Chapitre V

Le produit direct et semi-direct

Le quotient de groupe, dont nous avons discuté dans le chapitre précédent, permet de « décomposer » (d'une manière) un groupe G en deux groupes plus simples (d'une manière, encore), les groupes N et G/N (sous l'hypothèse que $N \trianglelefteq G$). Dans ce chapitre nous discuterons de la question inverse : peut-on reconstruire G à partir de ces deux « blocs » ? Bien évidemment, cette dernière question suppose que G est connu. Lorsque G n'est pas connu, on peut encore se demander quels sont les groupes que l'on peut construire à partir de deux groupes donnés (qui joueront les rôles de N et de G/N, respectivement).

1. Le produit direct : externe, puis interne

Commençons avec la version la plus facile de cette question : on nous donne deux groupes H et K, et c'est tout. Que pouvons-nous construire avec ?

Définition V.1.1. Soit H et K deux groupes. Nous munissons le produit cartésien

$$H \times K = \big\{(x, y) : x \in H,\ y \in K\big\}$$

de la loi

$$(x, y) \cdot (u, v) = (xu, yv).$$

On appelle $H \times K$, muni de cette loi, le **produit direct (externe)** de H et K.

Comme c'est un produit cartésien, il est muni également de deux **projections canoniques**

$$\begin{aligned} \pi_1 &\colon H \times K \to H, & \pi_1(x, y) &= x, \\ \pi_2 &\colon H \times K \to K, & \pi_2(x, y) &= y. \end{aligned}$$

(Ces projections pourront également être notées π_1 et π_2, ou avec toute autre notation non ambiguë.)

Proposition V.1.2. *L'ensemble $G = H \times K$, muni de cette loi, est un groupe, dans lequel le neutre est (e, e) (c'est à dire, (e_H, e_K)), et l'inverse est*

$$(x, y)^{-1} = (x^{-1}, y^{-1}).$$

Les projections canoniques π_1 et π_2 sont des épimorphismes (morphismes surjectifs).

Remarque V.1.3. Nous pouvons construire $G = H_1 \times H_2 \times \cdots \times H_n = \prod_{i=1}^{n} H_i$ de la même manière, avec projections canoniques $\pi_i \colon G \to H_i$ pour chaque $1 \leq i \leq n$.

Exemple V.1.4. $(\mathbf{R}^2, +) = (\mathbf{R}, +) \times (\mathbf{R}, +)$, et plus généralement, $(\mathbf{R}^{n+m}, +) = (\mathbf{R}^n, +) \times (\mathbf{R}^m, +)$

Voici une manière alternative de définir le produit direct $H \times K$. Elle peut sembler être bien trop compliquée, mais elle a ses avantages.

Définition V.1.5. Soit H, K et G des groupes, et soit $\varphi_1 \colon G \colon \to H$ et $\varphi_2 \colon G \to K$ des morphismes. On dit que le triplet $(G, \varphi_1, \varphi_2)$ vérifie la **propriété universelle du produit direct** $H \times K$ si pour tout autre triplet (L, ψ_1, ψ_2), où $\psi_1 \colon L \to H$ et $\psi_2 \colon L \to K$ sont des morphismes, il existe un unique morphisme $\rho \colon L \to G$ qui rend le diagramme suivant commutatif :

$$\begin{tikzcd}
& & H \\
L \arrow[r, dashed, "\exists!\rho"] \arrow[urr, bend left, "\psi_1"] \arrow[drr, bend right, "\psi_2"'] & G \arrow[ur, "\varphi_1"] \arrow[dr, "\varphi_2"'] & \\
& & K
\end{tikzcd}$$

Autrement dit, il existe un unique $\rho \colon L \to G$ qui vérifie $\psi_i = \varphi_i \circ \rho$ pour $i = 1, 2$.

Dans l'Exercice V.2 on montre que $(H \times K, \pi_1, \pi_2)$ vérifie cette propriété universelle, et de surcroît, ce triplet est caractérisé, à isomorphisme unique près, par la propriété universelle. Dans le contexte des **catégories**, que nous ne définirons pas ici, une caractérisation à isomorphisme unique près est le mieux que l'on peut espérer, et la propriété universelle est la **définition** du produit direct – qui n'est plus juste le groupe $H \times K$, mais le triplet $(H \times K, \pi_1, \pi_2)$.

