6. Extensions et produit semi-direct

[Perrin] chapitre I, §6

Dans l'objectif de « comprendre » « tous » les groupes (hum... objectif plutôt déraisonnable, d'où les guillemets, mais les objectifs déraisonnables sont la meilleure source d'inspiration en math), dans le cas des groupes finis la stratégie mise en oeuvre pour la CGFS (rappel séance d'intro) est la suivante :

① comprendre les groupes simples

② comprendre comment, étant donnés deux groupes N et Q, fabriquer tous les groupes G possédant N comme sous-groupe distingué avec Q comme quotient G/N.

L'étape ② permet en principe de fabriquer tous les groupes à partir des groupes simples. On appelle ces étapes :

① le problème de la classification,

② le problème de l'extension,

et on dit que G est extension de Q par N (attention à l'ordre !).
Dans le présent §6 on donne quelques outils pour formaliser ces notions et on décrit un cas simple d'extension : le produit semi-direct.

6.1. Produit semi-direct interne

Déf Soient G un groupe, H, N des sous-groupes avec $N \lhd G$.
On dit que G est produit semi-direct de H par N si les conditions suivantes sont vérifiées : (1) $NH = G$

(2) $H \cap N = 1$. ⊠

Dans ce cas tout élément de G s'écrit (grâce à (1)) de manière unique (grâce à (2)) sous la forme $g = nh$, $n \in N$, $h \in H$.
On écrit $G = N \rtimes H$.

Le symbole $\rtimes$ rappelle

- le symbole de produit direct $\times$ (les produits directs sont des PSD)
- le symbole $\triangleleft$ (le sous-groupe N est distingué).

Pour multiplier deux éléments $g_1 = n_1 h_1$ et $g_2 = n_2 h_2$ et les remettre sous la forme on fait comme ça:

$$g_1 g_2 = n_1 h_1 n_2 h_2 = \underbrace{n_1 \underbrace{h_1 n_2 h_1^{-1}}_{\substack{\in N \\ \text{car } N \triangleleft G}}}_{\in N} \underbrace{h_1 h_2}_{\in H}$$

Ici on voit que la « composante sur H » de $g_1 g_2$ est $h_1 h_2$, autrement dit l'application $G \longrightarrow H$
$g = hn \longmapsto h$ bien définie ($\exists!\, h$)

est un morphisme de groupes, surjectif (évident) et de noyau N (idem). Donc G est extension de H par N.

<u>Prop</u> Soient G, H, N tq $G = N \rtimes H$. Alors LCSSE(★):

(1) H est distingué dans G

(2) N centralise H (on dit aussi commute avec H, càd) $\forall n \in N, \forall h \in H, nh = hn$

(3) L'application $N \times H \to G$, $(n, h) \longmapsto nh$ est un isomorphisme de groupes.

produit direct (externe)

<u>NB</u> on note $Z_G(H)$ ou parfois $C_G(H)$ le sous-groupe

$$\{g \in G,\ gh = hg,\ \forall h \in H\}$$

appelé centralisateur ou commutant de H dans G.

Bien sûr, pour $H, N \subset G$ on a $N \subset Z(H) \iff H \subset Z(N)$ puisque les deux signifient que « tout élément de N commute avec tout élément de H »

(★) Les conditions suivantes sont équivalentes

<u>Dém prop</u> (1) $\Rightarrow$ (2) Si $n\in N$ et $h\in H$, l'écriture de nhn^{-1} sous la forme « nh » est $nhn^{-1} = \underbrace{n\underbrace{hn^{-1}h^{-1}}_{\in N}}_{\in N} h$ d'une part,

$$= 1\cdot \underbrace{nhn^{-1}}_{\in H} \quad \text{d'après (1), d'autre part.}$$

