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

Cadre : $(G,\cdot,e)$ un groupe, $H \subseteq G$ un sous-groupe de $G$.

# I] Généralités

## 1) Notion de classe [PER]p9

**déf :** Classe à gauche de $a \in G$ relativement à $H$ :
$aH := \{g \in G \,/\, \exists h \in H, / \, g = ah\}$.
(idem classes à droite) Notation : $G/H$ ensemble des classes.

**déf :** Indice de $H$ dans $G$ : $(G:H) = |G/H|$.

**THM** [LAGRANGE] Si $G$ est fini, $|G| = |H| \times (G:H)$. [CAL]p75

APP $G$ fini, $\forall x \in G$, l'ordre de $x$ divise $|G|$.

## 2) Sous-groupes distingués

**déf/prop :** $g \in G$, $\sigma_g : \begin{cases} G \to G \\ h \mapsto ghg^{-1} \end{cases}$ est un automorphisme de $G$, appelé automorphisme interne. On note $Int(G) = \{\sigma_g \,|\, g \in G\}$

**déf :** $H$ est distingué dans $G$, noté $H \lhd G$, [CAL]141
si $\forall \sigma_g \in Int(G)$, $\sigma_g(H) = H$. [PER]11

**ex :** – $\{e\}$, $G$ sont distingués dans $G$.
– $Int(G) \lhd Aut(G) := \{$automorphismes de $G\}$ [CAL]143
– Dans un groupe abélien, tout sous-groupe est distingué (Réciproque fausse : quaternions)
– contre-exemple : $GL_n(\mathbb{Z}) \ntriangleleft GL_n(\mathbb{R})$ [OA] 234

**prop :** Les assertions suivantes sont équivalentes :
(i) $H \lhd G$. (ii) $\forall g \in G, \forall h \in H$, $ghg^{-1} \in H$. [CAL]140
(iii) $\forall g \in G$, $gH = Hg$.

APP. Tout sous-groupe d'indice 2 est distingué [CAL]143
**ex :** $\langle r \rangle \lhd D_n$, $r$ rotation d'angle $\frac{2\pi}{n}$.

**THM :** Si $G$ est fini. Soit $p$ le plus petit diviseur premier de $|G|$. Alors tout sous-groupe de $G$ d'indice $p$ est distingué dans $G$. [Thm de Frobenius] [XENS1]52

## 3) Groupes quotients

**déf/prop :** Si $G \rhd H$, l'ensemble $G/H$ peut être muni d'une structure de groupe via $(xH)(x'H) = (xx')H$ et est appelé groupe quotient de $G$ par $H$. [PER]p11
$\pi : \begin{matrix} G \to G/H \\ g \mapsto gH \end{matrix}$ est alors un morphisme surjectif de noyau $H$.

**ex :** $\mathbb{Z} \lhd (\mathbb{R},+)$ donc $\mathbb{R}/\mathbb{Z} \simeq \mathbb{O}$ groupe.

APP. $H \lhd G \iff H$ est le noyau d'un morphisme de groupes. [PER]

**ex :** – $SL_n(K) \lhd GL_n(K)$, $SL_n(K) = \ker(\det)$
– $A_n \lhd S_n$, $A_n = \ker(\varepsilon)$, $\varepsilon$ signature

**prop :** (Correspondance des sous-groupes) Si $H \lhd G$, [CAL]150-2
$\{K$ sous-gpe de $G \,/\, H \subseteq K\}$ $\underset{\beta}{\overset{\alpha}{\rightleftarrows}}$ $\{$sous-groupes de $G/H\}$
$K \mapsto \pi(K)$
$\pi^{-1}(J) \leftarrow J$

$\alpha$ et $\beta$ sont des bijections réciproques qui **conservent** le caractère distingué, les inclusions et les intersections.

APP. Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont les $k\mathbb{Z}/n\mathbb{Z}$, où $k|n$.
. $Z(G)$ le centre de $G$.
$G/Z(G)$ monogène $\to$ $G$ abélien [CAL]142

## 4) Théorèmes d'isomorphismes : (dans ce §, $H \lhd G$)

**THM** [Propriété universelle du groupe quotient] Soit $\Gamma$ un groupe et $\varphi : G \to \Gamma$ un morphisme de groupe tel que $H \subseteq \ker \varphi$. [CAL]147
Alors il existe un unique morphisme
$\tilde{\varphi} : G/H \to \Gamma$ tel que $\varphi = \tilde{\varphi} \circ \pi$.
$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"'] & \Gamma \\ G/H \arrow[ur, dashed, "\tilde{\varphi}"'] & \end{tikzcd}$$

**COR :** [1er thm d'isomorphisme]
Avec les mêmes notations : $G/\ker\varphi \simeq Im\varphi$.

APP. – un groupe monogène infini est isomorphe à $(\mathbb{Z},+)$ [OA] 233
– un groupe monogène fini est cyclique, $\simeq (\mathbb{Z}/m\mathbb{Z},+)$ pour un $m \in \mathbb{Z}$.

