

103. Exemples de sous-groupes distingués et de groupes quotients. Applications.

Introduction : Les sous-groupes distingués et les groupes quotients jouent un rôle fondamental en théorie des groupes, que ce soit concernant la classification (notion de simplicité) ou pour les simplifications obtenues par passage au quotient.

Soit G un groupe.

1 Sous-groupes distingués, groupes quotients

1.1 Définitions et premières propriétés

Soit $H \leq G$. On définit la relation \sim par : $\forall x, y \in G, x \sim y \Leftrightarrow x^{-1}y \in H$.

Proposition 1. C'est une relation d'équivalence, dont les classes sont de la forme $gH, g \in G$ et sont en bijection avec H .

Définition 2. L'ensemble quotient est noté G/H . Son cardinal est appelé *indice* de G dans H , et noté $[G : H]$.

Théorème 3 (Lagrange). Si G est un groupe fini et $H \leq G$, alors $|G| = |H| \cdot [G : H]$.

Application 4. Un groupe d'ordre premier est cyclique.

Définition 5. Soit $H \leq G$. On dit que H est *distingué* dans G , et on note $H \triangleleft G$, si H est stable par conjugaison par des éléments de G , i.e. $\forall g \in G, gHg^{-1} \subseteq H$.

Exemple 6. $\{e_G\}$ et G sont toujours des sous-groupes distingués de G .

Exemple 7. Si G est commutatif, tous ses sous-groupes sont distingués.

Si $H \leq G$, on peut avoir $K \triangleleft H$ mais pas $K \triangleleft G$. Par exemple, si $G = A_4$, H est le groupe engendré par les bi-transpositions, et si σ est une bi-transposition, $\langle \sigma \rangle$ est distingué dans H mais pas dans G .

Définition 8. Si H sous-groupe de G , on appelle normalisateur de H et on note $\mathcal{N}_G(H)$ le plus grand sous-groupe de G dans lequel H est distingué.

Proposition 9. $\mathcal{N}_G(H) = \{g \in G, gHg^{-1} = H\}$.

Théorème 10. L'ensemble G/H est muni d'une structure de groupe induite par celle de G , si et seulement si, $H \triangleleft G$.

Ainsi, pour $g_1H, g_2H \in G/H, (g_1H)(g_2H) = (g_1g_2)H$, on a aussi $(g_1H)^{-1} = g_1^{-1}H$ et l'élément neutre est $H = e_GH$.

Exemple 11. Pour $n \in \mathbb{N}^*, \mathbb{Z}/n\mathbb{Z}$ est le groupe des classes d'entiers modulo n .

Proposition 12. Toute intersection de sous-groupes distingués de G est un sous-groupe distingué de G .

Proposition 13. $H \leq G$ est distingué dans G , si et seulement si, c'est le noyau d'un morphisme de groupes entre G et un autre groupe.

Exemple 14. Pour $n \in \mathbb{N}^*, \mathcal{A}_n = \ker(\varepsilon)$ est un sous-groupe distingué de \mathcal{S}_n .

Exemple 15. Si K est un corps, $SL_n(K) = \{A \in \mathcal{M}_n(K), \det(A) = 1\}$ est un sous-groupe distingué de $GL_n(K)$.

1.2 Propriétés des groupes quotients

Définition 16. Soit $H \triangleleft G$. L'application $\pi \begin{cases} G & \rightarrow G/H \\ g & \mapsto gH \end{cases}$ est appelée la *projection canonique* de G sur G/H .

Proposition 17. π est un morphisme de groupes.

Théorème 18 (de correspondance). Soit $H \triangleleft G$. L'application $K \mapsto K/H$ est une bijection entre l'ensemble des sous-groupes K tels que $H \leq K \leq G$, et l'ensemble des sous-groupes de G/H .

Application 19. Pour tout d diviseur de $n \in \mathbb{N}^*, \mathbb{Z}/n\mathbb{Z}$ possède un unique sous-groupe d'ordre d .

Théorème 20 (de factorisation). Soient $H \triangleleft G$ et $f : G \rightarrow G'$ morphisme de groupes. On suppose que $H \subseteq \ker(f)$. Alors il existe un unique morphisme $\bar{f} : G/H \rightarrow G'$ tel que $f = \bar{f} \circ \pi$, où $\pi : G \rightarrow G/H$ est la projection canonique.

Corollaire 21 (Premier théorème d'isomorphisme). Soit $f : G \rightarrow G'$ un morphisme de groupes. Alors f se factorise en un isomorphisme $\bar{f} : G/\ker(f) \rightarrow \text{Im}(f)$.

Exemple 22. \mathbb{R}/\mathbb{Z} et \mathbb{U} sont isomorphes.

Lemme 23. Soient H, K deux sous-groupes de G dont l'un est distingué dans G . Alors HK est un sous-groupe de G .

Théorème 24 (Deuxième théorème d'isomorphisme). Soient $H \leq G, K \triangleleft G$. Alors $H \cap K \triangleleft H$ et $H/(H \cap K) \simeq (HK)/K$.

Théorème 25 (Troisième théorème d'isomorphisme). Soient $K \triangleleft H \triangleleft G$. Alors $H/K \triangleleft G/K$ et $(G/K)/(H/K) \simeq G/H$.

1.3 Simplicité

Définition 26. G est dit simple si ses seuls sous-groupes distingués sont $\{e_G\}$ et G .

Proposition 27. Les groupes abéliens simples sont les $\mathbb{Z}/p\mathbb{Z}$ avec p premier.

Définition 28. On suppose que G est un groupe fini d'ordre $p^k m$, p premier et $p \wedge m = 1$. On appelle p -Sylow de G tout sous-groupe de G d'ordre p^k .

