## Le produit semi-direct de deux groupes

Soient $H$ et $K$ deux groupes, et soit

$$* : K \times H \longrightarrow H$$

une action de $K$ sur $H$ par morphismes de groupes, i.e., $*$ est une action de $K$ sur l'ensemble $H$, et en plus

$$k * (hh') = (k*h) \cdot (k*h').$$

Alors, on peut construire le produit semi-direct $H \rtimes K$ de $H$ et $K$ relativement à l'action $*$:

En tant qu'ensemble $H \rtimes K = H \times K$
la loi de composition interne sur $H \rtimes K$ est définie par

$$(h,k) \boxtimes (h',k') := (h \cdot (k*h'), kk')$$

où $(h,k), (h',k') \in H \rtimes K = H \times K$

Proposition : $H \rtimes K$ est un groupe

Démo : exo (indication : $(1,1)$ est l'élt neutre de $H \rtimes K$, $(h,k)^{-1} = ((k^{-1})*(h^{-1}), k^{-1})$)

Remarque si $K$ agit trivialement sur $H$, c-à-d, $\forall k \in K\ \forall h \in H$ : $k*h = h$, alors, le produit semi-direct $H \rtimes K$ coïncide avec le produit cartésien $H \times K$ de $H$ et $K$.

L'exemple motivant d'un produit semi-direct est le suivant.

Soit $G$ un groupe, $H \leq G$ distingué, $K \leq G$ sous-groupe avec $H \cap K = \{1\}$ et $HK = G$
Définit une action de $K$ sur $H$ par

$$k * h = khk^{-1} \qquad h \in H, k \in K$$

Soit
$$f : H \rtimes K \longrightarrow G$$
$$(h,k) \longmapsto hk.$$
Alors, l'application ensembliste $f$ est un morphisme de groupe (exo).
Le morphisme est injectif car $H \cap K = \{1\}$ et surjectif car $HK = G$. Par conséquent, $f$ est un isomorphisme de groupes.
En particulier, $G$ est isomorphe au produit semi-direct de $H$ et $K$ relativement à une action de $K$ sur $H$.

Exemple : Soit $D_n$ le groupe diédral de cardinal $2n$. Rappelons que $D_n$ est le groupe des isométries $\varphi$ du plan complexe $\mathbb{C}$ tq $\varphi(P_n) \subseteq P_n$ où $P_n$ est le $n$-gône régulier dans $\mathbb{C}$ de sommets les $n$ racines de l'unité $e^{2\pi i k/n}$ $k = 0, \ldots, n-1$.
Soit $r : \mathbb{C} \to \mathbb{C}$ la rotation de centre $0$ et d'angle $2\pi i/n$ i.e. $r(z) = e^{2\pi i/n} z$.
Soit $s : \mathbb{C} \to \mathbb{C}$ la symétrie par rapport à la droite réelle, i.e. $s(z) = \overline{z}$
Alors
$$D_n = \{1, r, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\}$$
Soit $H = \langle r \rangle = \{1, r, \ldots, r^{n-1}\}$ et
$K = \langle s \rangle = \{1, s\}$

$H$ est distingué dans $D_n$, $H \cap K = \{1\}$, $HK = D_n$
Donc $D_n$ est isomorphe au produit semi-direct $H \rtimes K$ où $K$ agit sur $H$ par :

$$1 * r^j = r^j \qquad j = 0, \ldots, n-1$$
$$s * r^j = s r^j s^{-1} =$$
$$= (srs^{-1})^j = r^{-j}$$
Plus abstraitement, on aurait pu définir le groupe diédral $D_n$ comme
$$\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$$

où $\mathbb{Z}/_{2\mathbb{Z}}$ agit sur $\mathbb{Z}/_{n\mathbb{Z}}$ par

$$\bar{0} * \bar{j} = \bar{j} \qquad j = 0, \dots, n-1$$
$$\bar{1} * \bar{j} = -\bar{j} \qquad j = 0, \dots, n-1$$

On peut vérifier que $*$ est effectivement une action du groupe $\mathbb{Z}/_{2\mathbb{Z}}$ sur $\mathbb{Z}/_{n\mathbb{Z}}$ par morphismes de groupes.

Plus généralement, soit $H$ un groupe <u>abélien</u>. Faisons agir $\mathbb{Z}/_{2\mathbb{Z}}$ sur $H$ par

$$\bar{0} * h = h$$
$$\bar{1} * h = -h$$

Cela définit une action de $\mathbb{Z}/_{2\mathbb{Z}}$ sur $H$ par morphismes. Le produit semi-direct $H \rtimes \mathbb{Z}/_{2\mathbb{Z}}$ a donc un sens. C'est un groupe non commutatif si $H \neq \{1\}, \mathbb{Z}/_{2\mathbb{Z}}$.