- $G/Z(G) \simeq \mathrm{Int}(G)$
[PER] 164 - $SO_3 \simeq Q/\{\pm 1\}$, $Q$ quaternions de norme 1.

[CAL 150] **prop** [2ème théorème d'isomorphisme] $H \triangleleft G$
Soit $K$ un sous-groupe de $G$, les groupes quotients $K/K\cap H$ et $HK/H$ existent et on a $K/K\cap H \simeq HK/H$.

**prop**: [3ème théorème d'isomorphisme]. Soit $K$ un sous-groupe de $G$ tel que $K \subset H$, $K \triangleleft G$, $H \triangleleft G$. Alors
$$G/H \simeq {}^{G/K}\!/_{H/K}.$$

## II] Groupes et sous-groupes remarquables

### 1) Groupes simples

[PER] 12 **déf**: Si $G \neq \{e\}$, $G$ est dit simple si ses seuls sous-groupes distingués sont $\{e\}$ et $G$.

[PER] 28 **ex** - pour $n \geq 5$, $A_n$ est simple.
[PER] 148 - $SO_3(\mathbb{R})$ est simple.
[PER] 150 - pour $n \geq 5$, $PSO_n(\mathbb{R})$ est simple.

**APP**. Soit $f: G \to \Gamma$ un morphisme. Si $G$ est simple, $f$ est injectif ou trivial.

[CAL] 138 **prop**: Les seuls groupes simples abéliens sont les groupes cycliques d'ordre premier.

[CAL] 157... 

### 2) Groupes caractéristiques

**déf** $H$ est caractéristique dans $G$ si $\forall \sigma \in \mathrm{Aut}(G)$, $\sigma(H) = H$.
Notation $H$ car $G$.

**ex**: $Z(G)$ car $G$.

**APP**. $H$ car $G \Rightarrow H \triangleleft G$.

**prop**: Soit $K$ un sous-groupe de $G$, $K \subset H$.
(i) $K$ car $H$ et $H$ car $G \Rightarrow K$ car $G$.
(ii) $K$ car $H$ et $H \triangleleft G \Rightarrow K \triangleleft G$.

Contre-ex: Dans $S_4$, $\langle (12)(34) \rangle \triangleleft V_4 \triangleleft S_4$ (groupe de Klein)
mais $\langle (12)(34) \rangle \not\triangleleft S_4$.

### 3) Groupe dérivé d'un groupe [CAL] 156..

**déf**: Commutateur de $x$ et $y$ dans $G$: $[x,y] = xyx^{-1}y^{-1}$.

**déf**: Le groupe dérivé de $G$, noté $D(G)$ est le sous-groupe de $G$ engendré par les commutateurs.

Rque $G$ est abélien $\Leftrightarrow D(G) = \{e\}$.

APP. - $D(G)$ car $G$.
- $D(S_n) = A_n$ pour $n \geq 2$ [PER] 28
- $D(GL_n) = SL_n$ [XENS2] 188 ($n \geq 2$ sauf un corps à $\geq 3$ e.)

**propo** (Caractérisation) $D(G)$ est le plus petit sous-groupe distingué de $G$ tel que $G/D(G)$ soit abélien.

APP: Tout morphisme de $G$ dans un groupe abélien se factorise par $D(G)$.

**THM**: [Frobenius - Zolotarev] [OA] 251
Soit $p$ premier impair. Soit $V$ un espace vectoriel de dimension finie sur $\mathbb{F}_p$. Alors $\forall u \in GL(V)$
$$\varepsilon(u) = \left(\frac{\det(u)}{p}\right).$$
DVP

### 4) Produit direct

**déf/prop** Soient $G, H$ deux groupes. L'ensemble $G \times H = \{(g,h) / g \in G, h \in H\}$ peut être muni d'une structure de groupe via $(g,h)\cdot(g',h') = (gg', hh')$. Il est appelé produit direct de $G$ et $H$. [COM] 25

**ex**: $V_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ [CAL] 57

**APP** lemme chinois: soient $p, q$ premiers entre eux. [PER] 21
$$\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}.$$

[COM] 26 **prop:** (Caractérisation) Si $H, K$ sont deux sous-groupes de $G$ tels que : $H \lhd G$, $K \lhd G$, $H \cap K = \{e\}$ et $HK = G$,
Alors $G \simeq H \times K$.

[COM] 27 **APP:** $U_6 \simeq U_2 \times U_3$ où $U_n$ groupe des racines $n$-ièmes de l'unité.

[COM] 66 **THM** [Structure des groupes abéliens finis]
$G$ abélien fini d'ordre $n \geq 2$. Il existe $q_1 | \dots | q_r$ des entiers uniques tels que $G \simeq \mathbb{Z}/q_1\mathbb{Z} \times \dots \times \mathbb{Z}/q_r\mathbb{Z}$.

