Groupes simples, groupes résolubles

Références : [P] : Daniel Perrin, cours d'algèbre
[D] : Jean Delcourt, Théorie des groupes
[CG] : P. Caldero, J. Germoni, Histoires hédonistes ..... Tome I
et aussi
[C] : J. Calais, éléments de théorie des groupes

1) Définition de simplicité et commentaires

. Un groupe $G \neq \{1_G\}$ est dit simple si ses seuls groupes normaux $H \triangleleft G$ sont $H = G$ ou $H = \{1_G\}$

Exercice (1) : vérifier que G simple et abélien $\Leftrightarrow G \simeq \mathbb{Z}/p\mathbb{Z}$, p premier (groupe simple banal).

Ici, simple doit être pris au sens de "indécomposable".

Typiquement, si un groupe, par exemple un groupe fini n'est pas simple, on peut lui associer 2 groupes d'ordre plus petit en prenant $H \triangleleft G$, H non trivial et le groupe quotient G/H et espérer "reconstituer" la structure de G à partir de celle de H et G/H. Dans les meilleurs cas, on obtient un produit semi-direct (PSD)

$$\boxed{G \simeq H \rtimes G/H}$$

⚠ : ne marche pas toujours. Exemple, $G = Q_8$ (quaternions). $H = \underbrace{Z(G)}_{\text{centre de } G} = \{\pm Id\}$ est le seul

11) : vérifier que G simple et abélien $\Leftrightarrow G \simeq \mathbb{Z}/p\mathbb{Z}$, p premier (groupe simple $\widetilde{\quad}$).

Justification : $\Leftarrow$: évident

$\Rightarrow$: soit $a \in G \setminus \{e_G\}$. Par simplicité et vu que tout $H < G$ est normal (par abélianité), on a $\langle a \rangle = G$.

Donc $\begin{cases} G \simeq \mathbb{Z} : \text{non simple } (m\mathbb{Z} \ntriangleleft \mathbb{Z},\ m \in \mathbb{N} \setminus \{0, 1, -1\}) \\ \text{ou} \\ G \simeq \mathbb{Z}/n\mathbb{Z} : \text{non simple si } n \text{ est pas premier (prendre} \end{cases}$

$\langle \overline{\frac{n}{d}} \rangle \ntriangleleft \mathbb{Z}/n\mathbb{Z}$ où $d \mid n$, $d \neq \pm 1, \pm n$

Sous-groupe d'ordre 2 et tout
Sous-groupe d'ordre 4 est cyclique et contient $Z(G)$.
([D], Ex 3.3.13)

(Par contre, on a $D_4 \simeq \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$)
([D], Ex 3.3.4)

2) Liste des groupes simples classiques

(volontairement réduite mais à connaître)

- Les groupes alternés A_n, $n \geq 5$ ([P], I.8)
- Les groupes projectifs spéciaux linéaires $PSL(n,k)$, $n \geq 2$ sauf les cas $\begin{cases} n=2, & k=\mathbb{F}_2 \\ n=2, & k=\mathbb{F}_3 \end{cases}$ ([P], IV.4)
- Les groupes projectifs orthogonaux $PSO(n,\mathbb{R})$, $n=3$ et $n \geq 5$ ([P] : VI.6, VI.7)

Remarque : Les A_n et les $PSL(n,\mathbb{F}_q)$ fournissent une liste infinie de groupes simples finis.

3) Comment montrer qu'un groupe est simple ?

Remarque fondamentale : Si $H \lhd G$, alors H est une union de classes de conjugaison d'éléments de G

La stratégie "classique" consiste à exhiber un système S

de générateurs de G dont les éléments sont tous conjugués et montrer que si $H \triangleleft G$, $H \neq \{1_G\}$, alors $H \cap S \neq \emptyset$, auquel cas on aura bien $H = G$

Exemples: A_n, $n \geq 5$, $S = \{3\text{-cycles}\}$

$SO(3,\mathbb{R})$, $S = \{\text{retournements}\}$

(Retournement = rotation d'angle π, i.e conjuguée à
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$)

Autres types d'argument sur deux exemples:

- A_5 ([P]: I.8) : on peut facilement décrire les classes de conjugaison de ces éléments:

$\{Id\}$, $\left\{\begin{matrix}(a\ b)(c\ d) \\ \text{avec } \{a,b\} \cap \{c,d\} = \emptyset\end{matrix}\right\}$, $\{3\text{-cycles}\}$, $\{5\text{-cycles}\}_{I}$, $\{5\text{-cycles}\}_{II}$

