103 Exemples et applications des notions de sous-groupe distingué et de groupe quotient. 2008/09

On note G un groupe, sa loi étant notée multiplicativement.

I. Faire d'un quotient un groupe.

• A. Sous-groupe distingué.

Déf: on dit qu'un sous-groupe H de G est distingué dans G si:

$$\forall h \in H,\ \forall g \in G,\quad ghg^{-1} \in H.$$

On note $H \triangleleft G$.

Ex: * $\{e\}$ et G sont toujours distingués dans G.
Si ce sont les seuls sous-groupes distingués, G est dit <u>simple</u>. A_5, par exemple, est simple.

* si G est commutatif, tout sous-groupe de G est distingué dans G.

* le groupe des translations d'un espace affine $\mathcal{E}$, $\tau(\mathcal{E})$, est distingué dans le groupe affine $GA(\mathcal{E})$.

* tout sous-groupe d'indice deux dans G est distingué; ainsi, pour tout n, $A_n \triangleleft \mathfrak{S}_n$.

Remarque: si $H \triangleleft G$ et $H \subset K$, un autre sous-groupe, alors $H \triangleleft K$.
En revanche, le fait d'être distingué n'est pas transitif.
Contre-exemple: $K = \langle (12)(34) \rangle \subset \mathfrak{S}_4$

On a $K \triangleleft V_4$, $V_4 \triangleleft \mathfrak{S}_4$ mais $K \not\triangleleft \mathfrak{S}_4$.

• B. Groupe quotient

Etant donnés un ensemble E et une relation d'équivalence R, on peut définir E/R et la projection $\pi : E \longrightarrow E/R$.

Etant donnés G un groupe, et R la relation d'équivalence:

$$xRy \iff xy^{-1} \in H,\quad H \text{ sous-groupe de } G,$$

on souhaite savoir si G/H peut être muni d'une structure de groupe de sorte que π soit un morphisme de groupes.
Ce n'est pas possible en général: si $G = GL_n(\mathbb{R})$ et $H = GL_n(\mathbb{Z})$, G/H n'est pas un groupe; mais:

Th: si $H \triangleleft G$, alors G/H est muni d'une structure de groupe et π est un morphisme de groupes.
La réciproque est vraie d'après le:

Th d'isomorphisme: si $\varphi : G \longrightarrow G'$ est un morphisme de groupes alors $\operatorname{Ker}\varphi \triangleleft G$ et $G/\operatorname{Ker}\varphi \simeq \operatorname{Im}\varphi$.

Exemples: * groupes $(\mathbb{Z}/n\mathbb{Z}, +)$ pour $n \geq 2$.
* pour tout $\alpha \neq 0$, $\mathbb{R}/\alpha\mathbb{Z} \simeq \mathbb{R}/\mathbb{Z}$ (groupes additifs)
* $GA(\mathcal{E})/\tau(\mathcal{E}) \simeq GL(E)$, où E est l'espace vectoriel associé à l'espace affine $\mathcal{E}$.

Applications: * $|SL_n(\mathbb{F}_q)| = \dfrac{(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})}{q-1}$

* les deux autres théorèmes d'isomorphisme:

2) Soit $H \triangleleft G$ et K un sous-groupe de G. Alors $K/H\cap K$ et HK/H sont des groupes quotient et sont isomorphes.

3) Si $H \subset K$ deux sous-groupes distingués dans G, alors

$$\left(G/H\right)\big/\left(K/H\right) \simeq G/K$$

II. Des sous-groupes distingués particuliers.

• A. Le centre

Déf: le centre de G, noté $Z(G)$, est l'ensemble des éléments de G qui commutent avec tous les éléments de G.

Prop: c'est un sous-groupe distingué de G.

Exemples: * si G abélien, $Z(G) = G$, et réciproquement.
* si G non abélien et simple, alors $Z(G) = \{e\}$.
la réciproque est fausse : en atteste $Z(\mathfrak{S}_3) = \{id\}$.
* $Z(GL_n(\mathbb{K})) = \{\lambda I_n \mid \lambda \in \mathbb{K}^*\}$ ($\mathbb{K}$ corps).
$Z(SL_n(\mathbb{K})) = \{\lambda I_n \mid \lambda^n = 1\}$

En quotientant $GL_n(\mathbb{K})$ et $SL_n(\mathbb{K})$ par leurs centres respectifs, on obtient les groupes $PGL_n(\mathbb{K})$ et $PSL_n(\mathbb{K})$, qui agissent sur les espaces projectifs $\mathbb{P}^{n-1}(\mathbb{K})$.
$PGL_2(\mathbb{C})$ est en bijection avec l'ensemble des homographies de la droite projective complexe.

