H sont deux sous-groupe de G tels que

1. $H \cap K = \{1\}$,
2. $KH = \{kh,\, k \in K,\, h \in H\} = G$,
3. Les éléments de H commutent avec ceux de K.

alors $G \approx K \times H$.

Remarque : Par la commutativité des éléments de H avec ceux de K, on voit que les deux sous-groupes jouent des rôles symétriques et que l'on a donc

$$K \times H \approx H \times K.$$

On peut reformuler la condition de commutativité à l'aide de la notion de normalisateur.

Définition 2.4 *(Normalisateur)*

Soit X une partie d'un groupe G. Le **normalisateur** de X est défini par

$$\mathcal{N}_X = \left\{g \in G,\, gXg^{-1} = X\right\}.$$

On dit que H normalise X si $H \subset \mathcal{N}_X$ c'est-à-dire si $\forall h \in H,\, hXh^{-1} = X$.

Exemple

Montrer que $H \triangleleft G$ si, et seulement si $\mathcal{N}_H = G$.
Solution :
(sens réciproque) évident.
(sens direct)
Par définition d'un sous-groupe distingué, on sait que $\forall g \in G,\, gHg^{-1} \subset H$.
La question est ici de montrer l'autre inclusion.
Pour $g \in G$, on pose

$$f_g : \left\{ \begin{array}{ccc} H & \to & H \\ x & \mapsto & gxg^{-1}. \end{array} \right.$$

f_g est un endomorphisme (car $H \triangleleft G$) d'application réciproque $f_{g^{-1}}$.
C'est donc un isomorphsime, ce qui prouve la surjectivité.
Ainsi $\operatorname{Im}\left(f_g\right) = H$ donc $gHg^{-1} = H$. Ainsi $\mathcal{N}_H = G$.

Exercice

1. Montrer que le normalisateur d'un sous-ensemble quelconque de G est un sous-groupe de G.
2. Pour H sous-groupe de G, montrer que $\mathcal{N}_H$ est le plus grand sous-groupe de G dans lequel H est distingué.

Propriété 2.5

Si K et H sont deux sous-groupes de G tels que $K \cap H = \{1\}$ alors
Les éléments de H commutent avec ceux de K si, et seulement si H et K se normalisent mutuellement.

Preuve

Il est évident que la commutativité donne la normalisation.
Pour le sens réciproque : $\forall (k,\, h) \in K \times H$

$$kh = hk \iff khk^{-1}h^{-1} = 1.$$

Si K normalise H alors $khk^{-1} \in H$, donc $khk^{-1}h^{-1} \in H$.
Par symétrie, comme H normalise K on obtient également $khk^{-1}h^{-1} \in K$.
Or $K \cap H = \{1\}$, donc $khk^{-1}h^{-1} = 1$ ce qui prouve la commutativité. ■

On obtient finalement le théorème :

Théorème 2.6

Soit G un groupe. Si K et H sont deux sous-groupes de G tels que

1. $K \cap H = \{1\}$,
2. $KH = \{kh,\ k \in K,\ h \in H\} = G$,
3. H et K se normalisent mutuellement,

alors $G \approx K \times H$.

Remarque : On voit en particulier que la dernière condition est toujours vérifiée quand $H \triangleleft G$ et $K \triangleleft G$.
La décomposition précédente peut alors se traduire par une suite exacte courte :

$$1 \longrightarrow K \xrightarrow{i} G = HK \xrightarrow{f} H \longrightarrow 1.$$

Pour cela, on a posé $i : \left\{ \begin{array}{ccc} K & \to & G \\ k & \mapsto & k = 1.k \end{array} \right.$ et $f : \left\{ \begin{array}{ccc} HK & \to & H \\ hk & \mapsto & h. \end{array} \right.$

On voit que la décomposition sur HK est unique (exercice) ce qui justifie que f est correctement définie, et on montre alors aisément que f est un morphisme de groupes.

Exercice

Peut-être sauté en première lecture.

Dans cet exercice, on veut montrer que tout produit direct peut être interprété à l'aide du théorème précédent.
On dispose donc de deux groupes K et H et on s'intéresse à leur produit direct $G = K \times H$.
On veut alors dévisser à nouveau G à partir du théorème précédent. Le problème est qu'on ne peut pas utiliser directement K et H pour le faire car ils ne sont pas des sous-groupes de G à proprement parler (G est constitué de couples).
L'idée est alors d'identifier K avec les couples dont on ne considère que le premier élément, et H avec les couples pour lesquels on ne considère que le deuxième élément.
Pour cela, on complète chaque couple par l'élément neutre de l'autre groupe.
Nous ferons la même chose plus loin avec le produit semi-direct.

Voici comment cela se traduit :
Soient K et H deux groupes.
On note $\overline{K} = \{(k,\ 1_H),\ k \in K\}$ et $\overline{H} = \{(1_H,\ h),\ h \in H\}$.

1. Montrer que $\overline{K}$ et $\overline{H}$ sont deux sous-groupes de $K \times H$.
2. Montrer que $\overline{K} \approx K$ et $\overline{H} \approx H$.
3. Montrer $\overline{K}$ et $\overline{H}$ vérifient les hypothèses du théorème précédent et en déduire que $K \times H \approx \overline{K} \times \overline{H}$.

Solution :

1. On pose l'application
$$i : \left\{ \begin{array}{ccc} K & \to & K \times H \\ k & \mapsto & (k,\ 1_H). \end{array} \right.$$
$\forall (k_1,\ k_2) \in K^2$,
$$i(k_1k_2) = (k_1k_2,\ 1_H) = (k_1,\ 1_H).(k_2,\ 1_H) = i(k_1)i(k_2).$$
Donc i est un morphisme de groupes d'image $\overline{K}$. Ceci justifie que $\overline{K}$ est un sous-groupe de $K \times H$. On fait de même avec $\overline{H}$.
2. $\ker(i) = \{1\}$ donc i est injectif. Ainsi i réalise un isomorphisme de K sur $\overline{K}$.
On fait de même avec H, ce qui prouve que $K \approx \overline{K}$ et $H \approx \overline{H}$.
3. $\overline{K} \cap \overline{H} = \{(1_K,\ 1_H)\} = \{1_{K \times H}\}$ et
$$\overline{K}\,\overline{H} = \{(k,\ 1_H).(1_K,\ h),\ (k,\ h) \in K \times H\} = \{(k,\ h),\ (k,\ h) \in K \times H\} = K \times H.$$
Enfin $\forall (k,\ 1_H) \in \overline{K}$, $\forall (1_K,\ h) \in \overline{H}$, $(k,\ 1_H).(1_K,\ h) = (k,\ h) = (1_K,\ h).(k,\ 1_H)$.
Ainsi les éléments de K commutent avec les éléments de H.
D'après le théorème précédent, on retrouve donc bien que
$$\overline{K} \times \overline{H} \approx K \times H.$$

D Avec un projecteur

On peut continuer l'analogie avec les espaces vectoriels pour lesquels la donnée d'un projecteur permettait d'obtenir H. Reprenons cette idée sur les groupes.

Définition 2.7 *(projecteur)*

Soit G un groupe et p un endomorphisme de G.
p est un **projecteur** si, et seulement si

1. $p \circ p = p$
2. tout élément de l'image commute avec tout élément du noyau.

Explications

On retrouve la définition du projecteur d'espaces vectoriels, mais, la loi du groupe n'étant pas toujours commutative, on a besoin de rajouter une condition de commutativité essentielle pour obtenir le produit direct.
La nécessité de cette seconde condition apparaît clairement dans la preuve qui suit, et son oubli conduira plus loin au produit semi-direct.

