$\boxed{103}$ EXEMPLES DE SOUS-GROUPES DISTINGUÉS ET DE GROUPES QUOTIENTS. APPLICATIONS.

Soit G un groupe et H un sous-groupe de G.

I. Définitions et premières propriétés [Per96, ChI, p9]

I. A. Classes à gauche

Définition d'une classe à gauche, ensemble quotient, indice, théorème de LAGRANGE.

I. B. Sous-groupes distingués [Rom17, §10.1, p277]

Définition groupe distingué, exemples (noyau d'un morphisme ...)
Cas des groupes abéliens (réciproque fausse, cf quaternions), sous-groupe distingué équivaut à réunion de classes de conjugaison
Exemple des sous-groupes d'indice 2 qui sont toujours distingués
Notion de groupe quotient, exemple de $\mathbb{Z}/n\mathbb{Z}$
Bijections entre sous-groupes de G contenant H et sous-groupes de G/H. Exemple des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.

I. C. Liens avec d'autres sous-groupes

Groupe caractéristique, caractéristique implique distingué
centre d'un groupe : caractéristique
Commutateurs, groupe dérivé : c'est un groupe caractéristique et $G/D(G)$ est abélien. C'est le plus petit sous-groupe distingué pour lequel G/H est abélien.
Exemples de groupes dérivés pour le groupe symétrique
Normalisateur de H : plus grand sous-groupe de G dans lequel H est distingué.

I. D. Passage au quotient [Lan14, Ch1.3, p17]

Propriété universelle du groupe quotient, isomorphisme $G/\ker(f) \simeq \mathrm{Im}(f)$.
Application au groupe cycliques d'ordre n : isomorphes à $\mathbb{Z}/n\mathbb{Z}$, isomorphisme $\mathbb{R}/2\pi\mathbb{Z} \simeq \mathbb{U}$ de l'exponentielle, déterminant
Théorèmes d'isomorphismes :

- si H est distingué dans G, H' est distingué dans G' et $f : G \longrightarrow G'$ tels que $f(H) \subset H'$, alors il existe $\overline{f} : G/H \longrightarrow G'/H'$ unique tel que $\pi' \circ f = \overline{f} \circ \pi$.
  Exemple de $u \in \mathcal{L}(E)$ possédant un sous-espace vectoriel F stable : endomorphisme quotient $u_{E/F}$ [MM16, §II.6, p18]. Exemple de l'opérateur par translation dans $\mathcal{L}^p$ laissant stable les fcts cstes pp : passage au quotient dans L^p,
- si $H \subset K$ sont distingués dans G : H est distingué dans K, K/H est distingué dans G/H et $G/K \simeq (G/H)/(H/K)$,
- si H est distingué dans G, $K < G$. Alors H est distingué dans KH, $H \cap K$ est distingué dans K et $HK/H \simeq K/(K \cap H)$.

II. Utilisation des sous-groupes distingués

II. A. Groupes simples [Per96, Ch1, p9]

Groupes simples. Exemple si G simple non abélien : $D(G) = G$.

PROPOSITION 1. *Pour $n \geq 5$, $\mathfrak{A}_n$ est simple.*

Application : sous-groupes distingués de $\mathfrak{S}_n$ pour $n \neq 4$: $\{\mathrm{id}\}, \mathfrak{A}_n, \mathfrak{S}_n$.
Un groupe infini possédant un sous-groupe strict d'indice fini n'est pas simple.

II. B. Théorèmes de SYLOW [Per96, §1.5, p18–20]

On suppose G fini d'ordre n.
Soit p un nombre premier diviseur de n. On notera $n = p^a m$ où $p \nmid m$.

DÉFINITION 2. **[p-GROUPE, p-SOUS-GROUPE DE SYLOW]**
Si n est une puissance de p ($m = 1$), on dit que G est un p-groupe.
Plus généralement, on appelle p-sous-groupe de SYLOW (ou p-SYLOW) un sous-groupe de G de cardinal p^a.

THÉORÈME 3. **[THÉORÈME DE SYLOW 1]** *Il existe au moins un p-SYLOW dans G.*

COROLLAIRE 4. *Il existe au moins un sous-groupe de G d'ordre p^i pour tout $i \in [\![1, a]\!]$.*

THÉORÈME 5. **[THÉORÈME DE SYLOW 2]**
(i) Si $H < G$ est un p-groupe, alors il existe un p-SYLOW S tel que $H < S$,
(ii) Les p-SYLOW de G sont tous conjugués,
(iii) Notons Σ le nombre de p-SYLOW de G. Alors $\Sigma \mid m$ et $\Sigma \equiv 1 \mod p$.

COROLLAIRE 6. *Soit S un p-SYLOW de G. Alors $S \lhd G \iff S$ est l'unique p-SYLOW de G.*

APPLICATION 7. Tout groupe d'ordre 63 ou 255 n'est pas simple.

II. C. Produits direct et semi-direct [Per96, §1.6, p20]

DÉFINITION 8. [PRODUIT DIRECT]
- Soit G un groupe et $N, H < G$ tels que N, H commutent, $N \cap H = \{1\}$ et $G = NH$. Alors on dit que G est le produit direct de N par H.
- Soit N et H des groupes. Le produit direct de N et H est le produit cartésien $G = N \times H$, muni de la loi $(n, h).(n', h') = (nn', hh')$.

LEMME 9. [LEMME CHINOIS]
$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ si et seulement si $m \wedge n = 1$.

DÉFINITION 10. [PRODUIT SEMI-DIRECT]
- Soit G un groupe, $N \lhd G$ et $H < G$ tel que $N \cap H = \{1\}$ et $G = NH$. Alors on dit que G est le produit semi-direct de N par H.
- Soit N et H des groupes et $\phi : H \longrightarrow \mathrm{Aut}(N)$. On définit le produit $(n, h).(n', h') = (n\phi(h)(n'), hh')$ sur $G = N \times H$. $(G, .)$ est alors une groupe appelé produit semi-direct de N par H. On note $G = N \rtimes_\phi H$.

