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

Soit G un groupe.

I - Conjugaison dans un groupe

1. Action de conjugaison

Lemme 1. On a une action de G sur lui-même : [ROM21] p. 19

$$\forall g, h \in G, g \cdot h = ghg^{-1}$$

Définition 2. L'action précédente est appelée **action de conjugaison**. Le morphisme structurel de G dans $S(G)$ est noté Int :

$$\forall g, h \in G, \operatorname{Int}(g)(h) = ghg^{-1}$$

L'image de G par ce morphisme $\operatorname{Int}(G)$ est le groupe des **automorphismes intérieurs** de G.

Exemple 3. Le groupe additif d'un espace vectoriel est un groupe abélien dont le seul automorphisme intérieur est l'identité. [ULM21] p. 20

Proposition 4. Muni de la composition, l'ensemble des automorphismes intérieurs de G est un groupe. [GOU21] p. 21

2. Orbites et stabilisateurs

Définition 5. On considère l'action de conjugaison de G. [PER] p. 15

— Ses orbites sont les **classes de conjugaison** de G.

— Le stabilisateur d'un élément est le **centralisateur** de celui-ci.

— Deux éléments sont dits **conjugués** s'ils appartiennent à la même classe de conjugaison.

Exemple 6. Les cycles de même ordre sont conjugués dans S_n.

Définition 7. On définit le **centre** de G noté $Z(G)$ par p. 12

$$Z(G) = \{g \in G \mid \forall h \in H, gh = hg\}$$

Autrement dit, $Z(G)$ est l'intersection des centralisateurs des éléments de G.

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

Proposition 9. Soit $g \in G$. Alors, $g \in Z(G)$ si et seulement si sa classe de conjugaison est réduite à un élément. [ULM21] p. 36

Ainsi, $Z(G)$ est l'union des classes de conjugaison de taille 1.

II - Sous-groupes distingués et groupes quotients

1. Classes à gauche et à droite

Proposition 10. Soit $H < G$. On définit la relation $\sim_H$ sur G par $g_1 \sim_H g_2 \iff g_1^{-1} g_2 \in H$. Alors : p. 24

(i) $\sim_H$ est une relation d'équivalence.

(ii) La classe d'équivalence d'un élément $g \in G$ pour $\sim_H$ est $\overline{g} = gH = \{gh \mid h \in H\}$ appelée **classe à gauche** de g modulo H.

Remarque 11. On définit de la même manière la **classe à droite** d'un élément $g \in G$ modulo H que l'on note Hg.

Exemple 12. Soit $n > 2$. On considère $\mathcal{D}_n = \langle r, s \rangle$ le groupe diédral d'ordre $2n$. Alors,

$$r\langle s \rangle = \{r, rs\} \neq \{r, sr\} = \langle s \rangle r$$

Proposition 13. Soit $H < G$. Alors,

$$\forall g \in G, |hG| = |Gh| = |H|$$

2. Sous-groupes distingués

Définition 14. Soit $H < G$. On dit que H est **distingué** dans G si, [ROM21] p. 3

$$\forall g \in G, gH = Hg$$

On note cela $H \lhd G$.

Exemple 15. — $\{e_G\} \lhd G$, $G \lhd G$ et $Z(G) \lhd G$.

— L'intersection de deux sous-groupes distingués dans G est distinguée dans G.

— Si G est abélien, tout sous-groupe de G est distingué dans G.

Remarque 16. Le symbole $\lhd$ n'est pas transitif. [GOU21] p. 20

Proposition 17.

$$H \lhd G \iff \forall g \in G, gHg^{-1} \subseteq H$$

Proposition 18. Soient G_1 et G_2 deux groupes, et soient H_1 et H_2 deux sous-groupes respectivement de G_1 et de G_2. Soit $\varphi : G_1 \to G_2$ un morphisme. Alors : [ULM21] p. 16

(i) Si $H_1 \lhd G_1$, alors $\varphi(H_1) \lhd \varphi(G_1)$.

(ii) Si $H_2 \lhd G_2$, alors $\varphi^{-1}(H_2) \lhd G_1$.

En particulier, $\mathrm{Ker}(\varphi) \lhd G_1$.

Proposition 19. Soient $K < H < G$ une suite de sous-groupes. Alors, p. 43

$$K \lhd G \implies K \lhd H$$

Proposition 20. Soit $H < G$. Si $(G : H) = 2$ (voir sous-section suivante), alors $H \lhd G$. p. 25

3. Groupes quotients

Définition 21. Soit $H < G$.