Théorème 2.8

Soit G un groupe et p un projecteur de G.
G est peut se décomposer en un produit direct

$$G \approx \ker(p) \times \mathrm{Im}\,(p) \approx \ker(p) \times (G/\ker(p)).$$

Preuve

On cherche à se ramener au cas précédent du produit direct interne.
On conseille de faire cette preuve en exercice tant elle est semblable à celle sur les espaces vectoriels.
$\ker(p)$ et $\mathrm{Im}\,(p)$ sont deux sous-groupes de G.

- Soit $y \in \ker(p) \cap \mathrm{Im}\,(p)$, on peut donc écrire $y = p(x)$ avec $x \in G$.
  Or $y \in \ker(p)$, donc $1 = p(y) = p \circ p(x) = p(x) = y$. Ainsi $\ker(p) \cap \mathrm{Im}\,(p) \subset \{1\}$ et l'inclusion réciproque est évidente.
  $$\ker(f) \cap \mathrm{Im}\,(f) = \{1\}.$$
- Soit $x \in G$. On peut écrire $g = p(x)\,(p(x))^{-1}\,x$.
  Or $p\left(p(x)^{-1}x\right) = p\left(p(x)^{-1}\right)p(x) = (p \circ p(x))^{-1}\,p(x) = (p(x))^{-1}\,p(x) = 1$.
  On a donc bien $(p(x))^{-1}\,x \in \ker(p)$ et $p(x) \in \mathrm{Im}\,(p)$ ce qui donne donc $G \subset HK$. L'autre inclusion est évidente ainsi
  $$G = HK.$$
- Enfin les normalisations mutuelles entre image et noyau sont données par la condition de commutativité utilisée pour définir le projecteur p.

Le deuxième isomorphisme du théorème : $\ker(p) \times \mathrm{Im}\,(p) \approx \ker(p) \times (G/\ker(p))$ est donné par la factorisation du morphisme comme cela avait été présenté dans le document sur les espaces quotients. ■

E Produit direct externe

Comme pour les espaces vectoriels, on souhaite désormais ne faire appel qu'à des groupes *extérieurs* à G.
On part donc d'une suite exacte courte :

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{f} Q \longrightarrow 1.$$

On veut alors avoir $G \approx N \times Q$.
D'un point de vue interne à G, l'analogie avec les espaces vectoriels demande l'existence d'un **complément** de $i(N)$ dans G :

- l'existence d'un sous-groupe H (isomorphe à Q) tel que $G = i(N)H$
- et vérifiant que $i(N) \cap H = \{1\}$
- avec normalisation mutuelle des deux sous-espaces.

Dans ce cas, chaque élément $g \in G$, se décompose de façon unique sous la forme $g = yz$ avec $y \in i(N)$ et $z \in H$ (et les deux commutent).
Pour $g = yz$, on note alors x l'unique antécédent de y par i et on définit l'application $r\ : G \to N$ telle que $r(g) = x$.
La construction du produit direct est alors possible sous réserve que r *soit lui-même un morphisme de groupes.*
On obtient ce qu'on appelle une *retraction* (on a retracté G dans N, après l'avoir « dilaté » avec l'injection).

Définition 2.9 *(retraction)*

Soient N et G deux groupes et $i\ : N \to G$ un morphisme de groupe.
Le morphisme r est une **retraction** de i (ou un **scindage à gauche**) si $r \circ i = \mathrm{Id}_N$.

Pour les applications, l'injectivité et l'existence d'un inverse à gauche sont équivalentes, mais pour les morphismes, on impose que la retraction soit également un morphisme, ce qui n'est pas le cas de tout inverse à gauche.
L'injectivité est donc nécessaire à l'existence d'une retraction, mais non suffisante.

Propriété 2.10

Si $i\ : N \to G$ admet une retraction, alors i est injective.
La réciproque est fausse.

Exemple *(Peut être sauté en première lecture)*

On veut montrer qu'un morphisme injectif $i\ : N \to G$ n'admet pas nécessairement de retraction.
Reprenons l'exemple du groupe des isométries du triangle S_3 vu dans le document d'introduction aux groupes (c'est aussi le groupe symétrique d'ordre 3).
On avait la table de Cayley :

$\circ$	Id	R	R^2	τ_A	τ_B	τ_C
Id	Id	R	R^2	τ_A	τ_B	τ_C
R	R	R^2	Id	τ_B	τ_C	τ_A
R^2	R^2	Id	R	τ_C	τ_A	τ_B
τ_A	τ_A	τ_C	τ_B	Id	R^2	R
τ_B	τ_B	τ_A	τ_C	R	Id	R^2
τ_C	τ_C	τ_B	τ_A	R^2	R	Id

On construit l'application $i\ : \mathbf{U}_3 \to S_3$ et qui à chaque racine 3ème de l'unité renvoie sa rotation correspondante.
i est bien un morphisme de groupes injectif.
Supposons par l'absurde qu'il admet une retraction r, alors

$$1 = r(\mathrm{Id}) = r\left(\tau_A^2\right) = (r(\tau_A))^2.$$

Or, 1 est la seule racine carrée de 1 dans $\mathbf{U}_3$, donc $r(\tau_A) = 1$.
On obtient de même que $r(\tau_C) = 1$.
Ainsi $r(R) = 1 \times r(R) = r(\tau_A)\,r(R) = r(\tau_A \circ R) = r(\tau_C) = 1$ ce qui est manifestement absurde.

Théorème 2.11 *(retraction et produit direct)*

On considère un groupe G et la suite exacte courte suivante :

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{f} Q \longrightarrow 1.$$

Si i admet une retraction r, alors

$$G \approx N \times Q.$$

En outre, en identifiant à isomorphisme près N avec $i(N)$,

$$\text{on a } N \lhd G \text{ et } Q \approx G/N.$$

Preuve

On construit φ par

$$\varphi : \left\{ \begin{array}{lcl} G & \to & N \times Q \\ g & \mapsto & (r(g),\, f\,(g)) \,. \end{array} \right.$$

φ est clairement un morphisme de groupes car r et f en sont.
Injectivité :
Soit $g \in \ker(\varphi)$, alors $g \in \ker(f) = \operatorname{Im}(i)$.
Donc il existe $x \in N$ tel que $i(x) = g$.
Or $r(g) = 1$, donc $1 = r \circ i(x) = x$ car $r \circ i = \operatorname{Id}_N$.
Ainsi $g = i(1) = 1$, ce qui prouve que $\ker(\varphi) \subset \{1\}$ et l'autre inclusion est évidente.
φ est donc bien injective.
Surjectivité :
Dans le cas de groupes finis, on peut facilement conclure par des arguments de cardinaux, mais nous allons ici faire le cas général.

Recherche au brouillon :
Soit $(x,\, y) \in N \times Q$.
On veut avoir $g \in G$ tel que $r(g) = x$ et $f(g) = y$.
Pour satisfaire la condition $f(g) = y$, on sait déjà, par surjectivité de f, qu'il existe $g_0 \in G$ tel que $f(g_0) = y$.
On cherche donc g sous la forme $g = g_0 \times z$ avec $z \in \ker(f) = \operatorname{Im}(i)$.
Donc on veut écrire g sous la forme $g = g_0 i(x_0)$.
D'un autre côté, la condition $r(g) = x$ nous pousse à chercher un candidat sous la forme $g = g_k \times i(x)$ avec $g_k \in \ker(r)$.
On essaie donc $g = g_0 i(x)$ et on obtient $r(g) = r(g_0) r\,(i(x)) = r(g_0)x$.
Pour annuler $r(g_0)$, il suffit donc de modifier en utilisant $r \circ i = \operatorname{Id}$:

$$g = (i \circ r(g_0))^{-1} g_0 i(x).$$

On trouve alors les bons résultats.

