103

Exemples de sous-groupes distingués et de groupes quotients. Applications.

Cadre : G est un groupe, $H \leq G$, $\mathbb{K}$ un corps.

I] Outils, premières propriétés

1. Sous-groupe distingué

Déf. 1 : H est distingué dans G s'il est stable par automorphisme intérieur, ie si $\forall g \in G$, $ghg^{-1} \in H$. On note $H \triangleleft G$.

Rem. 2 : Les sous-groupes triviaux $\{e\}$ et G sont toujours distingués.

Prop. 3 : Tout sous-groupe d'indice 2 est distingué.

Prop. 4 : Dans un groupe abélien, tout sous-groupe est distingué.

Prop. 5 : Si $\varphi : G \to G'$ est un morphisme, on a $\ker \varphi \triangleleft G$; et si $H \triangleleft G$, alors $\varphi(H) \triangleleft G'$.

Déf. 6 : Un groupe $G \neq \{e\}$ est simple si ses seuls sous-groupes distingués sont $\{e\}$ et G.

2. Groupe quotient

Déf. 7 : Si $H \triangleleft G$, l'ensemble G/H est muni d'une structure de groupe avec la loi de composition quotient $(gH).(g'H) = (gg'H)$. On appelle G/H le groupe quotient de G par H.

Prop. 8 : La projection canonique $p : G \to G/H$ est un morphisme surjectif de noyau H. De plus, si G est fini, on a $|G| = |G/H| . |H|$.

Th. 9 : Si $H \triangleleft G$, $p : G \to G/H$ et $f : G \to G'$ morphisme tel que $H \subseteq \ker f$, alors il existe un unique morphisme $\varphi : G/H \to G'$ tel que $\varphi \circ p = f$.

Th. 10 : Soit $\varphi : G \to G'$ un morphisme. Alors $G/\ker \varphi \simeq \mathrm{Im}\, \varphi$.

3. Premiers exemples de sous-groupes distingués naturels

Déf. 11 : On appelle centre de G et on note $Z(G)$ l'ensemble des éléments qui commutent avec tous les autres : $Z(G) = \{g \in G / \forall h \in G, hg = gh\}$.

Rem. 12 : G est abélien ssi $Z(G) = G$.

Prop. 13 : On a $Z(G) \triangleleft G$.

Déf. 14 : On appelle groupe dérivé et on note $D(G)$ le sous-groupe engendré par les commutateurs de G : $D(G) = \langle xyx^{-1}y^{-1}, x, y \in G \rangle$.

Rem. 15 : G est abélien ssi $D(G) = \{1\}$.

Prop. 16 : $D(G) \triangleleft G$.

Prop. 17 : $G/D(G)$ est abélien ; c'est le plus grand quotient abélien de G.

4. Produit direct

Déf. 18 : L'ensemble $G \times G' = \{(g, g'), g \in G, g' \in G'\}$ est muni d'une structure de groupe avec la loi de composition interne $(g_1, g_1') \times (g_2, g_2') \mapsto (g_1 g_2, g_1' g_2')$, et est appelé groupe produit direct de G et G'.

Th. 19 : Soient $H \triangleleft G$ et $K \triangleleft G$ avec $H \cap K = \{e\}$ et $HK = G$. Alors on a $G \simeq H \times K$.

App. 20 : (Théorème chinois.) $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/nm\mathbb{Z} \iff n \wedge m = 1$.

5. Sous-groupes distingués et table de caractères

Déf. 21 : Le noyau d'une représentation ρ est $K_\chi := \{x \in G / \chi(x) = \chi(1)\}$. C'est un sous-groupe distingué de G.

Th. 22 : Soit $\{\rho_1, \dots, \rho_r\}$ un système de représentants des classes d'isomorphies des représentations de G. Soient $\chi_1, \dots, \chi_r$ les caractères associés. Alors les sous-groupes distingués de G sont exactement de la forme $\bigcap_{i \in I} K_{\chi_i}$ où $I \subset \{1, \dots, r\}$.