Étudions un peu plus ce triplet $(H \times K, \pi_1, \pi_2)$. Que peut-on dire de $\pi_1 \colon H \times K \to H$, par exemple ? Calculons sont image et sont noyau :

— $\operatorname{img} \pi_1 = H$. Autrement dit, π_1 est surjectif. Bon, on le savait déjà, rien de nouveau ici.

— $\ker \pi_1 = \{e\} \times K$. Ça c'est plus intéressant – le noyau est isomorphe à K, et de surcroît par un isomorphisme canonique, qui est juste la restriction de π_2 :

$$\pi_2(e, y) = y.$$

$$\begin{tikzcd}
G = H \times K \arrow[d, "\pi_1"'] \arrow[drr, "\pi_2"] & & L \arrow[ll, dashed, "\exists!\,\rho"'] \arrow[dll, "\varphi_1"'] \arrow[d, "\varphi_2"] \\
H & & K
\end{tikzcd}$$

$$\rho(g) := \left(\varphi_1(g), \varphi_2(g)\right)$$

$$\begin{tikzcd}
G_1 \arrow[loop left, dashed, "\exists!"] \arrow[rr, dashed, bend left, "\exists!\,\rho"] \arrow[d, "\varphi_1"] \arrow[drr, "\varphi_2"] & & G_2 \arrow[ll, dashed, "\exists!\,\eta"] \arrow[dll, "\psi_1"'] \arrow[d, "\psi_2"] \\
H & & K
\end{tikzcd}$$

$(G_1, \varphi_1, \varphi_2)$
(G_2, ψ_1, ψ_2) vérifiant la prop. universelle

$\overset{?}{\Longrightarrow}$ isomorphes

$\exists!\, \rho : G_1 \to G_2$ et $\exists!\, \eta : G_2 \to G_1$

qui rendent le diag. commutatif : $\begin{cases} \varphi_1 = \psi_1 \circ \rho \\ \varphi_2 = \psi_2 \circ \rho \\ \psi_1 = \varphi_1 \circ \eta \\ \vdots \end{cases}$

$\Rightarrow \eta \circ \rho : G_1 \to G_1 \;\Big|\; \varphi_1 = \varphi_1 \circ (\eta \circ \rho) = \varphi_1 \circ id$

$\varphi_2 = \varphi_2 \circ (\eta \circ \rho) = \varphi_2 \circ id$

$\Rightarrow$ (prop. univ. pour G_1) : $\eta \circ \rho = id$

$\Rightarrow \rho \circ \eta = id$

même argument : $\rho \circ \eta = id_{G_2}$

$\therefore$ $\eta = \rho^{-1}$, η et ρ sont des isomorphismes.

Unicité donnée par la prop. univ.

$$\begin{tikzcd}
\ker \pi_2 = H \times \{e\} \arrow[dr] \arrow[dd, dashed] & & \ker \pi_1 = \{e\} \times K \arrow[dl] \arrow[dd, dashed, "\pi_2"] \\
& G = H \times K \arrow[dl, "\pi_1"'] \arrow[dr, "\pi_2"] & \\
H & & K
\end{tikzcd}$$

$$\pi_2\big|_{\ker \pi_1} : \ker \pi_1 \simeq K.$$

$$\pi_1\big|_{\ker \pi_2} : \ker \pi_2 \simeq H.$$

L'application inverse de cet isomorphisme est le **plongement canonique** de K dans $H \times K$:

$$\iota_2 \colon K \to H \times K, \qquad \iota_2(y) = (e, y).$$

— De la même manière, $\ker \pi_2 = H \times \{e\}$ est canoniquement isomorphe à H : dans un sens par la restriction de π_2, et dans le sens inverse par le plongement canonique

$$\iota_1 \colon H \to H \times K, \qquad \iota_1(x) = (x, e).$$

Puisque H est canoniquement isomorphe au sous-groupe $H \times \{e\} \leq H \times K$, nous aurons tendance à faire abstraction de la distinction. Autrement dit, nous allons prétendre que $x \in H$ est le même que $(x, e) \in H \times K$, de sorte que $H \leq H \times K$, et même $H \trianglelefteq H \times K$, puisque c'est le noyau de π_2. De la même manière, nous allons prétendre que $y \in K$ est le même que $(e, y) \in H \times K$, de sorte que $K \trianglelefteq H \times K$.