— On appelle **ensemble quotient** de G par la relation d'équivalence $\sim_H$ de la Proposition 10, et on note G/H, l'ensemble des classes à gauche de G modulo H.

— On appelle **indice** de G dans H, et on note $(G : H)$, le cardinal de G/H.

Proposition 22. Soit $H < G$. L'ensemble des classes à droite de G modulo H est aussi de cardinal égal à $(G : H)$.

p. 44

Théorème 23. Un sous-groupe H de G est distingué si et seulement si $*$ définit une loi de groupe sur G/H par :

$$\forall g_1, g_2 \in G,\ g_1H * g_2H = (g_1g_2)H$$

telle que la surjection canonique

$$\pi_H : \begin{array}{rcl} G & \to & G/H \\ g & \mapsto & gH \end{array}$$

soit un morphisme de groupes. Dans ce cas, π_H est un morphisme surjectif de noyau H.

Définition 24. Soit $H \lhd G$. On appelle **groupe quotient** le groupe $(G/H, *)$ définit dans le théorème précédent.

Exemple 25. Soit $m \in \mathbb{N}^*$. $m\mathbb{Z}$ est un sous-groupe du groupe abélien $\mathbb{Z}$. On peut définir le groupe quotient $\mathbb{Z}/m\mathbb{Z}$: c'est un groupe cyclique d'ordre m.

4. Théorèmes d'isomorphisme

[ULM21] p. 51

Théorème 26 (Premier théorème d'isomorphisme)**.** Soient G_1 et G_2 deux groupes et soit $\varphi : G_1 \to G_2$ un morphisme. Alors φ induit un isomorphisme

$$\overline{\varphi} : \begin{array}{rcl} G_1/\mathrm{Ker}(\varphi) & \to & \varphi(G_1) \\ g\mathrm{Ker}(\varphi) & \mapsto & \varphi(g) \end{array}$$

Exemple 27. — Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

— $G/Z(G) \cong \mathrm{Int}(G)$.

p. 80

Théorème 28 (Deuxième théorème d'isomorphisme)**.** Soient $H < G$ et $K \lhd G$. On pose $N = H \cap K$. Alors,

$$N \lhd H \text{ et } H/N \cong HK/K$$

Exemple 29. On note V le sous-groupe de S_4 d'ordre 4 isomorphe au groupe de Klein. Alors,

$$V/S_4 \cong S_3$$

p. 51

Théorème 30 (Troisième théorème d'isomorphisme)**.** Soient $H, K \lhd G$ tels que $H \subset K$. Alors,

$$K/H \lhd G/H \text{ et } (G/H)/(K/H) \cong G/K$$

Exemple 31.

$$(\mathbb{Z}/10\mathbb{Z})/(2\mathbb{Z}/10\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$$

III - Applications

1. Application aux p-groupes

Soit G un groupe fini opérant sur un ensemble fini X. [ROM21] p. 22

Définition 32. On dit que G est un p**-groupe** s'il est d'ordre une puissance d'un nombre premier p.

Théorème 33 (Formule des classes)**.** Soit Ω un système de représentants des orbites de l'action de G sur X. Alors,

$$|X| = \sum_{\omega \in \Omega} |G \cdot \omega| = \sum_{\omega \in \Omega} (G : \mathrm{Stab}_G(\omega)) = \sum_{\omega \in \Omega} \frac{|G|}{|\mathrm{Stab}_G(\omega)|}$$

Corollaire 34. Soit p un nombre premier. Si G est un p-groupe opérant sur X, alors,

$$|X^G| \equiv |X| \mod p$$

où X^G désigne l'ensemble des points fixes de X sous l'action de G.

Corollaire 35. On note $G \cdot h_1, \dots, G \cdot h_r$ les classes de conjugaison de G. Alors,

$$\begin{aligned} |G| &= |Z(G)| + \sum_{\substack{i=1 \\ |G \cdot h_i| = 2}}^{r} |G \cdot h_i| \\ &= |Z(G)| + \sum_{\substack{i=1 \\ |G \cdot h_i| = 2}}^{r} \frac{|G|}{|\mathrm{Stab}_G(h_i)|} \end{aligned}$$

Corollaire 36. Soit p un nombre premier. Le centre d'un p-groupe non trivial est non trivial.

Corollaire 37. Soit p un nombre premier. Un groupe d'ordre p^2 est toujours abélien.

Application 38 (Théorème de Cauchy)**.** On suppose G non trivial et fini. Soit p un premier divisant l'ordre de G. Alors il existe un élément d'ordre p dans G.

