103. Conjugaison dans un groupe - Exemples de sous-groupes distingués et de groupes quotients. Applications 103 (1)

<u>Cadre</u> : K est un corps commutatif. $(G,\cdot)$ est un groupe. $n \in \mathbb{N}^*$, et si $n \geq 2$, S_n (resp. A_n) désigne le groupe symétrique (resp. alterné) d'ordre n.

I. Conjugaison dans un groupe

[Ber] <u>Déf/Prop. (1)</u> : Soit $g \in G$. L'application $\mathrm{Int}_g : \begin{array}{l} G \to G \\ x \mapsto gxg^{-1} \end{array}$ est un automorphisme de G appelé automorphisme intérieur associé à g.

130 De plus, $\mathrm{Int} : \begin{array}{l} G \to (\mathrm{Aut}(G), \circ) \\ g \mapsto \mathrm{Int}_g \end{array}$ est un morphisme de groupes.

<u>Déf. (2)</u> : Deux éléments (resp. deux parties) $x, x' \in G$ (resp. $P, P' \subset G$) sont dits conjugués s'il existe $g \in G$ tel que $x' = \mathrm{Int}_g(x)$ (resp. $P' = \mathrm{Int}_g(P)$).

131 La classe de conjugaison de x est $\mathrm{Conj}_G(x) = \{gxg^{-1}, g \in G\}$.

<u>Déf. (3)</u> : Le centre de G est $Z(G) = \{x \in G \,/\, \forall g \in G, gx = xg\}$, soit

♡ $Z(G) = \{x \in G \,/\, \mathrm{Conj}_G(x) = \{x\}\}$. G est alors abélien SSI $Z(G) = G$.

<u>Déf. (4)</u> : L'action de G sur G induite par Int est appelée action par conjugaison. Si $x \in G$, son orbite pour cette action est $\omega(x) = \mathrm{Conj}_G(x)$,

♡ et son stabilisateur $\mathrm{Stab}_x(g) = \{g \in G \,/\, gxg^{-1} = x\}$ est appelé centralisateur de x.

<u>Rq (5)</u> : Si $H \leq G$, on ne peut pas toujours définir l'action par conjugaison de G sur H.

~236 <u>Ex. (6)</u> : $G = S_3$. $H = \langle (1\,2) \rangle = \{id, (1\,2)\}$, $\tau = (1\,3)$.

♡ $\tau (1\,2) \tau^{-1} = (3\,2) \notin H$.

II. Sous-groupes distingués. Groupes quotients

1) Définitions. Propriétés fondamentales

[Per] <u>Déf. (7)</u> : Soit $H \leq G$. H est dit distingué dans G s'il est stable par tout

11 automorphisme intérieur de G, i.e. $gHg^{-1} = H$ $\forall g \in G$. On le note $H \lhd G$.

<u>Rq (8)</u> : $H \lhd G \iff \forall g \in G, gHg^{-1} \subset H$.

<u>Ex (9)</u> : 1/ $Z(G) \lhd G$

~12 2/ Si G est abélien, alors tout sous-groupe de G est distingué dans G.

<u>Th. (10)</u> : Soit $H \leq G$. Alors G/H peut être muni d'une structure de [Ber]

groupe faisant de la projection canonique $\pi : G \to G/H$ un morphisme ~236

de groupes SSI $H \lhd G$.

<u>Déf. (11)</u> : Si $H \lhd G$, G/H est appelé groupe quotient de G par H. 237

<u>Prop. (12)</u> : Soit $H \lhd G$.

1) $A \leq G/H \iff \exists H' \leq G \,/\, H \subset H'$ et $A = \pi(H')$. 238

2) $A \lhd G/H \iff \exists H' \lhd G \,/\, H \subset H'$ et $A = \pi(H')$.

<u>Prop. (13)</u> : Soit $f : G \to G'$ un morphisme de groupes. Si $H' \lhd G'$ ♡

alors $f^{-1}(H') \lhd G$. En particulier $\mathrm{Ker} f \lhd G$.

