3. Groupe quotient

1. Sous-groupe distingué (ou normal, ou invariant)
2. Exemple déjà vu : $\mathbb{Z}/n\mathbb{Z}$
3. Propriété universelle du groupe quotient $(G/H, \pi)$
4. Factorisation des morphismes
5. Les groupes monogènes
6. Commutativité : centre $Z(G)$, commutateurs et groupe dérivé $D(G)$
7. Suite exacte
8. Groupes simples
9. Groupes résolubles

1. Sous-groupe distingué (ou normal, ou invariant)

<u>Objectif</u> : déterminer des CNS permettant de construire
le groupe quotient G/H à partir de $H \hookrightarrow G$, comme on a obtenu $\mathbb{Z}/n\mathbb{Z}$ à partir de $n\mathbb{Z} \hookrightarrow \mathbb{Z}$.

<u>Heuristique</u> : Soit $(G, *, e)$ un groupe.

• Pour tout sous-groupe $H \hookrightarrow G$, on définit deux relations d'équivalence

$$(\forall x, x' \in G) \qquad x\mathcal{R}_d x' \overset{\text{déf}}{\iff} x * x'^{-1} \in H \quad \text{et} \quad x\mathcal{R}_g x' \overset{\text{déf}}{\iff} x'^{-1} * x \in H$$

dont les classes d'équivalence de $x \in G$ sont respectivement :

$$\mathcal{R}_d(x) = Hx \quad \text{(classe à droite)} \quad \text{et} \quad \mathcal{R}_g(x) = xH \quad \text{(classe à gauche)}$$

• Dans le cas $n\mathbb{Z} \hookrightarrow \mathbb{Z}$, ces deux relations d'équivalence coïncident, de même lorsque G est abélien.

Heuristique (2)

• En général, $\mathcal{R}_d \neq \mathcal{R}_g$. Choisissons $\mathcal{R}_d$ (pour fixer les idées ...). Le candidat est l'ensemble quotient $G/\mathcal{R}_d$ muni de sa projection canonique π.

$$\begin{tikzcd} H \arrow[r, hook] & G \arrow[d, "\pi"] \\ & G/\mathcal{R}_d = \{\pi(x) = Hx \ : x \in G\} \end{tikzcd}$$

• Il s'agit de munir $G/\mathcal{R}_d$ d'une loi $*'$ qui fasse de π un morphisme, *i.e.*

$$(\forall x, x' \in G) \qquad \pi(x) *' \pi(x') \overset{\text{déf ?}}{=} \pi(x * x')$$

Cette définition est licite si et seulement si $\mathcal{R}_d$ est compatible avec la structure du groupe G :

$$(\forall x, x', y, y' \in G) \qquad \left(\begin{array}{cc} & \pi(x) = \pi(y) \\ \text{et} & \pi(x') = \pi(y') \end{array} \right) \overset{?}{\Longrightarrow} \pi(x * x') = \pi(y * y')$$

Heuristique (3)

Autrement écrit :

$$(\forall x, x', y, y' \in G) \qquad \begin{pmatrix} x * y^{-1} \in H \\ \text{et} \quad x' * y'^{-1} \in H \end{pmatrix} \overset{?}{\Longrightarrow} (x * x') * (y * y')^{-1} \in H$$

Par un petit calcul dans le groupe G, on remarque :

$$(x * x') * (y * y')^{-1} = x * (x' * y'^{-1}) * y^{-1}$$

Sous-groupe distingué (ou normal, ou invariant)

Soient $(G, *, e)$ un groupe et un sous-groupe $H \hookrightarrow G$.

