

4. Groupes résolubles

Déf Soit G un groupe, on appelle groupe dérivé de G le sous-groupe de G engendré par les commutateurs $[x, y] := xyx^{-1}y^{-1}$.

On le note G' ou DG ou parfois $[G, G]$.

Propriétés

- (1) G' est un sous-groupe distingué et même caractéristique
càd invariant par tous les automorphismes (pas seulement les conjugaisons = autom. intérieurs)
- (2) $G' = 1$ ssi G est abélien.
- (3) G/G' est abélien et pour tout morphisme $f: G \rightarrow A$ avec A abélien il existe un unique morphisme $\bar{f}: G/G' \rightarrow A$
tel que $f = \bar{f} \circ \pi$

$$\begin{array}{ccc} G & \xrightarrow{f} & A \\ & \searrow & \nearrow \bar{f} \\ & G/G' & \end{array}$$
- (4) Soit $H \subset G$ contenant G' . Alors $H \triangleleft G$ et G/H abélien.

Dém (1) si $\alpha \in \text{Aut}(G)$ on a $\alpha([x, y]) = \alpha(xyx^{-1}y^{-1}) = \alpha x \cdot \alpha y \cdot (\alpha x)^{-1} \cdot (\alpha y)^{-1} = [\alpha x, \alpha y]$ d'où (1).

(2)-(3)-(4) exercice ! $\square$

Déf (1) On appelle suite dérivée la suite

$$G = D^0 G \supset D^1 G \supset D^2 G \supset \dots$$

définie par $D^{i+1} G = D(D^i G)$.

- (2) On dit que G est résoluble s'il existe $n \geq 0$ tel que $D^n G = 1$.
Le plus petit tel n est appelé indice de résolubilité de G .

Prop Pour un groupe G les conditions suivantes sont équivalentes^(★):

- (1) G est résoluble i.e. la suite dérivée stationne à 1.
- (2) G possède une suite de composition à quotients abéliens.

Si de plus G possède une suite de Jordan-Hölder, ces conditions sont aussi équivalentes à:

- (3) Les facteurs de Jordan-Hölder de G sont abéliens.

Dém (1) $\Rightarrow$ (2) car la suite dérivée est une suite de composition à quotients abéliens.

(2) $\Rightarrow$ (1) Soit $G \supset G_1 \supset \dots \supset G_{n-1} \supset G_n = 1$ une suite telle que $G_{i+1} \triangleleft G_i$ et G_i/G_{i+1} abélien, pour tout i . Alors

$$G/G_1 \text{ abélien} \Rightarrow DG \subset G_1$$

$$G_1/G_2 \text{ abélien} \Rightarrow DG_1 \subset G_2 \Rightarrow D^2G \subset DG_1 \subset G_2$$

et par récurrence $D^i G \subset G_i$ pour tout i . Donc $D^n G = 1$.

Si de plus G possède une suite JH, alors:

(2) $\Rightarrow$ (3) car d'après le th. de JH la suite de composition Σ donnée par l'hypothèse (2) peut être raffinée en une suite Σ' de JH dont les quotients Q'_j seront des quotients de sous-groupes des quotients Q_i de Σ , donc abéliens.

(3) $\Rightarrow$ (2) car une suite de JH fournit une suite satisfaisant (2)

□

Rem un groupe H est un sous-groupe d'un quotient de G
ssi c'est un quotient d'un sous-groupe de G .

On appelle parfois un tel H un sous-quotient de G .

(★) Dans la suite, on écrira en abrégé : LCSSE.

Proposition (propriétés des groupes résolubles)

- (1) Tout sous-groupe et tout quotient d'un groupe résoluble sont résolubles.
- (2) Si $H \triangleleft G$, alors: G résoluble ssi (H et G/H sont résolubles).
- (3) Un groupe simple est cyclique si il est fini, cyclique d'ordre premier.

Dém Soit G résoluble

- (1) Si $H \subset G$, on a $D^i H \subset D^i G$ donc elle stationne à 1.