EXEMPLE 11. $\mathfrak{S}_n = \mathfrak{A}_n \rtimes \mathbb{Z}/2\mathbb{Z}$ et le produit n'est pas direct.

EXEMPLE 12. Groupe diédral

EXEMPLE 13. Contre-exemple : $\mathbb{Z}/8\mathbb{Z}$ et le groupe des quaternions H_8 ne peuvent être écrits comme un produit semi-direct non trivial.

PROPOSITION 14. *$N \rtimes_\phi H$ est bien un groupe dont $\overline{N} = N \times \{1_H\}$ est un sous-groupe distingué et $\overline{H} = \{1_N\} \times H$ est un sous-groupe, distingué si et seulement si $\phi = 1$.*

II. D. Théorie des représentations
[Rom17, Ch6, p182] [Ser98, Ch2, p23] [Pey04, §VIII.1.4/VIII.2.1, p228–232]

Caractères de degré 1. Isomorphisme $\widehat{G/D(G)} \simeq \hat{G}$ via la projection (par passage au quotient)
Représentation, caractère associé, produit scalaire sur les fonction centrales, caractères irréductibles : famille orthonormée *puis* base orthonormée, exemple des groupes abéliens
Cas de la représentation naturelle de G/N par permutation
$\overline{\rho}$ représentation de G/N implique $\rho = \overline{\rho} \circ \pi$ représentation de même degré, irréductible si et seulement si $\overline{\rho}$ l'est.
Table de caractères, exemple

Soit G un groupe fini. Soient $\chi_1, \ldots, \chi_r$ ses caractères irréductibles.

LEMME 15. *Soit χ associé à une représentation (ρ, V) de G. Alors $\ker(\rho) = \ker(\chi) = \{g \in G \,|\, \chi(g) = \chi(1)\}$.*

PROPOSITION 16. *Les sous-groupes distingués de G sont de la forme $\cap_{i\in I} \ker \chi_i$ où $I \subset [\![1, r]\!]$.*

APPLICATION 17. Table des caractères de $\mathfrak{S}_4$.

III. Le groupe linéaire [Per96, ChIV, p95]

E est un $\mathbb{K}$-espace vectoriel de dimension finie n.
Les transvections engendrent $\mathrm{SL}(E)$, sont conjuguées deux à deux dans $\mathrm{SL}(E)$ pour $n \geq 3$
Centre de $\mathrm{GL}(E)$, de $\mathrm{SL}(E)$, groupe (spécial) projectif
$\mathrm{PSL}_n(\mathbb{K})$ est simple pour $n \geq 3$
Suite exacte de $\mathrm{PGL}_n(\mathbb{K})$
Quelques isomorphismes simples

ANNEXE

Treillis de quelques groupes en soulignant les groupes distingués

QUESTIONS

Q Décomposer $\mathcal{GL}_n(\mathbb{K})$ en un produit (semi-)direct.

R $\mathcal{GL}_n(\mathbb{K}) \simeq \mathcal{SL}_n(\mathbb{K}) \rtimes \mathbb{K}^*$ et on a la suite exacte $1 \to \mathrm{SL}_n(\mathbb{K}) \to \mathrm{GL}_n(\mathbb{K}) \overset{\det}{\to} \mathbb{K}^* \to 1$.

Q Et pour $\mathbb{Z}$?

R $1 \to \mathbb{Z} \overset{\iota}{\to} \mathbb{Z} \overset{\pi}{\to} \mathbb{Z}/n\mathbb{Z} \to 1$ où $\iota : m \longmapsto nm$

Q Soit $\mathcal{E}$ un espace affine contenant 0. Décomposer $\mathrm{GA}(\mathcal{E})$.

R On montre que $1 \to T(\mathcal{E}) \to \mathrm{GA}(\mathcal{E}) \to \mathrm{GL}(\mathcal{E}) \to 1$.

Q Pour les isométries du cube ?

R On vérifie que $\mathrm{Isom}^+(\mathcal{C}) \rtimes \langle s \rangle \simeq \mathrm{Isom}(\mathcal{C})$ où s est une symétrie.
Ici le produit est direct car le groupe est abélien.

Q Soit G un groupe d'ordre 300. G est-il simple ?

R Écrivons $300 = 2^2 \times 3 \times 5^2$ et regardons les 5-Sylow. Notons Σ_5 leur nombre. On sait que $\Sigma_5 \mid 12$ et $\Sigma_5 \equiv 1 \mod 5$, donc $\Sigma_5 \in \{1, 6\}$. Si G est simple, $\Sigma_5 = 6$ et G agit sur Σ_5. Regardons $f : G \longrightarrow \mathfrak{S}_{\Sigma_5} \simeq \mathfrak{S}_6$. Son noyau ne peut être G, c'est donc $\{1\}$ et les 5-sylow sont distingués : contradiction. Donc G n'est pas simple.

BIBLIOGRAPHIE

[Lan14] S. Lang : *Algèbre*. Dunod, 3ème édition, 2014.

[MM16] R. Mansuy et R. Mneimné : *Algèbre linéaire : Réduction des endomorphismes*. De Boeck, 2 ème édition, 2016.

[Per96] D. Perrin : *Cours d'algèbre*. Ellipses, 1996.

[Pey04] G. Peyré : *L'algèbre discrète de la transformée de* Fourier. Ellipses, 2004.

[Rom17] J.-E. Rombaldi : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

[Ser98] J.-P. Serre : *Représentations linéaires des groupes finis*. Hermann, 1998.