

Leçon 103 : Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications

1 Action de conjugaison [PER,ROM]

Soit $(G, \cdot)$ un groupe, qu'on notera également G .

Pour $x, y \in G$ on note $xy = x \cdot y$.

1.1 Généralités sur les actions de groupe

On considère l'action de G sur un ensemble X , $(g, x) \in G \times X \mapsto g \cdot x$.

Définition 1. Soit $x \in X$ on note $G \cdot x = \{g \cdot x, g \in G\}$ l'orbite de x sous l'action de G . On note aussi $G_x = \{g \in G, g \cdot x = x\}$ le stabilisateur de x sous l'action de G

Théorème 2 (Equation aux classes). On considère l'action de G sur un ensemble fini X . En notant $\{G \cdot x_i, i \in \llbracket 1, r \rrbracket\}$ l'ensemble des orbites deux à deux distinctes on a :

$$\text{card}(X) = \sum_{i=1}^r \text{card}(G \cdot x_i) = \sum_{i=1}^r \frac{\text{card}(G)}{\text{card}(G_{x_i})}$$

1.2 Classes de conjugaison

Définition 3. Soit $g \in G$, on note $i_g : x \in G \mapsto gxg^{-1}$.

Il s'agit d'un automorphisme sur G , appelé automorphisme intérieur.

$\text{Int} : g \in G \mapsto i_g \in \text{Aut}(G)$ est un morphisme de groupes.

Définition 4. En posant $X = G$, $(x, g) \in X \times G \mapsto i_g(x)$ définit une action de groupe de G sur lui-même, appelée conjugaison. Ses orbites s'appellent classes de conjugaison.

Pour $a, a' \in G$ on dit que a et a' sont conjugués s'ils existe $g \in G$ tel que $a = ga'g^{-1}$.

Enfin, le stabilisateur de a s'appelle centralisateur : $G_a = \{g \in G, ag = ga\}$.

Exemple 5. G est abélien si et seulement si, pour tout $h \in G$, $G \cdot h = \{h\}$.

Exemple 6. Soit $n \in \mathbb{N}$ et $\mathbb{K}$ un corps, on dit que $M, N \in M_n(\mathbb{K})$ sont semblables s'il existe $P \in GL_n(\mathbb{K})$ telle que $M = PNP^{-1}$.

1.3 Centre

Définition 7. On note $Z(G) := \{g \in G, \forall h \in G, gh = hg\}$ le centre de G .

De manière équivalente $Z(G) := \ker \text{Int}$.

Exemple 8. Si G est abélien, $Z(G) = G$

Exemple 9. Soit $n \in \mathbb{N}$, $Z(M_n(\mathbb{R})) = \{\lambda Id_n, \lambda \in \mathbb{R}\}$

Exemple 10. Soit $H_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ le groupe des quaternions, alors $Z(H_8) = \{1, -1\}$

Définition 11. On appelle commutateurs de G les éléments s'écrivant sous la forme $xyx^{-1}y^{-1}$ avec $x, y \in G$.

On appelle groupe dérivé le sous-groupe $D(G)$ engendré par les commutateurs de G .

Exemple 12. G est abélien s.s.i. $D(G) = \{1\}$.

Exemple 13. Soit $n \in \mathbb{N}$, $D(GL_n(\mathbb{R})) = SL_n(\mathbb{R})$.

Exemple 14. $D(H_8) = \{1, -1\}$.

Proposition 15 (DEV 1). [IP] Si $G/Z(G)$ est monogène, alors G est abélien.

Théorème 16 (DEV 1 suite). [IP] Soit p un nombre premier, à isomorphisme près les groupes d'ordres p^2 sont $(\mathbb{Z}/p\mathbb{Z})^2$ et $(\mathbb{Z}/p^2\mathbb{Z})$

1.4 Sous-groupe distingué et groupe quotient

Définition 17. Soit H un sous-groupe de G , on dit que H est distingué dans G s'il est invariant par conjugaison, c'est-à-dire s'il vérifie l'une de ces deux propriétés équivalentes :

1. $\forall g \in G, \forall h \in H, ghg^{-1} \in H$
2. $\forall g \in G, gH = Hg$.

On note alors $H \triangleleft G$.