Par unicité on a $nhn^{-1}=h$ donc N centralise H

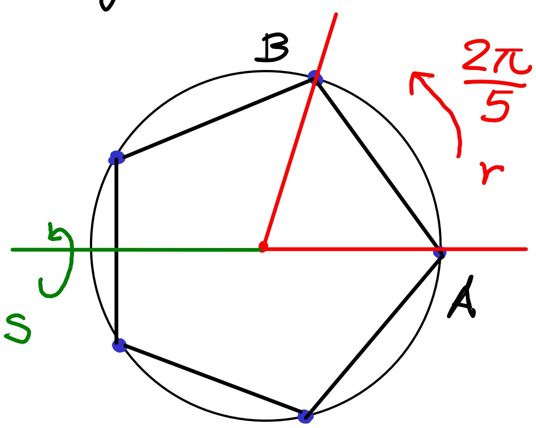
(2) $\Rightarrow$ (3) Notons $\varphi : N\times H \to G$, $\varphi(n,h)=nh$. On a

$$\varphi((n_1,h_1),(n_2,h_2)) = \varphi(n_1n_2,h_1h_2) = n_1n_2h_1h_2$$
$$= n_1h_1n_2h_2 \quad \text{car } n_2h_1=h_1n_2 \text{ d'après (2)}$$

donc φ est un morphisme de groupes. Il est surjectif car tout $g\in G$ s'écrit $g=nh=\varphi(n,h)$, injectif car $N\cap H=1$, donc iso.

(3) $\Rightarrow$ (1) clair car dans le produit direct $N\times H$, le sous-groupe $\{1\}\times H$ est distingué, donc $H=\varphi(\{1\}\times H)$ distingué dans G. $\boxtimes$

<u>Exemple</u> : le groupe diédral



$\mathbb{D}_n := \{$isométries planes du n-gone régulier$\}$

rotation $r = r_{O,2\pi/n}$ d'ordre n

symétrie de droite $s = s_{(O,\vec{\imath})}$ d'ordre 2
(réflexion)

Sommets = racines de 1
= les $r^i(A)$

$$srs^{-1} = r^{-1} \quad \text{(vérifiez !)}$$

Soit $G=\langle r,s\rangle \subset O_2(\mathbb{R})$, on a donc $G\subset \mathbb{D}_n$. Montrons $G=\mathbb{D}_n$.

Si $g\in \mathbb{D}_n$ isométrie du n-gone, $g(A)$ est un sommet : $g(A)=r^i(A)$
(pour un $i\in\{0,\dots,n-1\}$)

Posons $h = r^{-i}g$, donc $h(A) = A$.

Soit B un voisin de A, alors $h(B)$ est aussi un voisin de A :

(i) $h(B) = B$, dans ce cas posons $k = h$

ou (ii) $h(B) = B'$, dans ce cas posons $k = sh$.

Dans les deux cas on a $k(A) = A$ et $k(B) = B$ (et bien sûr $k(0) = 0$).

Or $(0, A, B)$ forme un <u>repère affine</u> du plan(★). Toute isométrie qui fixe un tel repère est l'identité, donc $k = id$.

Ceci démontre que $G = \mathbb{D}_n$ puisque $g = r^i$ dans le cas (ii)

$g = r^i s = s r^{-i}$ dans le cas (ii).

La relation $srs^{-1} = r^{-1}$ montre que $N = \langle r \rangle \simeq \mathbb{Z}/n\mathbb{Z}$ est distingué, posons $H = \langle s \rangle \simeq \mathbb{Z}/2\mathbb{Z}$, on a $\mathbb{D}_n = N \rtimes H \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

produit semi-direct, non direct.

<u>Rem</u> ★★ notez comment la géométrie (l'action sur le n-gone) est cruciale pour décrire l'algèbre (la structure interne de $\mathbb{D}_n$).

6.2. Produit semi-direct externe

En algèbre linéaire, un k-e.v. E est parfois somme directe $E = F \oplus G$ de deux sous-espaces. Un autre type de situation se présente lorsqu'on part de deux espaces abstraits F, G et qu'on forme leur somme directe $E \stackrel{\text{def}}{=} F \oplus G$.

(NB pour un nb fini d'espaces, ici $n = 2$, somme directe et produit direct sont les mêmes concepts).

(★) Cette notion sera revue et détaillée dans le chapitre de géométrie affine.

Dans la 1ère situation c'est E qui préexiste et on le réalise comme somme directe à partir de données <u>internes</u> (F et G), on parle de somme directe interne. Dans la 2ème situation ce sont F, G qui préexistent et on construit un espace E <u>extérieur</u> à eux ; on parle de somme directe externe.

