103 - Exemples et applications des notions de sous-groupe distingué et de groupe quotient

1 Sous-groupes distingués

Définition 1. Soit G un groupe et H un sous-groupe de G.
- On dit que H est *distingué* (ou *normal*) dans G, et note $H \triangleleft G$, s'il est stable par tout automorphisme intérieur de G, i.e. $\forall g \in g, gHg^{-1} \subset H$.
- On dit que H est *caractéristique* dans G s'il est stable par tout automorphisme de G.

Exemple.
- Tout groupe caractéristique est distingué dans G.
- $\{e\}$ et G sont caractéristiques.
- Si G est abélien, tout sous-groupe de G est distingué (réciproque fausse, cf H_8 le groupe des quaternions).
- L'image par un morphisme surjectif et l'image réciproque par un morphisme quelconque d'un sous-groupe distingué sont distingués.
- Soit G un groupe, $H \triangleleft G$ cyclique et K un sous-groupe de H. Alors $K \triangleleft G$.
- $Int\ G \triangleleft Aut\ G$.
- Les sous-groupes distingués de D_n...

Proposition 1. *Soit G un groupe et H un sous-groupe de G. Lpsse :*

(i) H est distingué dans G

(ii) H est un point fixe de l'action par conjugaison sur les sous-groupes i.e. $\forall g \in g, gHg^{-1} = H$

(iii) H est le noyau d'un morphisme de groupes

Exemple. Ainsi $\mathfrak{A}_n \triangleleft \mathfrak{S}_n$.

Proposition 2 ([Per p.35])**.** *Soit $f : G \to H$ un morphisme et $N \triangleleft H$, alors $f^{-1}(N) \triangleleft G$.*

Application. Un p-gpe a des sous-gpes distingués de tous les ordres possibles.

Remarque. Dans le cas du groupe symétrique, on a $\tau(a_1, \dots, a_p)\tau^{-1} = (\tau(a_1), \dots, \tau(a_p))$; les classes de conjugaison sont les ensembles de permutations dont les cycles ont même longueur.

Apparition des actions de groupes — outil.

Définition 2. Soit G un groupe et H un sous-groupe de G.
- On appelle *classe à gauche* de $g \in G$ modulo H l'ensemble $gH = \{gh \mid h \in H\}$, c'est l'orbite de g sous l'action par translations.
- L'ensemble des classes à gauche, noté G/H, forme une partition de G. On appelle *indice* de H dans G, noté $[G : H]$, le cardinal de G/H.

Théorème 1. *Soit G un groupe fini, p le plus petit facteur premier de $|G|$ et H un sous-groupe d'indice p de G. Alors $H \triangleleft G$ (action de G sur G/H par translation).*

Application. Un groupe d'ordre $p^n q$, avec $q < p$ n'est pas simple.

Proposition 3. *Si $|G| \neq 4$ et si G possède un sous groupe d'indice 2 simple, alors c'est le seul.*
Si $|G| = 2n$ avec n impair, alors G ne possède qu'un seul sous-groupe d'indice 2.

2 Groupes quotients

Proposition 4. *Soit $H \triangleleft G$. Alors l'ensemble G/H muni de la loi $gH.g'H = (gg')H$ est un groupe.*

Exemple. $\mathbf{Z}/n\mathbf{Z}$!

Exemple. On définit ainsi les groupes projectifs $P\mathbf{R}^n$, PGl_n, PSl_n...

Exemple. Le quotient d'un anneau par un idéal. $k[u]$.

Exemple. Le quotient d'un ev par un sev est un ev.

Proposition 5. *Caractérisation des transvections.*

Théorème 2. *Sl_n est engendré par les transvections.*

Théorème 3. *Si $\varphi : G \to G'$ est un morphisme de groupes, alors $Ker\varphi$ est distingué dans G et $G/Ker\varphi \simeq Im\varphi$.*

Application. Un groupe monogène est isomorphe à $\mathbf{Z}$ s'il est infini et à un $\mathbf{Z}/n\mathbf{Z}$ s'il est fini.

Application. Isomorphismes doubles quotients Noether (Calais p. 155)

3 Sous-groupes remarquables

Définition 3. On appelle *normalisateur* de H sous-groupe de G le sous-groupe $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$.

Remarque. $N_G(H)$ correspond au plus grand sous-groupe de G dans lequel H est distingué.

Application. Théorème d'isomorphisme de Noether (Combes).

Définition 4. On appelle *centre* de G le sous-groupe $Z(G) = \{g \in G \mid \forall h \in G, hg = gh\}$

Proposition 6. *Tout sous-groupe du centre d'un groupe qcq est distingué. $Z(G) = G$ ssi G est abélien.*

Proposition 7. *Le centre d'un p-groupe est non-trivial. Un p-groupe possède des sous-groupes de tous les ordres possibles.*

Exemple. Perrin p. 35.

Exemple. Pour $n \geq 3$, $Z(\mathfrak{S}_n) = \{Id\}$. Centre de Gl_n, de O_n...

Définition 5. On appelle *groupe dérivé* de G, noté $D(G)$, le sous-groupe de G engendré par les commutateurs $[g,h] = ghg^{-1}h^{-1}$.

