CHAPITRE 13

GROUPES

Faire de l'Algèbre, c'est essentiellement *calculer*, c'est-à-dire effectuer, sur des éléments d'un ensemble, des « opérations algébriques », dont l'exemple le plus connu est fourni par les «quatre règles» de l'arithmétique élémentaire.

La notion d'opération algébrique, d'abord restreinte aux entiers naturels et aux grandeurs mesurables, a peu à peu élargi son domaine, à mesure que se généralisait parallèlement la notion de «nombre», jusqu'à ce que, dépassant cette dernière, elle en vînt à s'appliquer à des éléments qui n'avaient plus aucun caractère «numérique». C'est sans doute la possibilité de ces extensions successives, dans lesquelles la *forme* des calculs restait la même, alors que la *nature* des êtres mathématiques soumis à ces calculs variait considérablement, qui a permis de dégager peu à peu le principe directeur des mathématiques modernes, à savoir que les êtres mathématiques, en eux-mêmes, importent peu : ce qui compte, ce sont leurs relations.

On peut considérer Évariste Galois comme le véritable initiateur de la théorie des groupes. Les première traces de ses travaux remontent à 1832 et ne furent publiés qu'après sa mort, en 1846. Il cherchait alors à prouver que les équations polynômiales de degré ≥ 5 à coefficients complexes ne pouvaient être résolues par radicaux. Pour ce faire, il s'intéressa à un groupe relié aux racines de l'équation considérée. Son génie consista à comprendre que les difficultés pour résoudre l'équation ne provenaient pas de son degré mais des propriétés de ce groupe.

Les mathématiciens ont compris depuis que les groupes interviennent dans de nombreux domaines. L'ensemble des isométries de l'espace ou du plan est un groupe appelé groupe orthogonal. L'ensemble des isométries préservant un objet donné a une structure de groupe. L'ensemble des transformations qui, en relativité restreinte, permettent de changer de référentiel galiléen tout en préservant les lois de la physique et la vitesse de la lumière forment un groupe appelé groupe de Lorenz. En chimie, les symétries des molécules permettent

de leur associer des groupes qui aident à comprendre mieux leurs propriétés. Plus concrètement encore, l'ensemble des manipulations qu'on peut effectuer sur un Rubik's cube a lui aussi une structure de groupe. L'étude de ce groupe permet de mettre en place des stratégies gagnantes pour le reconstituer.

13.1 LOI DE COMPOSITION

§1 Loi de composition ; associativité ; commutativité

Définition 1

Soit E un ensemble. On appelle **loi de composition interne** sur E une application

$$\top : E \times E \to E.$$

La valeur $\top(x, y)$ de $\top$ pour un couple $(x, y) \in E \times E$ s'appelle le **composé** de x et de y pour cette loi.

Le composé de x et de y se note le plus souvent en écrivant x et y dans un ordre déterminé et en les séparant par un signe caractéristique de la loi envisagée (signe qu'on pourra convenir d'omettre). L'écriture $x \top y$ au lieu de $\top(x, y)$ est traditionnelle et appelée **notation infixe**. Parmi les signes dont l'emploi est le plus fréquent, citons $+$ et $.$, étant convenu en général que ce dernier peut s'omettre à volonté ; avec ces signes, le composé de x et y s'écrira respectivement $x + y$, et $x.y$ ou xy. Une loi notée par le signe $+$ s'appelle le plus souvent **addition** (le composé $x + y$ s'appelant alors la **somme** de x et de y) et on dit qu'elle est **notée additivement** ; une loi notée par le signe $.$ s'appelle le plus souvent **multiplication** (le composé $x.y = xy$ s'appelant alors **produit** de x et de y), et on dit qu'elle est **notée multiplicativement**. Dans les raisonnements généraux des paragraphes 13.1 et 13.2 du présent chapitre, on se servira ordinairement des signes «étoile» $\star$ et «truc» $\top$ pour noter des lois de composition quelconques.

