103

Exemples et applications des notions de sous-groupes distingués et de groupe quotient.

I Généralités

Propo : Soit G un groupe et H un sous-groupe de G (noté $H < G$)
On définit la relation R_H par : $x R_H y$ ssi $y^{-1}x \in H$
et la relation R'_H par : $x R'_H y$ ssi $xy^{-1} \in H$
Ce sont deux relations d'équivalences.

Def : La classe de $y \in G$ modulo R_H est $yH = \{yh / h \in H\}$
et la classe de $y \in G$ modulo R'_H est $Hy = \{hy / h \in H\}$
On appelle Hy (resp. yH) la classe à gauche (resp. à droite) de y modulo H

Rq : On note G/H l'ensemble $G/R_H = \{yH / y \in G\}$
et $H\backslash G$ l'ensemble $G/R'_H = \{Hy / y \in G\}$

Rq : G/H et $H\backslash G$ ont même cardinal qu'on appelle indice de H dans G
et on le note $[G:H]$.

Th de Lagrange : Soit G un groupe fini et soient $H < G$, $K < G$ tq $K \subseteq H$
Alors : • $|G| = |H| \cdot [G:H]$
• $[G:K] = [G:H][H:K]$

Rq : En particulier, l'ordre de tout élément de $a \in G$ divise $|G|$.

Def : Soit G un groupe et H un sous-groupe de G.
H est distingué dans G si H vérifie l'une des conditions équivalentes
- $\forall x \in G$, $xH = Hx$ — $R_H = R'_H$
- $\forall x \in G$, $\forall h \in H$, $xhx^{-1} \in H$

On note alors $H \triangleleft G$.

Rq : Être distingué n'est pas transitif !
Par ex, $\langle (12) \rangle \triangleleft \langle (12)(34) \rangle \triangleleft A_4$ mais $\langle (12) \rangle \ntriangleleft A_4$

Ex : Le noyau de tout morphisme de groupes de G dans G' est un groupe distingué dans G.

Rq : Sert à prouver que H est distingué.

Ppté : Soit G un groupe et $H < G$ tel que $[G:H] = 2$
Alors $H \triangleleft G$

Def : Un groupe G est dit simple si ses seuls sous-groupes distingués sont $\{1\}$ et G.

Rq : Pour G abélien, tout sous-groupe est distingué !

Def : Soit $(G, \times)$ un groupe et H un sous-groupe distingué de G
On munit l'ensemble G/H de la loi induite par celle de G :
pour tout $(x,y) \in G^2$, $xH \times yH = xyH$ qui est bien une loi.
Alors $(G/H, \times)$ est un groupe, appelé groupe quotient de G par H

Ppté : Soit $\pi \left(\begin{array}{l} G \to G/H \\ x \mapsto \bar{x} \end{array} \right)$ pour $H \triangleleft G$
Alors π est un morphisme de groupes surjectif.

Théorème de factorisation : Soit G un groupe et $H \triangleleft G$
et soit $f : G \to G'$ un morphisme de groupes tq $H \subseteq \ker f$)
Alors il existe un morphisme de groupe $\bar{f} : G/H \to G'$
unique tel que $\bar{f} \circ \pi = f$
De plus $\mathrm{Im}(\bar{f}) = \mathrm{Im}(f)$ et $\ker(\bar{f}) = \pi(\ker f)$)

Rq : Factorisation en annexe. (parfois appelé ppté universelle du quotient)

Coro : Soient G un groupe et $H \triangleleft G$, $K \triangleleft G$ et $K \subseteq H$
Alors $G/K / H/K \simeq G/H$

Th : Soient G un groupe et $H \triangleleft G$. Alors
$\{K < G/H\} \simeq \{K < G$ tq $H \subseteq K\}$

Rq : Pour G un groupe abélien, tout sous-groupe H est distingué
et G/H est toujours un groupe quotient.

Cal

Com

Cal
(2)

II Exemples et applications

1) Sous-groupes distingués classiques

Déf : Soit G un groupe. Le centre de G est le sous-groupe de G $Z(G)$ où $Z(G) = \{h \in G / \forall g \in G, gh = hg\}$

Propté : $Z(G) \lhd G$ pour tout groupe G.

Ex : $Z(GL_n(\mathbb{R})) = \{\lambda I_n / \lambda \in \mathbb{R}^*\} \lhd GL_n(\mathbb{R})$

Déf : Soient G un groupe et $S \subseteq G$. Le normalisateur de S dans G noté $N_G(S)$ est le sous-groupe $N_G(S) = \{g \in G / gS = Sg\}$

En particulier, lorsque $S = \{g\}$ pour $g \in G$, on parle du centralisateur de g dans G.

