Algèbre 04 – Sous-groupes distingués, groupes quotients. Exemples et applications.

Soit G un groupe noté multiplicativement d'élément neutre e et H un sous-groupe de G.

1. Généralités et exemples

Définition. On dit qu'une relation d'équivalence $\mathcal{R}$ sur G est *compatible avec la loi du groupe* si pour tous $x, y, a \in G$, $x\mathcal{R}y$ implique $ax\mathcal{R}ay$ et $xa\mathcal{R}ya$.

Proposition. *Une relation d'équivalence $\mathcal{R}$ sur G est compatible avec la loi du groupe si et seulement si $G/\mathcal{R}$ est un groupe pour la loi $\overline{x} \cdot \overline{y} = \overline{xy}$.*

On considère les relations d'équivalence $\mathcal{R}_g$ et $\mathcal{R}_d$ définies par : $x\mathcal{R}_g y \iff x^{-1}y \in H$ et $x\mathcal{R}_d y \iff xy^{-1} \in H$. On note respectivement $(R/H)_g$ et $(R/H)_d$ les quotients par ces relations.

Définition et proposition. L'*indice* de H dans G est défini par $[G : H] = \mathrm{Card}(R/H)_g = \mathrm{Card}(R/H)_d$.
Lorsque G est fini, on a $[G : H] = |G| \,/\, |H|$.

Définition et proposition. Les assertions suivantes sont équivalentes :

(*i*) $\mathcal{R}_g$ est compatible avec la loi de G

(*ii*) $\mathcal{R}_d$ est compatible avec la loi de G

(*iii*) $\forall g \in G,\ gH = Hg$ *i.e.* $gHg^{-1} = H$

(*iv*) les relations $\mathcal{R}_g$ et $\mathcal{R}_d$ coïncident.

Lorsque ces conditions sont vérifiées, on dit que H est un *sous-groupe distingué* de G et on écrit $H \lhd G$.
L'ensemble quotient est alors noté G/H.

Exemple. $\{e\}$ et G sont distingués dans G.

Exemple. Si G est abélien alors tous ses sous-groupes sont distingués.

Exemple. Le groupe $\mathbb{H}_8$ des quaternions n'est pas abélien mais tous ses sous-groupes sont distingués.

Proposition. *Si $[G : H] = 2$ alors $H \lhd G$.*

Exemple. Si D_n est le groupe diédral d'ordre $2n$ alors le sous-groupe (cyclique) Γ_n des rotations de D_n est distingué dans D_n.

Proposition. *$H \lhd G$ si et seulement s'il existe un groupe G' et un morphisme $f : G \to G'$ tels que $H = \ker f$.*

Exemple. $SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$

Exemple. $\mathcal{A}_n \lhd \mathcal{S}_n$

Exemple. $Z(G) \lhd G$

Proposition. *Si $f : G \to G'$ est un morphisme de groupes alors* $\mathrm{Im}\ f \simeq G/\ker f$.

Application. Si G est monogène alors $G \simeq \mathbb{Z}$ ou $\mathbb{Z}/n\mathbb{Z}$.

Application. Si $[G : H]$ est le plus petit facteur premier de $|G|$ alors $H \lhd G$.

Application. Soit H et K deux sous-groupes de G.

(*i*) Si $H \lhd G$ alors $HK \leq G$, $H \cap K \lhd K$, $H \lhd HK$ et $K/(H \cap K) \simeq HK/H$.

(*ii*) Si $K \leq H$, $K \lhd G$ et $H \lhd G$ alors $H/K \lhd G/K$ et $G/H \simeq (G/K)/(H/K)$.

Définition. H est un *sous-groupe caractéristique* de G si $\varphi(H) \subset H$ pour tout $\varphi \in \mathrm{Aut}(G)$; on note $H \sqsubset G$.

Un sous-groupe caractéristique est donc distingué.

Exemple. $\mathrm{Int}(G) = \{x \mapsto gxg^{-1}; g \in G\} \sqsubset \mathrm{Aut}(G)$.

2. Dévissage et simplicité

2.1. Sous-groupes remarquables.

Définition. Le *normalisateur de H dans G* est le sous-groupe $N_G(H) = \{x \in G; xHx^{-1} = H\}$.

Remarque. $H \lhd G \iff N_G(H) = G$.

