103 : Exemples et applications des notions de sous-groupes distingués et groupes quotients

0. Notations et rappels

[PER]

- S_n : groupe des permutations à n éléments.
- $GL_n(\mathbb{K})$, $SL_n(\mathbb{K})$: groupes linéaire et spécial linéaire de $\mathbb{K}$ ($\mathbb{K}$ un corps)
- $O_n(\mathbb{K})$: groupe des matrices orthogonales
- $SO_n(\mathbb{K})$: groupe spécial orthogonal.
- $Aut(G)$: groupe des automorphismes de G (G groupe)
- $Int(G)$: groupe des automorphismes intérieurs de G
- $Isom(E)$: groupe des isométries de E (E espace affine)
- D_n : groupe des isométries du polygone régulier à n sommets
- $H_8 = \{\pm 1, \pm i, \pm j, \pm k\}$: groupe des quaternions défini par : $i^2 = j^2 = k^2 = -1$; $ij = -ji = k$; $jk = -kj = i$; $ki = -ik = j$
- G est un groupe, H un sous-groupe de G.

RAPPELS :

- G un groupe, X un ensemble. G opère sur X si on a :
$$G \times X \longrightarrow X, \quad (g,x) \mapsto g.x$$
vérifiant : $\forall g, g' \in G, \forall x \in X\ g(g'.x) = (gg').x$; $\forall x \in X,\ 1.x = x$
- $H_x = \{g \in G \mid g.x = x\}$, $x \in X$ et G opérant sur X, est le stabilisateur de x.

I - Simplifier des groupes

1) Sous-groupes distingués, groupes quotients

DEF : On dit que H est distingué dans G si on a :
$$\forall a \in G, \forall h \in H,\ aha^{-1} \in H.$$
On note $H \triangleleft G$. [PER]

PROP : $H \triangleleft G$ ssi il existe un groupe G' et un morphisme $f : G \to G'$ tel que $H = \mathrm{Ker} f$. [CA]

EX :
- $\{1\}$ et G sont des sous-groupes distingués de G. [PER]
- Si G est abélien, tout sous-groupe de G est distingué.
- $\varepsilon : S_n \longrightarrow \{-1,1\}$ signature. $A_n = \mathrm{Ker}\, \varepsilon$ donc $A_n \triangleleft S_n$
- $\det : GL_n(\mathbb{K}) \to \mathbb{K}^*$. $SL_n(\mathbb{K}) = \mathrm{Ker}(\det)$ donc $SL_n(\mathbb{K}) \triangleleft GL_n(\mathbb{K})$

DEF-THM : Soit $H \triangleleft G$. Alors G/H peut être muni d'une structure de groupe telle que la surjection canonique
$$p : G \longrightarrow G/H, \quad x \mapsto \bar{x}$$
soit un morphisme.

G/H est alors appelé groupe quotient de G par H. [MAD]

EX :
- $n\mathbb{Z} \triangleleft \mathbb{Z}$, $\forall n \in \mathbb{N}$ $\Rightarrow$ $\mathbb{Z}/n\mathbb{Z}$ groupe
- $\mathbb{Z} \triangleleft (\mathbb{R}, +)$ $\Rightarrow$ $\mathbb{R}/\mathbb{Z} \simeq \bigcirc$ est un groupe.

PROP : Si $[G : H] = 2$, alors H est distingué dans G. [CA]

EX :
- E espace vectoriel euclidien, $SO(E) \triangleleft O(E)$.
- $\Gamma_n = \{rot(O, \frac{2k\pi}{n}) \mid k \in [\![0, n-1]\!]\}$ distingué dans D_n

THM (Frobenius) : Soit G un groupe fini, p le plus petit diviseur premier de $|G|$. Alors tout sous-groupe de G d'indice p est distingué dans G. [EN8]

2) Les théorèmes d'isomorphisme

THM (1er thm d'isom) : Soit G' un groupe et $f : G \to G'$ un morphisme, alors $G/\mathrm{Ker} f \simeq \mathrm{Im} f$ [MAD]

EX : $S_n/A_n \simeq \mathbb{Z}/2\mathbb{Z}$; $GL_n(\mathbb{K})/SL_n(\mathbb{K}) \simeq \mathbb{K}^*$

APP :
- Tout groupe monogène infini est isomorphe à $(\mathbb{Z}, +)$.
- Tout groupe cyclique d'ordre $n \in \mathbb{N}^*$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$. [MAD]

THM (2ème thm d'isom). Soient $H_1 \lhd G$ et H_2 sous-groupe de G.
Alors : (i) $H_1 \cap H_2 \lhd H_2$
(ii) H_1H_2 est un sous-groupe de G, et $H_1 \lhd H_1H_2$
(iii) $H_2/H_1 \cap H_2 \simeq H_1H_2/H_1$ [MAD].