Définition-proposition

Les assertions ci-dessous sont équivalentes :

1. *L'une des relations d'équivalence $\mathcal{R}_d$ ou $\mathcal{R}_g$ est compatible avec la loi de G.*
2. $(\forall x \in G) \qquad xHx^{-1} \subset H$
3. $(\forall x \in G) \qquad xH = Hx \qquad$ *(ou, de façon équivalente, $\mathcal{R}_d = \mathcal{R}_g$)*
4. *H est invariant par les automorphismes intérieurs.*

Si l'une d'elles est vérifiée, on dit H est un sous-groupe distingué (ou normal, ou invariant) de G, et on note :

$$H \lhd G$$

Démonstration des équivalences précédentes

• $(1) \iff (2)$
L'heuristique donne directement $(1) \Longrightarrow (2)$. Pour la réciproque, tirer profit de l'associativité pour voir que :

$$x * (x' * y'^{-1}) * y^{-1} = \underbrace{x * \overbrace{(x' * y'^{-1})}^{\in H} * x^{-1}}_{\in H} * \overbrace{(x * y^{-1})}^{\in H}$$

• $(2) \iff (3)$: exercice de compréhension
• $(3) \iff (4)$: par définition des automorphismes intérieurs.

$\square$

Définition du groupe quotient G/H

Soient $(G, *, e)$ un groupe et un sous-groupe distingué, $H \lhd G$.
L'ensemble quotient $G/\mathcal{R}_d$ se note G/H. Il est muni de la loi de groupe, qu'on notera comme celle de G (ici $*$), qui fait de la projection canonique un morphisme de groupe :

$$(\forall x, x' \in G) \qquad \pi(x) * \pi(x') = \pi(x * x')$$

L'élément neutre de G/H est $\pi(e) = H$, qu'on notera $\overline{e}$, ou même e, le contexte se chargeant de lever l'ambiguïté ... On retiendra le diagramme :

$$\begin{tikzcd} H \arrow[r, hook, "\lhd"] & G \arrow[d, "\pi"] \\ & G/H \end{tikzcd}$$

Par construction : $\boxed{\mathrm{Ker}(\pi) = H}$

2. Exemple déjà vu : $\mathbb{Z}/n\mathbb{Z}$

Comme pour tout groupe commutatif, les sous-groupes de $(\mathbb{Z}, +, 0)$ sont tous distingués. Soit $n \in \mathbb{N}$. La construction précédente fournit le diagramme :

$$\begin{tikzcd} n\mathbb{Z} \arrow[r, hook, "\triangleleft"] & \mathbb{Z} \arrow[d, "\pi"] \\ & \mathbb{Z}/n\mathbb{Z} \end{tikzcd}$$

où : $(\forall x, x' \in \mathbb{Z}) \quad \pi(x) = \pi(x') \Longleftrightarrow x - x' \in n\mathbb{Z}$

3. Propriété universelle du groupe quotient $(G/H, \pi)$

Soit $h : G/H \to G'$ un morphisme (de groupe). Alors, par construction,

$$\begin{tikzcd} G \arrow[r, "f=h\circ\pi"] \arrow[d, "\pi"'] & G' \\ G/H \arrow[ur, "h"'] & \end{tikzcd}$$

$f = h \circ \pi$ est un morphisme tel que $H \subset \mathrm{Ker}(f)$. Réciproquement,

Propriété universelle du groupe quotient $(G/H, \pi)$

(PU) $\begin{cases} \text{Pour tout morphisme } f : G \to G' \text{ tel que } H \subset \mathrm{Ker}(f), \\ \exists!\ h : G/H \to G' \text{ qui rende commutatif le diagramme} \end{cases}$

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"'] & G' \\ G/H \arrow[ur, dashed, "h"'] & \end{tikzcd}$$

On dit que f se factorise à travers le quotient $(G/H, \pi)$.