Exemples 2

1. Les applications $(X, Y) \mapsto X \cup Y$ et $(X, Y) \mapsto X \cap Y$ sont des lois de composition sur l'ensemble des parties d'un ensemble E.
2. Dans l'ensemble $\mathbb{N}$ des entiers naturels, l'addition, la multiplication, l'exponentiation sont des lois de composition interne (les composés de $x \in \mathbb{N}$ et $y \in \mathbb{N}$ pour ces lois se notant respectivement $x + y$, xy ou $x.y$, et x^y).
3. La soustraction n'est pas une loi de composition interne sur $\mathbb{N}$ puisque $3 - 7$ n'existe pas. Mais c'est une loi de composition interne dans $\mathbb{Z}$.

Définition 3

Soit une loi de composition interne $(x, y) \mapsto x \star y$ sur un ensemble E.
On dit que $\star$ est **associative** si

$$\forall (x, y, z) \in E^3, (x \star y) \star z = x \star (y \star z).$$

Définition 4

- On dit que deux éléments x et y **commutent** (ou sont **permutables**) si
$$y \star x = x \star y.$$
- On dit que $\star$ est **commutative** si deux éléments quelconques de E commutent pour cette loi, c'est-à-dire si
$$\forall (x, y) \in E^2, y \star x = x \star y.$$

Exemple 5

La soustraction n'est pas associative dans $\mathbb{Z}$ car $7 - (3 - 1) \neq (7 - 3) - 1$ et n'est pas commutative car $8 - 4 \neq 4 - 8$.

Exemple 6

La composition des applications est une loi associative, mais en général non commutative dans l'ensemble $\mathcal{F}(E, E)$.
Par exemple, si $f, g : \mathbb{R} \to \mathbb{R}$ sont définies par $f(x) = x + 1$ et $g(x) = x^2$, alors $(g \circ f)(x) = (x + 1)^2$ et $(f \circ g)(x) = x^2 + 1$. Ces deux applications sont bien différentes car elles ne prennent pas la même valeur en 1.

Exemple 7

Quelles sont les propriétés de la loi $x \star y = \frac{x+y}{2}$ dans $\mathbb{R}$?
La loi $\star$ est commutative, non associative car $4 \star (4 \star 8) = 5$ et $(4 \star 4) \star 8 = 6$.

§2 Élément neutre ; éléments symétrisables

Définition 8

Soit une loi de composition interne $(x, y) \mapsto x \star y$ sur un ensemble E. Un élément e de E est dit **élément neutre** si
$$\forall x \in E, e \star x = x \star e = x.$$

Il existe au plus un élément neutre pour une loi donnée $\star$, car si e et e' sont éléments neutres, on a $e = e \star e' = e'$.

Exemple 9

L'application Id_E est l'élément neutre de la loi de composition $\circ$ dans $\mathcal{F}(E, E)$.

Exemple 10

La loi $x \star y = \frac{x+y}{2}$ dans $\mathbb{R}$ possède-t-elle un élément neutre?
La loi $\star$ n'admet pas d'élément neutre puisque $x \star e = x$ n'est réalisé que pour $e = x$, valeur qui dépend de x.

Définition 11

Soient une loi de composition interne $(x, y) \mapsto x \star y$ sur un ensemble E possédant un élément neutre e et x et x' deux éléments de E.

- On dit que x' est **symétrique** de x pour $\star$ si l'on a $x' \star x = x \star x' = e$.
- On dit qu'un élément x de E est **symétrisable** s'il possède un symétrique.

§3 Partie stable ; loi induite

Définition 12

Une partie A d'un ensemble E est dite **stable** pour un loi de composition interne $\star$ sur E si le composé de deux éléments de A appartient à A :

$$\forall (x,y) \in A^2, x \star y \in A.$$

L'application $(x,y) \mapsto x \star y$ de $A \times A$ dans A s'appelle alors la **loi induite** sur A par la loi $\star$.