Si $H \lhd G$, alors $f(H) \lhd f(G)$.

<u>Ex. (14)</u> : $A_n \lhd S_n$

<u>Th. (15)</u> : <u>(Théorème de factorisation et premier théorème d'isomorphisme)</u> 239

1/ Soit $f : G \to G'$ un morphisme de groupes et $H \lhd G$ tel que $H \subset \mathrm{Ker} f$.
Alors il existe un unique morphisme de groupes $\bar{f} : G/H \to G'$ tel que $f = \bar{f} \circ \pi$.

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ & {\scriptstyle\pi}\searrow & \nearrow{\scriptstyle\bar{f}} \\ & G/H & \end{array}$$

Il est défini par : $\bar{f}(\bar{x}) = f(x)$ $\forall \bar{x} \in G/H$.

2/ De plus, il y a correspondance bijective entre :

$$\begin{array}{ccc} \mathrm{Hom}(G/H, G') & \longrightarrow & \{f \in \mathrm{Hom}(G, G') \,/\, H \subset \mathrm{Ker} f\} \\ \varphi & \longmapsto & \varphi \circ \pi \\ \bar{f} & \longleftarrow & f \end{array}$$

3) Enfin, si $H = \mathrm{Ker} f$, $\bar{f}$ est injectif et $G/\mathrm{Ker} f \simeq \mathrm{Im} f$. 241

<u>Coro (16)</u> : Si $f : G \to G'$ est surjectif, alors $G/\mathrm{Ker} f \simeq G'$.

<u>Ex. (17)</u> : $GL_n(K)/SL_n(K) \simeq K^*$ ♡

<u>Déf. (18)</u> : G est dit simple si ses seuls sous-groupes distingués [Per]

sont $\{1\}$ et G. 12

<u>Exercice (18 bis)</u> : Montrer que si $2 \leq |G| < +\infty$, G est simple et abélien, ~♡

alors il existe p premier tel que $G \simeq \mathbb{Z}/p\mathbb{Z}$.

2) Premières applications

[Bu] 181 **Th. 19 :** Soit G un p-groupe. Alors $Z(G)$ est non trivial.

♡ **Appli. 20 :** Si $|G| = p^2$, p premier, alors G est abélien

[Pe] **Th. 21 :** (*Wedderburn*)

82 Tout corps fini est commutatif.

3) Groupe dérivé

[Pe] **Déf. 22 :** Un commutateur de G est un élément de la forme
13 $xyx^{-1}y^{-1}$ où $x, y \in G$. Le groupe dérivé de G, noté $\mathcal{D}(G)$, est le sous-groupe de G engendré par les commutateurs.

Prop. 23 : 1) $\mathcal{D}(G) \triangleleft G$. $\mathcal{D}(G)$ est même stable par tout automorphisme de G (il est dit caractéristique).
2) G est abélien SSI $\mathcal{D}(G) = \{1\}$

Ex. 24 : $\mathcal{D}(S_3) = \mathcal{A}_3 = \{1, \sigma, \sigma^2\}$ où $\sigma = (1\,2\,3)$

Prop. 25 : $G/\mathcal{D}(G)$ est abélien. De plus, si $H \triangleleft G$ et G/H est abélien, alors $\mathcal{D}(G) \subset H$

III. Conjugaison dans le groupe symétrique $n \geq 2$

1) Classes de conjugaison

[Bu] **Prop. 26 :** Soit $\tau \in S_n$ et $(a_1 \dots a_k)$ un k-cycle. Alors,
209 $\tau(a_1 \dots a_k)\tau^{-1} = (\tau(a_1) \dots \tau(a_k))$, qui reste un k-cycle.

204 **Th. 27 :** Toute permutation se décompose en produit de cycles à support disjoints, et cette décomposition est unique à l'ordre des facteurs près.