THM (3ème thm d'isom.). Soient H_1, H_2 sous-groupes de G tels que $H_1 \subset H_2$, $H_1 \lhd G$, $H_2 \lhd G$, alors :
(i) $H_2/H_1 \lhd G/H_1$ (ii) $G/H_2 \simeq (G/H_1)/(H_2/H_1)$ [MAD]

3) Simplicité

DEF. Un groupe $G \neq \{1\}$ est dit simple si ses seuls sous-groupes distingués sont $\{1\}$ et lui-même.

Ex : . $\mathbb{Z}/p\mathbb{Z}$ est simple ssi p premier.
. A_n est simple pour $n \geq 5$ (DELPITT) [PER]
. SO_3 est simple. (DUCPITT)

APP. Dévissage des groupes [PER]
L'intérêt des sous-groupes distingués est de permettre le dévissage des groupes : si $H \lhd G$, on peut ramener l'étude de G à celle de H et G/H. Les groupes simples ont l'avantage d'être indévissable.

II - Sous-groupes distingués particuliers

1) Le centre.

DEF. Le centre de G est le sous-groupe de G
$$Z(G) = \{a \in G \mid \forall g \in G,\ ag = ga\}$$
PROP. $Z(G) \lhd G$ [PER]

Ex. . Si G est commutatif, $Z(G) = G$.
. $Z(S_n) = \{1\}$ si $n \geq 3$.
. $Z(H_8) = \{-1; 1\}$.
. $GL_n(\mathbb{K})/Z(GL_n(\mathbb{K})) = PGL_n(\mathbb{K})$ groupe projectif linéaire
. Si n est impair, $Z(D_n) = \{1\}$; si n est pair, $|Z(D_n)| = 2$, ($n \geq 3$)
si $n = 2k$, $k \geq 2$, $D_{2k}/Z(D_{2k}) \simeq D_k$ [CA]

APP. Si le groupe $G/Z(G)$ est monogène, alors G est abélien [MAD]

2) Le groupe dérivé

DEF. Le groupe dérivé $D(G)$ est le sous-groupe engendré par les commutateurs de G (éléments de la forme $xyx^{-1}y^{-1}$).

PROP. $D(G) \lhd G$. [PER].

Ex. . Si G commutatif, $D(G) = \{1\}$
. Si $G = S_3$, $D(G) = \{1, \sigma, \sigma^2\}$; $D(S_n) = A_n$, $\forall n \geq 2$
. $D(H_8) = \{-1; 1\}$; $D(A_5) = A_5$.
. $D(PGL_n(\mathbb{K})) = PSL_n(\mathbb{K})$ groupe projectif spécial linéaire (pour $n \geq 2$ et $\mathbb{K} \neq \mathbb{F}_2$). [OA]

APP. Si $H \lhd G$, alors G/H abélien ssi $D(G) \subset H$.
En particulier, $G/D(G)$ est abélien. [MAD]

3) Théorèmes de Sylow

DEF. Soit G groupe fini de cardinal n et p diviseur premier de n. Si $n = p^\alpha m$ avec $p \nmid m$, on appelle p-sous-groupe de Sylow de G un sous-groupe de cardinal p^α. [PER]

THM (1er Sylow). G groupe fini et p diviseur premier de $|G|$.
Alors G contient au moins un p-sous-groupe de Sylow.

THM (2nd Sylow). Soit G groupe, $|G| = p^\alpha m$, $p \nmid m$, p premier [PER]
(i) Si H est un p-sous-groupe de G, alors il existe un p-Sylow S de G tel que $H \subset S$.
(ii) Les p-Sylow sont tous conjugués.
(iii) Le nombre de p-Sylow est congru à 1 modulo p, et divise $|G|$.

COR: Si S est un p-Sylow de G, on a [PER]
$$S \lhd G \Leftrightarrow S \text{ est l'unique } p\text{-Sylow de } G$$

APP: Un groupe d'ordre 255 n'est pas simple.

APP. PROP: G groupe fini d'ordre pq, où p et q premiers distincts, et q non congru à 1 modulo p, alors G n'a qu'un seul p-sous-groupe de Sylow (et est donc distingué). [GHT]

APP: Prop: G groupe fini d'ordre pq, p et q premiers distincts, alors G n'est pas simple.

APP: Tout groupe simple d'ordre 60 est isomorphe à A_5 [OR]

III - Classification des groupes.

