103

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

Cadre : Soit G un groupe.

I) Conjugaison et groupes distingués

A] Conjugaison dans un groupe, d'un sous-groupe

Prop-déf 1 : Soit $g \in G$. $\varphi_g : x \mapsto gxg^{-1}$ est un automorphisme de groupe appelé automorphisme intérieur. Ceci définit alors une action de G sur lui-même dont les orbites sont appelées classes de conjugaison. Les éléments d'une même orbite sont dits conjugués.

[3] Ex 2 : Tout élément de G est conjugué à lui-même. Si G est abélien, les orbites sont réduites à 1 élément.

Prop-déf 3 : Soit $Z(G) = \{g \in G \mid \forall x \in G, gx = xg\}$ le centre de G. C'est un sous-groupe de G dont l'action de G sur $Z(G)$ par automorphismes intérieurs est trivial.

App 4 : Le centre d'un p-groupe non trivial est non trivial.

[4] Prop-déf 5 : Soient $H < G$ et $g \in G$. Alors $gHg^{-1} = \varphi_g(H)$ est un groupe. On dit que H et gHg^{-1} sont conjugués.

Prop 6 : Soit $G \curvearrowright X$ une action. Soient x et y dans X dans une même orbite. Alors leur stabilisateurs sont conjugués.

B] Sous-groupes distingués

Def 7 : $H < G$ est dit distingué s'il est stable par automorphismes intérieurs. On note $H \lhd G$.

Ex 8 : $\{1\}$ et G sont distingués dans G.

[5] Rem 9 : Si G est abélien, tous ses sous-groupes sont distingués.

Prop 10 : $H \lhd G \Leftrightarrow \forall x \in G, xHx^{-1} = H$

Prop 11 : Si $f : G \to G'$ est un morphisme de groupes alors $\operatorname{Ker} f \lhd G$.

Cor 12 : $Z(G) \lhd G$.

[3] Prop 13 : Soit $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ le normalisateur de H dans G. Alors $N_G(H)$ est le plus grand sous-groupe de G tel que $H \lhd N_G(H)$.

Rem 14 : $H \lhd G \Leftrightarrow N_G(H) = G$.

II) Quelques exemples d'étude

A] Groupe symétrique

Soit $n \in \mathbb{N}^*$.

Def 15 : On note S_n le groupe des bijections de $[\![1;n]\!]$ dans lui-même. Un p-cycle est un élément de S_n de la forme $(a_1 \dots a_p)$ où $\forall i$, $a_i \in [\![1;n]\!]$ sont 2 à 2 distincts. Si $\sigma \in S_n$, son support est $\operatorname{supp}(\sigma) = \{x \in [\![1;n]\!] \mid \sigma(x) \neq x\}$.

Thm 16 : Tout élément de S_n se décompose de façon unique en produit de cycles à supports disjoints.

Lem 17 : Soit $(i_1 \dots i_k)$ un k-cycle et soit $s \in S_n$. Alors $s(i_1 \dots i_k)s^{-1} = (s(i_1) \dots s(i_k))$

Thm 18 : $\forall p \in [\![1;n]\!]$, les p-cycles sont conjugués dans S_n.

Cor 19 : $\forall n \geq 5$, les 3-cycles sont conjugués dans A_n le groupe des permutations paires de S_n.

Def 20 : Soit $\sigma \in S_n$ qu'on décompose en produit de cycles à supports disjoints de longueurs $l_1 \leq l_2 \leq \dots \leq l_r$ avec $\sum_{i=1}^{r} l_i = n$. $(l_1, \dots, l_r)$ est appelé type de σ.

Cor 21 : $\sigma, \sigma' \in S_n$ sont conjugués si et seulement si ils ont même types.

App 22 : (Théorème de Brauer) Soit $\mathbb{K}$ un corps, $\operatorname{car}(\mathbb{K}) = 0$. Deux permutations sont conjuguées dans S_n si et seulement si leur matrice de permutations sont conjuguées dans $GL_n(\mathbb{K})$.

[6] Cor 23 : On a une bijection entre les classes de conjugaison de S_n et les partitions de n.

B] Groupe de matrices

Soit $k = \mathbb{R}$ ou $\mathbb{C}$.

Def 24 : Deux matrices A et B de $M_n(k)$ sont semblables si $\exists P \in GL_n(k)$, $A = PBP^{-1}$. La classe de similitude de A est l'ensemble de ses matrices semblables.

On se propose d'étudier quelques classes de similitude.