Si $\pi: G \rightarrow G' = G/H$ est un quotient, alors π est surjectif donc $D^i G' = \pi(D^i G)$ qui stationne à 1.

- (2) Il reste à démontrer l'implication " $\Leftarrow$ ". Pour cela on relève par $\pi: G \rightarrow G/H$ (càd: on prend la préimage par π de) une suite de composition $G/H \supset K_1 \supset \dots \supset K_{p-1} \supset K_p = 1$ pour obtenir une suite:

$$\underbrace{G \supset \pi^{-1}K_1 \supset \dots \supset \pi^{-1}K_{p-1} \supset H}_{\text{Suite relevée}} \underbrace{\supset H_1 \supset \dots \supset H_{n-1} \supset H_n = 1}_{\text{Suite de comp. de } H}$$

pour obtenir une suite de composition à quotients abéliens pour G .

- (3) Si G est simple, il ne possède pas de ss-gr distingué non trivial donc sa seule suite de composition est $G \supset 1$.

Par hypothèse résoluble il est donc abélien. Un élément $x \neq 1$ engendre un sous-groupe $H \neq 1$ distingué donc égal à G .

L'élément x est d'ordre fini (sinon $\langle x^2 \rangle$ serait un ss-gr distingué non trivial), premier (sinon... complétez) $\square$

Exemples Nous connaissons déjà des groupes résolubles:

- les groupes abéliens
- le groupe S_4 (rappel $S_4 \supset A_4 \supset V \supset \mathbb{Z}/2\mathbb{Z} \supset 1$)
- les groupes diédraux $D_n = \{\text{isométries du } n\text{-gone régulier}\}$:

$$D_n \supset \underbrace{\mathbb{Z}/n\mathbb{Z}}_{\substack{\text{(sous-groupe) \\ \text{des rotations}}} } \supset 1.$$

- le groupe $\text{Aff}(\mathbb{R})$ des transformations affines $f_{a,b}: \mathbb{R} \rightarrow \mathbb{R}, x \mapsto ax+b$

$$\text{Aff}(\mathbb{R}) \supset \{\text{translations } x \mapsto x+b\} \supset 1$$

$$\begin{array}{c} \uparrow \text{isomorphe } \tilde{a}(\mathbb{R}, +) \\ \text{quotient isomorphe } \tilde{a}(\mathbb{R}^\times, \cdot) \text{ via le morphisme} \\ \pi: \text{Aff}(\mathbb{R}) \rightarrow \mathbb{R}^\times. \\ f_{a,b} \mapsto a \end{array}$$

On va maintenant décrire un autre exemple fondamental dans ce cours.

Prop Soit k un corps (commutatif), le groupe $T_n(k) = \left\{ \begin{pmatrix} * & \cdots & * \\ & \ddots & \\ 0 & \cdots & * \end{pmatrix} \right\}$ des matrices triangulaires supérieures est résoluble.
(Et ses sous-groupes aussi!)

Dém On a $T_n = T_n(k) = \{M = (m_{ij}) \text{ t.q. } m_{ij} = 0 \text{ si } i > j\}$.

On introduit $U_n = \left\{ \begin{pmatrix} 1 & \cdots & * \\ & \ddots & \\ 0 & \cdots & 1 \end{pmatrix} \right\} = \{M \in T_n, m_{ii} = 1 \ \forall i\}$

$$(0 \leq s \leq n-1) \quad U_{n,s} = \left\{ \begin{pmatrix} 1 & & & * \\ & \ddots & & \\ & & 0 & \\ & * & \ddots & \\ & & & 1 \end{pmatrix} \right\} = \{M \in U_n; m_{ij} = 0 \text{ si } 1 \leq |i-j| \leq s\}$$

d'où une suite $T_n \supset U_n = U_{n,0} \supset U_{n,1} \supset \cdots \supset U_{n,n-1} = 1$.