• B. Groupes dérivés

Déf: un commutateur de G est un élément de G qui s'écrit $xyx^{-1}y^{-1}$ avec $x, y \in G$. Le sous-groupe de G engendré par ces commutateurs est le groupe dérivé de G : $D(G)$.

Exemples: * si $D(G) = G$, G est dit parfait. $\mathfrak{A}_n$, pour $n \geq 5$, par exemple, est parfait.
* $D(G) = \{e\} \iff G$ abélien.

Prop: $D(G) \triangleleft G$ et $G/D(G)$ est abélien : on l'appelle l'abélianisé de G. De plus, si $H \triangleleft G$ et G/H abélien, alors $H \subset D(G)$.

Dérivés d'ordre supérieur et groupes résolubles:

On définit la suite des groupes dérivés par :

$$\begin{cases} D^0(G) = G \\ D^n(G) = D(D^{n-1}(G)) \text{ pour } n > 0. \end{cases}$$

Un groupe G est dit résoluble s'il existe une suite de sous-groupes $G = G_0 \supset G_1 \supset \dots \supset G_{p-1} \supset G_p = \{e\}$, avec $G_i \triangleleft G_{i-1}$ pour $i \in \{1, \dots, p\}$ et G_{i-1}/G_i abélien.

Prop: G est résoluble ssi $D^p(G) = \{e\}$ pour un $p \in \mathbb{N}^*$.

Exemples: * tout groupe commutatif est résoluble.
* $\{e\} \triangleleft \mathfrak{A}_3 \triangleleft \mathfrak{S}_3$: $\mathfrak{S}_3$ est résoluble.
* $\{e\} \triangleleft V_4 \triangleleft \mathfrak{A}_4 \triangleleft \mathfrak{S}_4$: $\mathfrak{S}_4$ est résoluble. (voir fig 1)

Contre-exemple: $\mathfrak{S}_n$ n'est pas résoluble si $n \geq 5$.

Intérêt des groupes résolubles : théorie de GALOIS.

Th: soit $\mathbb{K} \subset \mathbb{C}$ un corps et $P \in \mathbb{K}[X]$, de corps de décomposition N.
Si P est résoluble par radicaux, alors $Gal(N|\mathbb{K})$ est résoluble.

Ex: $P = X^5 - 10X + 5 \in \mathbb{Q}[X]$ n'est pas résoluble par radicaux.

• C. Normalisateur

Déf: soit H un sous-groupe de G. Une partie S de G normalise H si, $\forall s \in S$, $sHs^{-1} = H$.

La plus grande partie qui normalise un sous-groupe, est elle-même un sous-groupe : le normalisateur de H, $N_G(H)$.

Prop: $N_G(H)$ est le plus grand sous-groupe dans lequel H est distingué.

La notion de partie normalisante est utilisée dans les arguments de FRATTINI, qui sont une application d'un théorème de SYLOW...

III Dévissage de groupes finis.

• A. Cas abélien

<u>Th Chinois</u> : soit G cyclique d'ordre mn avec $m \wedge n = 1$: $G \simeq \mathbb{Z}/mn\mathbb{Z}$.

Alors $G \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

<u>Th. de structure des groupes abéliens finis</u> : si G abélien fini, alors il existe $d_1 | d_2 | \dots | d_r$, r éléments de $\mathbb{N}^*$, tels que :

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \dots \times \mathbb{Z}/d_r\mathbb{Z}.$$

• B. Un outil central : le théorème de Sylow.

<u>Th</u> : soit G un groupe fini d'ordre $p^\alpha m$, avec $p \nmid m$ premier, et $\alpha > 0$. Alors :

1) Il existe au moins un p-sylow (p-sous-groupe d'ordre p^α) dans G, et tout p-sous-groupe de G est contenu dans un p-sylow.

2) Les p-sylows sont conjugués entre eux, et un p-sylow est distingué <u>ssi</u> il est unique (r_p, défini ci-après, vaut 1).

3) Le nombre de p-sylows, r_p, est congru à 1 modulo p et divise m.

<u>Applications à la simplicité</u> :

* aucun groupe d'ordre 63 n'est simple.
* tout groupe simple d'ordre 60 est isomorphe à A_5 $\boxed{\text{DVT}}$

• C. Le produit semi-direct.