§4 Loi interne sur $\mathcal{P}(E)$ déduite d'une loi interne définie sur E

Soit $\varphi : \begin{array}{ccc} E \times E & \to & E \\ (x,y) & \mapsto & x \star y \end{array}$ une loi de composition interne sur un ensemble E.
Cette loi induit une loi de composition interne sur $\mathcal{P}(E)$ définie par

$$\begin{array}{ccc} \mathcal{P}(E) \times \mathcal{P}(E) & \to & \mathcal{P}(E) \\ (A,B) & \mapsto & \{\, x \star y \mid x \in A \text{ et } y \in B \,\} \end{array}.$$

Pourvu que cette notation ne prête pas à confusion[1], on note encore $A \star B$ l'ensemble des éléments $x \star y$ de E tels que $x \in A$ et $y \in B$ (autrement dit, l'image directe de $A \times B$ par l'application $\varphi : E \to E, (x,y) \mapsto x \star y$).

$$A \star B = \{\, x \star y \mid x \in A \text{ et } y \in B \,\}$$

d'où l'équivalence

$$u \in A \star B \iff \exists (x,y) \in A \times B, u = x \star y.$$

Si $a \in E$, on écrit généralement $a \star B$ au lieu de $\{ a \} \star B$, et $A \star a$ au lieu de $A \star \{ a \}$.

Exemple 13

L'addition sur $\mathbb{Z}$ induit une loi de composition interne sur $\mathcal{P}(\mathbb{Z})$, par exemple

$$\{ 3,7,10 \} + \{ 1,5,8 \} = \{ 4,8,11,12,15,18 \},$$
$$10 + \{ 1,5,8 \} = \{ 11,15,18 \},$$
$$\mathbb{Z} + \mathbb{Z} = \mathbb{Z}.$$

De même, la multiplication sur $\mathbb{Z}$ induit une loi de composition interne sur $\mathcal{P}(\mathbb{Z})$, par exemple

$$\{ 3,7,10 \}\{ 1,5,8 \} = \{ 3,7,10,15,24,35,50,56,80 \},$$
$$10\{ 1,5,8 \} = \{ 10,50,80 \},$$
$$2\mathbb{Z} = \{ \ldots, -8, -6, -4, -2, 0, 2, 4, 6, 8, \ldots \}$$

[1] Par exemple, si $\times$ désigne une multiplication, $A \times B$ désigne déjà le produit cartésien. On écrira alors plutôt $AB = \{ xy \mid x \in A \text{ et } y \in B \}$.

§5 Loi interne définie sur $\mathscr{F}(X, E)$ déduite d'une loi interne sur E

X étant un ensemble quelconque et E un ensemble muni d'une loi de composition interne $\star$, considérons deux applications f et g de X dans E, c'est-à-dire deux éléments de $\mathscr{F}(X, E)$; on désignera par $f \star g$ l'application définie par

$$\begin{array}{rccc} f \star g : & X & \to & E \\ & x & \mapsto & f(x) \star g(x) \end{array} .$$

On dit que $f \star g$ est définie ponctuellement. On voit que si $\star$ est associative et commutative sur E, il en est de même sur $\mathscr{F}(X, E)$. Si $\star$ possède un élément neutre e, la fonction constante prenant cette valeur e pour tout x de E est élément neutre pour la loi sur $\mathscr{F}(X, E)$.

Exemple 14

Soit $X = E = \mathbb{R}$, pour $f, g, s, p \in \mathscr{F}(\mathbb{R}, \mathbb{R})$, on aura

$$\begin{aligned} s = f + g &\iff \forall x \in \mathbb{R}, s(x) = f(x) + g(x); \\ p = fg &\iff \forall x \in \mathbb{R}, p(x) = f(x)g(x). \end{aligned}$$

Les applications s et p sont respectivement la somme et le produit des deux fonctions f et g.