~209 **Prop. 28 :** Les k-cycles sont conjugués dans S_n

Déf. 29 : Une partition de n est une suite d'entiers $(p_k)_{k \geq 1}$
211 décroissante, nulle à partir d'un certain rang telle que $\sum_{k \geq 1} p_k = n$. On note $P(n)$ l'ensemble des partitions de n.

Ex. 30 : $P(4) = \{(4), (3,1), (2,2), (2,1,1), (1,1,1,1)\}$

Déf. 31 : Soit $\sigma \in S_n$. Le type de σ est la partition de n dont les éléments non nuls sont les cardinaux des diverses σ-orbites rangés par ordre décroissant.

Ex. 32 : $\sigma = (1\,3)(4\,7\,6\,5) \in S_9$ est de type $(4,2,1,1,1)$

Th. 33 : Deux permutations sont conjuguées SSI elles ont le même type. 209 211

Ex. 34 : $\sigma = (1\,3\,5)(2\,4)$ et $\sigma' = (1\,2\,3)(6\,7)$ sont conjuguées dans S_7. 210
Si $\tau = \begin{pmatrix} 1&2&3&4&5&6&7 \\ 1&6&2&7&3&4&5 \end{pmatrix} = (2\,6\,4\,7\,5\,3)$ est telle que $\tau\sigma\tau^{-1} = \sigma'$

Coro 35 : Il y a $P(n)$ classes de conjugaison dans S_n 212

Appli 36 : Il existe 5 caractères irréductibles sur S_4. ♡

2) Applications de la conjugaison

[Bu]

Prop. 37 : Les parties suivantes sont génératrices de S_n : 212
1) les transpositions 2) $\{(1\,i), 2 \leq i \leq n\}$ 3) $\{(i\ i{+}1), 1 \leq i \leq n-1\}$

Prop. 38 : Si $n \geq 3$, alors $\mathcal{A}_n$ est engendré par : 216
1) les double transpositions 2) les 3-cycles

Lemme 39 : Si $n \geq 5$, les 3-cycles sont conjugués dans $\mathcal{A}_n$ 217

Prop. 40 : Si $n \geq 2$, $\mathcal{D}(S_n) = \mathcal{A}_n$. Si $n \geq 5$, $\mathcal{D}(\mathcal{A}_n) = \mathcal{A}_n$ [Pe] 28

Th. 41 : $\boxed{\text{Si } n \geq 3 \text{ et } n \neq 4, \text{ alors } \mathcal{A}_n \text{ est simple.}}$ DVP1

Rq 42 : Si $n = 4$, $\mathcal{D}(\mathcal{A}_4) = V_4$ où $V_4 = \{id, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ 29

Prop. 43 : Si $n \geq 3$, alors $Z(S_n) = \{id\}$ [Bu] 219

Coro 44 : Si $n \neq 4$, alors les sous-groupes distingués de S_n sont : $\{id\}$, $\mathcal{A}_n$, S_n. 220

Th. 45 : $\boxed{\text{Si } n \neq 6, \text{ alors } Aut(S_n) = Int(S_n)}$ DVP2 [Pe] 30

Rq 46 : Faux si $n = 6$: $Aut(S_n)/Int(S_n) \simeq \mathbb{Z}/2\mathbb{Z}$. 33

IV. Conjugaison dans les espaces de matrices $K = \mathbb{R}$ ou $\mathbb{C}$.

1) Généralités

Rq 47 : $M, M' \in \mathcal{M}_n(K)$ sont conjuguées s'il existe $P \in GL_n(K)$ tel que $PMP^{-1} = M'$. Elles représentent alors le même endomorphisme de K^n dans deux bases différentes.

Notation 48 : $\mathcal{D}_n(K) = \{M \in \mathcal{M}_n(K) \,/\, {}^tM = M\}$ est l'ensemble des matrices symétriques et $\mathcal{N}_n(K) = \{M \in \mathcal{M}_n(K) \,/\, M^n = 0\}$ celui des matrices nilpotentes.