Rédaction formelle :
Soit $(x,\, y) \in N \times Q$.
f surjective de G sur Q donc il existe $g_0 \in G$ tel que $f(g_0) = y$.
On pose alors $g = (i \circ r(g_0))^{-1}\, g_0 i(x) \in G$.
$r \circ i = \operatorname{Id}_N$ donc

$$r(g) = r\left((i \circ r(g_0))^{-1}\right) r(g_0)(r \circ i)(x) = (r \circ i \circ r(g_0))^{-1}\, r(g_0)x = x.$$

De plus $i \circ r(g_0) \in \operatorname{Im}(i) = \ker(f)$ car la suite est exacte.
Or $\ker(f)$ est un groupe, donc stable par passage à l'inverse ce qui donne $(i \circ r(g_0))^{-1} \in \ker(f)$. On a également $i(x) \in \ker(f)$, ainsi

$$f(g) = 1 \times f(g_0) \times 1 = g.$$

On a donc bien trouvé un antécédent de $(x,\, y)$ dans G par φ, ce qui prouve la surjectivité de φ.

$$G \approx N \times Q.$$

Par ailleurs, on a vu dans le document sur les quotients qu'il est toujours possible de quotienter par un noyau : $\ker(f) \lhd G$.
Donc, la factorisation du morphisme f donne bien $Q \approx G/\ker(f) \approx G/i(N)$. ■

Définition 2.12

Une suite exacte courte

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{f} Q \longrightarrow 1$$

pour laquelle i admet une retraction est dite **scindée à gauche.**
Une telle suite assure le dévissage de G en $G \approx N \times Q$.

F Comparaison des trois approches, caractère nécessaire

Les trois approches précédentes sont équivalentes (et en particulier nécessaires au dévissage en produit direct).

Théorème 2.13 *(Condition nécessaire et suffisante du produit direct)*

Soit G un groupe.
Les propriétés suivantes sont équivalentes.

1. G est isomorphe à un produit direct.
2. G admet une suite exacte courte scindée à gauche

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{f} Q \longrightarrow 1.$$

3. G admet un projecteur p.
4. G admet deux sous-groupes H et K qui vérifient
   (a) $H \cap K = \{1\}$,
   (b) $KH = G$,
   (c) H et K se normalisent mutuellement.

Remarque : Le caractère non trivial d'une propriété revient à celles des autres.
Par exemple, il est toujours possible d'écrire $G \approx G \times \{1\}$ et de construire la suite

exacte correspondante

$$1 \longrightarrow G \xrightarrow{i} G \xrightarrow{f} \{1\} \longrightarrow 1.$$

Preuve

- Montrons que (1) $\Rightarrow$ (2).
  On suppose que $G \approx H \times K$, on note donc φ un isomorphisme :
  $$\varphi : \left\{ \begin{array}{lll} G & \to & H \times K \\ g & \mapsto & \varphi(g) = (\varphi_1(g),\, \varphi_2(g))\,. \end{array} \right.$$
  On construit alors la suite exacte courte
  $$1 \longrightarrow K \xrightarrow{i} G \xrightarrow{\varphi_1} H \longrightarrow 1$$
  en posant : $i \ : k \mapsto \varphi^{-1}(1,\, k)$ qui est clairement injective et admet φ_2 comme retraction.
- Montrons (1) $\Rightarrow$ (3).
  On considère à nouveau
  $$\varphi : \left\{ \begin{array}{lll} G & \to & H \times K \\ g & \mapsto & \varphi(g) = (\varphi_1(g),\, \varphi_2(g))\,. \end{array} \right.$$
  On pose naturellement[3] $\forall x \in G$, $p(x) = \varphi^{-1}(\varphi_1(x),\, 1)\,.$
  Il est clair que p est un endomorphisme du groupe G et un calcul immédiat montre que $p^2 = p$.
  Montrons que les éléments du noyau commutent avec ceux de l'image.
  Soit $(x,\, y) \in \ker(p) \times \mathrm{Im}\,(p)\,.$
  $p(x) = 1$, donc $\varphi^{-1}(\varphi_1(x),\, 1) = 1$ et en composant par φ, on obtient
  $(\varphi_1(x),\, 1) = \varphi(1) = (1,\, 1)$, donc $\varphi_1(x) = 1$.
  $y \in \mathrm{Im}\,(p)$ donc il existe $z \in G$ tel que $y = p(z) = \varphi^{-1}(\varphi_1(z),\, 1)$.
  On obtient donc $\varphi(y) = (\varphi_1(z),\, 1)\,.$
  Ainsi
  $$\begin{aligned} \varphi(xy) = \varphi(x)\varphi(y) &= (1,\, \varphi_2(x)) \times (\varphi_1(z),\, 1) \\ &= (\varphi_1(z),\, \varphi_2(x)) \\ &= (\varphi_1(z),\, 1) \times (1,\, \varphi_2(x)) \\ &= \varphi(y)\varphi(x) \\ &= \varphi(yx). \end{aligned}$$
  Or φ est bijective, donc $xy = yx$ ce qui achève la preuve.
- On a déjà vu que (2) $\Rightarrow$ (1) et que (3) $\Rightarrow$ (4) $\Rightarrow$ (1).

Ainsi on a prouvé l'équivalence entre toutes les propriétés. ■

3 Le produit semi-direct interne

A Définition du produit semi-direct

Dans la construction du produit direct interne, la condition la moins naturelle était la commutativité entre les éléments de K et ceux de H, qu'on avait traduite par les normalisateurs.
Dans le cas d'un groupe abélien (commutatif), cette hypothèse est toujours vérifiée.
Mais dans le cas général, elle peut être mise en défaut ce qui nous conduit à trouver une « version faible » du produit direct dans laquelle on enlève la condition de commutativité. On l'appelera produit *semi-direct.*

On considère un groupe G et deux sous-groupes H et K qui vérifient

1. $H \cap K = \{1\}\,,$
2. $KH = G.$

Comme on souhaitera écrire ce produit avec une suite exacte, l'un des deux sous-groupe sera un noyau donc distingué dans G.
On rajoute donc la condition :

$$K \lhd G.$$

Cela reste plus faible que la normalisation mutuelle : seul H est supposé normaliser K et non plus l'inverse.