13.2 La structure de groupe

§1 Groupes

Définition 15

On appelle **groupe** un couple formé d'un ensemble G et d'une loi de composition interne $\star$ sur l'ensemble G associative, possédant un élément neutre et pour laquelle tout élément est symétrisable. Autrement dit,

- $\forall (x, y, z) \in G^3, x \star (y \star z) = (x \star y) \star z$.
- $\exists e_G \in G, \forall x \in G, e_G \star x = x \star e_G = x$.
- $\forall x \in G, \exists x' \in G, x \star x' = x' \star x = e_G$.

Si de plus la loi $\star$ est commutative, on dit que le groupe est **commutatif** ou **abélien**.

Le cardinal d'un groupe fini est généralement appelé son **ordre**, noté $|G|$.

Proposition 16

Soit $(G, \star)$ un groupe. Alors

1. *G est non-vide : il contient au moins son élément neutre.*
2. *L'élément neutre de G est unique.*
3. *Le symétrique de tout élément de G est unique.*

Remarque

- Pour définir un groupe, il ne suffit pas de se donner un ensemble G ; il faut aussi se donner une loi de composition interne sur l'ensemble G vérifiant les conditions ci-dessus ; néanmoins, on

désigne toujours un groupe par la même lettre, G par exemple, que l'ensemble qui en constitue l'une des données.[2]

- On peut noter la loi de composition d'un groupe avec à peu près n'importe quel symbole ($+, ., \times, \cup, \cap, \vee, \wedge, \top, \bot, *, \star, \circ, \oplus, \otimes, \odot, \dots$). Mais par habitude, on réserve le symbole $+$ pour des lois commutatives. En revanche, beaucoup de lois commutatives ne sont pas notées $+$.

Exemples 17

1. Munis de la multiplication usuelle, $(\mathbb{Q}^\star, \cdot), (\mathbb{R}^\star, \cdot), (\mathbb{R}_+^\star, \cdot), (\mathbb{C}^\star, \cdot)$ sont des groupes commutatifs. L'élément neutre est 1.
2. Munis de l'addition usuelle, $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ sont des groupes commutatifs. L'élément neutre est 0 et le symétrique de x est $-x$. En revanche, $(\mathbb{N}, +)$ n'est pas un groupe car si $n \in \mathbb{N}$ est strictement positif, il n'a pas de symétrique pour $+$.

Exemple 18

L'ensemble des similitudes directes du plan est un groupe (non commutatif) pour la composition $\circ$. En prenant l'écriture analytique complexe $z \mapsto az + b$ avec $a \in \mathbb{C}^\star$ et $b \in \mathbb{C}$, l'élément neutre est l'identité $z \mapsto z$ et le symétrique de $z \mapsto az + b$ est $z \mapsto \frac{1}{a}z - \frac{b}{a}$.

Exemple 19

Pour $n \in \mathbb{N}^\star$, $\left(\mathbb{U}_n, \cdot\right)$ est un groupe fini d'ordre n.

Notation

Fréquemment, on appelle produit la loi de composition interne du groupe G. On note le produit comme une multiplication et donc sans aucun symbole $(x, y) \mapsto xy$.

On emploie le mot **inverse** au lieu du mot symétrique, et le mot **inversible** au lieu du mot symétrisable. L'inverse de x se note alors généralement

$$x^{-1}.$$

Parfois l'élément neutre e_G se note 1 (ou 1_G) et s'appelle **élément unité** (ou **unité**).

Proposition 20

Soit $(G, \star)$ un groupe. Alors, pour tous $x, y \in G$

$$\left(x^{-1}\right)^{-1} = x \quad \text{et} \quad (x \star y)^{-1} = y^{-1} \star x^{-1}.$$

Proposition 21

Soit $(G, \star)$ un groupe. Pour tous $a, b, x \in G$,

$$\left(a \star x = b \iff x = a^{-1} \star b\right) \quad \text{et} \quad \left(x \star a = b \iff x = b \star a^{-1}\right).$$

En particulier, on a les implications

$$(a \star x = a \star y \implies x = y) \quad \text{et} \quad (x \star a = y \star a \implies x = y).$$

[2] On prendra soin de *ne pas* dire qu'un groupe «est un ensemble G sur lequel *il existe* une loi de composition interne vérifiant...» car on peut facilement démontrer que, sur tout ensemble, il existe une telle loi de composition interne, et même qu'on peut en construire une infinité pour peu que l'ensemble donné soit lui-même infini ; en disant qu'un groupe est «un ensemble sur lequel il existe» une loi de composition interne, on ne dit donc rien d'autre que ceci : «un groupe est un ensemble» — définition dont la stupidité est particulièrement claire...