Proposition 18. Soit $f : G \rightarrow G'$ un morphisme de groupe. $\ker f \triangleleft G$. De plus on a un isomorphisme de groupe $\text{Im} f \simeq G / \ker f$.

Proposition 19. $Z(G)$ et $D(G)$ sont distingués dans G

Définition 20. G est dit simple s'il possède exactement 2 sous-groupes distingués : $\{1\}$ et G

Exemple 21. H_8 et $GL_n(\mathbb{R})$ ne sont pas simples

Proposition 22. Soit H un sous-groupe de G , H est distingué si et seulement si G/H est muni d'une unique structure de groupe. Dans ce cas, H est le noyau du morphisme surjectif $\pi_H : g \in G \rightarrow gH \in G/H$.

Théorème 23. Soit $f : G \rightarrow G'$ un morphisme de groupes. Il existe un unique isomorphisme de groupe $\bar{f} : G / \ker f \rightarrow \text{Im} f$ vérifiant $f = i \circ \bar{f} \circ \pi$ où $i : \text{Im} f \rightarrow G'$ est l'injection canonique et $\pi : G \rightarrow G / \ker f$ la projection canonique.

Exemple 24. On a alors $G/Z(G) \simeq \text{Int}(G)$

Exemple 25. $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}^*$

2 Application au groupe des permutations [ROM]

Soit $n \in \mathbb{N}^\times$, on note $\mathcal{S}_n$ le groupe des permutations de $\llbracket 1, n \rrbracket$.

On considère l'action de $\mathcal{S}_n$ sur lui-même : $(\sigma, \gamma) \in \mathcal{S}_n \times \mathcal{S}_n \mapsto \sigma\gamma\sigma^{-1}$.

2.1 Groupe symétrique

Proposition 26. On a $Z(\mathcal{S}_n) = \begin{cases} \mathcal{S}_n & \text{si } n \leq 2 \\ \{Id\} & \text{sinon.} \end{cases}$

Proposition 27. $\mathcal{S}_n$ est engendré par les transpositions

Proposition 28. Soit $k \in \llbracket 1, n \rrbracket$, deux k -cycles sont conjugués dans $\mathcal{S}_n$.

Définition 29. Soit $\sigma \in \mathcal{S}_n$. On appelle type de σ la suite des longueurs des cycles de sa décomposition, rangés dans l'ordre croissant.

Proposition 30. Deux permutations ont même type si et seulement si elles sont conjuguées.

2.2 Groupe alterné

On note ε le morphisme signature $\varepsilon : \mathcal{S}_n \rightarrow \{\pm 1\}$.

Proposition 31. Soit $\sigma \in \mathcal{S}_n$ produit de p transpositions, $\varepsilon(\sigma) = (-1)^p$

Définition 32. On définit $\mathcal{A}_n = \ker \varepsilon$ le groupe alterné, ou groupe des permutations paires de $\mathcal{S}_n$.

Proposition 33. $\mathcal{A}_n$ est distingué dans $\mathcal{S}_n$. Si $n \geq 5$, c'est l'unique groupe distingué de $\mathcal{S}_n$ distinct de $\{Id\}$ et $\mathcal{S}_n$.

Proposition 34 (DEV 2 (ROM)). Si $n = 3$ ou $n \geq 5$, $\mathcal{A}_n$ est simple.

Exemple 35. $\mathcal{A}_1$ et $\mathcal{A}_2$ sont isomorphes au groupe trivial et $\mathcal{A}_4$ n'est pas simple.

3 Produits directs et semi-directs [PER]

3.1 Définitions

Définition 36 (Suite exacte). Soient N, H deux groupes, $i : N \rightarrow G, p : G \rightarrow H$ des morphismes vérifiant :

1. i est injectif
2. p est surjectif
3. $\text{Im } i = \ker p$.

Alors on dit qu'on a la suite exacte :

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{p} H \longrightarrow 1$$

Exemple 37. Soit $\sigma = (1 \ 2 \ 3) \in \mathcal{S}_3$, on a $\langle \sigma \rangle = \mathcal{A}_3 \triangleleft \mathcal{S}_3$.

