Produit semi-direct

1 Définitions générales

Soit G un groupe que l'on souhaite étudier. S'il n'est pas simple, il a un sous-groupe distingué $1 \subsetneq N \subsetneq G$ et on peut commencer par étudier N et le groupe quotient $Q := G/N$. Ceci conduit aux définitions abstraites suivantes :

Définition : Une *suite exacte* de groupes est une suite de groupes

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

(on écrit 1 au lieu de $\{1\}$) dont les flèches sont des morphismes de groupes tels que l'image de chacun est égale au noyau du suivant. Plus précisément cela signifie que :

(1) i est injectif,

(2) π est surjectif,

(3) l'image de i est égale au noyau de π.

Lorsqu'on a une telle suite exacte on dit que G est *extension de N par Q* (ou de Q par N chez certains auteurs ; peu importe). Dans ce cas N est distingué dans G.

Exemples : Les groupes $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/8\mathbb{Z}$ ou encore le groupe diédral $\mathbb{D}_4$ sont tous les trois extensions

$$1 \longrightarrow \mathbb{Z}/4\mathbb{Z} \longrightarrow G \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

Les groupes $(\mathbb{Z}/2\mathbb{Z})^3$ et le groupe des quaternions $\mathbb{H}_8$ sont tous les deux extensions

$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow G \longrightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

Rappelons que le groupe des quaternions est le groupe $\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. C'est un sous-groupe de l'algèbre des quaternions, ce qui explique son nom et sa notation. □

Étant donnée une extension $1 \to N \to G \xrightarrow{\pi} Q \to 1$, il existe une situation particulièrement simple :

Proposition : Les conditions suivantes sont équivalentes :

(1) Il existe un sous-groupe $H \subset G$ tel que $H \cap N = 1$ et $HN = G$ ([1]).

(2) $\pi\colon G \to Q$ a une section, c'est-à-dire un morphisme $s\colon Q \to G$ tel que $\pi \circ s = \mathrm{Id}_Q$.

Lorsqu'elles sont vérifiées on dit que G est *produit semi-direct* de N par H (en abrégé PSD) et on note $G = N \rtimes H$. On dit aussi que la suite exacte a une section, ou qu'elle est scindée. Enfin, on dit que H est un *complément* pour N.

Preuve : Sous les hypothèses de (1) on montre facilement que $\pi_{|H}$ est un isomorphisme, donc son inverse produit une section $s\colon Q \to G$. Ceci prouve que (1) $\Rightarrow$ (2). Réciproquement si on a une section il est facile de vérifier que le sous-groupe $H = s(Q)$ vérifie les conditions de (1). Donc (2) $\Rightarrow$ (1). □

Si N et Q sont fixés on appelle parfois *problème de l'extension* la question de retrouver tous les groupes G qui sont extensions de N par Q. C'est un problème difficile, et les seules extensions que l'on sait décrire de manière générale sont les PSD.

[1] Si $N \lhd G$, c'est un fait général que pour tout sous-groupe $H \subset G$ l'ensemble des produits hn (resp. des produits nh) avec $h \in H$ et $n \in N$ est un sous-groupe noté HN (resp. NH). En fait $HN = NH =$ le sous-groupe engendré par H et N.

$\therefore$

Soit $G = N \rtimes H$ un PSD, on observe que H agit sur N par conjugaison d'où un morphisme de groupes $H \to \mathrm{Aut}(N)$. Ceci mène à une autre manière de décrire les PSD. En effet supposons avoir des groupes abstraits N et H ainsi qu'un morphisme $\theta\colon H \to \mathrm{Aut}(N)$ qu'on note $\theta(h)(n) = h \cdot n$ comme une action. On peut définir un groupe noté $N \rtimes_\theta H$ de la façon suivante : comme ensemble il s'agit simplement du produit $N \times H$, et la loi de multiplication est

$$(n, h).(n', h') = (n(h \cdot n'), hh')$$

Exercice : vérifiez que ceci définit bien une loi de groupe. Soit N^* (resp. H^*) l'ensemble des éléments de la forme $(n, 1)$ (resp. $(1, h)$). Vérifiez que $N^* \simeq N$, $H^* \simeq H$ et $N \rtimes_\theta H$ est PSD de N^* par H^*. Il est intéressant aussi de noter que l'action initiale de H sur N n'est autre que la conjugaison dans le groupe $N \rtimes_\theta H$. Enfin, montrez que les quatre conditions suivantes sont équivalentes : (i) H^* est distingué dans $N \rtimes_\theta H$, (ii) θ est trivial, (iii) N^* et H^* commutent, (iv) le produit est un produit direct. On retiendra :

Proposition : Soient N et H des groupes. Alors c'est équivalent de se donner :

(1) Un groupe G avec des injections $N \hookrightarrow G$, $H \hookrightarrow G$ qui font de G le PSD de N et H.