Et voici une autre manière (tentative, pour l'instant) de présenter un produit direct $H \times K$, comme un groupe G dont H et K sont des sous-groupes. Que peut-on en dire ?

Définition V.1.6. Soit G et groupe et H et K deux sous-groupes. Alors on dit que G est un **produit direct interne** de H et K, que l'on notera provisoirement par $G = H \times_i K$, si :
— $H \cap K = \{e\}$.
— $G = HK$.
— Let sous-groupes H et K **commutent** : si $x \in H$ et $y \in K$, alors $xy = yx$.

Proposition V.1.7. *Soit H et K deux groupes, et $G = H \times K$ leur produit directe (externe). Identifions H avec $H \times \{e\}$ et K avec $\{e\} \times K$ comme plus haut. Sous cette identification, H et K sont des sous-groupes de G, et $G = H \times_i K$ est leur produit direct interne.*

Réciproquement, soit G un groupe, et $H, K \leq G$ des sous-groupes de sorte que $G = H \times_i K$ est le produit direct interne. Alors tout membre de G s'écrit d'une manière unique comme xy avec $x \in H$ et $y \in K$, et si $x, u \in H$ et $y, v \in K$, alors :

$$(xy)(uv) = (xu)(yv), \qquad (xy)^{-1} = x^{-1}y^{-1}$$

(où $xu, x^{-1} \in H$ et $yv, y^{-1} \in K$). Autrement dit, l'application

$$\rho \colon H \times K \to G, \qquad \rho(x, y) = xy = \pi_1(x, y)\pi_2(x, y)$$

est un isomorphisme $H \times K \cong G$.

Démonstration. .... ■

Autrement dit, le produit direct externe est aussi un produit direct interne, et tout produit direct interne est canoniquement isomorphe au produit direct externe. Dans la suite, nous ferons abstraction de la distinction, notant les deux par $G = H \times K$.

Preuve : On a $G = H \times K$.

$H = H \times \{e\} \trianglelefteq G$ $\qquad$ $K = \{e\} \times K \trianglelefteq G$

- $H \cap K = \{(e,e)\} = \{e_G\}$.

- $HK = \{(x,e)\cdot(e,y) : x \in H, \ y \in K\}$

$= \{(x,y) : x \in H, \ y \in K\} = \cancel{H \times K}$

$= G$.

- Soit $x = (x,e) \in H$.

$y = (e,y) \in K$

$(x,e)(e,y) = (x,y)$

$= (e,y)(x,e)$

<u>Réciproquement</u> : Soit $G = H \times_i K$.

<u>alors</u> : 1. $G = HK$ donc tout $z \in G$ s'écrit comme $z = xy$, $x \in H$, $y \in K$

2. unicité : supposons que $z = xy = x'y'$, $x, x' \in H$, $y, y' \in K$.

$$\Rightarrow \underbrace{(x')^{-1} x}_{\in H} = \underbrace{y' y^{-1}}_{\in K} \in H \cap K = \{e\}.$$

$$\Rightarrow x' = x, \quad y' = y.$$

Soit $x, y, u, v \in G$, $x, u \in H$ $y, v \in K$.

alors : $(xy)(uv) = x\underbrace{yu}v = x\underbrace{uy}v = \underbrace{(xu)}_{H}\underbrace{(yv)}_{K}$

car H et K commutent.

Conclusion : l'application

$$H \times K \longrightarrow G$$
$$(x, y) \longmapsto xy$$

est un morphisme, et il est bijectif d'après ce qu'on a montré avant. $\Rightarrow$ isomorphisme

$$H \times K \cong G$$

$$(x, y) \longmapsto xy$$

Rmq. Soit G un gr. $H, K \leq G$.

supposons $\underbrace{H \cap K = \{e\}}$ $\underbrace{HK = G}$.

alors sont équivalents :

I. H et K commutent : $xy = yx$ $\forall x \in H$ $y \in K$

II. $H, K \trianglelefteq G$.

Preuve. I $\Rightarrow$ II.

Soit $z \in G$. $\Rightarrow$ $\exists$ $x \in H$, $y \in K$ tq $z = xy$.

alors : $yH = Hy$ car H et K commutent

$\Rightarrow$ $zH = xyH = xHy = Hy = Hxy = Hz$.

$\therefore$ $H \trianglelefteq G$. Pareil pour K.

II $\Rightarrow$ I.

Soit $x \in H$, $y \in K$.