Qu'est-ce qu'une action d'un groupe sur un autre groupe par morphismes ? Revenons un instant sur une action d'un groupe sur un ensemble :

Soit $K$ un groupe et $E$ un ensemble. Supposons que

$$* : K \times E \to E$$

est une action. Soit $S(E)$ le groupe symétrique de $E$, i.e.,

$$S(E) = \{ f : E \to E \mid f \text{ bijection} \}$$

$S(E)$ est un groupe sous la composition.

$S(\{1, \dots, n\}) = S_n$.

Définissons

$$\varphi : K \longrightarrow S(E)$$

par

$$\varphi(k)(x) = k * x \qquad k \in K, \; x \in E.$$

On a $\varphi(kl) = \varphi(k) \circ \varphi(l)$

En effet,

$$\varphi(kl)(x) = (kl) * x = k * (l * x)$$
$$= \varphi(k)(\varphi(l)(x)) = \varphi(k) \circ \varphi(l)(x)$$

De plus, $\varphi(1) = id_E \in S(E)$
En effet,

$$\varphi(1)(x) = 1 * x = x = id_E(x).$$

En particulier

$$\varphi(k^{-1}) \circ \varphi(k) = \varphi(k^{-1}k) = \varphi(1) = id$$

et

$$\varphi(k) \circ \varphi(k^{-1}) = \varphi(kk^{-1}) = \varphi(1) = id$$

c-à-d $\varphi(k) : E \to E$ est une bijection
i.e, $\varphi : K \to S(E)$ est bien définie
De plus, $\varphi$ est un morphisme de groupes.
Par conséquent une action $*$ de $K$ sur $E$ donne lieu à un morphisme de groupes $\varphi = \varphi_* : K \to S(E)$. Réciproquement si $\psi : K \to S(E)$ est un morphisme de groupes, la loi externe

$$* = *_\psi : K \times E \to E$$

définie par

$$k * x = \psi(k)(x)$$

est une action de $K$ sur $E$. (vérifiez-le)
Cela établit une correspondance entre les actions de $K$ sur $E$ et les morphismes de $K$ dans $S(E)$:

$$\varphi_{(*_\psi)} = \psi \quad \text{et} \quad *_{(\varphi_{*'})} = *'$$

Si $K$ agit sur un groupe $H$ par morphismes, le morphisme associé

$$\varphi = \varphi_* : K \to S(H)$$

a son image dans le sous-groupe des automorphismes de $H$ $Aut(H)$ de $S(H)$. En effet si $*$ est une action par morphismes,

$$\varphi(k)(xy) = k * (xy) = (k*x)(k*y)$$
$$= \varphi(k)(x) \cdot \varphi(k)(y)$$

i.e, $\varphi(k)$ est un morphisme de $H$ dans lui-même. Comme $\varphi(k) : H \to H$ est une bijection, $\varphi(k) : H \to H$ est un automorphisme et $\varphi(k) \in Aut(H) \subseteq S(H)$.

Par conséquent, si $*$ est une action de $K$ sur $H$ par morphismes de groupes, $\varphi = \varphi_*$ est un morphisme de groupes de $K$ dans $\mathrm{Aut}(H)$. Réciproquement, si $\psi$ est un morphisme de groupes de $K$ dans $\mathrm{Aut}(H)$, alors $* = *_\psi$ est une action de $K$ sur $H$ par morphismes de groupes. On a donc une correspondance parfaite entre actions de $K$ sur $H$ par morphismes, d'une part, et morphismes de $K$ dans $\mathrm{Aut}(H)$, d'autre part.

Rappelons $\mathrm{Aut}(H)$ pour certains groupes $H$ :

$$\mathrm{Aut}(\mathbb{Z}) = \{ id_{\mathbb{Z}}, -id_{\mathbb{Z}} \} \cong \mathbb{Z}/2\mathbb{Z}$$

$$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times = \{ \bar{k} \in \mathbb{Z}/n\mathbb{Z} \mid (k,n) = 1 \}$$

<u>Application</u> Pour construire un produit semi-direct $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/m\mathbb{Z}$ il faudrait préciser un morphisme

$$\varphi : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$$

$|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n)$ où $\phi$ est la fonction totient d'Euler.

Si $\mathrm{pgcd}(m, \phi(n)) = 1$, tout morphisme de $\mathbb{Z}/m\mathbb{Z}$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$ est trivial, i.e., toute action par morphismes de $\mathbb{Z}/m\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$ est triviale.