Def 25 : A est dit diagonalisable (resp. trigonalisable) si elle est semblable à une matrice diagonale (resp. triangulaire)

Thm 26 : A est diagonalisable $\iff \pi_A$ est scindé à racines simples. A est trigonalisable $\iff \pi_A$ est scindé.

[1] Ex 27 : Une matrice nilpotente non nulle n'est jamais diagonalisable, mais toujours trigonalisable.

Def 28 : A est normal si $A^*A = AA^*$ où $A^* = {}^t\bar{A}$

Ex 29 : Les matrices unitaires ou hermitiennes sont normales

Thm 30 : Si $k = \mathbb{C}$, toute matrice normale est diagonalisable dans une base orthonormée.

Si $k = \mathbb{R}$, toute matrice normale est semblable, dans une base orthonormée, à une matrice de la forme $\begin{pmatrix} D_p & & 0 \\ & R_1 & \\ 0 & & R_r \end{pmatrix}$ où $D_p \in M_p(k)$ est diagonale et R_i de la forme $\begin{pmatrix} a_i & -b_i \\ b_i & a_i \end{pmatrix}$.

Cor 31 : (Théorème spectral) Toute matrice symétrique réelle (ou hermitienne complexe) est diagonalisable dans une base orthonormée.

Cor 32 : Dans le cas orthogonal, $R_i = \begin{pmatrix} \cos(\theta_i) & -\sin(\theta_i) \\ \sin(\theta_i) & \cos(\theta_i) \end{pmatrix}$

III] Groupes quotients, groupes produits

A] Groupes quotients

Soit $H < G$.

Prop-def 33 : Les relations $g_1 R_g g_2 \iff g_2^{-1} g_1 \in H$ et $g_1 R_d g_2 \iff g_1 g_2^{-1} \in H$ sont des relations d'équivalence. Leur quotient sont notés G/H et $H\backslash G$ et l'orbite de $g_1 \in G$ g_1H et Hg_1. [1

Prop-def 34 : Si G est fini, $\mathrm{Card}(G/H) = \frac{|G|}{|H|}$. Cette quantité est appelée indice de H dans G noté $[G:H]$.

App 35 : $|H|$ divise $|G|$. (Théorème de Lagrange)

Prop 36 : Si $[G:H] = 2$ alors $H \triangleleft G$.

Ex 37 : Si k est un corps fini, $[k^* : k^{*2}] = 2$ donc $k^{*2} \triangleleft k^*$

Thm 38 : Les propriétés suivantes sont équivalentes :

① $H \triangleleft G$

② $\forall g \in G, gH = Hg$

③ Il existe une unique structure de groupe de G/H telle que $\pi : G \to G/H$ soit un morphisme de groupe.

Ex 39 : $\forall n \in \mathbb{N}^*$, $n\mathbb{Z} \triangleleft \mathbb{Z}$ donc on peut donner une structure de groupe à $\mathbb{Z}/n\mathbb{Z}$.

Thm 40 : (d'isomorphisme) Soit $\varphi : G \to G'$ un morphisme de groupes. Alors $G/\ker\varphi \simeq \mathrm{im}\,\varphi$

App 41 : Si G est le groupe des quaternions de norme 1, alors $G/\{\pm 1\} \simeq SO_3(\mathbb{R})$. [3

App 42 : $k^* \simeq GL_n(k)/SL_n(k)$

Thm 43 : Si $H \triangleleft G$, on a une bijection entre les sous-groupes de G/H et les sous-groupes de G contenant H. [4

Thm 44 : Soient $H \triangleleft G$ et $K \triangleleft G$ contenant H. Alors $(G/H)/(K/H) \simeq G/K$.

App 45 : $\forall a, b \in \mathbb{N}^*$, $(\mathbb{Z}/ab\mathbb{Z})/(a\mathbb{Z}/ab\mathbb{Z}) \simeq \mathbb{Z}/a\mathbb{Z}$.

Def 46 : G est dit simple si ses seuls sous-groupes distingués [3 sont $\{1\}$ et G.

Rem 47 : L'intérêt de trouver $H \lhd G$, H non trivial, est de ramener l'étude de G à l'étude de H et G/H, qui peut être plus simple. Dans le cas des groupes simples, ce n'est pas possible.

Ex 48 : $\mathbb{Z}/p\mathbb{Z}$ est simple si et seulement si p est premier.

Prop 49 : (DEV 1) $\forall n \geq 5$, A_n est simple.

B] Produit direct de groupes

Soient H et K deux groupes.