La même chose se produit avec le PSD. La structure d'un groupe PSD interne $G = N \rtimes H$ est entièrement connue lorsqu'on connait la structure de N, celle de H, et la manière de commuter les éléments de N avec ceux de H :

$$n_1 h_1 n_2 h_2 = \underbrace{n_1 h_1 n_2 h_1^{-1}}_{\in N} \underbrace{h_1 h_2}_{\in H} = n_1 \varphi_{h_1}(n_2) \cdot h_1 h_2$$

> action de H par conjugaison sur N,
> notons-la $\varphi : H \longrightarrow \mathrm{Aut}(N)$. Il s'agit d'une
> action de H sur N par automorphismes de groupe.

On note $\varphi_h(n)$ ou $h \cdot n$, selon le contexte.

<u>Prop</u> : Soient H, N deux groupes et $\varphi : H \to \mathrm{Aut}(N)$ un morphisme de groupes, décrivant une action de H sur N. Alors :

(1) L'ensemble $G = N \times H$ muni de la loi de composition

$$(n_1, h_1) \cdot (n_2, h_2) := (n_1 \varphi_{h_1}(n_2),\ h_1 h_2)$$

est un groupe de neutre $(1,1)$. On le note $N \rtimes_\varphi H$.

(2) L'ensemble $N' = N \times \{1\}$ est un sous-groupe distingué isomorphe à N.

(3) L'ensemble $H' = \{1\} \times H$ est un sous groupe isomorphe à G.

(4) Le groupe G est PSD interne de H' par N' et l'action de conjugaison de H' sur N' (dans G ambiant) est donnée par φ au sens où $(1,h)(n,1)(1,h)^{-1} = (\varphi_h(n), 1)$.

conjugaison dans G ↑ ↖ action donnée φ

Dém c'est un exercice, un peu fastidieux mais instructif ! $\boxtimes$

Déf le groupe $N \rtimes_\varphi H$ est appelé PSD externe de H par N selon l'action φ.

Exemple dans le groupe diédral, l'action de $H = \langle s \rangle \simeq \mathbb{Z}/2\mathbb{Z}$ par conjugaison sur $N = \langle r \rangle \simeq \mathbb{Z}/n\mathbb{Z}$ se fait ainsi :

$$\varphi_s(r) = srs^{-1} = r^{-1} \quad \text{i.e.} \quad \varphi_s : \begin{array}{ccc} N & \longrightarrow & N \\ r^i & \longmapsto & r^{-i} \end{array}.$$

$(\mathbb{Z}/n\mathbb{Z}, +)$ en notation multiplicative

Rappelons que la structure de $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ est décrite par l'isomorphisme :

ici en notation additive

$$(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$$

$$u \longmapsto \begin{cases} \text{automorphisme } m_u : \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \rightarrow & \mathbb{Z}/n\mathbb{Z} \\ x & \mapsto & ux \end{array} \\ \text{de multiplication par } u \end{cases}$$

groupe multiplicatif des inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$

Le φ_s ci-dessus est l'inversion (multiplicativement parlant) càd la multiplication m_{-1} par -1 (additivement parlant).

On voit que $\varphi : H \to \mathrm{Aut}(N)$ s'identifie au morphisme

$$\varphi : \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^\times$$

qui envoie le générateur de $\mathbb{Z}/2\mathbb{Z}$ sur -1. On note au passage une petite singularité lorsque $n=2$ puisqu'alors $-1 = +1$: dans ce cas (et seulement dans ce cas) φ est trivial.

6.3. Suites exactes

Déf On dit qu'une suite de morphismes de groupes

$$\cdots \longrightarrow G_{i-1} \xrightarrow{f_{i-1}} G_i \xrightarrow{f_i} G_{i+1} \longrightarrow \cdots$$

est exacte lorsque pour tout i on a $\mathrm{im}(f_{i-1}) = \ker(f_i)$.

Exercice Une suite $1 \to H \xrightarrow{i} G \xrightarrow{p} Q \to 1$ est exacte ssi :
i est injectif, p est surjectif, et $G/H \xrightarrow{\sim} Q$ (par le morphisme induit).