Autrement dit, si $(m, \phi(n)) = 1$, $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/n \times \mathbb{Z}/m$

Revenons aux applications des Théorèmes de Sylow :

<u>Théorème</u>. Soit $G$ un groupe de cardinal $pq$ où $p$ et $q$ sont premiers, $p < q$. Alors, $G$ est isomorphe au produit semi-direct $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ pour une certaine action de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathbb{Z}/q\mathbb{Z}$ par morphismes

Exemples 1) Déterminons tous les groupes de cardinal 6 à isomorphisme près.
$6 = 2 \times 3$. Soient $p = 2$, $q = 3$.
D'après le Théorème précédent, tout groupe $G$ de cardinal 6 est isomorphe à

$$\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$$

pour une certaine action de $\mathbb{Z}/2$ sur $\mathbb{Z}/3$.
Or $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) = (\mathbb{Z}/3)^\times \cong \mathbb{Z}/2\mathbb{Z}$.
Il y a exactement deux morphismes de $\mathbb{Z}/2$ dans $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ : le morphisme trivial et l'identité.
Le morphisme trivial donne lieu à l'action triviale de $\mathbb{Z}/2\mathbb{Z}$ sur $\mathbb{Z}/3\mathbb{Z}$ et

$$G \cong \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \mathbb{Z}/6\mathbb{Z}$$

L'identité donne lieu à l'action non triviale de $\mathbb{Z}/2\mathbb{Z}$ sur $\mathbb{Z}/3\mathbb{Z}$ qu'on a vu dans l'exemple ci-dessus portant sur le groupe diédral. Dans ce cas

$$G \cong \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \cong D_3$$

Par conséquent, il y a exactement 2 groupes de cardinal 6 à isomorphisme près : $\mathbb{Z}/6\mathbb{Z}$ et $D_3$

2) Déterminons les groupes de cardinal 21
$21 = 3 \times 7$. Soient $p = 3$ et $q = 7$
(Remarquons que $q \equiv 1 \mod 3$)
Tout groupe $G$ de cardinal 21 est isomorphe à $\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$ pour une certaine action de $\mathbb{Z}/3\mathbb{Z}$ sur $\mathbb{Z}/7\mathbb{Z}$ par morphismes. Les actions correspondent à des morphismes de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/7\mathbb{Z}) \cong (\mathbb{Z}/7\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z}$.
Il y a 3 morphismes de $\mathbb{Z}/3$ dans $\mathbb{Z}/6$ :

$\varphi_1, \varphi_2, \varphi_3 : \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/6\mathbb{Z}$

$\varphi_1(\bar{1}) = \bar{0} \qquad \varphi_2(\bar{1}) = \bar{2} \qquad \varphi_3(\bar{1}) = \bar{4}$

les 3 morphismes donnent lieu à 3 groupes

$$\mathbb{Z}/7 \rtimes_{\varphi_1} \mathbb{Z}/3 \ , \quad \underbrace{\mathbb{Z}/7 \rtimes_{\varphi_2} \mathbb{Z}/3 \ \text{ et } \ \mathbb{Z}/7 \rtimes_{\varphi_3} \mathbb{Z}/3}_{\text{non commutatifs.}}$$

$$\mathbb{Z}/7 \rtimes_{\varphi_1} \mathbb{Z}/3 \cong \mathbb{Z}/7 \times \mathbb{Z}/3 \cong \mathbb{Z}/21$$

Donc, à isomorphisme près, il y a au plus 3 groupes de cardinal 21

<u>Exo</u> : les deux non commutatifs sont ils isomorphes ?

## §3 Groupes abéliens de type fini

Rappelons qu'un groupe $G$ est de type fini s'il admet une famille génératrice finie, i.e, s'il existe $n \in \mathbb{N}$ et $x_1, \dots, x_n \in G$ tels que

$$G = \langle x_1, \dots, x_n \rangle$$

sous-groupe engendré

Lorsque $G$ est abélien on a la caractérisation suivante :

__Proposition.__ Soit $G$ un groupe abélien. Alors $G$ est de type fini si et seulement si il existe $n \in \mathbb{N}$ et un morphisme surjectif

$$f : \mathbb{Z}^n \to G.$$

Autrement dit, $G$ est de type fini si et seulement si $G$ est isomorphe à un quotient de $\mathbb{Z}^n$.

__Démo.__ Supposons que $G$ est de type fini. Il existe donc $x_1, \dots, x_n \in G$ qui engendrent $G$. Soit

$$f : \mathbb{Z}^n \longrightarrow G$$

l'application définie par

$$f(a_1, \dots, a_n) = a_1 x_1 + a_2 x_2 + \dots + a_n x_n$$

Cette application est un morphisme car $G$ est commutatif. (exo) $f$ est surjectif car $\{x_1, \dots, x_n\}$ est générateur de $G$.
Réciproquement si $f : \mathbb{Z}^n \to G$ est un morphisme surjectif, $x_1 = f(e_1)$, $x_2 = f(e_2)$, …, $x_n = f(e_n)$ constituent une famille génératrice de $G$, où $e_1 = (1, 0, \dots, 0)$, $e_2 = (0, 1, 0, \dots, 0)$, …, $e_n = (0, \dots, 0, 1) \in \mathbb{Z}^n$.

$\square$

__Corollaire__ Soit $f : G \to H$ un morphisme surjectif de groupes abéliens. Si $G$ est de type fini, alors $H$ est de type fini. $\square$

En particulier, tout quotient d'un groupe abélien de type fini est de type fini.
Est-ce que tout sous-groupe d'un groupe abélien de type fini est de type fini ?