(2) Un morphisme de groupes $\theta\colon H \to \mathrm{Aut}(N)$.

Dans le cas (1) on parle plutôt de *PSD interne* car on prend le point de vue du groupe G, engendré par deux sous-groupes. Dans le cas (2) on parle de *PSD externe* car on part de H et N et on construit un groupe qui les contient.

2 Exemples

Extensions d'ordre 8. À isomorphisme près il y a 5 groupes finis d'ordre 8 : c'est un exercice aussi classique qu'instructif. Ce sont $(\mathbb{Z}/2\mathbb{Z})^3$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$, le groupe diédral $\mathbb{D}_4$ et le groupe des quaternions $\mathbb{H}_8$. Voici toutes les extensions entre groupes d'ordres 2 et 4 :

	$\mathbb{Z}/2\mathbb{Z} \to ? \to \mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z} \to ? \to \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \to ? \to (\mathbb{Z}/2\mathbb{Z})^2$	$(\mathbb{Z}/2\mathbb{Z})^2 \to ? \to \mathbb{Z}/2\mathbb{Z}$
$(\mathbb{Z}/2\mathbb{Z})^3$			×	×
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	×	×		
$\mathbb{Z}/8\mathbb{Z}$	×	×		
$\mathbb{D}_4$		×		
$\mathbb{H}_8$		×	×	

La colonne des extensions de $\mathbb{Z}/4\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$ montre qu'un groupe extension de deux groupes assez gentils peut être assez compliqué. On y trouve une extension qui est produit direct : $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, une extension qui est produit semi-direct non trivial : $\mathbb{D}_4$, et deux extensions qui ne sont même pas produits semi-directs : $\mathbb{Z}/8\mathbb{Z}$ et $\mathbb{H}_8$.

On voit aussi que les groupes non isomorphes $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/8\mathbb{Z}$ sont extensions tous deux de de $\mathbb{Z}/4\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$, et de $\mathbb{Z}/2\mathbb{Z}$ par $\mathbb{Z}/4\mathbb{Z}$. Donc ils sont « indistinguables » du point de vue des extensions.

Contre-exemples. Voici des exemples d'extensions non scindées. On a vu

$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{H}_8 \longrightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

Plus généralement on obtient une extension non scindée si on a un groupe G de centre Z tel que $Q = G/Z$ est un groupe non trivial de centre non trivial :

$$1 \longrightarrow Z \longrightarrow G \longrightarrow Q = G/Z \longrightarrow 1$$

En effet si l'extension était scindée, comme Z est central le PSD devrait être un produit direct. Donc $G \simeq Z \times Q$ mais comme $Z \times Z(Q)$ est inclus dans le centre de $Z \times Q$, ceci contredit le fait que Z est le centre de G. Voici une autre extension non scindée :

$$1 \longrightarrow \mathbb{C}^\times \longrightarrow \mathrm{GL}_n(\mathbb{C}) \longrightarrow \mathrm{PGL}_n(\mathbb{C}) \longrightarrow 1$$

