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

Pandou

12 avril 2022

G est un groupe fixé dans toute la suite.

1 Actions par conjugaison

1.1 Conjugaison

Définition 1. *Si $x \in G$, on définit $\mathrm{Int}(x) : y \in G \longmapsto xyx^{-1}$ l'automorphisme de conjugaison par x. On note $\mathrm{Int}(G)$ le groupe des automorphismes dit intérieurs de G.*

Remarque 2 : Le morphisme $\mathrm{Int} : G \longrightarrow \mathrm{Aut}(G)$ est une action de G sur G, appelée action par conjugaison. On dit alors que deux éléments sont conjugués s'ils sont dans la même orbite pour cette action.

Définition 3. *Le noyau de l'action par conjugaison est noté $Z(G) = \{x \in G, \forall y \in G, xy = yx\}$, appelé centre de G.*

Application 4 : Soit G un groupe fini non abélien et k le nombre de classes de conjugaisons de G, alors on a
$$k \leqslant \frac{5}{8}\mathrm{Card}(G)$$

Définition 5. *On dit qu'un sous-groupe H est distingué si pour tout $x \in G$, H est stable par $\mathrm{Int}(x)$. On dit que G est simple s'il n'admet aucun sous-groupe distingué autre que $\{1\}$ et G.*

Exemple 6 : Les groupes abéliens finis simples sont les $\mathbb{Z}/p\mathbb{Z}$ pour p premier.

Proposition 7. *H est distingué dans G si, et seulement si, $\forall x \in G, xH = Hx$.*

Proposition 8. *Soit $\varphi : G \longrightarrow G'$ un morphisme de groupes et H, H' des sous-groupes de G, G'. Alors,*

1. *Si H' est distingué dans G', alors $\varphi^{-1}(H')$ est distingué dans G. En particulier, tout noyau est toujours distingué.*
2. *Si H est distingué dans G et φ est surjectif, alors $\varphi(H)$ est distingué.*

Théorème 9. *Si p est le plus petit diviseur premier de $\mathrm{Card}(G)$ et H un sous-groupe d'indice p, alors H est distingué.*

1.2 Quotients

Théorème 10. *H est distingué dans G si, et seulement, si il existe une unique structure de groupe sur G/H tel que $\pi : G \longrightarrow G/H$ soit un morphisme groupes.*

Remarque 11 : Si H est un sous-groupe abélien de G, alors le quotient G/H est toujours un groupe.

Proposition 12. *Un sous-groupe de G/H s'identifie (via $G \longrightarrow G/H$) à un unique sous-groupe de G contenant H.*

Théorème 13 (Premier théorème d'isomorphisme)**.** *Soit $\varphi : G \longrightarrow G'$ un morphisme de groupes, alors on a un isomorphisme naturel*
$$G/\mathrm{Ker}(\varphi) \simeq \mathrm{Im}(\varphi)$$

Applications 14 :

- Dans $\mathbb{F}_q^\times$, il y a exactement $\dfrac{q-1}{2}$ carrés.
- $\mathrm{Card}\big(SL_n(\mathbb{F}_q)\big) = \dfrac{\mathrm{Card}\big(GL_n(\mathbb{F}_q)\big)}{q-1}$.
- $G/Z(G) \simeq \mathrm{Int}(G)$.

Corollaire 15. *Un sous-groupe H est distingué si, et seulement s'il existe un groupe G' et un morphisme $\varphi : G \longrightarrow G'$ tel que $H = \mathrm{Ker}(\varphi)$.*

Théorème 16 (Deuxième théorème d'isomorphisme)**.** *Soit H un sous-groupe distingué de H et K un autre sous-groupe de G, alors $H \cap K$ est distingué dans K et H est distingué dans HK et*
$$K/(H \cap K) \simeq HK/H$$

Remarque 17 : Si G est additif, ceci se réécrit $K/(H \cap K) \simeq (H+K)/H$. En particulier, si $H \cap K = 0$, alors on a $(H \oplus K)/H \simeq K$.