Remarque. $H \lhd N_G(H)$ et $N_G(H)$ est le plus grand sous-groupe de G dans lequel H soit distingué.

Définition. Le *groupe dérivé* de G est le sous-groupe de G, noté $D(G)$ ou $[G, G]$, engendré par les commutateurs $[x, y] = xyx^{-1}y^{-1}$ où $x, y \in G$.

Exemple. $D(\mathcal{A}_4) = \{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ et $D(\mathcal{A}_3) = \{\mathrm{id}\}$.

Exemple. $D(\mathcal{S}_n) \subset \mathcal{A}_n$ pour tout $n \geq 2$.

Définition. La *suite centrale descendante* $(\Delta_n(G))_{n\geq 0}$ de G est définie par $\Delta_0(G) = G$ et $\Delta_{n+1}(G) = [\Delta_n(G), G]$ pour tout $n \geq 1$.

Remarque. La suite $(\Delta_n(G))_n$ est décroissante et on a $\Delta_n(G) \lhd G$ et $\Delta_n(G)/\Delta_{n+1}(G) \subset Z(G/\Delta_{n+1}(G))$.

Définition. On dit que G est *nilpotent* s'il existe $n \geq 0$ tel que $\Delta_n(G) = \{e\}$. Le plus petit entier $c \geq 0$ tel que $\Delta_c(G) = \{e\}$ est appelé la *classe de nilpotence* de G.

Exemple. G est nilpotent de classe 0 si et seulement si $G = \{e\}$ et G est nilpotent de classe 1 si et seulement si G est abélien non trivial.

Exemple. Soit $UT_3(\mathbb{R})$ le sous-groupe de $GL_3(\mathbb{R})$ formé des matrices $\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$. Si $A, B, C \in UT_3(\mathbb{R})$ alors $[[A, B], C] = \mathrm{I}$ or $UT_3(\mathbb{R})$ n'est pas abélien donc $UT_3(\mathbb{R})$ est nilpotent de classe 2.

Exemple. Pour tout $n \geq 1$, on a $\Delta_n(\mathcal{S}_3) = \mathcal{A}_3$ donc $\mathcal{S}_3$ n'est pas nilpotent.

Définition. On définit $(D_n(G))_n$ par $D_0(G) = G$ et $D_{n+1}(G) = [D_n(G), D_n(G)]$ pour tout $n \geq 0$.

Remarque. La suite $(D_n(G))_n$ est décroissante et, pour tout $n \geq 0$, $D_{n+1}(G) \lhd D_n(G)$ et $D_n(G)/D_{n+1}(G)$ est abélien.

Définition. On dit que G est *résoluble* s'il existe $n \geq 1$ tel que $D_n(G) = \{e\}$.

Exemple. Si G est nilpotent alors G est résoluble.

Exemple. $\mathcal{S}_2, \mathcal{S}_3$ et $\mathcal{S}_4$ sont résolubles.

Exemple. Un p-groupe fini est résoluble.

2.2. **Simplicité.**

Lemme (théorèmes de Sylow)**.** *Si $|G| = p^\alpha m$ avec p premier ne divisant pas m alors*

(i) G admet un p-Sylow i.e. un sous-groupe d'ordre p^α,

(ii) les p-Sylow de G sont conjugués,

(iii) le nombre n_p de p-Sylow divise m et est congru à 1 modulo p,

(iv) si $n_p = 1$ alors le p-Sylow est distingué dans G.

Définition. On dit que G est *simple* si ses seuls sous-groupes distingués sont $\{e\}$ et G.

Exemple. Pour tout p premier, $\mathbb{Z}/p\mathbb{Z}$ est simple.

Exemple. $\mathcal{SO}(3)$ est simple.

Exemple. $\mathcal{A}_4$ n'est pas simple.

Proposition. *$\mathcal{A}_5$ est le seul (à isomorphisme près) groupe simple d'ordre 60.*

Proposition. *$\mathcal{A}_n$ est simple pour tout $n \geq 5$.*

Application. Si $n \geq 5$ alors $D(\mathcal{A}_n) = \mathcal{A}_n$.

Application. Si $n \geq 5$ alors $\mathcal{S}_n$ n'est pas résoluble.

