103

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

I- Notion de conjugaison : Soit G un groupe d'élément neutre e.

Déf 1 : Un groupe G agit sur un ensemble E par conjugaison si l'action est définie par : $G \times E \longrightarrow E$, $(g;x) \longmapsto gxg^{-1}$

Ex 2 : Si $H \leqslant G$, alors H agit sur G par conjugaison.

Ex 3 : $GL_n(\mathbb{R})$ agit par conjugaison sur $\mathcal{M}_n(\mathbb{R})$. De même pour $GL_n(\mathbb{C})$ sur $\mathcal{M}_n(\mathbb{C})$.

Ex 4 : Soit $\mathcal{H}(G)$ l'ensemble des sous-groupes de G. Alors G agit sur $\mathcal{H}(G)$ par conjugaison.

Déf 5 : L'action de G sur E est transitive si $\forall (x,y) \in E^2$, $\exists g \in G$ tq $g \cdot x = y$.

Ex 6 : $SO_3(\mathbb{R})$ agit transitivement sur l'ensemble des droites de $\mathbb{R}^3$.

Déf 7 : Soit $x \in E$. Si G agit sur E par conjugaison, alors l'orbite de x $O_x = \{gxg^{-1} \mid g \in G\}$ est appelée classe de conjugaison de x. Deux éléments $x, y \in E$ sont conjugués si $\exists g \in G$ tq $y = gxg^{-1}$, i.e : si $O_x = O_y$.

Ex 8 : Les renversements sont conjugués dans $SO_3(\mathbb{R})$.

Ex 9 : Les cycles d'ordre p sont conjugués dans S_n.

Ex 10 : Les transvections sont conjuguées dans $GL(E)$.

Ex 11 : Si G est un groupe d'ordre $p^n s$ (p premier, $n \in \mathbb{N}^*$, $p \nmid s$), alors tous les p-Sylows de G sont conjugués dans G.

Déf 12 : Un morphisme $G \longrightarrow G$ est un automorphisme de G s'il est bijectif. On note $Aut(G)$ l'ensemble des automorphismes de G.

Déf 13 : Soit $g \in G$. On appelle automorphisme intérieur associé à g l'automorphisme $G \longrightarrow G$, $x \longmapsto gxg^{-1}$. On note $Int(G)$ l'ensemble des automorphismes intérieurs de G.

App 14 : Soit $n \in \mathbb{N}^*$, $n \neq 6$. Alors les automorphismes de S_n sont intérieurs. DEV 1

Prop 15 : Soit G un groupe. Si $Aut(G) = \{id\}$, alors $G = \{e\}$ ou $G = \mathbb{F}_2$.

Rque 16 : $\forall g, h \in G$, hgh^{-1} a la même nature géométrique que g. Par exemple, dans $SO_3(\mathbb{R})$: si $R_D \in SO_3(\mathbb{R})$ est un renversement d'axe la droite D, alors hR_Dh^{-1} est un renversement d'axe $h(D)$: $hR_Dh^{-1} = R_{h(D)}$.

Ex 17 : Dans le groupe diédral D_{2n}, soit r une rotation et s une symétrie. Alors $\forall k \in \mathbb{N}^*$, $sr^ks^{-1} = r^{-k}$: le conjugué de r^k par s reste une rotation.

II- Sous-groupes normaux :

Déf 18 : Soit $H \leqslant G$. On dit que H est un sous-groupe distingué (ou normal) de G si $\forall h \in H, \forall g \in G$, $ghg^{-1} \in H$. On note alors $H \triangleleft G$.

Ex 19 : $G \triangleleft G$ et $\{e\} \triangleleft G$.

Ex 20 : Soit $Z(G) = \{x \in G \mid \forall g \in G, xg = gx\}$ le centre de G. Alors $Z(G) \triangleleft G$.

Prop 21 : Soit $f : G \longrightarrow K$ un morphisme de groupes. Alors $\ker(f) \triangleleft G$.

Ex 22 : $A_n \triangleleft S_n$, $\forall n \in \mathbb{N}^*$ car $A_n = \ker(\varepsilon)$.

Ex 23 : $\forall n \in \mathbb{N}^*$, $n\mathbb{Z} \triangleleft \mathbb{Z}$.

Ex 24 : Soit E un espace vectoriel de dimension finie sur un corps commutatif. Alors $SL(E) \triangleleft GL(E)$.

Prop 25 : Si G est abélien, alors tout sous-groupe de G est distingué dans G.

Rque 26 : La réciproque est fausse !

DEV 2

Prop 27 : Si $H \lhd G$, $K \lhd G$ et $H \leq K$, alors $H \lhd K$.

Rque 28 : Si $H \lhd K$ et $K \lhd G$, on n'a pas forcément $H \lhd G$.

Prop 29 : Soit $H \lhd G$, $K \lhd G$. Alors $H \cap K \lhd K$; $HK \lhd G$; et $H \lhd HK$.