Rq 49 : /!\ $\mathcal{D}_n(K)$ et $\mathcal{N}_n(K)$ ne sont pas des groupes !

[NH2G2] Prop. 50 : Le rang, le déterminant, la trace, le polynôme caractéristique et le polynôme minimal sont invariants par conjugaison.

122 Notation 51 : On notera O_M l'orbite de $M \in \mathcal{M}_n(K)$. O_M étant en bijection avec G/Stab_M, on notera $\mathcal{M}_n(K)/GL_n(K) = \{O_M, M \in \mathcal{M}_n(K)\}$.

$Sp(M)$ désigne le spectre de M où les valeurs propres sont comptées avec multiplicité. On considérera que $Sp(M) \in K^n/S_n$.

2) Action par conjugaison sur $\mathcal{D}_n(K)$

[NH2G2]

122 Th. 52 : $\varphi : \mathcal{D}_n(K)/GL_n(K) \longrightarrow K^n/S_n$ est bien définie et bijective

$$O_M \longmapsto Sp(M)$$

123 Coro 53 : Le polynôme caractéristique, le spectre sont des invariants totaux pour l'action par conjugaison de $GL_n(K)$ sur $\mathcal{D}_n(K)$.

♡ Rq 54 : Faux en général : I_2 et $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ne sont pas semblables

124 Prop. 55 : $M \in \mathcal{M}_n(\mathbb{C})$ est diagonalisable SSI O_M est fermée dans $\mathcal{M}_n(\mathbb{C})$

3) Action par conjugaison sur $\mathcal{N}_n(K)$

[Ber] adopté

976 Déf. 56 : Un bloc de Jordan de taille $r \in \mathbb{N}^*$ est $J_r = \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{pmatrix} \in \mathcal{M}_r(K)$.

977 Lemme 57 : Soit $M \in \mathcal{N}_n(K)$ d'indice de nilpotence $r \in \mathbb{N}^*$.

Alors : $\{0\} \subsetneq \mathrm{Ker}\, M \subsetneq \mathrm{Ker}\, M^2 \subsetneq \dots \subsetneq \mathrm{Ker}\, M^r = K^n$.

Th. 58 : (réduction de Jordan des matrices nilpotentes)

Soit $M \in \mathcal{N}_n(K)$. Alors M est semblable à une matrice diagonale par blocs dont chaque bloc est un bloc de Jordan, appelée réduite de Jordan de M. 978

Th. 59 : $M, M' \in \mathcal{N}_n(K)$ d'indices de nilpotence r et r' sont semblables SSI elles ont même réduite de Jordan. 980

Cela équivaut à $r = r'$ et $\dim \mathrm{Ker}\, M^i = \dim \mathrm{Ker}\, M'^i \quad \forall\, 1 \leq i \leq r$. [NH2G2] 133

Coro. 60 : Il y a $P(n)$ classes de conjugaison sur $\mathcal{N}_n(K)$.

Ex. 61 : Sur $\mathcal{N}_3(K)$, un représentant de chaque classe est ♡

$$\underset{(3)}{\begin{pmatrix} 0&0&0 \\ 0&0&0 \\ 0&0&0 \end{pmatrix}} \qquad \underset{(2\,1)}{\begin{pmatrix} 0&1&0 \\ 0&0&0 \\ 0&0&0 \end{pmatrix}} \qquad \underset{(1\,1\,1)}{\begin{pmatrix} 0&1&0 \\ 0&0&1 \\ 0&0&0 \end{pmatrix}}$$

<u>Références :</u>

- [Ber] Berhuy, *Algèbre ; le grand combat* (2ᵉ éd.)
- [Per] Perrin, *Cours d'algèbre*
- [NH2G2] Caldero, *Nouvelles...* Tome 1