**APP.** Un groupe abélien d'ordre 20 est $\simeq$ à $\mathbb{Z}/20\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$

## III) $p$-groupes et théorèmes de Sylow

### 1) $p$-groupes

ici $p$ désigne un nombre premier

[PER] 9 **déf:** On appelle $p$-groupe un groupe dont l'ordre est une puissance de $p$. (Idem $p$-sous-groupes)

**ex:** - $\mathbb{Z}/p^\alpha\mathbb{Z}$ est un $p$-groupe ($\alpha \in \mathbb{N}^*$)
- $V_4$ est un 2-groupe.

[COM] 65 **prop:** $G$ un $p$-groupe. Alors $Z(G)$ n'est pas réduit à $\{e\}$.

**APP.** Un groupe d'ordre $p^2$ est abélien.

### 2) Théorèmes de Sylow

($G$ fini, $|G| = p^\alpha m$, $p \nmid m$, $p$ premier)

[PER] 19.. [CAL] 26.. **déf:** On appelle $p$-sous-groupe de Sylow de $G$ un sous-groupe de $G$ de cardinal $p^\alpha$.

**ex:** $|Gl_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p)\dots(p^n - p^{n-1}) = m p^{n(n-1)/2}$ avec $p \nmid m$.
Les $p$-ss-gpes de $Gl_n(\mathbb{F}_p)$ sont d'ordre $p^{n(n-1)/2}$ ; par ex, l'ensemble des matrices triangulaires supérieures de diag. 1.

**THMS** [de Sylow] 1) $G$ contient au moins un $p$-ss-gpe de Sylow
2) Si $H$ est un $p$-s-gpe, il existe un $p$-Sylow de $G$ avec $H \subset S$.
3) Les $p$-Sylow sont tous conjugués
4) On note $n_p$ le nombre de $p$-Sylow de $G$ : $n_p | m$.
- $n_p \equiv 1 [p]$.

**cor** Un $p$-Sylow de $G$ est unique ssi il est distingué.

**APP.** - $G$ contient des sous-groupes d'ordre $p^i$, $\forall i \leq \alpha$.
- Un groupe fini d'ordre $pq$ n'est pas simple.
- Un groupe d'ordre 15 est cyclique.

## IV] Résolubilité [CAL] 236..

**Notations:** $D^0(G) = G$ et $D^i(G) = D(D^{i-1}(G))$ le $i^{\text{ème}}$ gpe dérivé de $G$ ($i \geq 1$).

**déf:** $G$ est dit résoluble s'il existe $n \geq 0$ tel que $D^n(G) = \{e\}$.

**ex:** - Tout groupe abélien est résoluble.
- $B := \{$matrices triangulaires supérieures$\}$ est résoluble. [CHA]

**prop:** 1) $G$ résoluble $\Rightarrow$ $H$ résoluble.
2) $\varphi : G \to \Gamma$ morphisme de groupes, on a $\varphi(D^i(G)) \subset D^i(\Gamma)$ avec égalité si $\varphi$ surjectif.
3) $G$ résoluble et $H \lhd G \Rightarrow G/H$ résoluble.
4) $H \lhd G$, $G$ est résoluble ssi $H$ et $G/H$ le sont.

**Caractérisation** $G$ est résoluble ssi il existe une suite finie de sous-groupes $\{e\} = H_0 \lhd H_1 \dots \lhd H_n = G$ tels que les quotients $H_i/H_{i-1}$ soient abéliens ($\forall i \in [\![1, n]\!]$). [CAL] 237

**APP.** - Tout $p$-groupe $G$ d'ordre fini est résoluble.
- Les seuls groupes simples résolubles sont les groupes cycliques d'ordre premier. [CAL] 238
- $S_n$ est résoluble pour $n \leq 4$. [CAL] 239
- **THM** [Lie-Kolchin] [CHA] 93 $\boxed{\text{DVP}}$
Tout sous-groupe connexe résoluble de $Gl_n(\mathbb{C})$ est conjugué à un sous-groupe de $B$.

## Références :

[CAL] Josette Calais, Eléments de théorie des groupes, PUF, 1996 (2ème edition)

[PER] Daniel Perrin, Cours d'algèbre, ellipses, 1996

[COM] François Combe, Algèbre et géométrie, Bréal, 1998

[OA] Vincent Beck, Jerôme Malick, Gabriel Peyré, Objectif Agrégation, 2ème édition 2005

[CHA] Antoine Chambert-Loir, Algèbre corporelle, 2005

[XENS 1] Serge Francinou, Hervé Gianella, Serge Nicolas, Exercices de mathématiques oraux X-ENS, algèbre 1, Cassini

[XENS 2] — — — —