Sous réserve de l'existence de tels sous-groupes K et H, on définit comme à la page 4, l'application :

$$\varphi : \left\{ \begin{array}{lll} K \times H & \to & G \\ (K,\, H) & \mapsto & kh. \end{array} \right.$$

Nous avions vu que cette application était un morphisme si, et seulement si K et H se normalisaient mutuellement.
À défaut d'avoir la normalisation mutuelle, l'idée est de construire une nouvelle loi de groupe sur $K \times H$ qui fasse à nouveau de φ un morphisme.

$$\varphi\,(k_1,\, h_1)\,.\,\varphi\,(k_2,\, h_2) = k_1h_1k_2h_2.$$

On remarque alors que

$$k_1h_1k_2h_2 = k_1h_1k_2h_1^{-1}h_1h_2.$$

Or $h_1k_2h_1^{-1} \in K$ car H normalise K (on avait même supposé $K \lhd G$), donc $k_1h_1k_2h_1^{-1} \in K$.
On reformule donc :

$$\begin{aligned} \varphi\,(k_1,\, h_1)\,.\,\varphi\,(k_2,\, h_2) &= \underbrace{k_1h_1k_2h_1^{-1}}_{\in K}\underbrace{h_1h_2}_{\in H} \\ &= \varphi\left(k_1h_1k_2h_1^{-1},\, h_1h_2\right). \end{aligned}$$

On veut que cette dernière expression soit égale à $\varphi\,(\,(k_1,\, h_1).(k_2,\, h_2)\,)$ ce qui donne la loi de groupe sur $K \times H$:

$$\forall (k_1,\, h_1),\, (k_2,\, h_2) \in K \times H, \quad (k_1,\, h_1).(k_2,\, h_2) = (k_1h_1k_2h_1^{-1},\, h_1h_2).$$

3. On trouve cette expression par analogie avec les projecteurs pour les espaces vectoriels.

Théorème 3.1

Soit G un groupe, K et H deux sous-groupes de G.
Si

1. $H \cap K = \{1\}$,
2. $KH = G$,
3. $K \triangleleft G$,

alors on peut alors définir le **produit semi-direct** interne de K par H noté $K \rtimes H$ par la loi de groupe sur $K \times H$:

$$\forall (k_1,\, h_1),\, (k_2,\, h_2) \in K \times H, \quad (k_1,\, h_1).(k_2,\, h_2) = (k_1 h_1 k_2 h_1^{-1},\, h_1 h_2).$$

Dans ce cas :

$$G \approx K \rtimes H.$$

Preuve

On vérifie d'abord que $K \rtimes H$ est un groupe.

1. L'opération est interne car H normalise K.
2. L'opération est associative (s'obtient par le calcul, l'expression est un peu lourde).
3. $(1,\, 1)$ est l'élément neutre.
4. Pour $(k,\, h) \in K \rtimes H$, on trouve un inverse $(h^{-1}k^{-1}h,\, h^{-1}) \in K \rtimes H$.

On définit ensuite l'application

$$\varphi : \left\{ \begin{array}{ccc} K \rtimes H & \to & G \\ (k,\, h) & \mapsto & kh. \end{array} \right.$$

Avec la loi de groupes sur $K \rtimes H$, on vérifie que φ est bien un morphisme (immédiat).
$KH = G$, donc le morphisme est surjectif.
Soit $(k,\, h) \in \ker(\varphi)$, alors $kh = 1$, donc $k = h^{-1} \in K \cap H = \{1\}$, donc $h = k = 1$, ce qui justifie que φ est injective (noyau réduit à l'élément neutre).
On a donc bien prouvé que φ est un isomorphisme de groupes. ■

⚠ Contrairement au cas du produit produit direct, K et H ne jouent pas des rôles symétriques dans le produit semi-direct.
Plus simplement, on peut[4] définir le produit semi-direct de deux sous-groupes sans exiger qu'il soit égal à G. On obtient alors des conditions allégées :

4. Par analogie avec les espaces vectoriels, cela correspond à la somme directe de deux sous-espaces vectoriels non supplémentaires.

Définition 3.2 *(produit semi-direct interne)*

Soit G un groupe, K et H deux sous-groupes de G.
On suppose que H normalise K.
On définit alors le **produit semi-direct** interne de K par H noté $K \rtimes H$ par la loi de groupe sur $K \times H$:

$$\forall (k_1,\, h_1),\, (k_2,\, h_2) \in K \times H, \quad (k_1,\, h_1).(k_2,\, h_2) = (k_1 h_1 k_2 h_1^{-1},\, h_1 h_2).$$

Preuve

immédiat : on vérifie les axiomes. ■

Remarque : Comme cela a été fait pour le produit direct (exercice de la page 5), on peut alors considérer H et K comme des sous-groupes de $K \rtimes H$ et on obtient qu'ils vérifient les hypothèses du théorème plus haut : $K \cap H = \{1\}$, $KH = K \rtimes H$ et $K \triangleleft (K \rtimes H)$ (à quelques isomorphismes près).
Ceci sera détaillé à la page 10.

Exemple *(Groupe symétrique S_3)*

On s'intéresse à S_3 déjà étudié dans le document d'introduction aux groupes. On a déjà vu dans l'exemple de la page 6 que le sous-groupe des rotations noté $\mathbf{U}_3$ ne donne pas de produit direct pour dévisser S_3 (suite exacte non scindée à gauche). Cependant la lecture de la table de Cayley permet de voir que $H =< \tau_A >= \{\mathrm{Id},\, \tau_A\}$ est un sous groupe de S_3 :

$\circ$	Id	R	R^2	τ_A	τ_B	τ_C
Id	Id	R	R^2	τ_A	τ_B	τ_C
R	R	R^2	Id	τ_B	τ_C	τ_A
R^2	R^2	Id	R	τ_C	τ_A	τ_B
τ_A	τ_A	τ_C	τ_B	Id	R^2	R
τ_B	τ_B	τ_A	τ_C	R	Id	R^2
τ_C	τ_C	τ_B	τ_A	R^2	R	Id

Une extraction de la table permet aussi de voir que $\mathbf{U}_3 H = S_3$:

$\circ$	Id	τ_A
Id	Id	τ_A
R	R	τ_B
R^2	R^2	τ_C
τ_A	τ_A	Id

Enfin, il est clair que $\mathbf{U}_3 \cap H = \{\mathrm{Id}\}$ et que $\mathbf{U}_3 \triangleleft S_3$.
On peut donc définir le produit semi-direct interne :

$$S_3 \approx \mathbf{U}_3 \rtimes < \tau_A > .$$

Intuitivement, cela veut dire que l'on peut obtenir S_3 (muni de sa structure de groupe), à partir des trois rotations et de la reflexion τ_A.

Nous invitons le lecteur à chercher la décomposition explicite de chaque élément de S_3. Elle sera détaillée dans l'exemple de la partie suivante.

Exemple *(Groupe diédral D_n)*

Pour $n \geqslant 2$, on définit le groupe diédral D_n comme le groupe des isométries du plan $\mathbf{R}^2$ qui préservent le polygone régulier à n côtés.
On généralise donc l'exemple précédent qui étudiait le groupe $D_3 \approx S_3$.
Ce groupe est constitué de n rotations et de n réflexions (symétries par rapport à une droite).
Si on note R, la rotation d'angle $\frac{2\pi}{n}$, alors l'ensemble des rotations s'écrit $\mathbf{U}_n = \left\{R^k,\ k \in [\![0,\ n-1]\!]\right\}$.
Si on note τ une des reflexions de D_n et $H = \{\tau, \mathrm{Id}\}$ le groupe engendré par τ, alors

$$D_n \approx \mathbf{U}_n \rtimes H.$$

B À partir d'un semi-projecteur

J'appelle ici « semi-projecteur » un morphisme de groupes qui vérifie $p \circ p = p$ mais pour lequel on n'impose aucune condition de commutativité entre les éléments du noyau et de l'image.

