1.2 Classes suivant un sous-groupe

Soit G un groupe *(non forcément commutatif)*, dont l'opération est notée multiplicativement, et $H \subset G$ un sous-ensemble de G. Dans cette section nous noterons, pour $x \in G$:

$$xH = \{y \in G \text{ où } y = xh \text{ avec } h \in H\} \text{ et } Hx = \{y \in G \text{ où } y = hx \text{ avec } h \in H\}$$

1.2.1 Théorème

Soient G un groupe noté multiplicativement et $H \subset G$ un sous-groupe de G
Nous considérons la relation ${}_H\mathcal{R}$ suivante :

$$(\forall x \in G)\,(\forall y \in G)\,\big((x{}_H\mathcal{R}y) \Longleftrightarrow (x^{-1}y \in H)\big)$$

1. ${}_H\mathcal{R}$ est une relation d'équivalence
2. La classe d'équivalence $\dot{x}$ d'un élément $x \in G$ est l'ensemble $\dot{x} = xH$
3. L'application φ_x ainsi définie :

$$\begin{cases} \varphi_x : H & \longrightarrow & xH \\ \quad\; h & \longmapsto & \varphi_x(h) = xh \end{cases}$$

   est une bijection

Démonstration

Nous appellerons e l'élément neutre de G

1. ${}_H\mathcal{R}$ est une relation d'équivalence
   → **Elle est réflexive**
   Soit $x \in G$. Avons nous $x{}_H\mathcal{R}x$?
   Nous avons $xx^{-1} = e$; comme H est un sous-groupe de G, $e \in H$ et donc $xx^{-1} \in H$, c'est à dire que nous avons $x{}_H\mathcal{R}x$
   ${}_H\mathcal{R}$ est bien réflexive.
   → **Elle est symétrique**
   Soient $x \in G$ et $y \in G$ tels que $x{}_H\mathcal{R}y$. Avons nous $y{}_H\mathcal{R}x$?
   Nous avons, par définition $(x{}_H\mathcal{R}y) \Longleftrightarrow \left(x^{-1}y \in H\right)$
   Comme H est un sous-groupe, H contient l'inverse de tous ses éléments. Ainsi, si $x^{-1}y \in H$, alors $\left(x^{-1}y\right)^{-1} \in H$.
   Comme $\left(x^{-1}y\right)^{-1} = y^{-1}x$, nous avons donc $y^{-1}x_inH$ et donc $y{}_H\mathcal{R}x$
   ${}_H\mathcal{R}$ est bien symétrique
   → **Elle est transitive**
   Soient $x \in G$, $y \in G$ et $z \in G$ tels que $x{}_H\mathcal{R}y$ et $y{}_H\mathcal{R}z$. Avons nous $x{}_H\mathcal{R}z$?
   Nous avons, par définition $(x{}_H\mathcal{R}y) \Longleftrightarrow \left(x^{-1}y \in H\right)$ et $(y{}_H\mathcal{R}z) \Longleftrightarrow \left(y^{-1}z \in H\right)$
   Comme H est un sous-groupe, la composition déléments de H est interne. Ainsi, si $x^{-1}y \in H$ et $y^{-1}z \in H$, alors $\left(x^{-1}y\right)\left(y^{-1}z\right) \in H$.
   Or, $\left(x^{-1}y\right)\left(y^{-1}z\right) = x^{-1}z$ et donc $x^{-1}z \in H$ d'où $x{}_H\mathcal{R}z$
   ${}_H\mathcal{R}$ est bien transitive
   La relation ${}_H\mathcal{R}$ est bien une relation d'équivalence.
2. La classe d'équivalence $\dot{x}$ d'un élément $x \in G$ est l'ensemble $\dot{x} = xH$
   Soit $y \in \dot{x}$; alors $x^{-1}y \in H$ et donc il existe $h \in H$ tel que $x^{-1}y = h \Longleftrightarrow y = xh$, ce qui veut dire que $y \in xH$. Donc $\dot{x} \subset xH$
   Réciproquement, soit $y \in xH$; il existe $h \in H$ tel que $y = xh$ et donc $x^{-1}y = h \in H$, ce qui veut dire que $x{}_H\mathcal{R}y$ et que $y \in \dot{x}$. Ce qui veut dire que $xH \subset \dot{x}$
   Et donc $xH = \dot{x}$
3. L'application φ_x est bijective

→ **Elle est injective**
Soient $h_1 \in H$ et $h_2 \in H$ tels que $\varphi_x(h_1) = \varphi_x(h_2)$.
Alors $xh_1 = xh_2$ et donc $h_1 = h_2$. φ_x est donc injective
→ **Elle est surjective**
Soit $y \in xH$; il existe alors $h \in H$ tel que $y = xh$, et donc $\varphi_x(h) = y$. φ_x est donc surjective
L'application φ_x est donc bijective.