Propriété universelle du groupe quotient (suite)

Démonstration : En effet, h doit vérifier

$$(\forall u \in G/H)(\forall x \in G) \qquad \pi(x) = u \implies h(u) = f(x),$$

ce qui définit h si et seulement si $\pi(x) = \pi(x') \implies f(x) = f(x')$. Vérifier cette condition et que h est un morphisme (exercice). $\square$

Unicité à isomorphisme (unique) près du groupe quotient

Théorème (unicité à isomorphisme (unique) près de $(G/H, \pi)$)

Si (E, p), où $p : G \to E$ est un morphisme de groupe tel que $Ker(p) = H$, vérifie aussi la propriété universelle, alors il existe un unique isomorphisme $\varphi : G/H \to E$ tel que ce diagramme commute :

$$\begin{tikzcd} G \arrow[r, "p"] \arrow[d, "\pi"'] & E \\ G/H \arrow[ur, dashed, "\varphi"'] & \end{tikzcd}$$

<u>Démonstration</u> :

$$\begin{tikzcd} G \arrow[r, "p"] \arrow[d, "\pi"'] & E \\ G/H \arrow[ur, dashed, "h_1"'] & \end{tikzcd} \quad \begin{tikzcd} G \arrow[r, "\pi"] \arrow[d, "p"'] & G/H \\ E \arrow[ur, dashed, "h_2"'] & \end{tikzcd} \quad \begin{tikzcd} G \arrow[r, "p"] \arrow[d, "p"'] & E \\ E \arrow[ur, dashed, "Id_E = h_1 \circ h_2"'] & \end{tikzcd} \quad \begin{tikzcd} G \arrow[r, "\pi"] \arrow[d, "\pi"'] & G/H \\ G/H \arrow[ur, dashed, "Id_{G/H} = h_2 \circ h_1"'] & \end{tikzcd}$$

$\square$

4. Factorisation des morphismes

Pour tout morphisme de groupe $f : G \to G'$, on a $\mathrm{Ker}(f) \lhd G$.
f se factorise à travers le quotient $(G/\mathrm{Ker}(f), \pi)$ en un isomorphisme :

factorisation canonique

Il existe un unique isomorphisme $\widetilde{f}$ qui rende commutatif le diagramme :

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"'] & G' \\ G/\mathrm{Ker}(f) \arrow[r, "\widetilde{f}"'] & \mathrm{Im}(f) \arrow[u, hook, "i"'] \end{tikzcd}$$

<u>Démonstration</u> : exercice. $\square$

5. Les groupes monogènes

Soit $G =< g >$ un groupe monogène. Considérons le morphisme surjectif

$$\begin{array}{rcl} \varphi : \mathbb{Z} & \longrightarrow & G \\ n & \longmapsto & g^n \end{array}$$

Théorème (caractérisation des groupes monogènes)

On a l'alternative :

1. *Soit $Ker(\varphi) = \{0\}$, et G est isomorphe à $\mathbb{Z}$;*
2. *Soit $Ker(\varphi) = n\mathbb{Z}$ avec $n \in \mathbb{N} \setminus \{0\}$, et G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, et on dit que G est cyclique d'ordre n.*

<u>Démonstration</u> : $\mathrm{Ker}(\varphi)$ est un sous-groupe de $\mathbb{Z}$, et φ se factorise en un isomorphisme selon :

$$\begin{tikzcd} \mathbb{Z} \arrow[r, two heads, "\varphi"] \arrow[d, "\pi"'] & G \\ \mathbb{Z}/n\mathbb{Z} \arrow[ur, dashed, "\widetilde{\varphi}"'] & \end{tikzcd}$$

$\square$

6. Commutativité : centre $Z(G)$, commutateurs et groupe dérivé $D(G)$

Soit $(G, *, e)$ un groupe.

Définition-proposition (centre)

Le centre de G est l'ensemble des éléments de G qui commutent avec tous.

$$Z(G) \stackrel{\text{déf}}{=} \{x \in G \ : \quad (\forall y \in G) \quad x * y = y * x\}$$

$Z(G)$ est un sous-groupe distingué : $Z(G) \lhd G$.