Théorème 29 (Sylow). On a alors :

1. G possède des p -Sylow.
2. Tous ses p -Sylow sont conjugués entre eux. En particulier, s'il n'y a qu'un p -Sylow, il est distingué dans G .
3. Si on note n_p le nombre de p -Sylow, $n_p \equiv 1[p]$ et $n_p | m$.

Application 30. Il n'y a pas de groupe simple d'ordre 30 ou 42.

Application 31. \mathcal{A}_n est un groupe simple pour tout $n \geq 5$.

Proposition 32. Si G est muni d'une topologie séparée rendant la loi de groupe et l'inversion continues, alors G^0 , la composante connexe de e_G , est un sous-groupe distingué de G .

Application 33. $SO_3(\mathbb{R})$ est un groupe simple.

2 Sous-groupes distingués classiques

2.1 Centre d'un groupe

Définition 34. On appelle centre de G l'ensemble $Z(G) = \{g \in G, \forall h \in G, gh = hg\}$.

Proposition 35. Le centre de G est un sous-groupe distingué de G .

Exemple 36. Pour $n \geq 3$, $Z(\mathcal{S}_n) = \{\text{Id}\}$.

Exemple 37. Soit \mathbb{H}_8 le groupe quaternionique. On a $Z(\mathbb{H}_8) = \{-1, 1\}$.

Exemple 38. Si K est un corps, $Z(GL_n(K)) = K^* I_n$.

2.2 Groupe dérivé

Définition 39. Pour $g, h \in G$, on définit leur commutateur par $[g, h] = ghg^{-1}h^{-1}$. On définit le groupe dérivé de G par $D(G) = [G, G]$, groupe engendré par les commutateurs de G .

Proposition 40. $D(G)$ est distingué dans G .

Exemple 41. Si $n \geq 3$ ou si $\text{car}(K) > 3$, on a $D(GL_n(K)) = SL_n(K)$.

Application 42 (Frobenius-Zolotarev). Soit $p \geq 3$ premier, soit $u \in GL_n(\mathbb{F}_p)$.

Sa signature est donnée par $\varepsilon(u) = \left(\frac{\det(u)}{p}\right)$.

Proposition 43. Si $H \triangleleft G$, alors G/H est abélien, si et seulement si, $D(G) \subseteq H$.

2.3 Groupes résolubles

Définition 44. G est dit résoluble s'il existe une suite $(H_i)_{0 \leq i \leq n}$ de sous-groupes de G , telle que :

- $H_0 = \{e_G\}, H_n = G$.
- Pour tout $i \in \llbracket 0, n-1 \rrbracket$, $H_i \triangleleft H_{i+1}$.
- Pour tout $i \in \llbracket 0, n-1 \rrbracket$, H_{i+1}/H_i est abélien.

Définition 45. On définit la suite dérivée de G par $G_0 = G$ et $\forall i \in \mathbb{N}, G_{i+1} = D(G_i)$.

Proposition 46. La suite dérivée est décroissante. De plus, G est résoluble, si et seulement si, sa suite dérivée stationne en $\{e_G\}$.

Proposition 47. Si G est résoluble et H distingué dans G , alors G/H est résoluble.

Proposition 48. Soit H distingué dans G . G est résoluble ssi H et G/H sont résolubles.

Exemple 49. \mathcal{S}_3 et \mathcal{S}_4 sont résolubles. Pour $n \geq 5$, \mathcal{S}_n n'est pas résoluble.

3 Représentations et caractères

Lemme 50. Soient H distingué dans G et $\bar{\rho} : G/H \rightarrow GL(V)$ une représentation de G/H . Alors $\rho = \bar{\rho} \circ \pi$ définit une représentation de G , irréductible si et seulement si $\bar{\rho}$ est irréductible.

Proposition 51. Les caractères irréductibles de $G/D(G)$ sont en bijection avec les caractères de degré 1 de G .

Application 52. $D(\mathbb{H}_8) = \{-1, 1\}$ et $\mathbb{H}_8/\{-1, 1\}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
On en déduit la table de caractères de \mathbb{H}_8 .

Théorème 53. Soit G un groupe fini dont on connaît la table de caractères, on note $\{\chi_1, \dots, \chi_r\}$ l'ensemble de ses caractères irréductibles (deux à deux non isomorphes). Alors, si H est un sous-groupe de G , H est distingué dans G , si et seulement si, il existe $I \subseteq \llbracket 1, r \rrbracket$, $H = \bigcap_{i \in I} \ker(\chi_i)$ (où $\ker(\chi_i) = \{g \in G, \chi_i(g) = \chi_i(e_G)\}$).

Corollaire 54. G est simple ssi $\forall i, \forall g \in G \setminus \{1\}, \chi_i(g) \neq \chi_i(1)$.

Annexe

Table de caractères de \mathbb{H}_8 :

	1	-1	i	j	k
χ_0	1	1	1	1	1
χ_1	1	1	-1	-1	1
χ'_1	1	1	1	-1	-1
χ''_1	1	1	-1	1	-1
χ_2	2	-2	0	0	0

Développements

- Simplicité de $SO_3(\mathbb{R})$.
- Théorème de Frobenius-Zolotarev.
- Table de caractères et sous-groupes distingués.

Références

- [1] F. Combes, ALGÈBRE ET GÉOMÉTRIE, Bréal.
- [2] J. Delcourt, THÉORIE DES GROUPES, Dunod.
- [3] G. Peyré, L'ALGÈBRE DISCRÈTE DE LA TRANSFORMÉE DE FOURIER, Ellipses.
- [4] G. Rauch, LES GROUPES FINIS ET LEURS REPRÉSENTATIONS, Ellipses.
- [5] A. Szpirglas, ALGÈBRE L3, Pearson.