Propté : Pour $H < G$, on les propriétés :

- $H \lhd N_G(H)$
- $H \lhd G$ ssi $N_G(H) = H$

Rq : $N_G(H)$ est le plus grand sous-groupe K de G tq $H \lhd K$.

Déf : Soit G un groupe et soient $(x, y) \in G^2$.
On appelle commutateur de x et y dans G l'élément $x^{-1}y^{-1}xy$.
On appelle groupe dérivé de G l'ensemble des commutateurs de G, on le note $D(G)$

Propté : $D(G) \lhd G$ pour tout groupe G
Si $N \lhd G$, alors $D(G) \subseteq N$ ssi G/N est abélien
et en particulier, $G/D(G)$ est abélien.

Ex : $D(S_n) = A_n$ $\forall n \in \mathbb{N}$

Ajouter plus d'exemples !

2) Produit direct et produit semi-direct

Déf : Soient H, K deux groupes (de loi $\cdot$) et on pose $G = H \times K$
Alors on munit l'ensemble G de la loi $*$ définie par
$(h, k) * (h', k') = (hh', kk')$ pour tout $(h, h') \in H^2$ et $(k, k') \in K^2$
Alors $(G, *)$ est un groupe, appelé produit direct de H et de K

Rq : $\{e_H\} \times K$ et $H \times \{e_K\}$ sont des groupes distingués de G isomorphes respectivement à K et H.

Prop : Soient G un groupe et $H < G$, $K < G$ tel que $H \lhd G$, $K \lhd G$, $HK = G$ et $H \cap K = \{e_G\}$
Alors $G \simeq H \times K$

Th de classification des groupes abéliens finis :
Soit G un groupe abélien fini non réduit à $\{e_G\}$
Alors il existe $d_1, \dots, d_n$ tel que $d_1 | d_2 | \dots | d_n$ où $d_i \in \mathbb{N}$
et tel que $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_n\mathbb{Z}$
Les (d_i) sont uniques et appelés facteurs invariants de G.

$\boxed{\text{DEV 1}}$ — Loi de réciprocité quadratique

> Soient p, q deux nombres distincts premiers non égaux à 2
> Soit $G = (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z})^*$ et $U = \{(1,1), (-1,-1)\} \lhd G$.
> Le groupe quotient G/U admet comme représentants
> $E_1 = \{(x, y) \in G / x \in [\![1, \frac{p-1}{2}]\!] \text{ et } y \in [\![1, \frac{q-1}{2}]\!]\}$
> et $E_2 = \{(l, l) \in G / l \in [\![1, \frac{pq-1}{2}]\!] \text{ et } l \wedge pq = 1\}$
> Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

Déf : Soient H, K deux groupes tel que K agit (à gauche) sur H via le morphisme $\varphi : \left(\begin{array}{l} K \to \mathrm{Aut}(H) \\ k \mapsto \varphi_k \end{array}\right)$ et soit $G = H \times K$.
On munit l'ensemble G de la loi $\times_\varphi$ définie par
$(h, k) \times_\varphi (h', k') = (h\varphi_k(h'), kk')$ pour tout $(h, h') \in H^2$ et $(k, k') \in K^2$
Alors $(G, \times_\varphi)$ est un groupe, appelé produit semi-direct associé à l'action φ de K sur H et on le note $H \rtimes_\varphi K$

Prop : Soient G un groupe et H, K deux sous-groupes de G tq
$H \lhd G$, $HK = G$ et $H \cap K = \{e_G\}$
Alors $G \simeq H \rtimes_\varphi K$ où $\varphi \left(\begin{array}{l} K \to \mathrm{Aut}(H) \\ k \mapsto \varphi_k \end{array}\right)$ où $\varphi_k(h) = khk^{-1}$

Ex : 1) Le groupe diédral D_n
C'est le groupe des isométries qui préservent les polygones réguliers à n côtés.
$D_n = \langle s \rangle \langle r \rangle$ où s est une symétrie $\in D_n$ et r est la rotation d'angle $\frac{2\pi}{n}$ et de centre le centre dudit polygone
Alors $\langle r \rangle \lhd D_n$ et $\langle s \rangle < D_n$ et $\langle s \rangle \cap \langle r \rangle = \{id\}$
Donc $D_n \simeq \langle r \rangle \rtimes \langle s \rangle \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$

2) Le groupe symétrique S_n

Via la signature ε, $\ker(\varepsilon)=A_n \triangleleft S_n$
et on démontre que $S_n \simeq A_n \rtimes \mathbb{Z}/2\mathbb{Z}$

3) Théorème de Sylow et étude de la simplicité

Déf : Soit G un groupe fini d'ordre $p^\alpha q$ où $p\in\mathbb{P}$, $p\nmid q$ et $\alpha\in\mathbb{N}$.
Un p-sous-groupe de Sylow de G est un groupe d'ordre p^α.