Def 50 : On munit $H \times K$ de la structure de groupe : $(h_1; k_1) \cdot (h_2; k_2) = (h_1h_2; k_1k_2)$ appelé produit direct.

Prop 51 : Soient $G = H \times K$ et $\hat{H} = H \times \{1\}$ et $\hat{K} = \{1\} \times K$. Alors $\hat{H} \lhd G$, $\hat{K} \lhd G$, $G = \hat{H}\hat{K}$ et $\hat{H} \cap \hat{K} = \{(1,1)\}$.

Thm 52 : Soient G un groupe et H et K deux sous-groupes tels que $G = HK$, $H \lhd G$, $K \lhd G$, $H \cap K = \{1\}$. Alors $G \simeq H \times K$.

Ex 53 : (Lemme d'isomorphisme chinois) si $p \wedge q = 1$, alors $\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

IV) Théorie des représentations

On suppose G fini.

A] Représentation d'un groupe

Def 54 : On appelle représentation de G tout couple (ρ, V) où V est un $\mathbb{C}$-espace vectoriel et $\rho : G \to GL(V)$ est un morphisme de groupe. La représentation est dite fidèle si ρ est injectif. Son noyau est $\operatorname{Ker}\rho$.

Ex 55 : Si $V = \operatorname{Vect}(e_g)_{g \in G}$, $\rho : g \mapsto (e_h \mapsto e_{gh})$ est une représentation fidèle.

Ex 56 : Si (ρ_1, V_1) et (ρ_2, V_2) sont des représentations, $(\rho_1 \oplus \rho_2, V_1 \oplus V_2)$ est une représentation où $\forall x = h_1 + h_2 \in V_1 \oplus V_2$, $\rho_1 \oplus \rho_2(x) = \rho_1(h_1) + \rho_2(h_2)$

Def 57 : Soient (ρ, V) une représentation et $W < V$. W est dit G-stable si $\forall g \in G$, $\rho(g)(W) \subset W$. (ρ, V) est dit irréductible s'il n'admet aucun sous-espace G-stable non trivial.

Thm 58 : (de Maschke) Toute représentation de G se décompose en somme directe de représentations irréductibles.

B] Caractère d'une représentation

Def 59 : On appelle caractère de (ρ, V) l'application : $\forall g \in G$, $\chi_\rho(g) = \operatorname{Tr}(\rho(g))$

Prop-def 60 : Les fonctions de $\mathbb{C}^G$ constantes sur les classes de conjugaison de G sont appelées fonctions centrales. On note $\mathcal{H}$ l'ensemble de telles applications. Alors $\chi_\rho \in \mathcal{H}$

Thm 61 : Soit le produit scalaire : $\forall \varphi, \psi \in \mathcal{H}$, $\langle \varphi | \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\varphi(g)}\psi(g)$

Alors l'ensemble des caractères irréductibles forme une base orthonormée de $\mathcal{H}$. Il y a donc autant de caractères irréductibles que de classes de conjugaison de G.

Def 62 : (ρ_1, V_1) et (ρ_2, V_2) sont isomorphes si $\exists u \in \mathcal{L}(V_1, V_2)$ bijectif tel que $\forall g \in G$, $\rho_2(g) = u \circ \rho_1(g) u^{-1}$

Cor 63 : La décomposition de Thm 58 est unique à isomorphisme près.

Cor 64 : (ρ_1, V_1) est isomorphe à $(\rho_2, V_2) \Leftrightarrow \chi_{\rho_1} = \chi_{\rho_2}$.

Thm 65 : (DEV 2) Soient $\chi_1, \dots, \chi_r$ les caractères irréductibles de G 2 à 2 distincts. Soit $H < G$. Alors $H \lhd G$ si et seulement si il existe $I \subset [\![1; r]\!]$ tel que $H = \bigcap_{i \in I} K_{\chi_i}$ où $\forall i \in [\![1; r]\!]$, $K_{\chi_i} := \{g \in G \mid \chi_i(g) = \chi_i(1)\}$.

App 66 : G est simple si et seulement si pour tout caractère irréductible χ non trivial, $\chi(g) \neq \chi(1)$ $\forall g \in G$

Références:

- Algèbre et géométrie, Rambaldi [1]
- Algèbre et géométrie, Combes [2]
- Cours d'algèbre, Perrin [3]
- Toute l'algèbre de la licence, Escofier [4]
- L'algèbre discrète de la transformée de Fourier, Peyré [5]
- Éléments d'analyse et d'algèbre, Colmez [6]