Théorème 18 (Troisième théorème d'isomorphisme)**.** *Soit $H \subset K$ deux sous-groupes de G tous les deux distingués dans G, alors K/H est distingué dans G/H et on a*
$$G/K \simeq (G/H)\big/(K/H)$$

Définition 19. *On dit qu'un sous-groupe H est caractéristique s'il est stable par tous les automorphismes de G.*

Proposition 20. *Un sous-groupe caractéristique est toujours distingué.*

Exemples 21 :
- Le groupe dérivé $D(G)$ engendré par les commutateurs $xyx^{-1}y^{-1}$ est distingué. Ainsi, l'abélianisé $G/D(G)$ est un groupe.
- $\mathrm{Int}(G)$ est caractéristique dans $\mathrm{Aut}(G)$.

1.3 Conjugaison dans $\mathfrak{S}_n$

Proposition 22. *Soit $\sigma \in \mathfrak{S}_n$, alors*

$$\sigma \begin{pmatrix} a_1 & \dots & a_p \end{pmatrix} \sigma^{-1} = \begin{pmatrix} \sigma(a_1) & \dots & \sigma(a_p) \end{pmatrix}$$

En particulier, tous les cycles de même longueur sont conjugués dans $\mathfrak{S}_n$.

Corollaire 23. *Deux éléments de $\mathfrak{S}_n$ sont conjugués dans $\mathfrak{S}_n$ si, et seulement s'ils ont le même nombre de cycles de même longueur.*

DEVELOPPEMENT 1

Lemme 24. *Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$ qui transforme toute transposition en une transposition, alors φ est intérieur.*

Théorème 25. *Si $n \neq 6$,*

$$\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n)$$

Remarque 26 : $\mathrm{Aut}(\mathfrak{S}_6) \neq \mathrm{Int}(\mathfrak{S}_6)$.

Théorème 27. *Si $n \geqslant 5$, $\mathfrak{A}_n$ est simple.*

Corollaire 28. *Les sous-groupes distingués de $\mathfrak{S}_n$ sont $\{1\}$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$.*

2 Groupe linéaire

On fixe un K-espace vectoriel E de dimension finie.

2.1 Groupe spécial linéaire

Théorème 29.
- *Les transvections engendrent $SL(E)$.*
- *Les transvections et les dilatations engendrent $GL(E)$.*

Proposition 30. *Deux dilatations sont conjuguées dans $GL(E)$ si, et seulement si, elles ont même rapport.*

Proposition 31.
- *Deux transvections sont conjuguées dans $GL(E)$.*
- *Si $\dim(E) \geqslant 3$, deux transvections sont conjuguées dans $SL(E)$.*
- *Dans $SL_2(K)$, toute transvection est conjugué à une matrice $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$. De plus, $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$ sont conjuguées si, et seulement si, $\dfrac{\lambda}{\mu}$ est un carré dans K.*

Théorème 32. *$PSL_n(\mathbb{F}_q)$ est simple, sauf si $(n, q) \in \{(2,2), (2,3)\}$.*

Remarque 33 : On a

$$PSL_2(\mathbb{F}_2) \simeq \mathfrak{S}_3 \qquad \text{et} \qquad PSL_2(\mathbb{F}_3) \simeq \mathfrak{A}_4$$

2.2 Réduction des matrices

Définition 34. *Soit $M \in M_n(K)$, on dit que M est diagonalisable (resp. trigonalisable) s'il existe $P \in GL_n(K)$ tel que PMP^{-1} est diagonale (resp. triangulaire).*

Théorème 35. *Soit $M \in M_n(K)$. Alors, on a équivalence entre :*
1. *M est diagonalisable.*
2. *M est annulé par un polynôme scindé à racines simples.*
3. *Le polynôme minimal de M est scindé à racines simples.*

Théorème 36. *Soit $M \in M_n(K)$. Alors, on a équivalence entre :*
1. *M est trigonalisable.*
2. *M est annulé par un polynôme scindé.*
3. *Le polynôme minimal de M est scindé.*

Théorème 37 (Décomposition de Dunford)**.** *Soit $M \in M_n(K)$ tel que χ_M est scindé. Alors, il existe un unique couple (D, N) de matrices telles que*
1. *D est diagonalisable, N est nilpotente.*
2. *D et N commutent.*
3. *$M = D + N$.*

De plus, D et N sont des polynômes en M.