Quand on déduit l'égalité $x = y$ de l'égalité $a \star x = a \star y$, on dit que l'on **simplifie à gauche** par a ; si on la déduit de $x \star a = y \star a$, on dit que l'on **simplifie à droite** par a. Si le groupe est commutatif, on se contente de dire que l'on **simplifie** par a.

Notation

Supposons la loi de composition interne commutative notée $(x, y) \mapsto x + y$, comme une addition.

L'élément neutre se note souvent 0 (ou 0_G) et s'appelle **zéro** ou **élément nul** (ou parfois **origine**).

La définition de groupe se traduit comme suit:

- $\forall (x, y, z) \in G^3, x + (y + z) = (x + y) + z$.
- $\exists 0_G \in G, \forall x \in G, 0_G + x = x + 0_G = x$.
- $\forall x \in G, \exists x' \in G, x + x' = x' + x = 0_G$.

À laquelle il faut rajouter la commutativité

- $\forall (x, y) \in G^2, x + y = y + x$.

On dit **opposé** au lieu de symétrique, et on note l'opposé de x

$$-x$$

L'équation

$$a + x = b$$

possède une et une seule solution à savoir

$$x = b + (-a)$$

que l'on écrit d'ailleurs

$$x = b - a.$$

Convention Nous conviendrons qu'une loi notée additivement est toujours associative et commutative.

§2 Itérés, puissances, multiples

Notation

Supposons la loi de composition interne notée $(x, y) \mapsto x \star y$, Dans ce cas, étant donnés des éléments $x_1, x_2, \ldots, x_n$ de G, on pose par définition

$$\bigstar_{i=1}^{n} x_i = x_1 \star x_2 \star \cdots \star x_n = \left(x_1 \star x_2 \star \cdots \star x_{n-1}\right) \star x_n$$

(récurrence sur n), et on a alors la relation pour tout entier p tel que $1 \leq p \leq n$,

$$x_1 \star x_2 \star \cdots \star x_n = \left(x_1 \star x_2 \star \cdots \star x_p\right) \star \left(x_{p+1} \star x_2 \star \cdots \star x_n\right)$$

Lorsque la loi de composition interne est notée comme une multiplication, on écrit

$$\prod_{i=1}^{n} x_i = x_1 \cdots x_n.$$

Lorsque la loi de composition interne est notée comme une addition, on écrit

$$\sum_{i=1}^{n} x_i = x_1 + \cdots + x_n.$$

Définition 22

Soit $(G, \star)$ un groupe, d'élément neutre e_G et $x \in G$. On définit les **puissances entières** de x de la manière suivante:

- On pose $x^0 = e_G$.
- Pour tout $n \in \mathbb{N}^\star$, on pose $x^n = x \star x^{n-1}$, c'est-à-dire

$$x^n = x \star x \star \cdots \star x \quad (n \text{ facteurs}).$$

- Pour tout $n \in \mathbb{N}^\star$, on pose $x^{-n} = \left(x^{-1}\right)^n$.

L'élément x^n est donc bien un élément du groupe $(G, \star)$.

À l'aide de l'associativité de la multiplication dans G, on vérifie facilement les règles de calculs suivantes.

