

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 :

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

[ROM21]
p. 19

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

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

L'image de G par ce morphisme $\text{Int}(G)$ 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 .

- 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.

[PER]
p. 15

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

p. 12

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

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

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.

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

[ULM21]
p. 36

3. Application aux p -groupes

Définition 10. On dit que G est un **p -groupe** s'il est d'ordre une puissance d'un nombre premier p .

[ROM21]
p. 22

Proposition 11. Soit p un nombre premier. Si G est un p -groupe opérant sur un ensemble X , alors,

$$|X^G| \equiv |X| \pmod{p}$$

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

Corollaire 12. On note $G \cdot h_1, \dots, G \cdot h_r$ les classes de conjugaison de G . Alors,

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

Corollaire 13. Soit p un nombre premier. Le centre d'un p -groupe non trivial est non trivial.

Corollaire 14. Soit p un nombre premier. Un groupe d'ordre p^2 est toujours abélien.

Application 15 (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 .

II - Sous-groupes distingués et groupes quotients

1. Classes à gauche et à droite

Proposition 16. 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 :

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

[ULM21]
p. 24

Remarque 17. On définit de la même manière la **classe à droite** d'un élément $g \in G$ modulo H que l'on note Hg .

Exemple 18. 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 19. Soit $H < G$. Alors,

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

2. Sous-groupes distingués

Définition 20. Soit $H < G$. On dit que H est **distingué** dans G si,

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

On note cela $H \triangleleft G$.

[ROM21]
p. 3

Exemple 21. — $\{e_G\} \triangleleft G, G \triangleleft G$ et $Z(G) \triangleleft G$.

- 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 22. Le symbole \triangleleft n'est pas transitif.

[GOU21]
p. 20

Proposition 23.

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

[ULM21]
p. 16

Proposition 24. 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 $\varphi : G_1 \rightarrow G_2$ un morphisme. Alors :

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

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

En particulier, $\text{Ker}(\varphi) \triangleleft G_1$.

Proposition 25. Soient $K < H < G$ une suite de sous-groupes. Alors,

$$K \triangleleft G \implies K \triangleleft H$$

p. 43

Proposition 26. Soit $H < G$. Si $(G : H) = 2$, alors $H \triangleleft G$.

p. 25

3. Groupes quotients

Définition 27. Soit $H < G$.

— On appelle **ensemble quotient** de G par la relation d'équivalence \sim_H de la Proposition 16, 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 .

[ULM21]

p. 25

Proposition 28. Soit $H < G$. L'ensemble des classes à droite de G modulo H est aussi de cardinal égal à $(G : H)$.

Théorème 29. 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

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

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

p. 44

Définition 30. Soit $H \triangleleft G$. On appelle **groupe quotient** le groupe $(G/H, *)$ défini dans le théorème précédent.

Exemple 31. 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

Théorème 32 (Premier théorème d'isomorphisme). Soient G_1 et G_2 deux groupes et soit $\varphi : G_1 \rightarrow G_2$ un morphisme. Alors φ induit un isomorphisme

[ULM21]
p. 51

$$\bar{\varphi} : \begin{array}{l} G_1/\text{Ker}(\varphi) \rightarrow \varphi(G_1) \\ g\text{Ker}(\varphi) \mapsto \varphi(g) \end{array}$$

Exemple 33. — Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

$$— G/Z(G) \cong \text{Int}(G).$$

Théorème 34 (Deuxième théorème d'isomorphisme). Soient $H < G$ et $K \triangleleft G$. On pose $N = H \cap K$. Alors,

p. 80

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

Exemple 35. On note V le sous-groupe de S_4 d'ordre 4 isomorphe au groupe de Klein. Alors,

$$V/S_4 \cong S_3$$

Théorème 36 (Troisième théorème d'isomorphisme). Soient $H, K \triangleleft G$ tels que $H \subset K$. Alors,

p. 51

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

Exemple 37.

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

III - Applications

1. Application au groupe symétrique

Lemme 38. Les 3-cycles sont conjugués dans A_n pour $n \geq 5$.

[PER]
p. 15

Lemme 39. Le produit de deux transpositions est un produit de 3-cycles.

[ROM21]
p. 49

Proposition 40. A_n est engendré par les 3-cycles pour $n \geq 3$.

Théorème 41. A_n est simple pour $n \geq 5$.

[PER]
p. 28

Corollaire 42. Pour $n \geq 5$, les sous-groupes distingués de S_n sont S_n , A_n et $\{\text{id}\}$.