DEF: · Si N et H sont deux groupes, alors l'ensemble $N \times H$ muni de la loi $(n,h)(n',h') = (nn', hh')$ est un groupe, appelé produit direct de N et H.

· Si N et H sont deux groupes, $\varphi : H \to Aut(N)$ morphisme alors $N \times H$ muni de la loi $(n,h) *_\varphi (n',h') = (n\varphi(h)(n'), hh')$ est un groupe, appelé produit semi-direct de N et H, noté $N \rtimes_\varphi H$.

Notation: On notera $\varphi(h)(n) = h.n$. [AL]

PROP: $N \rtimes_\varphi H$ est abélien ssi φ est triviale et N et H sont abéliens.

PROP: $\overline{N} = \{(n,1), n \in N\}$, $\overline{H} = \{(1,h), h \in H\}$ sont des sous-groupes de $N \rtimes_\varphi H$, isomorphes à N et H, vérifiant $\overline{N} \cap \overline{H} = \{(1,1)\}$, $\overline{N} \lhd N \rtimes_\varphi H$ et $N \times H = \overline{N}\,\overline{H} = \overline{H}\,\overline{N}$

PROP: Soient N et H deux sous-groupes de G avec $N \lhd G$ [PER] $N \cap H = \{1\}$ et $G = NH$, alors on a $G \simeq N \rtimes_\varphi H$, $\varphi : \begin{array}{l} H \to Aut\, N \\ h \mapsto (n \mapsto hnh^{-1}) \end{array}$

DEF: Soit $f : G \to H$ morphisme, $\overline{H}$ sous-groupe de G est dit un relèvement de H si la restriction de f à $\overline{H}$ est un isomorphisme de $\overline{H}$ sur H. Autrement dit, f possède une section, càd il existe $s : H \to G$ tel que $f \circ s = Id_H$. [PER]

DEF: Soient N, G, H des groupes, i, p des morphismes. Alors
$$1 \to N \xrightarrow{i} G \xrightarrow{p} H \to 1$$
est une suite exacte si i est injectif, p est surjectif et $\operatorname{Im} i = \operatorname{Ker} p$.

THM: Si on a une suite exacte $1 \to N \xrightarrow{i} G \xrightarrow{p} H \to 1$, et s'il existe un relèvement $\overline{H}$ de H, alors $G \simeq N \rtimes H$.

Ex: $\{id\} \to A_n \xrightarrow{i} S_n \xrightarrow{\varepsilon} \{-1;1\} \to \{1\}$ est une suite exacte. En choisissant $\tau \in S_n$ une transposition, on a que $\{id, \tau\}$ est un relèvement de $\{-1,1\}$, et donc $S_n \simeq A_n \rtimes \mathbb{Z}/2\mathbb{Z}$ [AL]

APP: Classification des groupes d'ordre 8 (DULPITT)

Ex: $D_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$

IV - Application en géométrie

$\mathcal{T} = \{$translations d'un espace affine $\mathcal{E}\}$, $\mathcal{T} \lhd Isom(\mathcal{E})$ [CO]

G_A stabilisateur de A par l'action de $Isom(\mathcal{E})$ sur $\mathcal{E}$.

$G_A \cap \mathcal{T} = \{id\}$ et $Isom\, \mathcal{E} = \mathcal{T} G_A$.

THM: $Isom\, \mathcal{E} \simeq \mathcal{T} \rtimes G_A \simeq E \rtimes GL(E)$

PROP: E un espace vectoriel sur un corps K, $\mathcal{E}$ espace affine sur E, $H = \{f \in Aut(\mathcal{E}) \mid \exists \lambda \in K_*, \vec{f} = \lambda Id_E\}$.
Alors (i) $H \lhd Aut\, \mathcal{E}$ (ii) $\mathcal{T} \lhd H$
(iii) $H_A = \{$homothéties de centre $A\}$, $\forall A \in \mathcal{E}$, sous-groupe de H, deux à deux conjugués H_B.
(iv) H est réunion de $\mathcal{T}$ et des sous-groupes H_A, $A \in \mathcal{E}$.
(v) $H \simeq E \rtimes_\alpha K_*$, $\alpha : \begin{array}{l} K_* \to E \\ (\lambda, \vec{x}) \mapsto \lambda\vec{x} \end{array}$

Références:
[PER] Perrin, Cours d'algèbre
[MAD] Madère, Leçons d'algèbre
[CA] Calais, Eléments de th. des gp.
[OR] Ortiz, Exercices d'algèbre
[GUI] Guin, Algèbre
[AL] Alessandri, Thèmes de géométrie
[CO] Combes, Algèbre et géométrie
[ENS] Francinou, Oraux X-ENS