<u>Prop</u> : soit G un groupe, et $H \triangleleft G$. On a la suite exacte :

$$e \longrightarrow H \xrightarrow{i} G \xrightarrow{\pi} G/H \longrightarrow e$$

S'il existe un morphisme $s : G/H \to G$ tel que $\pi \circ s = id_{G/H}$, alors G est isomorphe au <u>produit semi-direct</u> $H \rtimes_\tau G/H$: c'est un groupe dont l'ensemble est $H \times G/H$ et la loi est :

$$((n,h),(n',h')) \longmapsto (n\,\tau(h)\,n',\ hh'), \text{ avec } \tau(h)(n') = s(h)\,n\,(s(h))^{-1}$$

<u>Exemple</u> : le groupe diédral D_{2n}.

C'est le groupe des isométries conservant un polygone régulier de centre O à n côtés. Il est engendré par r : rotation de centre O et d'angle $\frac{2\pi}{n}$ et une réflexion s. (voir Fig. 2). D_{2n} est isomorphe au produit semi-direct $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

• D. Classification des groupes finis.

* Etant donné un groupe, on peut expliciter ses sous-groupes. Une représentation possible pour montrer la structure d'un groupe est le <u>treillis</u>. (voir Fig 3.)

* Etant donné un entier naturel, on peut déterminer avec les outils qui précèdent quelles structures de groupe sont possibles.

<u>Ex</u> : * groupes d'ordre pq, $p < q$ premiers. Soit G d'ordre pq.

- Si $p | q-1$, alors $G \simeq \mathbb{Z}/pq\mathbb{Z}$ ou $G \simeq \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ et tous les produits semi-directs sont isomorphes.

- Si $p \nmid q-1$, alors $G \simeq \mathbb{Z}/pq\mathbb{Z}$.

$\Rightarrow$ groupes d'ordre 14 (1er cas), d'ordre 15 (2e cas).

* groupes d'ordre 8 $\boxed{\text{DVT}}$

FIG.1 : Représentation géométrique du groupe A_4.

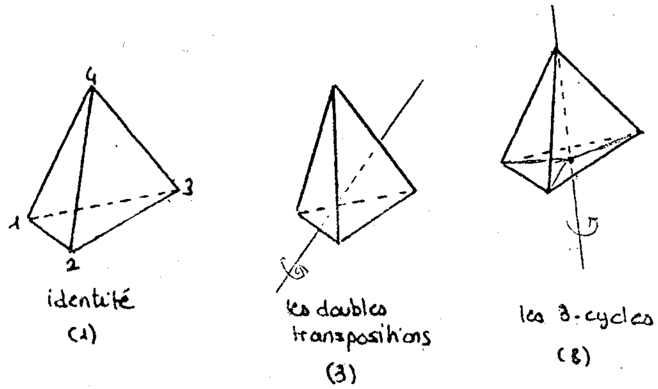
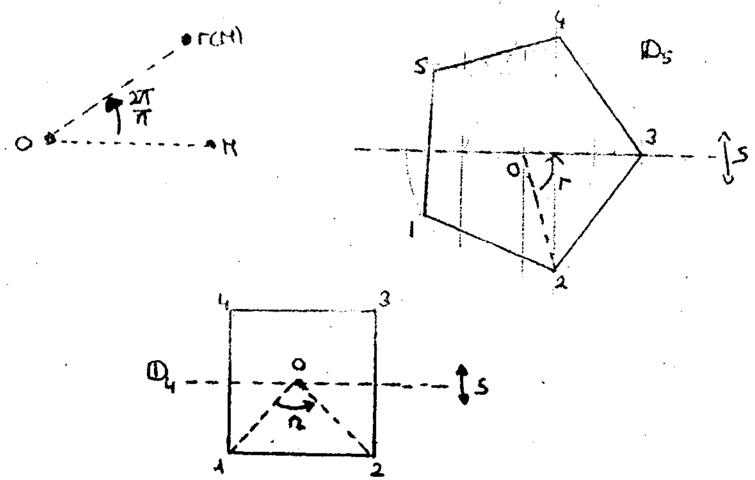


FIG.2 le groupe diedral $D_n \cong \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.



Bibliographie :

(1) Exercices de mathématiques pour l'agrégation Algèbre 1 - Francinou Gianella.

(2) cours d'algèbre - Perrin

(3) Éléments de géométrie - Mneimné

(4) Exercices d'algèbre - Ortiz

(5) Groupes - Bouvier. Richard

(6) Théorie de Galois - Escofier

(7) Delcourt - Théorie des groupes

FIG.3 Treillis