Application 43. A_5 est le seul groupe simple d'ordre 60 à isomorphisme près.

[ULM21]
p. 92

2. 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 44. Soit H un hyperplan de E et soit $u \in \text{SL}(E) \setminus \{\text{id}_E\}$. Posons $D = \text{Im}(u - \text{id}_E)$. On dit que u est une **transvection** d'hyperplan H et de droite D si $u|_H = \text{id}_H$ (et dans ce cas, $D \subset H$).

[PER]
p. 97

Proposition 45. $u \in \text{GL}(E)$ est une transvection de droite D si et seulement si $u|_D = \text{id}_D$ et le morphisme induit $\bar{u} : E/D \rightarrow E/D$ est l'identité.

Proposition 46. Soit τ une transvection de droite D et d'hyperplan H et soit $u \in \text{GL}(E)$. Alors $u\tau u^{-1}$ est une transvection de droite $u(D)$ et d'hyperplan $u(H)$.

Corollaire 47. (i) $Z(\text{GL}(E)) = \{\lambda \text{id}_E \mid \lambda \in \mathbb{K}^*\}$.
(ii) $Z(\text{SL}(E)) = Z(\text{GL}(E)) \cap \text{SL}(E) \cong \mu_n(\mathbb{K})$.

b. Conjugaison

Définition 48. Soit H un hyperplan de E et soit $u \in \text{GL}(E) \setminus \text{SL}(E)$. Posons $D = \text{Im}(u - \text{id}_E)$. On dit que u est une **dilatation de droite D et d'hyperplan H** si $u|_H = \text{id}_H$.
Le **rapport** de cette dilatation est le scalaire $\det(u)$.

Proposition 49. Deux dilatations sont conjuguées dans $\text{GL}(E)$ si et seulement si elles ont le même rapport.

Proposition 50. Deux transvections sont toujours conjuguées dans $\text{GL}(E)$. Si $n \geq 3$, elles le sont aussi dans $\text{SL}(E)$.

c. Groupe projectif

Définition 51. Le quotient de $GL(E)$ par son centre est appelé **groupe projectif linéaire** et est noté $PGL(E)$. De même, le quotient de $SL(E)$ par son centre est noté $PSL(E)$.

Remarque 52. Soit $h_\lambda : x \mapsto \lambda x$, on a $\det h_\lambda = \lambda^n$, de sorte qu'on a une suite exacte :

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

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, $PSL(E) \cong PGL(E)$.

Théorème 53. Le groupe $PSL(E)$ est simple sauf si $n = 2$ et $\mathbb{K} = \mathbb{F}_2$ ou \mathbb{F}_3 .

3. Représentations linéaires de groupes finis

Dans cette partie, on suppose que G est d'ordre fini.

[ULM21]
p. 144

Définition 54. — Une **représentation linéaire** ρ est un morphisme de G dans $GL(V)$ 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 55. Soit $\varphi : G \rightarrow S_n$ 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 associée à l'action. Elle est de degré n .

Définition 56. 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 57. On peut associer à toute représentation linéaire ρ , son **caractère** $\chi = \text{trace} \circ \rho$. On dit que χ est **irréductible** si ρ est irréductible.

p. 150

Proposition 58. (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 59. Soit $\rho : G \rightarrow GL(V)$ 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 60 (Maschke). Toute représentation linéaire de G est somme directe de représentations irréductibles.

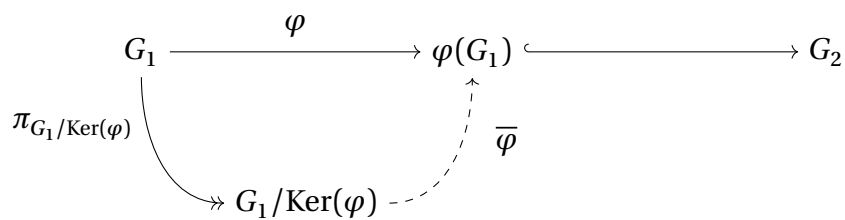
Théorème 61. Les sous-groupes distingués de G sont exactement les

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

Corollaire 62. G est simple si et seulement si $\forall i \neq 1, \forall g \neq e_G, \chi_i(g) \neq \chi_i(e_G)$.

[PEY]
p. 231

Annexes



[ULM21]

p. 51

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*. 3^e 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*. 2^e 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*. 2^e éd. Ellipses, 3 août 2021.

<https://www.editions-ellipses.fr/accueil/13760-25304-theorie-des-groupes-2e-edition-9782340057241.html>.