$n_1 = 1$, $n_2 = 15$, $n_3 = 20$, $n_4 = 12$, $n_5 = 12$

(on a bien le compte : $\sum n_i = 60 = |A_5|$)

Si $H \triangleleft A_5$, on a donc $|H| = 1 + \sum_{i=2}^{5} \varepsilon_i n_i$ avec $\varepsilon_i \in \{0,1\}$. Par ailleurs, $|H| \,/\, |A_5| = 60$ (Lagrange)

On vérifie alors facilement que ces deux conditions entraînent $H = \{Id\}$ ou $H = A_5$

• $SO(3,\mathbb{R})$ ([C,G] : VII A.3, p 239)

Soit $H \triangleleft SO(3,\mathbb{R})$, $H \neq \{Id\}$. On montre alors que $H = SO(3,\mathbb{R})$ en considérant pour $h \in H \setminus \{Id\}$ fixé l'application

$$\begin{aligned} SO(3,\mathbb{R}) &\longrightarrow \mathbb{R} \\ g &\longmapsto \operatorname{trace} g h g^{-1} h^{-1} \end{aligned}$$

(détails ?)(2)

Ingrédients de la preuve :

a) $SO(3,\mathbb{R})$ est connexe (et compact)

b) $Z(SO(3,\mathbb{R})) = \{Id\}$

c) Un élément de $SO(3,\mathbb{R})$ est conjugué à une matrice de la forme $R_\theta = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$

4) Groupes résolubles et propriétés de base. ([C], chap VII.2)

• Suite dérivée : Soit G un groupe, on définit par récurrence la suite décroissante de sous-groupes :

$$D^0(G) := G, \quad D^{i+1}(G) = D(D^i(G))$$

(On rappelle que $D(H) = \langle x y x^{-1} y^{-1},\ x, y \in H \rangle$)

Propriété 4.1 :

2) $SO(3,\mathbb{R})$ simple :

ingrédients de la preuve :

a) $SO(3,\mathbb{R})$ est connexe (et compact)

b) $Z(SO(3,\mathbb{R})) = \{Id\}$

c) Un élément de $SO(3,\mathbb{R})$ est conjugué à une matrice de la forme $R_\theta = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$

Détails : on rappelle que $SO(3,\mathbb{R}) = \{M \in GL(3,\mathbb{R}) \mid {}^tMM = Id, \det M = 1\}$ = groupe des rotations vectorielles de $\mathbb{R}^3$

Rques préliminaires :

- Soit $M \in SO(3,\mathbb{R})$, d'après c), $\exists P \in SO(3,\mathbb{R}) \mid M = PR_\theta P^{-1} = PR_\theta {}^tP$ (rotation d'angle θ). En particulier $\text{trace}(M) = 1 + 2\cos\theta$

Rappel : la trace ne change pas par conjugaison

- $\text{trace}(R_\theta) = \text{trace}(R_{\theta'}) \Leftrightarrow \theta = \pm\theta' \Leftrightarrow R_{\theta'} = R_\theta^{\pm 1}$

Par ailleurs, $R_\theta \sim R_{-\theta}$ ($\sim$ = conjugué dans $SO(3,\mathbb{R})$ à) : $R_{-\theta} = PR_\theta P^{-1}$ avec $P = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ (géométriquement, cela est lié au fait que le signe l'angle orienté est défini par une orientation de l'axe de la rotation, laquelle n'est pas canonique : 2 choix possibles)

Conséquences : Soit $M \in SO(3,\mathbb{R})$, il existe alors un unique $\theta \in [0,\pi]$ tel que $M \sim R_\theta$, ou encore (puisque $\varphi : [0,\pi] \to [-1,3]$, $\theta \mapsto 1 + 2\cos\theta$ est bijective),

$M \sim M' \Leftrightarrow \text{trace}(M) = \text{trace}(M')$

Cas extrêmes : $\begin{cases} \text{trace}(M) = 3 \Leftrightarrow M = Id \\ \text{trace}(M) = -1 \Leftrightarrow M \text{ est un retournement} \end{cases}$

- La connexité par arcs est une conséquence facile de c) : considérer le chemin continu $\gamma : [0,1] \to SO(3,\mathbb{R})$

$t \mapsto M_t = PR_{t\theta}P^{-1}$ $\quad \begin{pmatrix} \gamma(0) = Id \\ \gamma(1) = M \end{pmatrix}$

Preuve de la simplicité :

soit $H \triangleleft SO(3,\mathbb{R})$, $H \neq \{Id\}$ et $h \in H \setminus \{Id\}$

