1.3 Groupe quotient d'un groupe commutatif

Introduction

Soit G un groupe commutatif et $H \subset G$ un sous-groupe de G.
On appelle $\mathcal{R}$ la relation d'équivalence dans G :

$$x\mathcal{R}y \Longleftrightarrow x^{-1}y \in H \Longleftrightarrow y \in xH$$

G étant commutatif, nous ne privilégions pas la relation à droite ou à gauche.
On appelle $E = G/\mathcal{R}$ l'ensemble quotient de G par $\mathcal{R}$ et nous y définissons une loi de composition :

$$\mathring{x} \times \mathring{y} = \mathring{\widehat{xy}}$$

1.3.1 Proposition

Soit G un groupe commutatif et $H \subset G$ un sous-groupe de G.
Nous considérons $\mathcal{R}$ la relation d'équivalence dans G définie par :

$$x\mathcal{R}y \Longleftrightarrow x^{-1}y \in H \Longleftrightarrow y \in xH$$

et l'opération dans l'ensemble quotient $E = G/\mathcal{R}$ définie, pour tout $\mathring{x} \in G/\mathcal{R}$ et tout $\mathring{y} \in G/\mathcal{R}$ par :

$$\mathring{x} \times \mathring{y} = \mathring{\widehat{xy}}$$

Alors, cette opération est indépendante du choix du représentant

Démonstration

Soient $u \in \mathring{x}$ et $v \in \mathring{y}$; alors $\mathring{u} = \mathring{x}$ et $\mathring{v} = \mathring{y}$.

Il faut donc montrer que $\mathring{\widehat{xy}} = \mathring{\widehat{uv}}$, c'est à dire $uv\mathcal{R}xy$

- ▷ Si $u \in \mathring{x}$, alors $u\mathcal{R}x$ et donc $u \in xH$; de même, comme $v \in \mathring{y}$, alors $v \in yH$
- ▷ Il existe donc $h_1 \in H$ et $h_2 \in H$ tels que $u = xh_1$ et $v = yh_2$ et donc $uv = xyh_1h_2$
- ▷ Comme H est un sous groupe de G, $h_1h_2 \in H$ et donc $uv \in xyH$ et nous avons $uv\mathcal{R}xy$, c'est à dire $\mathring{\widehat{xy}} = \mathring{\widehat{uv}}$

Ce que nous voulions

1.3.2 Théorème

Soit G un groupe commutatif et $H \subset G$ un sous-groupe de G.
Nous considérons l'opération dans l'ensemble quotient $E = G/\mathcal{R}$ définie, pour tout $\mathring{x} \in G/\mathcal{R}$ et tout $\mathring{y} \in G/\mathcal{R}$ par :

$$\mathring{x} \times \mathring{y} = \mathring{\widehat{xy}}$$

Alors

1. $E = G/\mathcal{R}$, muni de cette opération est un groupe commutatif
2. L'application canonique $\varphi : E \longrightarrow G$ définie par :

$$\left\{ \begin{array}{ccc} \varphi : E = G/\mathcal{R} & \longrightarrow & G \\ x & \longmapsto & \varphi(x) = \mathring{x} \end{array} \right.$$

est un homomorphisme de groupe

Le groupe E ainsi défini se note G/H et est appelé groupe quotient de G par H

Démonstration

1. Démontrons que G/H est un groupe commutatif

   $\Rightarrow$ Clairement, puisque $\mathring{x} \times \mathring{y} = \mathring{\widehat{xy}}$, la loi est une loi de composition interne.

   $\Rightarrow$ **La loi est associative**
   En effet, soient $\mathring{x} \in E$, $\mathring{y} \in E$ et $\mathring{z} \in E$; alors :

   $$\mathring{x} \times [\mathring{y} \times \mathring{z}] = \mathring{x} \times \mathring{\widehat{yz}} = \mathring{\widehat{xyz}}$$
   $$[\mathring{x} \times \mathring{y}] \times \mathring{z} = \mathring{\widehat{xy}} \times \mathring{z} = \mathring{\widehat{xyz}}$$

   Nous avons donc $\mathring{x} \times [\mathring{y} \times \mathring{z}] = [\mathring{x} \times \mathring{y}] \times \mathring{z}$ et la loi est associative.