Lemme : Soit G comme précédemment et $H<G$ et soit S un p-Sylow de G.
Alors il existe $a\in G$ tel que $aSa^{-1}\cap H$ soit un p-Sylow de H.

Th de Sylow : Soit G groupe fini d'ordre $p^\alpha q$ où $p\in\mathbb{P}$, $p\nmid q$, $\alpha\in\mathbb{N}^*$.
Alors : - G admet au moins un p-Sylow et si n_p est le nombre de p-Sylow alors n_p vérifie $n_p\equiv 1[p]$ et $n_p \mid q$
- Les p-Sylow sont conjugués
- Si $n_p=1$, l'unique p-Sylow de G est distingué.

Rq : On obtient un critère pour savoir si un groupe est simple ou non.

~~DEV2~~ — Simplicité de A_n pour $n\geq 5$, $n\in\mathbb{N}$

Pour $n\in\mathbb{N}$ et $n\geq 5$, le groupe A_n est simple

Ex : Tout groupe d'ordre 63 n'est pas simple.
Un groupe abélien est simple s'il est d'ordre $n\in\mathbb{P}$.

4) Résolubilité

Déf : Soit G un groupe. G est dit résoluble s'il admet $H_0,\dots,H_p$ une suite de sous-groupes telle que :
- $G=H_0$, $H_{i-1}\supseteq H_i$ $\forall i\in[\![1,p]\!]$ et $H_p=\{e\}$
- $H_i \triangleleft H_{i-1}$ et H_{i-1}/H_i pour tout $i\in[\![1,p]\!]$.

Prop : On note $D_i(G)$ le i-ème groupe dérivé de G défini par $D_i(G)=D(D_{i-1}(G))$ pour $i\geq 1$.
Alors G est résoluble s'il existe $n\in\mathbb{N}$ tel que $D_n(G)=\{e\}$

Ex : Un groupe abélien est résoluble (son groupe dérivé est $\{e\}$)
$D(S_n)=A_n$ et $D(A_n)=A_n$ pour $n\geq 5$
Le groupe S_n, $n\geq 5$ n'est pas résoluble mais S_2, S_3 et S_4 sont résolubles.

Rq : En théorie de Galois, un groupe résoluble permet de caractériser les équations polynomiales résolubles par radicaux.

Applications aux groupes de matrices ?

Représentations ?

*

DEV 2 — Groupe d'ordre pq

Soient p,q deux nombres premiers tel que $p<q$
Alors : - si $p\nmid q-1$, tout groupe fini d'ordre pq est cyclique (donc $\simeq \mathbb{Z}/pq\mathbb{Z}$)
- si $p \mid q-1$, il existe à isomorphisme près deux groupes finis d'ordre pq : $\mathbb{Z}/pq\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z}\rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$ où φ morphisme de $\mathbb{Z}/p\mathbb{Z}$ ds $\mathbb{Z}/q\mathbb{Z}$ non trivial

1) $\begin{pmatrix} H \longrightarrow gH \\ h \mapsto gh \end{pmatrix}$ bijective $\forall g \in G$

d'où $G = \cup g_i H = \cup\cup g_i h_j K$

2) Les th d'isomorphismes justifient l'intérêt des groupes quotients (donc des groupes distingués) : il suffit de découper un groupe en groupe quotient qu'on étudie séparément

3) Normalisateur (ce rend H normal ou distingué)

4) Lorsque $H \not\triangleleft G$, on introduit une notion pour s'en sortir.

5) Les groupes simples sont classifiés
cas cycliques, A_n, $n \geq 5$
les monstres
etc...

En intro, expliquer que le lien entre les deux notions
(G/H quotient $\Leftrightarrow H \triangleleft G$)
et l'intérêt des groupes quotients.

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \pi \downarrow & \exists & \nearrow \bar{f} \\ G/H & & \end{array}$$

Schéma 1

Références

[Com] COMBES
[Cal] J. CALAIS - Éléments de théorie des groupes
[Per] PERRIN