étudions $[x,y] = xyx^{-1}y^{-1}$ = le <u>commutateur</u> de x, y.

$yx^{-1}y^{-1} \in yHy^{-1} = H$ (car $H \trianglelefteq G$)

$\Rightarrow xyx^{-1}y^{-1} \in xH = H$

$xyx^{-1} \in xKx^{-1} = K$ ($K \trianglelefteq G$)

$xyx^{-1}y^{-1} \in Ky^{-1} = K$.

$\therefore [x,y] \in H \cap K = \{e\} \Rightarrow xyx^{-1}y^{-1} = e$

$\boxed{xy = yx}$. donc H et K commutent ! ✓.

Remarque V.1.8. Soit G un groupe, $H, K \leq G$ des sous-groupes, et supposons que les deux premières conditions de la définitions d'un produit directe interne sont vérifiées :
— $H \cap K = \{e\}$.
— $G = HK$.
Alors H et K commutent si et seulement si les deux sont des sous-groupes distingués.

Démonstration. Dans un sens, supposons que H et K commutent. Soient $x \in H$, $u \in K$, et $w \in G$. Puisque $G = HK$, on a $w = yv$ avec $y \in H$ et $v \in K$. Ainsi,

$$wxw^{-1} = yvxv^{-1}y^{-1} = yxy^{-1}vv^{-1} = yxy^{-1} \in H,$$
$$wuw^{-1} = yvuv^{-1}y^{-1} = vuv^{-1}yy^{-1} = vuv^{-1} \in K.$$

Autrement dit, $wHw^{-1} \subseteq H$ et $wKw^{-1} \subseteq K$ pour tout $w \in G$, d'où $H, K \trianglelefteq G$.

Pour la réciproque, supposons que $H, K \trianglelefteq G$. Soit $x \in H$ et $u \in K$, et étudions $[x, u] = xux^{-1}u^{-1}$ (cet élément s'appelle le **commutateur** de x et u). Puisque $H \trianglelefteq G$, on a $ux^{-1}u^{-1} \in uHu^{-1} = H$, donc $[x, u] \in H$. D'une manière similaire, $xux^{-1} \in xKx^{-1} = K$, donc $[x, u] \in K$. Donc $[x, u] \in H \cap K = \{e\}$, c'est à dire $[x, u] = e$. Autrement dit, $xu = ux$, et nous avons montré que H et K commutent. ■

Par conséquent, $G = H \times_i K$ si et seulement si :
— $H \cap K = \{e\}$.
— $G = HK$.
— $H, K \trianglelefteq G$.

2. Le produit semi-direct : interne, puis externe

Le produit direct interne nous permet de dire que un groupe G est obtenu de deux sous-groupes $H, K \leq G$ d'une manière particulièrement simple. Il s'avère être très utile d'affaiblir la définition en prenant que « la moitié » de la dernière condition :

Définition V.2.1. Soit G un groupe et $H, K \leq G$ deux sous-groupes. Nous disons que $G = H \rtimes K$, ou que G est le **produit semi-direct interne** de H avec K (l'ordre est important) si
— $H \cap K = \{e\}$.
— $G = HK$. (ou : $G = KH$)
— $\underline{H \trianglelefteq G}$. (ou : $K \leq N_G(H)$)

9431

$N_G(H) = \{g \in G : gHg^{-1} = H\}$

⚠ Notez bien que dans $H \rtimes K$ et dans $H \trianglelefteq G$, le triangle pointe vers H !
On pourrait également définir $G = H \ltimes K$, en replaçant $H \trianglelefteq G$ par $K \trianglelefteq G$: le triangle pointe alors toujours vers K.

On pourrait également définir $G = H \ltimes K$ (triangle vers K) si $H \cap K = \{e\}$, $HK = G$, et $K \trianglelefteq G$ – autrement dit, si $G = K \rtimes H$.

Remarque V.2.2. Soit G un groupe, et $H, K \leq G$. Si $H \trianglelefteq G$, alors $N_G(H) = G$, et en particulier, $K \leq N_G(H)$. Réciproquement, d'après le 2e théorème d'isomorphisme (Théorème III.3.3), si $K \leq N_G(H)$, alors $H \trianglelefteq HK = KH$. Si on sait d'ailleurs que $HK = G$ (ou que $KH = G$), alors $H \trianglelefteq G$.