Théorème 3.3

Soit G un groupe et p un endomorphisme de G qui vérifie $p \circ p = p$.
G se dévisse alors en le produit semi-direct

$$G \approx \ker(p) \rtimes \mathrm{Im}\,(p).$$

Preuve

- $\ker(p) \triangleleft G$.
- Soit $x \in \ker(p) \cap \mathrm{Im}\,(p)$, alors il existe $z \in G$ tel que $x = p(z)$, donc $1 = p(x) = p^2(z) = p(z) = x$.
Ainsi $\ker(p) \cap \mathrm{Im}\,(p) = \{1\}$ (on n'a prouvé que l'inclusion non évidente).
- Soit $x \in G$, on pose alors $k = xp(x^{-1})$ et $h = p(x)$.
on obtient que $kh = x$.
De plus $p(k) = 1$, donc $k \in \ker(p)$ et $h \in \mathrm{Im}\,(p)$.
Ainsi $\ker(p)\mathrm{Im}\,(p) = G$ (autre inclusion évidente).

On a donc montré que $G \approx \ker(p) \rtimes \mathrm{Im}\,(p)$. ■

Exemple *(Groupe symétrique S_3)*

On reprend le produit semi-direct réalisé pour le groupe symétrique :

$$S_3 \approx \mathbf{U}_3 \rtimes < \tau_A > .$$

Cela revient à décomposer chaque élément de S_3 de façon unique comme un couple de $\mathbf{U}_3 \rtimes < \tau_A >$. Si on reprend l'extraction de la table de Cayley de la partie précédente, on retrouve alors cette décomposition :

$\circ$	Id	τ_A
Id	Id	τ_A
R	R	τ_B
R^2	R^2	τ_C
τ_A	τ_A	Id

$\xrightarrow{}$ décomposition sur $\mathbf{U}_3 \rtimes <\tau_A>$

S_3	$\mathbf{U}_3$	$< \tau_A >$
Id	Id	Id
R	R	Id
R^2	R^2	Id
τ_A	Id	τ_A
τ_B	R	τ_A
τ_C	R^2	τ_A

Dans le théorème p est un projecteur sur K parallèment à H.
Ainsi, à chaque élément de S_3, le projecteur associe l'élément de $H =< \tau_A >$ de sa décomposition. On trouve ici que l'image par p d'une rotation est Id et que l'image d'une reflexion est τ_A.
Nous étudierons ce produit semi-direct plus en détail à la page 14.

C Suite exacte associée à un produit semi-direct

Cette partie reprend et approfondit ce qui a été proposé dans l'exercice page 5 pour le produit direct, *elle peut être sautée en première lecture.*
On part d'un produit semi-direct $K \rtimes H$ avec K et H deux sous-groupes de G.
On sait donc par définition que $H \cap K = \{1\}$ et que H normalise K.

On veut montrer ici deux choses :

1. que le produit semi-direct peut se traduire avec une suite exacte courte.
2. que H et K vérifient les hypothèses du théorème 3.1, c'est-à-dire que (dans un sens à préciser) :
   (a) $H \cap K = \{1_{K \rtimes H}\}$,
   (b) $KH = K \rtimes H$,
   (c) $K \triangleleft K \rtimes H$,

Nous invitons le lecteur à chercher cette partie comme un exercice.

Commençons par créer la suite exacte, ce qui nous indiquera dans quel sens, on peut interpréter K et H comme des sous-groupes de $K \rtimes H$.

- On pose l'application
$$i : \left\{ \begin{array}{ccc} K & \to & K \rtimes H \\ k & \mapsto & (k,\ 1). \end{array} \right.$$
$\forall (k_1,\ k_2) \in K^2$,
$$i(k_1 k_2) = (k_1 k_2,\ 1) = (k_1.1.k_2.1^{-1},\ 1) = (k_1,\ 1).(k_2,\ 1) = i(k_1)i(k_2).$$

Donc i est un morphisme de groupes.
Cherchons son noyau :
$\forall k \in \ker(i)$, $i(k) = 1$, donc $(k, 1) = (1, 1)$, donc $k = 1$.
On obtient donc que $\ker(i) = \{1\}$, ce qui justifie que i est injectif.
Ainsi i réalise un isomorphisme de K sur $\overline{K} = \{(k, 1),\ k \in K\} \subset K \rtimes H$.

- On pose également

$$f : \left\{ \begin{array}{ccc} K \rtimes H & \to & H \\ (k, h) & \mapsto & h. \end{array} \right.$$

$\forall (k_1, h_1), (k_2, h_2) \in K \rtimes H$,

$$f((k_1, h_1).(k_2, h_2)) = f(k_1 h_1 k_2 h_1^{-1}, h_1 h_2) = h_1 h_2 = f(k_1, h_1).f(k_2, h_2).$$

Donc f est un morphisme de groupes.
Montrons que f est surjective.
Soit $h \in H$, alors $f(1, h) = h$, ce qui justifie la surjectivité.

- On remarque de plus que $\ker(f) = \overline{K} = \mathrm{Im}\,(i)$.

On dispose donc de la suite exacte courte

$$1 \longrightarrow K \xrightarrow{\ i\ } K \rtimes H \xrightarrow{\ f\ } H \longrightarrow 1.$$

$K \approx \overline{K}$ qui est un sous-groupe distingué de $K \rtimes H$ (car c'est un noyau), donc on peut considérer, à isomorphisme près, que $K \triangleleft K \rtimes H$.
Montrons que H peut aussi être « injecté » dans $K \rtimes H$.
Pour cela on définit

$$s : \left\{ \begin{array}{ccc} H & \to & K \rtimes H \\ h & \mapsto & (1, h). \end{array} \right.$$

Avec la loi de groupes définie sur $K \rtimes H$, s est un morphisme et il est clairement injectif.
Ainsi s réalise un isomorphisme de H sur $\overline{H} = \{(1, h),\ h \in H\}$.
On peut donc, à isomorphisme près, considérer que H est un sous-groupe de $K \rtimes H$.

On obtient enfin : $\overline{K} \cap \overline{H} = \{(1, 1)\} = \{1_{K \rtimes H}\}$ et

$$KH = \{(k, 1).(1, h),\ (k, h) \in K \times H\} = \{(k, h),\ (k, h) \in K \times H\} = K \rtimes H.$$

Tout ceci permet de vérifier que K et H vérifient bien les bonnes propriétés vis-à-vis de leur propre semi-produit (heureusement).
Ainsi, en identifiant K avec $\overline{K}$ et H avec $\overline{H}$, on trouve :

- $K \cap H = \{1\}$
- $KH = K \rtimes H$
- $K \triangleleft K \rtimes H$.

On obtient :

Théorème 3.4

Tout produit semi-direct peut s'écrire comme extension de groupe :

$$1 \longrightarrow K \xrightarrow{\ i\ } K \rtimes H \xrightarrow{\ f\ } H \longrightarrow 1.$$

Remarque : Nous verrons bientôt le rôle essentiel joué par le morphisme s pour la décomposition en produit semi-direct. C'est l'existence de ce morphisme qui permet d'obtenir la réciproque à ce théorème.

D Liens avec le produit direct

Théorème 3.5

Soit G un groupe.
Soient K et H deux sous-groupes de G avec H qui normalise K.
Les propriétés suivantes sont équivalentes

1. Le produit semi-direct $K \rtimes H$ est direct.
2. K normalise H.
3. $\left\{khk^{-1}h^{-1},\ (k, h) \in K \times H\right\} = \{1\}$.

Remarque : Il n'y a aucune raison que $K \rtimes H = G$.

Preuve
Immédiat. ■

4 Le produit semi-direct externe

A Se ramener au produit semi-direct interne

On part à présent d'une suite exacte courte.

$$1 \longrightarrow N \xrightarrow{\ i\ } G \xrightarrow{\ f\ } Q \longrightarrow 1.$$

On reprend le même raisonnement que pour le produit direct, mais en privilégiant désormais la recherche d'un antécédent par f plutôt que par i.
On cherche donc à écrire $g \in G$ sous la forme $g = yz$, avec $y \in i(N)$ et $z \in f^{-1}(Q) = H$.
Pour obtenir z, on suppose l'existence d'un morphisme[5] s tel que $f \circ s = \mathrm{Id}_Q$: ce morphisme permet de « choisir » un antécédent de façon unique pour tout élément de Q.