Remarque 3 :

1. Du théorème 1.2.1 ci-dessus, nous tirons que, si G est d'ordre fini, H l'est aussi et $\operatorname{Card} H = \operatorname{Card} xH$
2. ${}_H\mathcal{R}$ est la **relation d'équivalence à gauche**
3. Nous définirions, et avec des résultats semblables, **une relation d'équivalence à droite** $\mathcal{R}_H$ définie par :
$$(\forall x \in G)\,(\forall y \in G)\,\big((x\mathcal{R}_H y) \Longleftrightarrow \big(xy^{-1} \in H\big)\big)$$
La classe d'équivalence $\dot{x}$ d'un élément $x \in G$ devient alors $\dot{x} = Hx$
4. (a) Les ensembles de la forme xH sont appelés **les classes à gauche**
   (b) Les ensembles de la forme Hx sont appelés **les classes à droite**
   (c) Dans un groupe commutatif, il n'y pas lieu de différencier les classes à gauche ou les classes à droite. On parle alors, plus simplement, **de classes suivant le sous-groupe** H
5. Comme d'habitude, nous notons $G/{}_H\mathcal{R}$ l'ensemble des classes d'équivalence à gauche et $G/\mathcal{R}_H$ l'ensemble des classes d'équivalences à droite. On note souvent :
$$G/{}_H\mathcal{R} = (G/H)_g \text{ et } G/\mathcal{R}_H = (G/H)_d$$
6. Il est clair que si G est un groupe commutatif, alors ${}_H\mathcal{R} = \mathcal{R}_H = \mathcal{R}$; l'ensemble des classes d'équivalence est noté G/H
7. Il est aussi très facile de démontrer que $\dot{e} = H$
8. Il est clair, aussi, que nous avons, la plupart du temps $xH \neq Hx$

Exemple 2 :

1. Si $H = G$, il n'y a qu'une seule classe d'équivalence et $(G/H)_g = (G/H)_d = G$
2. Autre exemple si $H = \{e\}$, alors la relation $\mathcal{R}_H$ devient
$$(x\mathcal{R}_H y) \Longleftrightarrow \big(xy^{-1} = e\big) \Longleftrightarrow (x = y)$$
C'est à dire que la relation $\mathcal{R}_H$ est la relation d'égalité ; il en est de même de ${}_H\mathcal{R}$
3. l'exemple le plus canonique est celui du groupe additif $(\mathbb{Z}, +)$ des nombres relatifs. Tous les sous-groupes de $(\mathbb{Z}, +)$ sont du type $n\mathbb{Z}$ avec $n \in \mathbb{N}^*$.
La relation $\mathcal{R}$ définie par $x\mathcal{R}y \Longleftrightarrow x-y \in n\mathbb{Z}$ est la relation de congruence. La classe d'équivalence d'un entier $x \in \mathbb{Z}$ est donnée par $\dot{x} = x + n\mathbb{Z} = \{\cdots x - 2n, x_n, x, x + n, x + 2n, \cdots x + kn\}$

Exercice 16 :

Nous considérons $(\mathbb{C}^*, \times)$ le groupe multiplicatif des nombres complexes et $\mathcal{U}$ le sous-groupe des nombres complexes de module 1. Quelles sont les classes d'équivalence modulo $\mathcal{U}$?

Exercice 17 :

Soit G un groupe cyclique d'ordre 12. Montrer qu'il existe un sous-groupe H d'ordre 4 et un seul. Déterminer alors l'ensemble des classes à gauche G/H.

1.2.2 Le théorème de Lagrange

Soit G un groupe fini et $H \subset G$, un sous-groupe de G
Alors, l'ordre de H divise l'ordre de G

Démonstration

L'opération interne du groupe G est notée multiplicativement.
Soit ${}_H\mathcal{R}$ la relation d'équivalence à gauche modulo le sous-groupe H. Les classes d'équivalence $xH \in (G/H)_g$ forment une partition de G. D'après 1.2.1, toutes ces classes d'équivalence ont le même nombre d'éléments que H.
Comme $G = \bigcap\limits_{x\in G} xH$, nous avons $\operatorname{Card} G = \sum\limits_{x\in G} \operatorname{Card} H$, c'est à dire $\operatorname{Card} G = p\operatorname{Card} H$
Ce que nous voulions

Remarque 4 :

On dit souvent :

Dans un groupe fini, l'ordre d'un sous-groupe divise l'ordre du groupe

1.2.3 Corollaire

Dans un groupe G d'ordre p nombre premier, les seuls sous-groupes sont G et $\{e\}$

Démonstration

La démonstration est simple.
Si $H \subset G$ est un sous-groupe de G, alors $\operatorname{Card} H$ est un nombre qui divise p. Ainsi, $\operatorname{Card} H = 1$ ou $\operatorname{Card} H = p$, c'est à dire $H = G$ ou $H = \{e\}$

Exercice 18 :

Montrer qu'un groupe fini d'ordre un nombre p premier est cyclique *(et donc commutatif)*.

Exercice 19 :

Soient S_1 et S_2 deux sous-groupes finis d'un groupe G d'ordres respectifs n_1 et n_2. Montrer que si n_1 est premier avec n_2 alors $S_1 \cap S_2 = \{e\}$.

Exercice 20 :

Montrer que si deux éléments d'un groupe ont des ordres finis premiers entre eux, l'intersection des sous-groupes qu'ils engendrent est réduite au singleton $\{e\}$.