Il en découle que dans Définition V.2.1 :
— La condition $G = HK$ peut être remplacée par $G = KH$.
— La condition $H \trianglelefteq G$ peut être remplacée par $K \leq N_G(H)$ (qui est, superficiellement, plus faible).

Lemme V.2.3. *Soit G un groupe, et $H, K \leq G$ des sous-groupes de sorte que $G = H \rtimes K$ est le produit semi-direct interne. Pour $x \in H$ et $y \in K$, posons*

$$\varphi_y(x) = yxy^{-1}$$

(c'est la conjugaison par y). Alors
— *L'application $y \mapsto \varphi_y$ est un morphisme $K \to \mathrm{Aut}(H)$ (en particulier, chaque φ_y est un automorphisme de H).*
— *Tout membre de G s'écrit d'une manière unique comme xy avec $x \in H$ et $y \in K$, et si $x, u \in H$ et $y, v \in K$, alors :*

$$(xy)(uv) = \big(x\varphi_y(u)\big)\big(yv\big), \qquad (xy)^{-1} = \varphi_{y^{-1}}(x^{-1})y^{-1}$$

(où $x\varphi_y(u), \varphi_{y^{-1}}(x^{-1}) \in H$ et $yv, y^{-1} \in K$).

(Donc $(x, y) \mapsto xy$ est une bijection entre pe produit cartésien $H \times K$ et G, bien que ce ne soit pas forcément un isomorphisme de groupes.)

Ainsi, si $G = H \rtimes K$, alors nous pouvons reconstruire G avec sa loi de H et K – à conditions de connaître également l'application $y \mapsto \varphi_y$. Essayons de faire pareil mais sans connaître G à l'avance.

Définition V.2.4. Soit H et K deux groupes, et soit $\alpha \colon K \to \mathrm{Aut}(H)$ un morphisme. Pour $y \in K$, notons $\alpha(y) \in \mathrm{Aut}(H)$ plutôt par α_y, de sorte que l'on puisse écrire $\alpha_y(x)$ pour $x \in H$.

Le produit **semi-direct externe** de H et de K **selon** α, noté $H \rtimes_\alpha K$, consiste de l'ensemble $H \times K$ (le produit cartésien), muni de la loi suivante :

$$(x, y) \cdot_\alpha (u, v) = \big(x\alpha_y(u), yv\big).$$

Preuve :

D'abord : $\forall y \in K$: $\varphi_y \in \mathrm{Aut}(H)$.

En effet : $\forall x \in H$: $\varphi_y(x) = yxy^{-1} \in yHy^{-1} = H$

$(H \trianglelefteq G)$

$\Rightarrow \varphi_y : H \to H$. ($\varphi_y$ est un endomorphisme de H)

On sait déjà que c'est un morphisme : $\varphi_y(xx') = \varphi_y(x)\varphi_y(x')$

Soit $v \in K$ aussi. alors.

$$\underbrace{\varphi_y \circ \varphi_v (x) = \varphi_y(vxv^{-1}) = yvxv^{-1}y^{-1} = yvx(yv)^{-1}}_{= \varphi_{yv}(x)}$$

$\Rightarrow \varphi_y \circ \varphi_{y^{-1}} = \varphi_{y^{-1}} \circ \varphi_y = \varphi_e = id$.

$\Rightarrow \varphi_y$ est un morphisme inversible, c'est donc un isomorphisme.

Donc : $\varphi_y : H \xrightarrow{\sim} H$ est un automorph. de H : $\underline{\forall y \in K}$ $\varphi_y \in \mathrm{Aut}(H)$.

<u>et</u> : on a vu que $\varphi_y \circ \varphi_{y'} = \varphi_{yy'}$

<u>c'à'd</u> : $y \longmapsto \varphi_y$ est un morphisme

$$K \longrightarrow \mathrm{Aut}(H).$$

Tout $z \in G$ s'écrit d'une manière unique comme xy avec $x \in H$, $y \in K$: comme pour le pr. directe.

$$\left(\Longleftrightarrow \quad \begin{aligned} H \times K &\longrightarrow G \\ (x, y) &\longmapsto xy \end{aligned} \quad \text{est une bijection} \right)$$