En effet ici encore on quotiente par le centre, donc si l'extension était scindée ce serait un produit direct $G = \mathbb{C}^\times \times H$ avec $H \simeq \mathrm{PGL}_n(\mathbb{C})$. En particulier $H \lhd G$ donc $H \cap \mathrm{SL}_n(\mathbb{C}) \lhd \mathrm{SL}_n(\mathbb{C})$. Comme $\mathrm{PSL}_n(\mathbb{C})$ est simple on en déduit facilement que $H = \mathrm{SL}_n(\mathbb{C})$. Ceci est impossible car $\mathrm{SL}_n(\mathbb{C})$ a un centre alors que $\mathrm{PGL}_n(\mathbb{C})$ n'en a pas. (Voir les trois premiers exercices dans les Exercices du chapitre IV de [Per], p. 108). Pour finir mentionnons l'extension non scindée

$$1 \longrightarrow \{\pm 1\} \longrightarrow G \longrightarrow \mathrm{SO}_3(\mathbb{R}) \longrightarrow 1$$

où G est le groupe des quaternions de norme 1. En effet supposons qu'il existe un sous-groupe $H \subset G$ tel que $G = \{\pm 1\} \rtimes H$ (un complément). Comme $i \in H$ ou $i \in -H$, on déduit dans tous les cas que $-1 = i^2 \in H$. Ceci est impossible. (Lire [Per] chap. VII remarque 2.2.)

Différents PSD. Un groupe qui est PSD de deux sous-groupes peut l'être de différentes façons. Considérons par exemple le groupe $G = \mathfrak{S}_3 \times \mathbb{Z}/2\mathbb{Z}$ qui est produit de ses deux sous-groupes $N = \mathfrak{S}_3$ et $H = \mathbb{Z}/2\mathbb{Z}$. Soit $\tau = (12)$ la transposition dans N et x l'élément non trivial de H, alors il est facile de voir que si on choisit pour H' le sous-groupe d'ordre 2 engendré par (τ, x) on obtient une expression comme PSD non trivial $G = N \rtimes H'$.

Déterminant. Le morphisme qui à $\lambda \in k^\times$ associe la matrice diagonale $(\lambda, 1, \ldots, 1)$ donne une section du déterminant de sorte que

$$\mathrm{GL}_n(k) = \mathrm{SL}_n(k) \rtimes k^\times$$

Symétries des polygones réguliers. On a

$$\mathbb{D}_n = \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$$

Signature. N'importe quelle transvection de $\mathfrak{S}_n$ donne un section de la signature d'où

$$\mathfrak{S}_n = \mathfrak{A}_n \rtimes \mathbb{Z}/2\mathbb{Z}$$

Groupe affine. Soit $\mathcal{E}$ un espace affine de direction E, alors

$$\mathrm{GA}(\mathcal{E}) = \mathrm{T}(\mathcal{E}) \rtimes \mathrm{GL}(E)$$

Groupe de Galois de $X^n - a$. Quand ce polynôme est-il irréductible ? Si a est une puissance d-ème pour un $d|n$ alors il est réductible. Lorsque $n = 4k$ il peut aussi se produire un gag si $a = -4b^4$:

$$X^{4k} + 4b^4 = (X^{2k} + 2bX^k + 2b^2)(X^{2k} - 2bX^k + 2b^2)$$

Le théorème 6.9.1 de [Lan] affirme que dans tous les autres cas le polynôme est irréductible : *soit k un corps et $n \geq 2$ un entier, a un élément non nul de k, alors si a n'est une puissance $d^{\text{ème}}$ pour aucun $d|n$ et si a n'est pas de la forme $-4b^4$ lorsque $4|n$, alors $X^n - a$ est irréductible.* C'est donc une CNS.

Soit $a \in \mathbb{Q}$ choisi comme dans ce théorème, de sorte que le polynôme $P(X) = X^n - a$ est irréductible. Soit $K \subset \mathbb{C}$ le corps de décomposition de P et $G = \mathrm{Gal}(K/\mathbb{Q})$. Soit α une racine de P et ζ une racine primitive n-ème de l'unité, alors

$$P(X) = (X - \alpha)(X - \zeta\alpha) \ldots (X - \zeta^{n-1}\alpha)$$

On voit ainsi que $K = \mathbb{Q}(\alpha, \zeta)$. Un automorphisme $\sigma \in G$ doit envoyer α sur une autre racine $\zeta^i \alpha$ pour un $i \in \mathbb{Z}/n\mathbb{Z}$ et ζ sur une autre racine primitive n-ème de l'unité ζ^j pour un $j \in (\mathbb{Z}/n\mathbb{Z})^\times$. Soit $\sigma_{i,j}$ le $\mathbb{Q}$-automorphisme de K ainsi défini :

$$\sigma_{i,j}(\alpha) = \zeta^i \alpha \quad \text{et} \quad \sigma_{i,j}(\zeta) = \zeta^j$$