On dit que le **morphisme** s est une *section* de f.

5. On retrouve le morphisme s explicité plus haut et qui nous avait permis d'interpréter H comme un sous-groupe de $K \rtimes H$.

Définition 4.1 *(section)*

Soient G et Q deux groupes et $f\ : G \to Q$ un morphisme de groupe.
Le morphisme s est une **section** de f (ou un **scindage à droite**), si $f \circ s = \mathrm{Id}_Q$.

Remarque : on voit alors que s réalise un isomorphisme de Q sur $f^{-1}(Q) = \mathrm{Im}\,(s)$.

Revenons à notre décomposition $g = yz$.
Comme pour le produit direct, on écrit naturellement $z = (s \circ f)(g) \in \mathrm{Im}\,(s) = H$.
Pour avoir $g = yz$, on pose donc $y = gz^{-1} = g\,.\,\big((s\circ f)(g^{-1})\big)\,.$
Vérifions que $y \in \mathrm{Im}\,(i)$, c'est-à-dire $y \in \ker(f)$:

$$f(y) = f(g)\,(f\circ s\circ f)\,(g^{-1}) = f(g)\,(\mathrm{Id}_Q \circ f)\,(g^{-1}) = f(g)f(g^{-1}) = 1.$$

On a donc décomposé $g = yz$ avec $y \in \mathrm{Im}\,(i) = \ker(f)$ et $z \in \mathrm{Im}\,(s) = H$ comme souhaité.

Montrons que $\mathrm{Im}\,(i)$ et H vérifient les conditions pour constituer un produit semi-direct interne.

- Soit $y \in \mathrm{Im}\,(i) \cap H$, alors il existe $z \in Q$ tel que $y = s(z)$.
  Or $y \in \mathrm{Im}\,(i)$, donc $f(y) = 1$.
  Ainsi $1 = f(y) = f \circ s(z) = z$.
  Ce qui donne donc $y = s(z) = s(1) = 1$.
  On obtient donc que $\mathrm{Im}\,(z) \cap H = \{1\}\,.$
- La décomposition précédente montre de plus que $\mathrm{Im}\,(i)H = G$ en posant pour tout $g \in G$, $g = g\left(s\circ f(g^{-1})\right)(s\circ f(g))\,.$
- Enfin $\mathrm{Im}\,(i) = \ker(f) \lhd G$.

Ces trois propriétés vérifiées, on peut construire le produit semi-direct interne à partir de $\mathrm{Im}\,(i)$ et de $H = \mathrm{Im}\,(s)$:

Théorème 4.2 *(section et produit semi-direct)*

Soit G un groupe, et la suite exacte courte suivante.

$$1 \longrightarrow N \xrightarrow{\ i\ } G \xrightarrow{\ f\ } Q \longrightarrow 1.$$

Si f admet une section s, alors

$$G \approx \mathrm{Im}\,(i) \rtimes s(Q).$$

En outre, en identifiant à isomorphisme près N avec $i(N)$,

on a $N \lhd G$ et $s(Q) \approx Q \approx G/N$.

B Vers le cas général

Cette petite section est un peu technique et peut être sautée sans grand dommage. Elle a pour but d'introduire au mieux la définition générale du produit semi-direct qui sera présentée dans la section suivante.

Dans la partie précédente, on remarque que i réalise un isomorphisme de N sur $\mathrm{Im}\,(i)$.
On peut alors écrire la décomposition précédente avec l'isomorphisme :

$$\varphi : \left\{\begin{array}{ccccc} G & \to & \mathrm{Im}\,(i) \rtimes H & \to & N \rtimes_? Q \\ g & \mapsto & \Big(g.(s\circ f)(g^{-1}),\ (s\circ f)(g)\Big) & \mapsto & \Big(\underbrace{i^{-1}\Big(g.(s\circ f)(g^{-1})\Big)}_{n\in N},\ \underbrace{f(g)}_{x\in Q}\Big). \end{array}\right.$$

L'idée est de trouver la loi de groupe sur le produit $N \rtimes_? Q$ pour que l'application φ soit bien un morphisme.
On considère donc $(g,\, g') \in G^2$.
Si on note $(n,\, x) = \varphi(g)$ et $(n',\, x') = \varphi(g')$, alors on remarque que $n = i^{-1}\left(g.s\left(x^{-1}\right)\right)$ et $n' = i^{-1}\left(g'.s\left(x'^{-1}\right)\right).$

On obtient

$$\varphi(gg') = \Big(i^{-1}\left(gg'.s(x'^{-1}x^{-1})\right),\ xx'\Big).$$

On s'intéresse à la première composante (la seconde ne pose pas de difficultés) et on cherche à faire apparaître n et n' :

$$\begin{aligned} i^{-1}\Big(gg's(x'^{-1})s(x^{-1})\Big) &= i^{-1}\Big(g.s\left(x^{-1}\right)s(x).g's(x'^{-1})s\left(x^{-1}\right)\Big) \\ &= \underbrace{i^{-1}\Big(gs\left(x^{-1}\right)\Big)}_{=n}.i^{-1}\Big(s(x)g's(x'^{-1})s\left(x^{-1}\right)\Big) \\ &= n.i^{-1}\Big(s(x)i(n')s\left(x^{-1}\right)\Big). \end{aligned}$$

On voit donc que le produit semi-direct revient à faire agir $s(x)$ par conjugaison sur $i(n')$.
Pour tout $x \in Q$, on définit alors

$$\psi_x : \left\{\begin{array}{ccc} N & \to & N \\ n & \mapsto & i^{-1}\Big(s(x)i(n)s\left(x^{-1}\right)\Big). \end{array}\right.$$

Avant d'appliquer i^{-1}, on a vérifié que $s(x)i(n)s(x^{-1}) \in \mathrm{Im}\,(i)$ car $\mathrm{Im}\,(i) = \ker(f) \lhd G$.
ψ_x est alors clairement un automorphisme de N et on obtient l'action de groupe de Q sur N avec

$$\forall (x,\, n) \in Q \times N,\ x \cdot n = \psi_x(n) \in N.$$

On vérifie que c'est bien une action de groupes :

- $\forall n \in N,\ 1 \cdot n = \psi_1(n) = n.$

- $\forall (x,\, x') \in Q^2,\ \forall n \in N,$

$$x \cdot (x' \cdot n) = \psi_x\left(\psi_{x'}(n)\right) = \left(\psi_x \circ \psi_{x'}\right)(n) = \psi_{xx'}(n) = (xx') \cdot n.$$

Le produit semi-direct de N par Q est alors défini par la loi de groupe $\star$: $\forall (n,\, x),\ (n',\, x') \in N \times Q,$

$$(n,\, x) \star (n',\, x') = (n(x \cdot n'),\, xx')\,.$$

On vérifie aisément qu'il s'agit d'une loi de groupes et qu'elle donne l'isomorphisme $N \rtimes_\psi Q \to G$.