II] Le cas du groupe linéaire

1. Étude de $GL_n(\mathbb{K})$

Déf. 23 : On appelle $SL_n(\mathbb{K})$ le sous-groupe de $GL_n(\mathbb{K})$ des matrices de déterminant 1 : $SL_n(\mathbb{K}) = \{A \in GL_n(\mathbb{K}) / \det(A) = 1\}$.

Prop. 24 : Dans $GL_n(\mathbb{K})$, toutes les transvections sont conjuguées.

Prop. 24 bis : On a $SL_n(\mathbb{K}) \triangleleft GL_n(\mathbb{K})$.

Prop. 25 : • $Z(GL_n(\mathbb{K})) = \{\lambda I_d, \lambda \in \mathbb{K}^*\}$.

• $Z(SL_n(\mathbb{K})) = \{\lambda I_d, \lambda^n = 1\}$.

Prop. 25 bis : Pour $n \geq 3$, $D(GL_n(\mathbb{K})) = D(SL_n(\mathbb{K})) = SL_n(\mathbb{K})$.

Déf. 26 : Le quotient de $SL_n(\mathbb{K})$ par son centre est appelé groupe projectif spécial linéaire et est noté $PSL_n(\mathbb{K})$.
Th. 26bis : Le groupe $PSL_n(\mathbb{K})$ est simple, sauf pour $(n,\mathbb{K})=(2,\mathbb{F}_2)$ ou $(2,\mathbb{F}_3)$.

2. Le groupe orthogonal

Déf. 27 : Le groupe orthogonal est $O_n(\mathbb{R})=\{A\in GL_n(\mathbb{K}) \,/\, {}^tA=A^{-1}\}$.
On appelle $SO_n(\mathbb{R})$ le sous-groupe de $O_n(\mathbb{R})$ des matrices de déterminant 1 : $SO_n(\mathbb{R})=\{A\in O_n(\mathbb{R}) \,/\, \det(A)=1\}$.

Prop. 28 : On a $SO_n(\mathbb{R}) \lhd O_n(\mathbb{R})$.

Prop. 29 : • $Z(O_n(\mathbb{R}))=\{-Id, Id\}$
• $Z(SO_n(\mathbb{R}))=\{Id\}$ si n impair, $\{-Id, Id\}$ si n pair.

Th. 30 : Le groupe $SO_3(\mathbb{R})$ est simple.

Prop. 31 : • $D(O_n(\mathbb{R}))=SO_n(\mathbb{R})$. DEV①
• $D(SO_n(\mathbb{R}))=SO_n(\mathbb{R})$.

III] Les groupes finis   Soit G fini.

1. Groupes abéliens finis

Th. 32 : Soit G abélien fini, $G\neq\{e\}$. Alors il existe des entiers $1<d_1 | d_2 | \dots | d_r$ tels que $G\simeq \mathbb{Z}/d_1\mathbb{Z}\times\dots\times\mathbb{Z}/d_r\mathbb{Z}$.
Les d_i sont uniques et sont appelés facteurs invariants de G.

Prop. 33 : $n\in\mathbb{N}^*$ Alors $n\mathbb{Z}\lhd\mathbb{Z}$.

Prop. 34 : Le quotient $\mathbb{Z}/n\mathbb{Z}$ est ainsi un groupe.

Cor. 35 : Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont les $k\mathbb{Z}/n\mathbb{Z}$ où $k|n$.

Prop. 36 : Les seuls groupes abéliens simples sont les groupes cycliques d'ordre premier.
Ex. : $\mathbb{Z}/p\mathbb{Z}$ est simple ssi p est premier.

2. Le groupe diédral

Déf. 37 : Pour $n\geq 2$, on note P_n un polygone régulier à n sommets, dans le plan $\mathbb{R}^2$. On appelle groupe diédral et on note $\mathbb{D}_n$ l'ensemble des isométries du plan qui conservent P_n.