Soit $x y, u v \in G$; $x, u \in H$
$y, v \in K$:

$$(xy)(uv) = xyuv = x(yuy^{-1})yv$$

$$= \underbrace{\left(x\,\varphi_y(u)\right)}_{H} \cdot \underbrace{\left(y v\right)}_{K}$$

$$(xy)^{-1} = y^{-1}x^{-1} = (y^{-1}x^{-1}y)y^{-1} = \underbrace{\varphi_{y^{-1}}(x^{-1})}_{H} \cdot \underbrace{y^{-1}}_{K}$$

$(x,y) \cdot_\alpha (u,v) = (x\alpha_y(u), yv)$

Ainsi, tout produit semi-direct interne est aussi un produit direct externe. La réciproque est vraie également :

Proposition V.2.5. *Soit H et K deux groupes, et soit $\alpha\colon K \to \mathrm{Aut}(H)$ un morphisme.*

(i) *Le produit semi-direct externe $H \rtimes_\alpha K = (H \times K, \cdot_\alpha)$ est un groupe.*

(ii) *Les applications*

$$\iota_1\colon H \to H \times K, \qquad \iota_1(x) = (x,e),$$
$$\iota_2\colon K \to H \times K, \qquad \iota_2(y) = (e,y),$$

sont des plongements de H et K dans $H \rtimes_\alpha K$. Ainsi, identifiant $x \in H$ avec (x,e) et $y \in K$ avec (e,y), nous pouvons considérer que H et K sont des sous-groupes de $H \rtimes_\alpha K$.

(iii) *Avec ces identifications, $H \rtimes_\alpha K$ est un produit semi-direct interne de $H \rtimes K$. En particulier, pour $x \in H$ et $y \in K$:*

$$\varphi_y(x) = yxy^{-1} = \alpha_y(x),$$

et α est l'application $y \mapsto \varphi_y$.

Exemple V.2.6. Soit G le groupe diédral D_n, pour $n \geq 3$. Soit $H \subseteq D_n$ les rotations, et soit $s \in D_n$ une réflexion. Posons $K = \langle s \rangle = \{e,s\}$. Alors H et K sont des sous-groupes, $H \cap K = \{e\}$ et $HK = D_n$. De surcroît, $H \trianglelefteq D_n$ (car tout sous-groupe d'indice 2 est distingué).

Ainsi, $D_n = H \rtimes K$, en tant que produit directe interne. Nous pouvons calculer φ_y explicitement pour $y \in \{e,s\}$:

$$\varphi_e(x) = x, \qquad \varphi_s(x) = x^{-1}$$

(ça on "trouve dans l'autre sens")

En particulier, H et K ne commutent pas, donc $D_n \ncong H \times K$.

Lemme V.2.7. *Soit $(G,+)$ un groupe additif (donc abélien). Définissons $\alpha_i\colon G \to G$ pour $i \in \mathbf{Z}/2\mathbf{Z}$ par :*

$$\alpha_{\bar{0}}(x) = x, \qquad \alpha_{\bar{1}}(x) = -x.$$

Alors $\alpha_i \in \mathrm{Aut}(G)$, et $\alpha\colon \mathbf{Z}/2\mathbf{Z} \to \mathrm{Aut}(G)$ est un morphisme.

Ceci nous permet de construire D_n comme produit semi-direct externe : $D_n \cong \mathbf{Z}/n\mathbf{Z} \rtimes_\alpha \mathbf{Z}/2\mathbf{Z}$, selon le α du Lemme V.2.7.

Preuve :

I. $H \rtimes_\alpha K$ est un groupe, avec la loi $(x,y)\cdot_\alpha(u,v) = (\underbrace{x\alpha_y(u)}_{H}, \underbrace{yv}_{K})$.

(i) clos pour la loi. ✓

(ii) associatif :

$$\big((x,y)\cdot_\alpha(u,v)\big)\cdot_\alpha(s,t) = (x\alpha_y(u), yv)\cdot_\alpha(s,t)$$

$$= (x\alpha_y(u)\alpha_{yv}(s), \underline{yvt})$$

$$\text{———} \; (\text{—} \quad \text{—}) = (x,y)\cdot_\alpha(u\alpha_v(s), vt)$$

$$= (x\alpha_y(u\alpha_v(s)), \underline{yvt}) \checkmark$$

$$x\alpha_y(u)\alpha_y\circ\alpha_v(s)$$

$$\ldots = \quad x\alpha_y(u)\alpha_{yv}(s) \checkmark$$

(iii) neutre à gauche :

$$\underbrace{(e,e)}\cdot_\alpha (x,y) = (e\,\underbrace{\alpha_e}_{\text{id}}(x),\ ey) = (x,y)\ \checkmark$$

(α_e = le neutre de Aut(H) = id_H).

