COURS

GROUPE SIMPLE, CENTRE ET GROUPE DÉRIVÉ

GROUPE SIMPLE

Définition. Un groupe $(G, \star, e)$ est dit *simple* si ses seuls sous-groupes distingués sont triviaux ($\{e\}$ et G).

EXEMPLES.
- $\mathbb{Z}/p\mathbb{Z}$ avec p premier. `[Démontrer le]`
- Le *groupe alterné* $A_n := \big\{\mathrm{Ker}\,\big(\text{signature} : \mathbb{S}_n \to \{+1, -1\}\big)\big\}$. `[La démonstration est plus hardue.]`

L'utilité de la notion de quotient est de permettre d'étudier les groupes de la manière suivante. Si un groupe G est "gros", on peut chercher un sous-groupe distingué H. On étudie alors le groupe quotient G/H qui sera nécessairement plus "petit". À partir de H et de G/H, on peut espérer reconstruire G tout entier. Nous verrons une manière de le faire dans la suite du cours.
Cette méthode ne peut pas être appliquée aux groupes simples. Ils forment les "briques de base" de la théorie des groupes, un peu comme les nombres premiers pour la théorie des nombres.
La classification complète des groupes finis simples n'a été achevée que très récemment en ... 1981.

CENTRE

Lorsqu'un groupe n'est pas abélien, comment peut-on mesurer le défaut à ne pas l'être ?

Définition. Le *centre* d'un groupe $(G, \star, e)$ est le sous-groupe formé des éléments qui communtent avec tous les autres :

$$Z(G) := \{x \in G \,|\, \forall g \in G, g \star x = x \star g\}$$

`[Montrer que c'est bien un sous-groupe de` G`.]`

Proposition. Le centre $Z(G)$ est un sous-groupe distingué de G.

DÉMONSTRATION. `Démontrer le.` □

EXEMPLES.
- Un groupe G est abélien si et seulement si $Z(G) = G$.
- Pour $n \geq 3$, on a $Z(\mathbb{S}_n) = \{\mathrm{id}\}$. `[Montrer le.]`

Plus le centre d'un groupe est "petit", plus le groupe est loin d'être abélien.

Groupe dérivé

Définition. Le *groupe dérivé* d'un groupe $(G, \,.\,, e)$ est le sous-groupe engendré par les *commutateurs*, c'est-à-dire les éléments de la forme

$$[x, y] := x.y.x^{-1}.y^{-1}, \qquad \forall\, x, y \in G$$

On le note $D(G)$.

Exemples.

- Un groupe G est abélien si et seulement si $D(G) = \{e\}$. `[Montrer le.]`
- Pour $G = \mathbb{S}_3$, on a $D(\mathbb{S}_3) = \{\mathrm{id}, (123), (132)\}$. `[Montrer le.]`

Proposition. Le groupe dérivé $D(G)$ est distingué dans G et le quotient $G/D(G)$ est abélien.

Démonstration. Pour g, x, y dans G, on a

$$g.(x.y.x^{-1}.y^{-1}).g^{-1} = \underbrace{(g.x.g^{-1})}_{=X} . \underbrace{(g.y.g^{-1})}_{=Y} . \underbrace{(g.x^{-1}.g^{-1})}_{=X^{-1}} . \underbrace{(g.y^{-1}.g^{-1})}_{=Y^{-1}} .$$

Cela signifie que le conjugué de tout commutateur est un commutateur. Donc le sous-groupe engendré par les commutateurs est distingué.
Dans le quotient $G/D(G)$, notons par $\overline{x}$ la classe à gauche qui contient x. Pour tout x et y dans G, on a le calcul suivant dans $D(G)$

$$\overline{x}.\overline{y} = \overline{x}.\overline{e}.\overline{y} = \overline{x}.\overline{x^{-1}.y.x.y^{-1}}.\overline{y} = \overline{x}.\overline{x}^{-1}.\overline{y}.\overline{x}.\overline{y}^{-1}.\overline{y} = \overline{y}.\overline{x}.$$

D'où, le groupe quotient $G/D(G)$ est abélien. □

Le quotient $G/D(G)$ est appelé l'*abélianisé* de G. Nous verrons dans la suite du cours que $G/D(G)$ est le plus "gros" quotient de G qui soit abélien, d'où ce nom.
Mais pour montrer cette propriété, nous aurons besoin d'un nouvel ingrédient : la *propriété universelle du quotient*. À suivre ...