Vérifions que c'est une suite de composition à quotients abéliens:

D'abord on note que l'application $T_n \rightarrow (k^\times)^n$ ← groupe multiplicatif
 $M \mapsto (m_{11}, m_{22}, \dots, m_{nn})$

est un morphisme, c'ad "les coefs diagonaux d'un produit MN sont les produits des coefs diagonaux". De cela il découle que les coefs diagonaux de $MNM^{-1}N^{-1}$ sont $m_{ij} n_{ij} m_{ij}^{-1} n_{ij}^{-1} = 1$,
 donc $[T_n, T_n] \subset U_n$.

Ensuite on note que l'application $U_{n,s} \rightarrow k^{n-s-1}$ ← groupe additif
 $M \mapsto (m_{1,s+2}, m_{2,s+3}, \dots, m_{n-s-1,n})$

est un morphisme, c'ad que quand on forme un produit MN « les coefs de la $s^{\text{ième}}$ surdiagonale (= la 1^{ère} non nulle) s'ajoutent ». Noter que cette application est bien définie pour tout $s \in \{0, \dots, n-2\}$ et que pour $s=n-1$ on a $U_{n,n-1} = \left\{ \begin{pmatrix} 1 & \dots & 0 & m_{1,n} \\ & \ddots & & \\ 0 & & 1 & \end{pmatrix} \right\} \simeq k$.

De cela il découle que si $M, N \in U_{n,s}$ les coefs de la s^{e} surdiagonale de $MNM^{-1}N^{-1}$ sont $m_{i,s+1+i} + n_{i,s+1+i} - m_{i,s+1+i} - n_{i,s+1+i} = 0$.

Ceci signifie que $MNM^{-1}N^{-1} \in U_{n,s+1}$ donc $[U_{n,s}, U_{n,s}] \subset U_{n,s+1}$.

Ceci suffit à établir les propriétés de la suite de sous-groupes, donc T_n est résoluble (et les $U_{n,s}$ aussi!) $\square$

Un autre exemple important sera fourni par les p -groupes (finis) et nous y reviendrons avec le vocabulaire des actions de groupes.

Note terminologique:

La théorie des groupes est née dans les mains d'Évariste Galois pour étudier les racines des polynômes. On dit qu'une équation polynomiale $P(x) = 0$ est résoluble par radicaux
 ↑ poly. à coefs dans un corps k

si l'on peut exprimer ses racines en fonctions des coeffs de P à l'aide des symboles $+, -, \times, \div$ et $\sqrt[n]{}$.

$\underbrace{}_{\text{opérations de base dans } k}$ $\underbrace{\phantom{\sqrt[n]{}}}_{\text{racines } n^{\text{ièmes}} \text{ pour } n \text{ variable.}}$

L'extraction de racines $n^{\text{ièmes}}$ produit des extensions $k(\sqrt[n]{\alpha})$ de k qui sont galoisiennes de groupe de Galois $\mathbb{Z}/n\mathbb{Z}$ ($\Rightarrow$ abélien).

L'extraction itérée de telles racines $\sqrt[n_1]{\alpha_1}, \dots, \sqrt[n_s]{\alpha_s}$ produit des extensions K/k dont le groupe de Galois a pour facteurs de JH les groupes $\mathbb{Z}/n_1\mathbb{Z}, \dots, \mathbb{Z}/n_s\mathbb{Z}$: un tel groupe est donc nécessairement résoluble (au sens que nous avons défini). En fait :

Théorème de Galois — Une équation polynomiale à coefficients dans k est résoluble par radicaux si et seulement si son groupe de Galois est résoluble.

On trouvera des détails sur la page

[https://fr.wikipedia.org/wiki/Th%C3%A9or%C3%A8me_d%27Abel_\(alg%C3%A8bre\)](https://fr.wikipedia.org/wiki/Th%C3%A9or%C3%A8me_d%27Abel_(alg%C3%A8bre))

ou mieux, dans un cours de théorie de Galois...