C Loi sur les groupes externes

La travail de la section précédente permet de définir (enfin) le produit semi-direct en toute généralité :

Définition 4.3 *(Produit semi-direct)*

Soient N et Q deux groupes.
Soit $\psi\ : Q \to \mathrm{Aut}(N)$ un morphisme de groupes.
On définit l'action de groupe de Q sur N par

$$\forall (x,\, n) \in Q \times N,\ x \cdot n = \psi(x)(n) \in N.$$

On définit alors l'opération interne . sur $N \times Q$:

$$\forall (n,\, x),\ (n',\, x') \in N \times Q,\ (n,\, x).(n',\, x') = (n(x \cdot n'),\, xx').$$

Muni de cette opération $N \times Q$ est un groupe appelé **produit semi-direct** de N par Q pour l'action ψ et noté

$$N \rtimes_\psi Q.$$

Remarque : La possibilité de choisir différentes actions de groupes indique que le produit semi-direct n'est pas défini de manière unique.
C'est la raison pour laquelle le morphisme ψ est indiqué en indice.

Exemple *(Produit semi-direct interne)*

Le produit semi-direct interne défini plus haut, est constuit à partir de l'action de conjugaison où $\psi\ : x \mapsto \left\{\begin{array}{ccc} N & \to & N \\ n & \mapsto & xnx^{-1}. \end{array}\right.$

Exemple *(Produit direct)*

Le produit direct est un cas particulier de produit semi-direct en choisissant l'action triviale définie par

$$\psi\ : x \mapsto \left\{\begin{array}{ccc} N & \to & N \\ n & \mapsto & n. \end{array}\right.$$

Théorème 4.4 *(section et produit semi-direct)*

Soient G un groupe et la suite exacte courte suivante :

$$1 \longrightarrow N \xrightarrow{\ i\ } G \xrightarrow{\ f\ } Q \longrightarrow 1.$$

Si f admet une section s alors

$$G \approx N \rtimes_\psi Q$$

avec $\forall x \in Q,\ \psi(x)\ : n \mapsto i^{-1}(s(x)i(n)s(x^{-1})).$

D Condition nécessaire et suffisante de produit semi-direct

Théorème 4.5

Soit G un groupe.
Les propriétés suivantes sont équivalentes.

1. G est isomorphe à un produit semi-direct $N \rtimes_\psi Q$.
2. G admet une suite exacte courte scindée à droite
$$1 \longrightarrow N \xrightarrow{\ i\ } G \xrightarrow{\ f\ } Q \longrightarrow 1.$$
3. G admet un semi-projecteur p (voir p.10).
4. G admet deux sous-groupes H et K qui vérifient
   (a) $H \cap K = \{1\}\,,$
   (b) $KH = G,$
   (c) H normalise K.
   de façon équivalente $K \lhd G$.

Preuve

- (1) $\Rightarrow$ (2) et (1) $\Rightarrow$ (4).
  On reprend le théorème 3.4 de la page 11 en remplaçant l'automorphisme intérieur par ψ.
- (2) $\Rightarrow$ (1).
  Voir le théorème 4.4 de la page 13.
- (3) $\Rightarrow$ (1).
  Voir le théorème 3.3 de la page 10.
- (4) $\Rightarrow$ (1).
  Voir le théorème 3.1 de la page 9.
- (4) $\Rightarrow$ (3).
  On pose $p = f \circ s$ en utilisant une suite exacte scindée à droite.

■

E Exemple avec le groupe symétrique

Prérequis : signature d'un morphisme. Il est conseillé d'avoir déjà étudié le cours de MPSI sur le groupe symétrique.
Dans la suite $n \geqslant 2$ et S_n désigne le groupe symétrique d'ordre n. Par exemple pour $n = 3$, c'est le groupe des isométries du triangle qui déjà été un peu étudié dans le document d'introduction aux groupes et les exemples précédents.

Suite exacte et produit semi-direct : on note ε la fonction signature d'une permutation de S_n et $\mathscr{A}_n$ le noyau de ε (c'est-à-dire le *groupe alterné* qui contient les permutations paires).
On peut construire la suite exacte

$$1 \longrightarrow \mathscr{A}_n \xrightarrow{i} S_n \xrightarrow{\varepsilon} \{-1,\, 1\} \longrightarrow 1$$

où i envoie chaque permutation paire sur elle-même.
La suite est scindée à droite :
on définit $s : \{-1,\, 1\} \to S_n$ par $s(1) = \mathrm{Id}$ et $s(-1) = (12)$ (ou toute autre transposition).
En notant ψ comme dans le théorème 4.4 on obtient alors que

$$S_n = \mathscr{A}_n \rtimes_\psi \{-1,\, 1\}\,.$$

Par isomorphie, on peut également remplacer $\{-1,\, 1\}$ par $\mathbf{Z}/2\mathbf{Z}$ ce qui donne

$$S_n \approx \mathscr{A}_n \rtimes_\psi \mathbf{Z}/2\mathbf{Z}.$$

On remarque que le produit semi-direct obtenu dépend du choix de la permutation pour définir s.

Cardinal : La factorisation du morphisme ε donne $\mathbf{Z}/2\mathbf{Z} \approx S_n/\mathscr{A}_n$.
Or $\mathbf{Z}/2Z$ contient 2 éléments et S_n en contient $n!$. Ainsi $\mathscr{A}_n$ est de cardinal $\frac{n!}{2}$.

Visualisation sur le groupe S_3 : Le produit semi-direct $\mathscr{A}_n \rtimes_\psi (\mathbf{Z}/2\mathbf{Z})$, un peu comme un produit direct, permet de reconstituer S_n à partir des couples formés d'une permutation paire et d'un entier dans $\{-1,\, 1\}$.
On retrouve bien qu'il existe deux fois plus de permutations dans S_n qu'il n'y en a dans $\mathscr{A}_n$.

Prenons l'exemple d'une permutation $g \in S_3$.
On cherche sa décomposition sur le produit semi-direct, c'est-à-dire son image par l'isomorphisme φ

$$\varphi : \left\{ \begin{array}{ccc} G & \to & N \rtimes_? Q \\ g & \mapsto & \Big(\underbrace{i^{-1}\left(g.(s\circ\varepsilon)(g^{-1})\right)}_{n\in N},\, \underbrace{\varepsilon(g)}_{x\in Q} \Big). \end{array} \right.$$

- Si g est une permutation paire.
  Ici, nous conseillons au lecteur de suspendre un instant sa lecture et d'essayer de deviner quel sera le couple correspondant.
  On trouve :

$$\begin{aligned} \varphi(g) &= \Big(i^{-1}\left(g.(s\circ\varepsilon)(g^{-1})\right),\, \varepsilon(g)\Big) \\ &= \Big(i^{-1}\left(g.s(1)\right),\, 1\Big) \\ &= \big(i^{-1}(g),\, 1\big) = (g,\, 1). \end{aligned}$$

  C'est très intuitif : si la permutation est déjà dans le groupe alterné, la fonction φ renvoie exactement cette même permutation (avec 1 en deuxième coordonnée puisqu'elle est paire).

- Si g est une permutation impaire.
  À nouveau le lecteur peut avoir une idée, au moins approximative, du résultat.

$$\begin{aligned} \varphi(g) &= \big(i^{-1}\left(g.(s\circ\varepsilon)(g^{-1})\right),\, \varepsilon(g)\big) \\ &= \big(i^{-1}\left(g.s(-1)\right),\, -1\big) \\ &= \big(i^{-1}(g.(12)),\, -1\big) = (g.(12),\, -1). \end{aligned}$$

  Cette fois-ci, la fonction renvoie la même permutation rendue paire par la composition à droite avec la transposition (12), assortie du nombre -1 pour bien indiquer que $g.(12)$ n'est pas la permutation initiale.