   $\Rightarrow$ **La loi admet un élément neutre**
   Evidemment, si $e \in G$ est le neutre de G, le neutre de l'opération dans G est donné par $\mathring{e}$; en effet :

   $$\mathring{e} \times \mathring{x} = \mathring{\widehat{ex}} = \mathring{x}$$

   $\Rightarrow$ **Chaque élément $\mathring{x} \in E$ admet un inverse**

   Evidemment, nous avons $(\mathring{x})^{-1} = \mathring{\widehat{x^{-1}}}$; en effet :

   $$\mathring{x} \times \mathring{x^{-1}} = \mathring{\widehat{xx^{-1}}} = \mathring{e}$$

   Comme $\mathring{e}$ est l'élément neutre, nous avons bien $(\mathring{x})^{-1} = \mathring{\widehat{x^{-1}}}$

   $\Rightarrow$ **La loi est évidemment commutative**

2. φ est bien un homomorphisme de G sur G/H
   Soient $x \in G$ et $y \in G$, alors :

   $$\varphi(x) \times \varphi(y) = \mathring{x} \times \mathring{y} = \mathring{\widehat{xy}} = \varphi(xy)$$

   φ est donc bien un homomorphisme de G sur G/H

Exemple 3 :

1. $\mathbb{Z}$ est un groupe additif et tous les sous-groupe de $\mathbb{Z}$ est de la forme $a\mathbb{Z}$ où $a \in \mathbb{N}^*$.
   $\mathbb{Z}/a\mathbb{Z}$ est le groupe des entiers modulo a et $\mathbb{Z}/a\mathbb{Z}$ a n éléments. Les représentants canoniques de $\mathbb{Z}/a\mathbb{Z}$ sont les restes $\{0, 1, 2, \cdots, a-1\}$ dans la division par a.
2. $\mathbb{Z}$ est un sous-groupe de $\mathbb{R}$; qu'est ce que le groupe $\mathbb{R}/\mathbb{Z}$?.
   $\mathbb{R}/\mathbb{Z}$ est défini par la relation $x\mathcal{R}y \iff x - y \in \mathbb{Z}$, et tout $x \in \mathbb{R}$, nous avons $x = [x] + (x - [x])$, où $[x]$ désigne la partie entière de x, et donc $(x - [x]) \in [0; +1[$.
   Ainsi, $\mathring{x} = x + \mathbb{Z} = \{\cdots, x-2, x-1, x, x+1, \cdots\}$ et $\mathbb{R}/\mathbb{Z} \simeq [0; +1[$.

   Un exemple d'opération dans $\mathbb{R}/\mathbb{Z}$ est $\mathring{\widehat{1,425}} + \mathring{\widehat{3,730}} = \mathring{\widehat{5,155}} = \mathring{\widehat{0,155}}$

1.3.3 Proposition

Soient G et G' deux groupes ; on suppose G commutatif. Soit $f : G \longrightarrow G'$ un homomorphisme de groupe. Alors, l'application $\overline{f}$:

$$\begin{array}{rcl} \overline{f} : G/\ker f & \longrightarrow & f(G) \\ \mathring{x} & \longmapsto & h(\mathring{x}) = \overline{f}(x) \end{array}$$

est un isomorphisme

Démonstration

Il faut d'abord dire que $f(G)$ *(parfois aussi noté* $\mathrm{Im}f$*)* est un sous-groupe de G' de neutre e'