Considérons $\varphi_h : SO(3,\mathbb{R}) \longrightarrow [-1,3]$

$g \longmapsto \mathrm{trace}(g h g^{-1} h^{-1})$

on a alors $\underbrace{\mathrm{Im}\,\varphi_h}_{\overset{\shortparallel}{I}} =]a,3]$ ou $[a,3]$ avec $a < 3$. En effet :

$\begin{cases} \mathrm{Im}\,\varphi_h \text{ est un intervalle (connexité de } SO(3,\mathbb{R}) \text{ et continuité de } \varphi_h) \\ \{3\} \not\subset \mathrm{Im}\,\varphi_h \quad (g = h \text{ et } Z(SO(3,\mathbb{R})) = \{Id\}) \end{cases}$

De plus, $g h g^{-1} h^{-1} \in H$ ($H \triangleleft G$)

soit $\theta \in [0,\pi]$; puisque $\varphi : [0,\pi] \longmapsto [-1,3]$ est une bijection continue, il en résulte qu'il existe $n \in \mathbb{N}^*$ tel que $1 + 2\cos(\frac{\theta}{n}) \in I$, i.e

$R_{\frac{\theta}{n}} \in H$ et donc $R_\theta = (R_{\theta/n})^n \in H$. Finalement, $H = SO(3,\mathbb{R})$, CQFD

Variante : on prend $\theta = \pi$ et on conclut de même que $R_\pi \in H$, d'où $H = SO(3,\mathbb{R})$ puisque

$SO(3,\mathbb{R}) = \langle \text{retournements} \rangle$

a) $\forall i \geq 0$, $D^i(G) \lhd G$

b) les quotients successifs sont abéliens

c) si $f : G \longmapsto H$ est un morphisme de groupes, on a

$\forall i \geq 0$, $f(D^i(G)) = D^i(f(G))$

· Définition de résolubilité : un groupe est résoluble s'il existe $n \geq 0$ tel que $D^n(G) = \{1_G\}$.

exemples ▲ G abélien $\Rightarrow$ G résoluble $(D(G) = \{1_G\})$

▲ Le groupe $G = \mathrm{Aff}(\mathbb{R})$ des transformations affines de $\mathbb{R}$: $x \to ax + b$, $a \in \mathbb{R}^*$, $b \in \mathbb{R}$ est résoluble. On vérifie en effet facilement que $D(G) = T$ où T est le groupe abélien formé par les translations : $x \longmapsto x + b$, $b \in \mathbb{R}$ et donc $D^2(G) = \{Id\}$

Proposition 4.2 : Soit G un groupe et $N \lhd G$, alors G est résoluble $\Leftrightarrow$ N et G/N sont résolubles.

preuve : Conséquence facile de la propriété 4.1 c). (3)

Applications : Tout p-groupe est résoluble

(3)

Soit G un groupe et $N \lhd G$,
alors G est résoluble $\Leftrightarrow$ N et G/N sont résolubles.

preuve : $\Rightarrow$ exercice

$\Leftarrow$ Soit $\pi : G \longmapsto G/N$ la projection canonique

on a $\pi(D^i(G)) = D^i(\pi(G)) = D^i(G/N) = \{e_{G/N}\}$ pour $i \geq i_0$ (résolubilité de G/N). De façon equivalente, $D^{i_0}(G) \leq N = D^0(N)$ et donc $D^i(G) \leq D^{i-i_0}(N)$ pour $i \geq i_0$. Par résolubilité de N, il existe $j_0 \geq i_0$ tel que $D^i(G) = \{e_G\}$ pour $i \geq j_0$.

(p-groupe = groupe d'ordre p^n, p premier, $n>0$)

En effet, on rappelle que le centre $Z(G)$ d'un p-groupe G n'est pas réduit à $\{1_G\}$ et on peut alors raisonner par récurrence sur n en considérant $N = Z(G)$ et $G/Z(G)$

<u>Théorème 4.3</u> : Un groupe fini G est résoluble ssi il existe une suite de sous-groupes

$$\{1_G\} = G_m \triangleleft G_{m-1} \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G$$

tels que les G_i / G_{i-1} soient cycliques (et on peut même se ramener à cyclique d'ordre premier)

Exercice (4) : Montrer que le groupe des permutations S_4 est résoluble et vérifier sur cet exemple le théorème 4.3.

(4) Montrer que le groupe des permutations S_4 est résoluble et vérifier sur cet exemple le théorème 4.3.