Il est immédiat de vérifier que $\sigma_{i,j} \circ \sigma_{k,l} = \sigma_{i+kj,jl}$ On a donc un isomorphisme $\sigma_{i,j} \mapsto (i,j)$:

$$G \simeq \mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$$

Théorème de Schur-Zassenhaus. Terminons par un très beau résultat de théorie des groupes, dont la preuve est difficile. Ce théorème dit que toute extension de groupes finis

$$1 \longrightarrow A \longrightarrow G \xrightarrow{\pi} Q \longrightarrow 1$$

avec $|A|$ et $|Q|$ premiers entre eux est scindée. Notons que pour démontrer ce théorème il suffit de trouver un sous-groupe $H \subset G$ d'ordre égal à $[G : A] = |Q|$. En effet si H est un tel sous-groupe alors $\ker(\pi_{|H}) = A \cap H$ est trivial car $|A|$ et $|H|$ sont premiers entre eux, donc $\pi_{|H}$ est un isomorphisme, d'où le résultat.

En particulier la démonstration est simple si Q est un p-groupe, car alors il suffit de choisir pour H un p-Sylow de G. Ainsi dans $\mathfrak{A}_4$ le sous-groupe $V = \{1, (12)(34), (13)(24), (14)(23)\}$ est un sous-groupe distingué isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$ et le quotient est $\mathbb{Z}/3\mathbb{Z}$. Il en découle que $\mathfrak{A}_4 \simeq V \rtimes \mathbb{Z}/3\mathbb{Z}$.

Pour démontrer le théorème de Schur-Zassenhaus on observe d'abord que de manière générale le nombre de conjugués $g^{-1}Hg$ d'un sous-groupe $H \subset G$ est égal à l'indice $[G : N]$ du normalisateur $N = N_G(H)$. En effet le groupe G agit transitivement sur l'ensemble des conjugués de H, et le stabilisateur de H est N.

Preuve (esquisse) : On fait une récurrence sur $|G|$ et $|A|$. Dans le cas $|G| = |A| = 1$ il n'y a rien à dire. Rappelons qu'il suffit de trouver un sous-groupe $H \subset G$ d'ordre égal à $[G : A]$.

Soit p un facteur premier de A, S un p-Sylow de A, $N = N_G(S)$. Alors S est aussi un p-Sylow de G et $N_A(S) = N \cap A$. Les p-Sylow de G (qui sont conjugués à S) sont tous dans A donc d'après l'observation précédente :

$$[G : N] = [A : N \cap A]$$

On en déduit $[N : N \cap A] = [G : A]$.

Si $N \cap A \subsetneq A$, par l'hypothèse de récurrence appliquée à $(N, N \cap A)$ le groupe N contient un sous-groupe d'ordre $[N : N \cap A] = [G : A]$. Cela fournit un sous-groupe de G qui répond à la question.

Si $N \cap A = A$ alors $[G : N] = 1$ donc S est distingué dans G. Par l'hypothèse de récurrence appliquée à $(G/S, A/S)$ il existe un sous-groupe $H \subset G$ contenant S avec $[H : S] = [G : A]$. Soit $Z \neq 1$ le centre de S, un petit calcul montre que $Z \lhd H$: si $z \in Z$ alors $h^{-1}zh \in S$ et

$$h^{-1}zhs = h^{-1}z(hsh^{-1})h = h^{-1}(hsh^{-1})zh = sh^{-1}zh$$

donc $h^{-1}zh$ commute avec S donc est dans Z. Par l'hypothèse de récurrence appliquée à $(H/Z, S/Z)$ il existe un sous-groupe $K \subset H$ contenant Z avec $[K : Z] = [G : A]$.

On s'est ramené à résoudre le problème pour (K, Z) i.e. au cas où A est un p-groupe central abélien. Pour conclure la preuve en traitant ce cas particulier, on doit faire appel à la *cohomologie des groupes*, théorie qui nous emmènerait trop loin du programme de l'Agrégation.

Bibliographie

[Lan] Lang, Algèbre, *Dunod*.
[Per] Perrin, Cours d'Algèbre, *Ellipses* ou *ENSJF*.