1. Tout d'abord, $\overline{f}$ est un morphisme. En effet, pour tout $\mathring{x} \in G/\ker f$ et tout $\mathring{y} \in G/\ker f$:
$$\overline{f}(\mathring{x}\mathring{y}) = \overline{f}\left(\mathring{\widehat{xy}}\right) = f(xy) = f(x)\,f(y) = \overline{f}(\mathring{x})\,\overline{f}(\mathring{y})$$
2. Ensuite, $\overline{f}$ est injective :
$$\overline{f}(\mathring{x}) = e' \iff f(x) = e' \iff x \in \ker f \iff x \in \mathring{e} \iff \mathring{x} = \mathring{e}$$
3. Et, pour finir, $\overline{f}$ est surjective :
En effet, soit $y \in f(G)$, il existe $x \in G$ tel que $y = f(x)$, et nous avons donc :
$$\overline{f}(\mathring{x}) = f(x) = y$$
Donc, pour tout $y \in f(G)$, il existe $\mathring{x} \in G/\ker f$ tel que $\overline{f}(\mathring{x}) = y$

1.3.4 Décomposition canonique d'un morphisme $f : G \longrightarrow G'$

Soient G et G' deux groupes ; on suppose G commutatif. Soit $f : G \longrightarrow G'$ un homomorphisme de groupe.
Alors, $f : G \longrightarrow G'$ se décompose de manière canonique en $f = i \circ \overline{f} \circ \varphi$ où :
- φ est la projection canonique $\varphi : G \longrightarrow G/\ker f$
- $\overline{f}$ est l'isomorphisme $\overline{f} : G/\ker f \longrightarrow f(G)$ défini en 1.3.3
- Et $i : f(G) \longrightarrow G'$ est l'application d'insertion

Nous obtenons alors le diagramme suivant :

$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & G' \\ {\scriptstyle\varphi}\downarrow & & \uparrow{\scriptstyle i} \\ G/\ker f & \xrightarrow[\ \overline{f}\ ]{} & f(G) \end{array}$$

Démonstration

1. On considère donc la projection canonique φ :
$$\left\{\begin{array}{ccc} \varphi : G & \longrightarrow & G/\ker f \\ x & \longmapsto & \varphi(x) = \dot{x} \end{array}\right.$$
2. De même, considérons l'insertion i définie par :
$$\left\{\begin{array}{ccc} i : f(G) & \longrightarrow & G' \\ y & \longmapsto & i(y) = y \end{array}\right.$$
C'est l'application identique restreinte à $f(G)$
3. Pour terminer, considérons $\overline{f}$:
$$\begin{array}{ccc} \overline{f} : G/\ker f & \longrightarrow & f(G) \\ \mathring{x} & \longmapsto & \overline{f}(\mathring{x}) = f(x) \end{array}$$
On sait déjà que $\overline{f}$ est un isomorphisme.
4. Alors, pour tout $x \in G$, nous avons $f(x) = i \circ \overline{f} \circ \varphi(x)$. Nous avons donc le diagramme suivant. On dit qu'il est commutatif.
$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & G' \\ {\scriptstyle\varphi}\downarrow & & \uparrow{\scriptstyle i} \\ G/\ker f & \xrightarrow[\ \overline{f}\ ]{} & f(G) \end{array}$$

1.3.5 Théorème

Soit G un groupe quelconque et $x \in G$ un élément de G. Nous notons toujours $\langle x \rangle$ le groupe engendré par x.

1. Si l'ordre de x est infini, alors les puissances de x sont 2 à 2 distinctes et $\langle x \rangle$ est isomorphe à $\mathbb{Z}$
2. Si l'ordre de x est un nombre fini alors $\langle x \rangle$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ où $n \in \mathbb{N}$ et nous avons $x^p = x^q \iff p \equiv q\,[n]$