[DEV] **Application 39** (Premier théorème de Sylow)**.** On suppose G fini d'ordre np^α avec $n, \alpha \in \mathbb{N}$ et p premier tel que $p \nmid n$. Alors, il existe un sous-groupe de G d'ordre p^α. [GOU21] p. 44

2. Application au groupe symétrique

Lemme 40. Les 3-cycles sont conjugués dans A_n pour $n \geq 5$. [PER] p. 15

Lemme 41. Le produit de deux transpositions est un produit de 3-cycles. [ROM21] p. 49

Proposition 42. A_n est engendré par les 3-cycles pour $n \geq 3$.

[DEV] **Théorème 43.** A_n est simple pour $n \geq 5$. [PER] p. 28

Corollaire 44. Pour $n \geq 5$, les sous-groupes distingués de S_n sont S_n, A_n et $\{\mathrm{id}\}$.

Application 45. A_5 est le seul groupe simple d'ordre 60 à isomorphisme près. [ULM21] p. 92

3. Application au groupe linéaire d'un espace vectoriel

Dans cette partie, E désignera un espace vectoriel sur un corps $\mathbb{K}$ de dimension finie n.

a. Centre

Définition 46. Soit H un hyperplan de E et soit $u \in \mathrm{SL}(E) \setminus \{\mathrm{id}_E\}$. Posons $D = \mathrm{Im}(u - \mathrm{id}_E)$. On dit que u est une **transvection** d'hyperplan H et de droite D si $u_{|H} = \mathrm{id}_H$ (et dans ce cas, $D \subset H$). [PER] p. 97

Proposition 47. $u \in \mathrm{GL}(E)$ est une transvection de droite D si et seulement si $u_{|D} = \mathrm{id}_D$ et le morphisme induit $\overline{u} : E/D \to E/D$ est l'identité.

Proposition 48. Soit τ une transvection de droite D et d'hyperplan H et soit $u \in \mathrm{GL}(E)$. Alors $u\tau u^{-1}$ est une transvection de droite $u(D)$ et d'hyperplan $u(H)$.

Corollaire 49. (i) $Z(\mathrm{GL}(E)) = \{\lambda \,\mathrm{id}_E \mid \lambda \in \mathbb{K}^*\}$.

(ii) $Z(\mathrm{SL}(E)) = Z(\mathrm{GL}(E)) \cap \mathrm{SL}(E) \cong \mu_n(\mathbb{K})$.

b. Conjugaison

Définition 50. Soit H un hyperplan de E et soit $u \in \mathrm{GL}(E) \setminus \mathrm{SL}(E)$. Posons $D = \mathrm{Im}(u - \mathrm{id}_E)$. On dit que u est une **dilatation de droite** D **et d'hyperplan** H si $u_{|H} = \mathrm{id}_H$.

Le **rapport** de cette dilatation est le scalaire $\det(u)$.

Proposition 51. Deux dilatations sont conjuguées dans $\mathrm{GL}(E)$ si et seulement si elles ont le même rapport.

Proposition 52. Deux transvections sont toujours conjuguées dans $\mathrm{GL}(E)$. Si $n \geq 3$, elles le sont aussi dans $\mathrm{SL}(E)$.

c. Groupe projectif

Définition 53. Le quotient de $\mathrm{GL}(E)$ par son centre est appelé **groupe projectif linéaire** et est noté $\mathrm{PGL}(E)$. De même, le quotient de $\mathrm{SL}(E)$ par son centre est noté $\mathrm{PSL}(E)$.

Remarque 54. Soit $h_\lambda : x \mapsto \lambda x$, on a $\det h_\lambda = \lambda^n$, de sorte qu'on a une suite exacte :

$$\{\overline{\mathrm{id}_E}\} \to \mathrm{PSL}(E) \to \mathrm{PGL}(E) \xrightarrow{\det} \mathbb{K}^* / \mathbb{K}^{*n} \to \{\overline{\mathrm{id}_E}\}$$

où on a posé $\mathbb{K}^{*n} = \{\lambda \in \mathbb{K}^* \mid \exists \mu \in \mathbb{K}^*, \lambda = \mu^n\}$. En particulier, si $\mathbb{K}$ est algébriquement clos, $\mathrm{PSL}(E) \cong \mathrm{PGL}(E)$.

Théorème 55. Le groupe $\mathrm{PSL}(E)$ est simple sauf si $n = 2$ et $\mathbb{K} = \mathbb{F}_2$ ou $\mathbb{F}_3$.