(iv) inverse à gauche.

$$\underbrace{(\alpha_{y^{-1}}(x^{-1}), y^{-1})}\cdot_\alpha (x,y) = (\alpha_{y^{-1}}(x^{-1})\alpha_{y^{-1}}(x),\ y^{-1}y)$$

$$= (\alpha_{y^{-1}}(\overbrace{x^{-1}x}^{e}),\ \overbrace{y^{-1}y}^{e})$$

$$= (e,e).\ \checkmark$$

<u>Mq :</u> $H \to H \rtimes_\alpha K$ $\quad\quad$ $K \to H \rtimes_\alpha K$

$x \mapsto (x, e)$ $\quad\quad$ $y \mapsto (e, y)$

sont des plongements = morphismes injectifs.

Injectifs : ✓

Morphismes : $(x, e) \circ_\alpha (u, e) = (x\alpha_e(u), ee)$

$= (xu, e)$ ✓

$(e, y) \circ_\alpha (e, v) = (e\alpha_y(e), yv) = (e, yv)$. ✓

désormais on identifie H et K

avec leurs images dans G : $x = (x, e) \in H$

$y = (e, y) \in K$.

Mq avec ces identifications : $H \rtimes_\alpha K = H \rtimes K$ (interne), et $\alpha_y = \varphi_y$.

- $H \cap K = (H \times \{e\}) \cap (\{e\} \times K) = \{(e,e)\}$. ✓

- $HK = \left\{ \underbrace{(x,e)}_{x} \cdot_\alpha \underbrace{(e,y)}_{y} \; ; \; \begin{array}{l} x \in H \\ y \in K \end{array} \right\}$

$= \left\{ \begin{array}{l} (x\,\alpha_e(e), y) \\ = (x,y) \end{array} \; ; \; \begin{array}{l} x \in H \\ y \in K \end{array} \right\} = \underbrace{H \times K}_{\text{pr. cartésien}}$

= l'ensemble sous-jacent du groupe $H \rtimes_\alpha K$.

– $H \trianglelefteq H \rtimes_\alpha K$:

Soit $a = (x, e) \in H$.

$$(\underset{\overset{\cap}{H}}{u}, \underset{\overset{\cap}{K}}{v}) \in H \rtimes_\alpha K.$$

$$(u,v) \cdot_\alpha (x,e) = (u\,\alpha_v(x), v)$$

$$= (u\,\alpha_v(x)\,u^{-1} \underbrace{u}_{=\alpha_e(u)}\ v)$$

$$= \underbrace{(u\,\alpha_v(x)\,u^{-1}, e)}_{\in H \times \{e\} = H} \cdot_\alpha (u,v)$$

$$\therefore \quad (u,v) \cdot_\alpha H \subseteq H \cdot_\alpha (u,v).$$

$$\therefore \quad H \trianglelefteq H \rtimes_\alpha K$$

Donc : $H \rtimes_\alpha K$ est bien un pr. semi-direct interne de H et K.

Soit $y \in K$. $\varphi_y \in \mathrm{Aut}(H)$ $= ?$

Soit $x \in H$

on a calculé l'inv. dans $H \rtimes_\alpha K$

$$\varphi_y(x) = yxy^{-1} = (e,y) \circ_\alpha (x,e) \circ_\alpha \overbrace{(e,y^{-1})}$$

$$(e\alpha_y(x)\alpha_{ye}(e),\ yey^{-1}) = (\alpha_y(x), e)$$

$$= \alpha_y(x).$$

autrement dit : $\forall g \in K$:

$$\varphi_g = \alpha_g \in \mathrm{Aut}(H).$$

Preuve de : Si $(G,+)$ est un gp additif (abélien)

$\alpha_{\bar{0}}(x) = x$

$\alpha_{\bar{1}}(x) = -x$

$\alpha_i \in \mathrm{Aut}(G)$

et $\mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(G)$ est un morphisme.

$i \mapsto \alpha_i$

$\alpha_{\bar{0}} = id \in \mathrm{Aut}(G)$.