Démonstration

1. Soit $f : \mathbb{Z} \longrightarrow G$ définie par :
$$\left\{ \begin{array}{ccc} f : \mathbb{Z} & \longrightarrow & G \\ n & \longmapsto & f(n) = x^n \end{array} \right.$$
f est clairement un homomorphisme de groupe de $\mathbb{Z}$ dans G et nous avons $f(\mathbb{Z}) = \langle x \rangle$, et donc, d'après 1.3.3, $\langle x \rangle$ est isomorphe à $\mathbb{Z}/\ker f$.
Remarquons que $\ker f$ est un sous-groupe de $\mathbb{Z}$ et il est donc du type $\ker f = b\mathbb{Z}$ où $b \in \mathbb{N}$
2. Si $\ker f = \{0\}$, alors f est injective et $\mathbb{Z}$ et $\langle x \rangle$ sont isomorphes.
Les puissances de x sont 2 à 2 distinctes.
En effet, supposons qu'il existe 2 entiers $p \in \mathbb{Z}$ et $q \in \mathbb{Z}$ avec $p \neq q$ tels que $x^p = x^q$, alors $x^{p-q} = e$ et donc $p - q \in \ker f$. Or si $p \neq q$, alors $p - q \neq 0$, ce qui contredit le fait que $\ker f = \{0\}$, et donc nous pouvons conclure que les puissances de x sont 2 à 2 distinctes.
3. Si $\ker f \neq \{0\}$ alors, il existe $b \in \mathbb{N}^*$ tel que $\ker f = b\mathbb{Z}$, et alors, toujours d'après 1.3.3, $\langle x \rangle$ est isomorphe à $\mathbb{Z}/b\mathbb{Z}$ et n'a donc que b éléments
Soient 2 entiers $p \in \mathbb{Z}$ et $q \in \mathbb{Z}$ tels que $x^p = x^q$; alors $x^{p-q} = e$ et donc $p - q \in \ker f$, c'est à dire $p - q \in b\mathbb{Z}$ et donc $p \equiv q\,[b]$

1.3.6 Corollaire

Soit G un groupe et $x \in G$
Si x est un élément d'ordre n, alors n est le plus petit entier positif tel que $x^n = e$

Démonstration

On suppose que x est d'ordre n ; nous avons donc Card $(\langle x \rangle) = n$.
Soit $p \in \mathbb{N}$, avec $0 < p < n$ tel que $x^p = e$. En effectuant la division de n par p, nous obtenons $n = kp + r$ où $0 \leqslant r < p$, et donc $x^n = x^{kp+r} = (x^p)^k x^r = e^k x^r = x^r$
Dans ce cas, nous avons alors Card $(\langle x \rangle) = p$, ce qui est contraire à l'hypothèse.
Donc, n est le plus petit entier positif tel que $x^n = e$

1.3.7 Corollaire

Soit G un groupe fini d'ordre n et de neutre e ; alors, pour tout $x \in G$, $x^n = e$

Démonstration

Soit $x \in G$, et on suppose que p est l'ordre de x.
Ceci signifie donc que le cardinal du sous-groupe $\langle x \rangle$ engendré par x est donc p et que $x^p = e$.
D'après le théorème de Lagrange 1.2.2, p est un diviseur de n. Il existe donc $k \in \mathbb{N}$ tel que $n = kp$ d'où :
$$x^n = x^{kp} = (x^p)^k = e^k = e$$
Ce que nous voulions

1.3.8 Corollaire

Tout groupe G d'ordre premier p est cyclique et isomorphe à $\mathbb{Z}/p\mathbb{Z}$

Démonstration

Soit p un nombre premier et G un groupe d'ordre p.
Comme $p \geqslant 2$, il existe $x \in G$ tel que $x \neq e$ et $\langle x \rangle$ est un sous-groupe de G. Card $(\langle x \rangle)$ divisant p, nous avons Card $(\langle x \rangle) = 1$ ou Card $(\langle x \rangle) = p$
Comme nous ne pouvons pas avoir Card $(\langle x \rangle) = 1$, nous avons Card $(\langle x \rangle) = p$, et donc $\langle x \rangle = G$; G est donc cyclique.
$\langle x \rangle = G$ est isomorphe à un $\mathbb{Z}/n\mathbb{Z}$; comme l'ordre de G est p, G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$