On a alors la suite exacte

$$1 \longrightarrow \mathbb{Z}/3\mathbb{Z} \xrightarrow{i} \mathcal{S}_3 \xrightarrow{p} \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

Définition 38 (Produit direct). Soit N, H deux groupes, on note leur produit direct $G := N \times H$ le produit cartésien muni de la loi de groupe $(n, h)(n', h') \mapsto (nn', hh')$.

On a alors la suite exacte

$$1 \longrightarrow N \xrightarrow{i} N \times H \xrightarrow{p} H \longrightarrow 1$$

On dit de plus que G est une extension de N par H .

Exemple 39. Le lemme chinois donne : si $p, q \in \mathbb{N}^*$ sont premiers entre eux alors on a un isomorphisme $\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$

Définition-Proposition 40 (Produit semi-direct). Soient N, H deux groupes et $\varphi : H \rightarrow \text{Aut}N$, on définit une opération de H sur N par la formule $h.n = \varphi(h)(n)$.

On munit le produit cartésien $N \times H$ de la loi $(n, h)(n', h') = (n(h.n'), hh')$, c'est alors un groupe appelé produit semi-direct de N par H relativement à φ , noté $N \rtimes_{\varphi} H$ ou $N \rtimes H$.

On a alors une suite exacte

$$1 \longrightarrow N \xrightarrow{i} N \rtimes H \xrightarrow{p} H \longrightarrow 1$$

Remarque 41. $N \rtimes H$ contient les sous-groupes $\overline{H} = \{(1, h), h \in H\} \simeq H$ et $\overline{N} = \{(1, n), n \in N\}$ avec $\overline{N} \triangleleft N \rtimes H$.

On a de plus $\overline{N} \cap \overline{H} = \{1\}$ et $N \rtimes H = \overline{N} \overline{H}$

Exemple 42. Soient $n \in \mathbb{N}^\times$ et V un $\mathbb{R}$ -espace vectoriel de dimension n . On définit $\text{Aff}(V) := V \rtimes GL(V)$ avec la loi de composition $(v, P) \circ (v', P') \in (V \times GL(V))^2 \mapsto (v + P(v'), P \circ P')$.

3.2 Décomposition en produit

Proposition 43. Si on a une suite exacte

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{p} H \longrightarrow 1$$

et s'il existe un sous-groupe $\tilde{H}$ (appelé relèvement de H) un sous-groupe de G tel que $p|_{\tilde{H}} : \tilde{H} \rightarrow H$ soit un isomorphisme,

alors $G \simeq N \rtimes H$. On dit alors que l'extension est scindée.

Remarque 44. il est équivalent de dire que p possède une section

Proposition 45. Si on a N, H deux sous groupes de G vérifiant

1. $N \triangleleft G$
2. $N \cap H = \{1\}$
3. $G = NH$

alors $G \simeq N \rtimes H$

Exemple 46. On a la suite exacte scindée suivante :

$$1 \longrightarrow \mathcal{A}_n \longrightarrow \mathcal{S}_n \xrightarrow{\varepsilon} \{\pm 1\} \longrightarrow 1$$

donc $\mathcal{S}_n \simeq \mathcal{A}_n \rtimes \mathbb{Z}/2\mathbb{Z}$

Proposition 47. Soit $G = N \rtimes_{\varphi} H$ un produit semi-direct, les propriétés suivantes sont équivalentes :

1. $\varphi : h \mapsto \text{Id}_N$ (morphisme trivial)
2. $\overline{H}$ est distingué dans G
3. la loi de groupe sur G est celle du produit direct.

On note que c'est le cas si $N \subset Z(G)$, on dit alors que l'extension est centrale.

Exemple 48. L'exemple [numéro] n'est pas isomorphe au produit direct $\mathcal{A}_n \times \mathbb{Z}/2\mathbb{Z}$

Exemple 49. H_8 n'est pas décomposable en produit semi-direct

Exemple 50 (Groupes d'ordre 8)(DEV 1 fin). Les groupes d'ordre 8 sont à isomorphismes près $(\mathbb{Z}/2\mathbb{Z})^3, (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}), (\mathbb{Z}/8\mathbb{Z}), D_8$ et H_8 .

4 Bibliographie

- *Algèbre, Perrin [PER]*
- *Algèbre et géométrie, 2e édition, Rombaldi [ROM]*
- *L'oral à l'agrégation de mathématiques, 2e édition, Isenmann Pécatte [IP]*