3 Vers la théorie de Lie

3.1 Un isomorphisme exceptionnel quaternionique

Définition 38. *L'algèbre des quaternions est la $\mathbb{R}$-algèbre de dimension 4, notée $\mathbb{H}$, ayant pour base $(1, i, j, k)$ telle que*

$$i^2 = j^2 = k^2 = ijk = -1$$

On note $\mathbb{I} = \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ l'ensemble des imaginaires purs.
Enfin, si $h = x + yi + zj + tk \in \mathbb{H}$, on définit

$$\overline{h} = x - yi - zj - tk \qquad \text{et} \qquad N(h) = h\overline{h}$$

Proposition 39. *$\mathbb{H}$ est associative. De plus, on a*
- $h \in \mathbb{R} \iff h = \overline{h}$.
- $h \in \mathbb{I} \iff h^2 \in \mathbb{R}_- \iff \overline{h} = -h$.
- *N est une forme quadratique réelle définie positive sur $\mathbb{H}$.*
- $\forall h, h' \in \mathbb{H}, N(hh') = N(h)N(h')$.

Corollaire 40. *$\mathbb{H}$ est un corps non commutatif où l'inverse est donné par* $h^{-1} = \dfrac{1}{N(h)}\overline{h}$.

Théorème 41. *On a les isomorphismes suivants*

$$\mathbb{H} \simeq \left\{ \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix}, a, b \in \mathbb{C} \right\} \qquad \text{et} \qquad \{h \in \mathbb{H}, N(h) = 1\} \simeq \mathbb{S}^3 \simeq SU(2)$$

DEVELOPPEMENT 2

Théorème 42. *On a les isomorphismes exceptionnels suivants*

$$PSU(2) \simeq SO(3) \qquad \text{et} \qquad PSO(4) \simeq SO(3) \times SO(3)$$

3.2 Algèbre de Lie et crochet de Lie

Définition 43. *Un groupe de Lie matriciel est un sous-groupe de $GL_n(\mathbb{R})$ tel que G est une sous-variété de $M_n(\mathbb{R})$. Le plan tangent à G en l'identité est noté $\mathfrak{g}$. Si $\varphi : G \longrightarrow G$, on notera $T\varphi : \mathfrak{g} \longrightarrow \mathfrak{g}$ la différentielle en l'identité.*

Définition 44. *Soit $x \in G$, alors $\mathrm{Int}(x) : G \longrightarrow G$ est différentiable et sa différentielle en l'identité est notée*

$$\mathrm{Ad}(x) := T\mathrm{Int}(x) : \mathfrak{g} \longrightarrow \mathfrak{g}$$

Proposition 45. *Pour tout $x \in G$, $\mathrm{Ad}(x) \in GL(\mathfrak{g})$, de sorte qu'on a une application différentiable*

$$\mathrm{Ad} : G \longrightarrow GL(\mathfrak{g})$$

Définition 46. *On pose pour $X \in \mathfrak{g}$, $\mathrm{ad}(X) = T\mathrm{Ad}(X)$ et le crochet de Lie sur G est défini par*

$$\forall X, Y \in \mathfrak{g}, [X, Y] = \mathrm{ad}_X(Y)$$

Proposition 47. *On suppose ici que $G = GL_n(\mathbb{R})$, alors*

$$\forall X, Y \in \mathfrak{g}, [X, Y] = XY - YX \qquad \text{et} \qquad \forall g \in G, \forall X \in \mathfrak{g}, \mathrm{Ad}(g) \cdot X = gXg^{-1}$$

Proposition 48. *Pour tout $X \in M_n(\mathbb{R})$,*

$$\exp\big(\mathrm{ad}(X)\big) = \mathrm{Ad}\big(\exp(X)\big)$$

Théorème 49 (Admis)**.** *Les groupes de Lie matriciels sont exactement les sous-groupes fermés de $GL_n(\mathbb{R})$ et*

$$\mathfrak{g} = \left\{ X \in M_n(\mathbb{R}), \forall t \in \mathbb{R}, e^{tX} \in G \right\}$$

Références :

- Calais, Éléments de théorie des groupes.
- Caldero, Germonie, H2H2.
- Gourdon, Algèbre.
- Perrin, Cours d'algèbre.