Proposition 8. *$D(G)$ est caractéristique, et $G/D(G)$ est le plus grand quotient abélien de G, appelé* abélianisé. *Tout sur-groupe du groupe dérivé est distingué.*

Exemple. Le groupe dérivé d'un groupe abélien est réduit au neutre. Pour $n \geq 2$, on a $D(\mathfrak{S}_n) = \mathfrak{A}_n$.

Proposition 9. *Tout morphisme d'un groupe dans un groupe abélien se factorise au départ par le groupe dérivé.*

Théorème 4. *On a $D(Gl_n(k)) = Sl_n(k)$ sauf si $n = 2$ et $k = \mathbf{F}_2$. $D(O_n)$?*

Application (Frobénuis-Zolotarev)*.* Soit p un nombre premier impair et V un $\mathbf{F}_p$-e.v. de dimension finie. Alors pour tout $u \in Gl(V)$, on peut considérer u comme un élément de $\mathfrak{S}(V)$, si bien qu'on peut lui associer sa signature. On a alors $\varepsilon(u) = \left(\frac{det(u)}{p}\right)$ (**Théorème 2**).

4 Simplicité

Définition 6. On dit que G est *simple* si ses seuls sous-groupes distingués sont triviaux.

Exemple. Les seuls groupes simples abéliens sont les $\mathbf{Z}/p\mathbf{Z}$.
Les p-groupes ne sont pas simples.

Théorème 5. *Pour tout $n \geq 5$, $\mathfrak{A}_n$ est simple. Par contre le sous-groupe non trivial V_4 de $\mathfrak{A}_4$ est distingué.*

Corollaire 1. *Les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\{1\}$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$.*

Application ([Per p.30]). Tout groupe d'indice n de $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$. On ne peut pas plonger $\mathfrak{S}_n$ dans $\mathfrak{A}_{n+1}$.

Proposition 10. *Pour $n \geq 5$, $D(\mathfrak{A}_n) = D(\mathfrak{S}_n) = \mathfrak{A}_n$.*

Théorème 6. *Le groupe $PSl_n(k)$ est simple, sauf si $n = 2$ et $k = \mathbf{F}_2$ ou $k = \mathbf{F}_3$.*

Théorème 7 (Sylow)**.** *Soit G un groupe fini de cardinal $p^\alpha m$, avec p premier et $m \wedge p = 1$. On note N_p le nombre de p-Sylow de G. Alors :*
– *deux p-Sylow sont conjugués*
– *Tout sous p-groupe de G est contenu dans un p-Sylow*
– *$N_p \equiv 1$ $[p]$ et $N_p | m$*
– *si $N_p = 1$, alors le p-Sylow de G est distingué.*

Remarque. Si $N_p = 1$, le p-Sylow de G est distingué, et donc G n'est pas simple.

Application.
– Les groupes d'ordre $p^\alpha q^\beta$, $p^\alpha < q - 1$ ne sont pas simples [Per p. 37].
– Les groupes d'ordres pq ou pq^2 ne sont pas simples.

5 Produits

5.1 Produit direct

Définition 7. On appelle *produit direct* des groupes G et H le produit cartésien $G \times H$ muni de la loi : $(g, h).(g', h') = (gg', hh')$.

Théorème 8 (lemme chinois)**.** *Si $m \wedge n = 1$, alors on a l'isomorphisme : $\mathbf{Z}/mn\mathbf{Z} \simeq \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$.*

Théorème 9. *Classification des groupes abéliens finis.*

Théorème 10. *Automorphismes de $\mathbf{Z}/n\mathbf{Z}$.*

5.2 Produit semi-direct

Définition 8. Si G agit sur H par automorphismes (i.e. $\varphi : G \to Aut(X)$), on définit le *produit semi-direct* $H \rtimes G$ comme l'ensemble $H \times G$ muni de la loi $(h, g)(h', g') = (h(g.h'), gg')$.

Remarque. Dans le groupe $H \rtimes G$, H est distingué et pour $h \in H, g \in H \rtimes G$, $g.h = ghg^{-1}$.

Proposition 11. *Soit G un groupe et H, K des sous-groupes de G tq H distingué dans G, $H \cap K = \{1\}$ et $HK = G$. Alors G est isomorphe au produit semi-direct $H \rtimes K$, avec l'action $k.h = khk^{-1}$. De plus, lpsse :*

(i) $G \approx H \times K$

(ii) $K \triangleleft G$

(iii) *l'action φ est triviale.*

Proposition 12. *Critères isomorphisme FG.*

Exemple.
- $\mathfrak{S}_n \simeq \mathfrak{A}_n \rtimes \mathbf{Z}/2\mathbf{Z}$.
- $Gl_n(\mathbf{R}) \simeq Sl_n(\mathbf{R}) \rtimes \mathbf{R}^*$?
- $O_n \simeq SO_n \rtimes \mathbf{Z}/2\mathbf{Z}$.
- $D_n \simeq \mathbf{Z}_n \rtimes \mathbf{Z}/2\mathbf{Z}$.

Application. Classification des groupes d'ordre pq (**Théorème 9**). Application : tout groupe d'ordre $2p$ est soit cyclique soit diédral.