Déf 30 : Un groupe G est simple s'il ne possède pas de sous-groupes distingués non-triviaux :
$\forall H \leq G,\ H \lhd G \Longrightarrow H = \{e\}$ ou $H = G$.

Ex 31 : Si p est premier, alors $\mathbb{Z}/p\mathbb{Z}$ est simple.

Ex 32 : $\forall n \geq 5$, A_n est simple.

Ex 33 : $SO_3(\mathbb{R})$ est simple.

Ex 34 : Si K est un corps, $\forall n \geq 2$, $PSL_n(K)$ est simple, sauf $PSL_2(\mathbb{F}_2)$ et $PSL_2(\mathbb{F}_3)$.

Déf 35 : Soient $x, y \in G$. On note $[x,y] = xyx^{-1}y^{-1}$ le commutateur de x et de y.

Déf 36 : Soit $D(G) = \{[x,y],\ x,y \in G\}$. $D(G)$ est appelé groupe dérivé de G.

Prop 37 : $D(G) \lhd G$.

III - Groupes quotients

Déf 38 : Soient $x, y \in G$. On appelle classe à droite (resp. à gauche) modulo H la classe d'équivalence de la relation $xy^{-1} \in H$ (resp. $x^{-1}y \in H$). On note $(G/H)_d$ (resp. $(G/H)_g$) l'ensemble des classes à droite (resp. à gauche).

Thm 39 : Soit $H \leq G$. Alors $H \lhd G$ si et seulement si G/H peut être muni d'une structure de groupe telle que la surjection canonique $\begin{array}{ccc} G & \longrightarrow & G/H \\ g & \longmapsto & gH \end{array}$ soit un morphisme de groupes.

Déf 40 : On note $[G:H] = \mathrm{Card}((G/H)_d) = \mathrm{Card}((G/H)_g)$ l'indice de H dans G.

Thm 41 : (Lagrange) : Si $H \leq G$, alors : $\mathrm{Card}(G) = [G:H]\,\mathrm{Card}(H)$. En particulier : $\mathrm{Card}(H)$ divise $\mathrm{Card}(G)$.

Prop 42 : Soit $H \leq G$. Alors $[G:H] = 2 \Longrightarrow H \lhd G$.

Thm 43 : Soit $f : G \longrightarrow K$ un morphisme de groupes. Alors $G/\ker(f) \simeq \mathrm{Im}(f)$.

Thm 44 : Soient $H \lhd G$ et $K \leq G$. Alors $K/H \cap K \simeq HK/H$.

Thm 45 : Soient $H, K \lhd G$, $H \subset K$. Alors $G/K \simeq (G/H)/(K/H)$.

Thm 46 : Soit $H \lhd G$. Alors il y a une bijection entre l'ensemble des sous-groupes de G contenant H, et l'ensemble des sous-groupes de G/H ; et cette bijection préserve les sous-groupes distingués.

Coro 47 : Comme contre-exemple de la Prop 25 et la Rque 26, on montre que tout sous-groupe de $\mathbb{H}_8$ est distingué dans $\mathbb{H}_8$. Pourtant, $\mathbb{H}_8$ n'est pas abélien.

Thm 48 : Soit $c : \begin{array}{ccc} G & \longrightarrow & \mathrm{Int}(G) \\ g & \longmapsto & \left(\begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & gxg^{-1} \end{array}\right) \end{array}$.
Alors c est un morphisme de groupes, et $\ker(c) = Z(G)$. On a donc $G/Z(G) \simeq \mathrm{Int}(G)$. De plus, on a $\mathrm{Int}(G) \lhd \mathrm{Aut}(G)$.

App 49 : On a $S^1 \simeq \mathbb{R}/\mathbb{Z}$.

App 50 : Lemme chinois : Soient $n, m \in \mathbb{N}^*$.
$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/nm\mathbb{Z} \iff \mathrm{pgcd}(n,m) = 1$.

App 51 : Thm de structure des groupes abéliens finis :
Soit G un groupe abélien fini. Alors il existe un unique $l \in \mathbb{N}$, et des uniques $q_1, \dots, q_t$ puissances de nombres premiers telles que :

$$G \simeq \mathbb{Z}/q_1\mathbb{Z} \times \mathbb{Z}/q_2\mathbb{Z} \times \dots \times \mathbb{Z}/q_t\mathbb{Z} \times \mathbb{Z}^l.$$

DEV ① : Soit $n \in \mathbb{N}^*$, $n \neq 6$. Alors les automorphismes de S_n sont intérieurs.

DEV ② : $SO_3(\mathbb{R})$ est simple.

Autre développement possible : simplicité de A_n, $n \geqslant 5$.

Références :

- Perrin, Cours d'Algèbre
- Francinou, Gianella, Nicolas, Oraux X-ENS Algèbre 3
- Lelong-Ferrand, Arnaudiès, Algèbre