4. Représentations linéaires de groupes finis

Dans cette partie, on suppose que G est d'ordre fini. **[ULM21]** p. 144

Définition 56.
— Une **représentation linéaire** ρ est un morphisme de G dans $\mathrm{GL}(V)$ où V désigne un espace-vectoriel de dimension finie n sur $\mathbb{C}$.
— On dit que n est le **degré** de ρ.
— On dit que ρ est **irréductible** si $V \neq \{0\}$ et si aucun sous-espace vectoriel de V n'est

stable par $\rho(g)$ pour tout $g \in G$, hormis $\{0\}$ et V.

Exemple 57. Soit $\varphi : G \to S_n$ le morphisme structurel d'une action de G sur un ensemble de cardinal n. On obtient une représentation de G sur $\mathbb{C}^n = \{e_1, \dots, e_n\}$ en posant

$$\rho(g)(e_i) = e_{\varphi(g)(i)}$$

c'est la représentation par permutations de G associé à l'action. Elle est de degré n.

Définition 58. La représentation par permutations de G associée à l'action par translation à gauche de G sur lui-même est la **représentation régulière** de G, on la note ρ_G.

Définition 59. On peut associer à toute représentation linéaire ρ, son **caractère** $\chi = \operatorname{trace} \circ \rho$. On dit que χ est **irréductible** si ρ est irréductible. p. 150

Proposition 60. (i) Les caractères sont des fonctions constantes sur les classes de conjugaison.

(ii) Il y a autant de caractères irréductibles que de classes de conjugaisons.

Définition 61. Soit $\rho : G \to \mathrm{GL}(V)$ une représentation linéaire de G. On suppose $V = W \oplus W_0$ avec W et W_0 stables par $\rho(g)$ pour tout $g \in G$. On dit alors que ρ est **somme directe** de ρ_W et de ρ_{W_0}.

Théorème 62 (Maschke)**.** Toute représentation linéaire de G est somme directe de représentations irréductibles.

Théorème 63. Les sous-groupes distingués de G sont exactement les [PEY] p. 231

$$\bigcap_{i \in I} \operatorname{Ker}(\rho_i) \text{ où } I \in \mathscr{P}(\llbracket 1, r \rrbracket)$$

Corollaire 64. G est simple si et seulement si $\forall i \neq 1$, $\forall g \neq e_G$, $\chi_i(g) \neq \chi_i(e_G)$.

Annexes

[ULM21]
p. 51

$$
\begin{tikzcd}
G_1 \arrow[rr, "\varphi"] \arrow[dr, two heads, bend right, "\pi_{G_1/\mathrm{Ker}(\varphi)}"'] & & \varphi(G_1) \arrow[rr, hook] & & G_2 \\
& G_1/\mathrm{Ker}(\varphi) \arrow[ur, dashed, bend right, "\overline{\varphi}"'] & & &
\end{tikzcd}
$$

FIGURE 1 – Illustration du premier théorème d'isomorphisme par un diagramme.

Bibliographie

Les maths en tête **[GOU21]**

Xavier Gourdon. *Les maths en tête. Algèbre et probabilités.* 3e éd. Ellipses, 13 juill. 2021. https://www.editions-ellipses.fr/accueil/13722-25266-les-maths-en-tete-algebre-et-probabilites-3e-edition-9782340056763.html.

Cours d'algèbre **[PER]**

Daniel Perrin. *Cours d'algèbre. pour l'agrégation.* Ellipses, 15 fév. 1996. https://www.editions-ellipses.fr/accueil/7778-18110-cours-d-algebre-agregation-9782729855529.html.

L'algèbre discrète de la transformée de Fourier **[PEY]**

Gabriel Peyré. *L'algèbre discrète de la transformée de Fourier. Niveau M1.* Ellipses, 15 jan. 2004. https://adtf-livre.github.io.

Mathématiques pour l'agrégation **[ROM21]**

Jean-Étienne Rombaldi. *Mathématiques pour l'agrégation. Algèbre et géométrie.* 2e éd. De Boeck Supérieur, 20 avr. 2021. https://www.deboecksuperieur.com/ouvrage/9782807332201-mathematiques-pour-l-agregation-algebre-et-geometrie.

Théorie des groupes **[ULM21]**

Felix Ulmer. *Théorie des groupes. Cours et exercices.* 2e éd. Ellipses, 3 août 2021. https://www.editions-ellipses.fr/accueil/13760-25304-theorie-des-groupes-2e-edition-9782340057241.html.