Remarque : Ce produit direct externe pouvait être aussi vu comme un produit direct interne $S_n \approx \mathscr{A}_n \rtimes \{\mathrm{Id},\, (12)\}$.
De plus, on voit que $\mathscr{A}_n$ correspond au groupe des rotations noté $\mathbf{U}_3$ dans les exemples précédents.

Autres décompositions en produit : On peut se demander s'il existe d'autres décompositions (hormis celles en produit semi-direct sur le modèle précédent où on change seulement la transposition qui définit l'action de groupe).

Toute décomposition en produit direct ou semi-direct demande la présence d'un sous-groupe distingué pour jouer le rôle de N (à isomorphisme près).
En effet, on se rappelle que $\ker(f) \lhd G$ pour tout morphisme $f\ : G \to Q$.

Dans le cas $n \geqslant 5$, un théorème (admis) nous indique que les seuls sous-groupes distingués de S_n sont

$$S_n,\, \mathscr{A}_n,\, \{1\}\,.$$

On voit donc que, sauf produit trivial, la suite exacte s'écrit nécessairement sous la forme

$$1 \longrightarrow \mathscr{A}_n \xrightarrow{i} S_n \xrightarrow{\varepsilon} Q \longrightarrow 1.$$

Dans, ce cas $Q \approx S_n/\mathscr{A}_n$, donc Q ne contient que deux éléments, c'est-à-dire qu'il s'agit nécessairement de $\{-1,\, 1\}$ à isomorphisme près.

Or, ε est le seul morphisme non constant[6] de S_n dans $\{-1, 1\}$ ce qui justifie que la suite exacte trouvée précédemment est la seule possible (à isomorphismes près).

Reste à voir s'il n'y a pas de produit direct, c'est-à-dire si la suite n'est pas également scindée à gauche.
Si tel était le cas, il existerait un retraction de i :

$$r\ : S_n \to \mathscr{A}_n.$$

On aurait alors $r_{|\mathscr{A}_n} = \mathrm{Id}_{\mathscr{A}_n}$.
Or $\ker(r) \lhd S_n$ et d'après le théorème plus haut, on a donc $\ker(r) = \{1\}$ ou $\mathscr{A}_n$ ou $\mathscr{S}_n$.

- r étant surjective, elle ne peut être injective (car S_n et $\mathscr{A}_n$ n'ont pas le même nombre d'éléments), ce qui exclut le premier cas.
- Comme la restriction de s à $\mathscr{A}_n$ est l'identité, $\ker(s)$ ne peut être égal à $\mathscr{A}_n$.
- Enfin, s n'est pas le morphisme nul, donc $\ker(f) \neq S_n$

Aucune possibilité ne convient, donc la suite exacte n'est pas sindée à gauche.

Conclusion pour $n \geqslant 5$: à isomorphisme prés et au choix de la section près, le produit semi-direct présenté au début est le seul possible pour $n \geqslant 5$.
Pour $n \in \{1, 2\}$, on sait que le cardinal de tout sous-groupe divise celui du groupe (théorème de Lagrange : voir le cours d'introduction aux groupes).
Ainsi les seuls sous-groupes possibles sont $\{1\}$ ou S_n lui-même et il n'existe donc aucune suite exacte non triviale.

Pour $n = 3$, $\mathrm{Card}\,(S_3) = 6!$ et les sous-groupes non trivaux sont de cardinal 2 ou 3.
On avait déjà vu la table de Cayley plus haut et il est clair que le seul sous-groupe d'ordre 3 est $\mathscr{A}_3$, qui correspond au groupe des trois rotations du triangle : cela nous ramène alors au produit semi-direct déjà étudié plus haut.
Les sous-groupes d'ordre 2 sont composés de l'identité et d'une transposition (pour les triangle : l'identité et une symétrie).
Mais, on se convaincra rapidement à l'aide de la table de Cayley qu'aucun de ces sous-groupes n'est distingué.
Le résultat vu plus haut est donc encore valable pour $n = 3$.

Pour $n = 4$, la situation est différente.
On remarque que le groupe des reflexions du carré est un sous-groupe strict de S_4 et même un sous groupe strict de $\mathscr{A}_4$ car il ne contient pas les rotations (sauf l'identité).
On trouve :

$$V = \{\mathrm{Id}, (12)(34), (13)(24), (14)(23)\}.$$

On l'appelle groupe de Klein.
On peut montrer que c'est le seul sous-groupe distingué de S_4 autre que ceux vus précédemment.

6. Voir le cours sur le groupe symétrique.

On fait alors agir S_3 par automorphisme intérieur sur V (car V distingué dans S_4) ce qui donne le produit semi-direct $V \rtimes S_3$. On voit que $V \rtimes S_3 \subset S_4$ (plus précisément, $V \rtimes S_3$ se plonge dans S_4).
Or $\mathrm{Card}\,(V \rtimes S_3) = \mathrm{Card}\,(V) \times \mathrm{Card}\,(S_3) = 4 \times 6 = \mathrm{Card}\,(S_4)$.
Ainsi $S_4 \approx V \rtimes S_3$.

5 Résumé

Non exhaustif.

A Définition

Soient N et Q deux groupes.
Soit $\psi : Q \to \mathrm{Aut}(N)$ un morphisme de groupes.
On définit une action de groupe de Q sur N par $\forall (x,\, n) \in Q \times N,\ x \cdot n = \psi(x)(n) \in N$.
On définit alors l'opération interne . sur $N \times Q$:

$$\forall (n,\, x),\, (n',\, x') \in N \times Q,\ (n,\, x).(n',\, x') = (n(x \cdot n'),\, xx').$$

Muni de cette opération $N \times Q$ est un groupe appelé **produit semi-direct** de N par Q pour l'action ψ et noté

$$N \rtimes_{\psi} Q.$$

Lorsque $\psi : q \mapsto \mathrm{Id}_N$, alors le produit est **direct**, il est noté $N \times Q$.

Remarque : Deux groupes peuvent donc toujours être mis en produit direct et en produit semi-direct. Le problème est plutôt de dévisser en groupe donné en produit.

B Dévissage en produit direct

Soit G un groupe.
Les propriétés suivantes sont équivalentes.

1. G est isomorphe à un produit direct.
2. G admet une suite exacte courte scindée à gauche

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{f} Q \longrightarrow 1.$$

3. G admet un projecteur p (voir p.5).
4. G admet deux sous-groupes H et K qui vérifient
   (a) $H \cap K = \{1\}$,
   (b) $KH = G$,
   (c) H et K se normalisent mutuellement.
   de façon équivalente, les éléments de H commutent avec les éléments de K.

C Dévissage en produit semi-direct

Soit G un groupe.
Les propriétés suivantes sont équivalentes.

1. G est isomorphe à un produit semi-direct.
2. G admet une suite exacte courte scindée à droite

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{f} Q \longrightarrow 1.$$

3. G admet un semi-projecteur p (voir p.10).
4. G admet deux sous-groupes H et K qui vérifient
   (a) $H \cap K = \{1\}$,
   (b) $KH = G$,
   (c) H normalise K.
   de façon équivalente $K \triangleleft G$.

D Lien entre produit direct et semi-direct interne

Soit G un groupe, K et H deux sous-groupes de G avec H qui normalise K.

Le produit semi-direct $K \rtimes H$ est direct
$\iff$ K normalise H.
$\iff$ $\left\{khk^{-1}h^{-1},\, (k,\, h) \in K \times H\right\} = \{1\}$.