Prop. 38 : $\mathbb{D}_n$ est engendré par la symétrie axiale s et la rotation d'angle $\frac{2\pi}{n}$ r : $\mathbb{D}_n=\{e,r,r^2,\dots,r^{n-1},s,rs,r^2s,\dots,r^{n-1}s\}$.

Prop. 39 : On a $\langle r\rangle \lhd \mathbb{D}_n$.

Prop. 40 : • Si n est impair, on a $Z(\mathbb{D}_n)=\{e\}$.
• Si n est pair ie $n=2k$, on a $Z(\mathbb{D}_n)=\{e, r^k\}$.

Cor. 41 : • Si $n=2k$, on a $\mathbb{D}_{2k}/Z(\mathbb{D}_{2k})\simeq\mathbb{D}_k$.
• Si $n=2k+1$, on a $\mathbb{D}_{2k+1}/Z(\mathbb{D}_{2k+1})\simeq\mathbb{D}_{2k+1}$.

Prop. 42 : • Si n est impair, $D(\mathbb{D}_n)=\langle r\rangle$.
• Si n est pair, $D(\mathbb{D}_n)=\langle r^2\rangle$.

3. Théorèmes de Sylow

Déf. 43 : • G est un p-groupe si $|G|=p^n$ où p est premier.
• Si $|G|=sp^n$, où $p\nmid s$ est premier, alors tout sous-groupe d'ordre p^n de G est appelé p-sous-groupe de Sylow.

Th. 44 : (Théorèmes de Sylow.) Soit $|G|=mp^n$, p premier.
• G contient au moins un p-sous-groupe de Sylow.
• Les p-Sylow sont tous conjugués et leur nombre n_p divise $|G|$.
• $n_p\equiv 1\ [p]$, ie $n_p | m$.

Cor. 45 : $S\lhd G$ ssi S est l'unique p-Sylow de G.

App. 46 : A_5 est le seul groupe simple d'ordre 60 à isomorphisme près.

Ex. 47 : Un groupe d'ordre 63 n'est pas simple. DEV②

IV] Le groupe symétrique

Déf. 48 : On appelle groupe symétrique et on note S_n le groupe des permutations de l'ensemble $\{1, 2, \dots, n\}$.

Déf. 49 : On appelle groupe alterné et on note A_n le noyau du morphisme signature $\varepsilon : S_n \to \{-1, 1\}$.

Prop. 50 : On a $A_n \triangleleft S_n$.

Cor. 51 : Le quotient (S_n / A_n) est ainsi un groupe.

Prop. 52 : Pour $n \neq 4$, le groupe A_n est simple.

Cor. 53 : Les sous-groupes distingués de S_n sont $\{1\}$, A_n et S_n pour $n \geq 5$.

Prop. 54 : Le sous-groupe de A_4 engendré par les double-transpositions est distingué dans A_4.

Prop. 55 : On a $\mathrm{Int}(S_n) \triangleleft \mathrm{Aut}(S_n)$ où $\mathrm{Int}(S_n)$ désigne l'ensemble des morphismes intérieurs.

Centre et groupe dérivé

Prop. 56 : • On a $Z(S_n) = \{1\}$.

• On a $Z(A_n) = \{1\}$, pour $n \geq 4$, et $Z(A_3) = A_3$.

Prop. 57 : On a $D(S_n) = A_n$.

Prop. 58 : • Pour $n \geq 5$, on a $D(A_n) = A_n$.

• Sinon, $D(A_3) = \{e\}$ et $D(A_4) = \langle \text{double-transpositions} \rangle$.

Références :

- Calais
- Ulmer
- Perrin
- Delcourt, Théorie des groupes
- Peyré : I]5.

Développements :

① Nouvelles Histoires Hédonistes de Groupes et Géométries II (NH2G2 II)

② Szpirglas, Algèbre L3