Exercices :

1. $Z(G) = G \iff G$ commutatif.
2. Montrer que $Z(G)$ est invariant par $\mathrm{Aut}(G)$, et en particulier $Z(G) \lhd G$.
3. $Z(\mathfrak{S}_3) = \{1\}$.

commutateurs et groupe dérivé $D(G)$

Soit $(G, *, e)$ un groupe. Ses commutateurs sont ses éléments de la forme :

$$[x, y] \overset{\text{déf}}{=} (x * y) * (y * x)^{-1} = x * y * x^{-1} * y^{-1}$$

On désigne par $S(G)$ l'ensemble des commutateurs de G. En général, $S(G)$ n'est pas un sous-groupe de G, d'où cette définition :

Définition (groupe dérivé)

Le groupe dérivé de G est le sous-groupe engendré par les commutateurs.

$$D(G) \overset{\text{déf}}{=} < S(G) >$$

<u>Exercices</u> :

1. $D(G) = \{e\} \iff G$ commutatif.
2. Montrer que $D(G)$ est invariant par $\mathrm{Aut}(G)$, et donc $D(G) \lhd G$.
3. $D(\mathfrak{S}_3) = \{1; c; c^2\}$.
4. $G/D(G)$ est commutatif.

7. Suite exacte

Soient $(G, *, e)$ un groupe et N un sous-groupe normal : $N \lhd G$. Alors on a :

la suite exacte du groupe quotient :

$$e \longrightarrow N \overset{\lhd}{\hookrightarrow} G \xrightarrow{\pi} G/N \longrightarrow e$$

Définition (suite exacte)

On dit que la suite

$$G_0 \xrightarrow{\varphi_0} G_1 \xrightarrow{\varphi_1} G_2 \xrightarrow{\varphi_2} G_3 \xrightarrow{\varphi_3} G_4 \xrightarrow{\varphi_4} \cdots$$

est exacte si les morphismes φ_k sont tels que :

$$(\forall k = 0, \dots) \qquad \mathrm{Im}(\varphi_k) = \mathrm{Ker}(\varphi_{k+1})$$

(c'est un concentré d'informations ...)

8. Groupes simples

Définition (groupe simple)

Un groupe $(G, *, e)$ est dit simple si $G \neq \{e\}$ et s'il n'a pas d'autre sous-groupe distingué que G et $\{e\}$.

Exercice :
A quelle condition nécessaire et suffisante sur $n \in \mathbb{N}$, le groupe $\mathbb{Z}/n\mathbb{Z}$ est-il simple ?

9. Groupes résolubles

Définition (groupe résoluble)

Un groupe $(G, *, e)$ est dit résoluble s'il possède des sous-groupes distingués $G_0, \ldots, G_n$ tels que :

$$\begin{cases} G = G_0 \rhd \cdots \rhd G_n = \{e\} \\ (\forall k \in [\![0, n-1]\!]) \quad G_k / G_{k+1} \ \ \text{commutatif.} \end{cases}$$

sous-groupes dérivés successifs :

$$D^0(G) \overset{\text{déf}}{=} G, \quad \text{puis :} \quad (\forall n \in \mathbb{N}) \quad D^{n+1}(G) = D(D^n(G))$$

Proposition (1)

$$G \ \textit{résoluble} \iff (\exists n \in \mathbb{N}) \quad D^n(G) = \{e\}$$

Proposition (2)

Soit une suite exacte courte de groupes :

$$\{e\} \xrightarrow{\varphi_0} G_1 \xrightarrow{\varphi_1} G_2 \xrightarrow{\varphi_2} G_3 \xrightarrow{\varphi_3} \{e\}$$

Alors :

$$G_2 \text{ résoluble } \iff G_1 \text{ et } G_2 \text{ résolubles}$$

Corollaire

Si G possède des sous-groupes distingués $G_0, \ldots, G_n$ tels que :

$$\begin{cases} \{e\} = G_0 \lhd \cdots \lhd G_n = G \\ (\forall k \in [\![0, n-1]\!]) \quad G_{k+1}/G_k \text{ résoluble.} \end{cases}$$

alors G est résoluble.

<u>Démonstration</u> : à rédiger. $\square$