$\alpha_{\bar{1}}$ est bij, $\alpha_{\bar{1}}(x+y) = -x-y$

$= \alpha_{\bar{1}}(x) + \alpha_{\bar{1}}(y)$

$\Rightarrow \alpha_{\bar{1}} \in \mathrm{Aut}(G)$

$\alpha_{\bar 0} \circ \alpha_{\bar 0} = id = \alpha_{\bar 0}$

$\alpha_{\bar 0} \circ \alpha_{\bar 1} = \alpha_{\bar 1}$

$\alpha_{\bar 1} \circ \alpha_{\bar 0} = \alpha_{\bar 1}$.

$\alpha_{\bar 1} \circ \alpha_{\bar 1} = id = \alpha_{\bar 0}$ (facile à vérifier).

$\therefore$ $i \longmapsto \alpha_i$ est un morphisme de $\mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(G)$ $\blacksquare$

$\Rightarrow$ $\forall$ grp additif $(G,+)$ on peut construire : $G \rtimes_\alpha \mathbb{Z}/2\mathbb{Z}$ (où α est comme plus haut.)

En particulier :

$$\underbrace{\mathbb{Z}/n\mathbb{Z}}_{\substack{\wr \\ \{\text{rotations dans } D_n\}}} \rtimes_{\alpha} \mathbb{Z}/2\mathbb{Z} \simeq D_n$$

$$\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\} \quad \wr \quad \{e, \underbrace{\text{une réflexion}}_{s}\}$$

si on identifie par ces isom : $\varphi_e = \alpha_{\bar{0}} = id$, $\varphi_s = \alpha_{\bar{1}} =$ inverse

Exo Soit $s \in D_n$ une rotation.

Soit $r \in D_n$ un générateur du groupe des rotations.

Mq

$$\mathbb{Z}/n\mathbb{Z} \rtimes_\alpha \mathbb{Z}/2\mathbb{Z} \to D_n$$

$$(\bar{k}, \bar{0}) \longmapsto (r^k, e) = r^k$$

$$(\bar{k}, \bar{1}) \longmapsto (r^k, s) = r^k s$$

est un isomorphisme.

Exercices

Exercice V.1. Montrer que si $H \cong H'$ et $K \cong K'$ alors $H \times K \cong H' \times K'$.
Montrer que $(H \times K) \times L \cong H \times (K \times L)$.

Exercice V.2. Soit H et K deux groupe, $H \times K$ leur produit direct, et π_1 et π_2 les projection canoniques. Montrer que :

— $(H \times K, \pi_1, \pi_2)$ vérifie la propriété universelle du produit direct (Définition V.1.5).

— Si $(G, \varphi_1, \varphi_2)$ vérifie la propriété universelle du produit direct, alors il existe un **unique isomorphisme** $\rho\colon G \to H \times K$ de sorte que $\varphi_i = \pi_i \circ \rho$ (et donc $\pi_i = \varphi_i \circ \rho^{-1}$).

Exercice V.3 (Théorème des restes chinois)**.** Soit m et n sont premiers entre eux. Alors l'application $a + mn\mathbf{Z} \mapsto (a + n\mathbf{Z}, a + m\mathbf{Z})$ est un isomorphisme $\mathbf{Z}/mn\mathbf{Z} \cong \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$.
Indication : montrer que c'est un morphisme (en particulier, que c'est bien défini), et calculer son noyau.

que des évidences

Exercice V.4. Supposons que $G = H \rtimes K$.

(i) L'application $\pi\colon G \to K$, $\pi(xy) = y$ (où $x \in H$ et $y \in K$) est un épimorphisme. On l'appelle la **projection canonique** sur K.

(ii) Le noyau de la projection canonique sur est H.

(iii) Soit $s\colon K \to G$ l'application identité. Alors c'est encore un morphisme (un plongement), et $\pi \circ s = \mathrm{id}_K$.

Exercice V.5. Montrer la réciproque de l'exercice précédent. Soit G un groupe, $\pi\colon G \to K$ un épimorphisme, et soit $H = \ker \pi$. Supposons en outre que $s\colon K \to G$ est un morphisme tel que $\pi \circ s = \mathrm{id}_K$ (on dit dans ce cas que s est une **section** de π). Alors s est un plongement, de sorte que $\operatorname{img} s \cong K$, et $G = H \rtimes (\operatorname{img} s)$. $(= H \rtimes K)$

$$H \hookrightarrow G \overset{\pi}{\twoheadrightarrow} K, \qquad K \xrightarrow{s} G$$