On a $D(S_4) = A_4$, $D(A_4) = V_4 = \{Id, (12)(34), (13)(24), (14)(23)\}$ (Groupe de Klein $\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$) et finalement $D(V_4) = D^3(S_4) = \{Id\}$

(Ces points seront rappelés lors du CCA du 20/1/21)

Si on pose $G_0 = S_4$, $G_1 = A_4$, $G_2 = V_4$, $G_3 = \{Id, (12)(34)\}$, $G_4 = \{Id\}$, on a bien

$$\frac{G_0}{G_1} \simeq \mathbb{Z}/2\mathbb{Z}, \quad \frac{G_1}{G_2} \simeq \mathbb{Z}/3\mathbb{Z}, \quad \frac{G_2}{G_3} \simeq \mathbb{Z}/2\mathbb{Z}, \quad \frac{G_3}{G_4} \simeq \mathbb{Z}/2\mathbb{Z}$$

Remarque : G résoluble et simple $\Leftrightarrow G \simeq \mathbb{Z}/p\mathbb{Z}$ p premier. La notion de résolubilité est en quelque sorte "opposée" à celle de "simplicité"

5) Quelques points culturels

Le terme "résoluble" vient de la résolubilité des équations polynomiales par radicaux (Travaux de Galois)[5]

Théorème (Burnside) : Tout groupe d'ordre $p^m q^n$ (p, q premiers) est résoluble

La classification des groupes finis simples a été achevée au début des années 1980. Elle repose en grande partie sur le résultat fondamental

(5) Quelques mots sur la résolubilité des équations par radicaux et liens (heuristiques) avec les groupes résolubles

Extension radicale : soit K un corps ($K = \mathbb{Q}$ ici pour simplifier)

$L = K(a_1, \dots, a_p)$, $a_i \in \mathbb{C}$ est une extension radicale de K si $\forall i, \exists n_i > 0$ tel que $a_i^{n_i} \in K(a_1, \dots, a_{i-1})$

Une équation du type $P(x) = 0$, $P \in K[X]$ est dite résoluble par radicaux si chaque racine $x_1, \dots, x_n$ est contenue dans une extension radicale

exemples $P(x) = x^2 + bx + c$, $L = K(\sqrt{\Delta})$ convient

en degré 3, $P(x) = 0$ est résoluble par radicaux par la formule de Cardan : $x^3 + px + q = 0 \Rightarrow x = \sqrt[3]{-q/2 + \sqrt{\Delta}} + \sqrt[3]{-q/2 - \sqrt{\Delta}}$ où $\Delta = \frac{q^2}{4} + \frac{p^3}{27}$

De même pour le degré 4 (Ferrari)

Faux à partir du degré $n = 5$ (Ruffini, Abel)

Le lien entre la résolubilité d'une équation et celle du groupe $G = \{$automorphismes de corps de $\mathbb{Q}(x_1, \dots, x_n)\}$ a été établi par Galois ($\simeq 1830$).

Cela permet de produire des exemples d'équations non résolubles par radicaux.

ex : $x^5 - 6x + 3 = 0$ n'est pas résoluble par radicaux (on montre que son groupe de Galois G est S_5, qui n'est pas résoluble)

Théorème de Feit-Thompson (1963)

Tout groupe fini simple non banal (non $\simeq \mathbb{Z}/p\mathbb{Z}$, p premier) est d'ordre pair.

Aperçu de la classification :

4 catégories :

- $\mathbb{Z}/p\mathbb{Z}$, p premier
- A_n, $n \geqslant 5$
- Les groupes de type Lie (les $PSL(n, \mathbb{F}_q)$ sont dans cette catégorie)
- 26 groupes sporadiques.

Le plus gros s'appelle le monstre ($|\text{Monstre}| \simeq 8{,}5 \cdot 10^{53}$)

6) Les derniers commentaires :

- Une formulation équivalente du théorème de Feit-Thompson est :

"Tout groupe fini d'ordre impair est résoluble" (Pourquoi ?) (6)

- Il paraît assez vain d'espérer une classification des groupes finis résoluble. Par exemple, on ignore le nombre de classes d'isomorphisme des groupes d'ordre $2048 = 2^{11}$ (et donc résolubles)

(6). Admettons le th de F.T (ce qui est préférable !) et constatons alors que tout groupe fini G d'ordre impair est résoluble :

OPS $|G| \neq 1, p$ (premier impair). D'après FT, $\exists$ $H \triangleleft G$, $H \neq \{e_G\}$ et G

On remarque alors que H et G/H sont d'ordre impair $< |G|$

En utilisant la prop 4.2, ceci permet de conclure en raisonnant par récurrence sur $|G|$.

$\sim$