2.3. **Produit semi-direct.**

Remarque. Si K et L sont des sous-groupes de G tels que $H \lhd G$, $K \lhd G$, $H \cap K = \{e\}$ et $G = HK$, alors G est isomorphe au *produit direct* $H \times K$.

Définition et proposition. Soit $\varphi : L \to \mathrm{Aut}(K)$ un morphisme où K et L sont deux groupes. Alors le produit $H \times K$ muni de la loi $(k, \ell) \cdot (k', \ell') = (k\varphi(\ell)(k'), \ell\ell')$ est un groupe appelé *produit semi-direct* de H et K relativement à φ et est noté $H \rtimes_\varphi K$.

Proposition. *Si $H \lhd G$, $K \leq G$, $H \cap K = \{e\}$ et $G = HK$ alors $G \simeq H \rtimes_\varphi K$ où $\varphi(k)$ est l'application $h \mapsto khk^{-1}$.*

Application. Classification des groupes d'ordre 12.

Application. Classification des groupes d'ordre pq avec p et q premiers distincts.

3. Applications

3.1. **Factorisation dans un anneau d'entier de corps de nombres** A**.** On rappelle que :

- A est un anneau de Dedekind
- le groupe des classes d'idéaux $\mathrm{C}(A)$ est le quotient du groupe abélien des idéaux fractionnaires par le sous-groupe des idéaux fractionnaires principaux
- $\mathrm{C}(A)$ est fini et toute classe non nulle "contient" des idéaux premiers

Lemme. *Soit $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ des idéaux premiers de A tels que $\mathfrak{p}_1 \cdots \mathfrak{p}_r = A\pi$ alors π est irréductible si et seulement s'il n'existe par de sous-produit strict $\mathfrak{p}_{i_1} \cdots \mathfrak{p}_{i_s}$ principal.*

Lemme. *Soit $\mathfrak{p}$ un idéal premier de A dont la classe $\overline{\mathfrak{p}}$ est d'ordre r dans $\mathrm{C}(A)$ alors on a $\mathfrak{p}^r = A\pi$ avec π irréductible dans A.*

Définition. On dit que A est un *anneau semi-factoriel* si la longueur des factorisations d'un élément ne dépend que de l'élément *i.e.* toute égalité du type $\pi_1 \cdots \pi_r = \tau_1 \cdots \tau_s$, où les π_i, τ_j sont irréductibles dans A, implique $r = s$.

Théorème de Carlitz. *A est semi-factoriel si et seulement si $|\mathrm{C}(A)| \leq 2$.*

3.2. **Action du groupe modulaire sur le demi-plan de Poincaré.** On identifie le plan $\mathbb{R}^2$ à $\mathbb{C}$, on note $\mathcal{P}$ le demi-plan $\{z \in \mathbb{C}; \mathrm{Im}\ z > 0\}$ et on considère le *groupe modulaire* $PSL_2(\mathbb{Z}) \simeq SL_2(\mathbb{Z})/\{\pm \mathrm{I}_2\}$.

Proposition. $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ *et* $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *engendrent* $SL_2(\mathbb{Z})$.

Proposition. *L'action de $PSL_2(\mathbb{Z})$ sur $\mathcal{P}$ définie par*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az + b}{cz + d}$$

admet pour transversale le domaine $\mathcal{D}_0$ défini par

- *soit $-\frac{1}{2} \leq \mathrm{Re}\ z < \frac{1}{2}$ et $|z| > 1$,*
- *soit $-\frac{1}{2} \leq \mathrm{Re}\ z \leq 0$ et $|z| = 1$.*

Proposition. *À $\mathbb{C}^*$-homothétie près, les réseaux du plan sont en bijection avec $\mathcal{D}_0$.*

Développements

$\mathcal{A}_5$ est le seul groupe simple d'ordre 60.

Classification des groupes d'ordre pq.

Théorème de Carlitz.

Références

[1] M. Alessandri, *Thèmes de géométrie. Groupes en situation géométrique*, Dunod, 1999.

[2] J. Calais, *Éléments de théorie des groupes*, P.U.F., 1996.

[3] F. Combes, *Algèbre et géométrie*, Bréal, 1998.

[4] S. Francinou et H. Gianella, *Exercices d'algèbre 1*, Masson, 1993.

[5] S. Francinou, H. Gianella et S. Nicolas, *Oraux X-ENS, algèbre 1*, Cassini, 2001.

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