Proposition 23

Pour tout $x \in G$ et tout $(p, q) \in \mathbb{Z}^2$,

$$x^p x^q = x^{p+q} \quad \text{et} \quad (x^p)^{-1} = x^{-p} \quad \text{et} \quad (x^p)^q = x^{pq}.$$

Notation

Lorsqu'une loi de groupe sur G est noté $+$ ayant pour élément neutre 0_G, on note à la place

- $0 \cdot x = 0_G$,
- Si $n \in \mathbb{N}^\star$, $n \cdot x = x + x + \cdots + x$ (n facteurs),
- et $(-n) \cdot x = n \cdot (-x)$ si n est un entier négatif.

On dit que les nx sont les **multiples entiers** de x. On retrouve les formules

$$px + qx = (p+q)x \quad \text{et} \quad -(px) = (-p)x \quad \text{et} \quad p(qx) = (pq)x.$$

On a aussi la relation

$$px + py = p(x+y).$$

Remarque

Dans un groupe quelconque G (donc noté multiplicativement), la formule analogue

$$x^p y^p = (xy)^p$$

est fausse en général. Par exemple

$$(xy)^2 = xyxy \neq xxyy = x^2 y^2,$$

sauf si x et y commutent.

§3 Groupe produit

Théorème 24

Soient deux groupes $(G_1, \top)$ et $(G_2, \bot)$. On définit une loi $\star$ sur $G = G_1 \times G_2$ par

$$(x_1, x_2) \star (y_1, y_2) = (x_1 \top y_1, x_2 \bot y_2).$$

1. *La loi $\star$ confère à $G_1 \times G_2$ une structure de groupe appelé **produit direct des groupes** $(G_1, \top)$ et $(G_2, \bot)$.*
2. *Le produit de deux groupes commutatifs est un groupe commutatif.*

De manière analogue, on peut définir le produit direct $G = G_1 \times \cdots \times G_n$ de n groupes $G_1, \ldots, G_n$.

13.3 Sous-groupes

§1 Sous-groupes d'un groupe

Définition 25

Soit $(G, \star)$ un groupe. On appelle **sous-groupe** de G une partie H de G possédant les propriétés suivantes

1. L'élément neutre de G appartient à H
$$e_G \in H;$$
2. H est stable pour $\star$, c'est-à-dire
$$\forall (x, y) \in H^2, x \star y \in H;$$
3. H est **stable par passage à l'inverse**, c'est-à-dire
$$\forall x \in H, x^{-1} \in H.$$

Proposition 26

Soit $(G, \star)$ un groupe et H une partie de G. Alors H est un sous-groupe de G si, et seulement si

$$H \neq \emptyset \quad \text{et} \quad \forall (x, y) \in H^2, x \star y^{-1} \in H.$$

Proposition 27

1. *Soient $(G, \star)$ un groupe et H un sous-groupe de G. Alors $(H, \star)$ est lui-même un groupe pour la loi de composition induite sur H par la loi de composition de G:*
$$\begin{array}{ccc} H \times H & \to & H \\ (x, y) & \mapsto & x \star y \end{array}.$$
2. *Réciproquement, si H est une partie du groupe G telle que $(H, \star)$ est un groupe, alors H est un sous-groupe de G.*

Dans la pratique, pour montrer qu'un ensemble H est un groupe, il peut être plus facile de montrer que c'est un sous-groupe d'un groupe connu.

Remarque

Pour montrer que H est un sous-groupe

Si $(G, \star)$ est un groupe et H une partie de G, vérifier que H est un sous-groupe de G consiste à vérifier des propriétés d'*appartenance*. Il faut vérifier que l'élément neutre e *appartient* à H, pas que $e \star x = x \star e = x$ pour tout $x \in H$. En effet cette dernière propriété est évidente, vu que G est un groupe et que tout élément de H appartient à G. De même, si $x, y \in H$, c'est x^{-1} *appartient* à H et $x \star y$ *appartient* à H qu'il faut vérifier.

Exemples 28

1. Si $(G, \star)$ est un groupe d'élément neutre e, alors $\{ e \}$ est un sous-groupe de G. De même, G est un sous-groupe de G. Le sous-groupe $\{ e \}$ est appelé **sous-groupe trivial** de G.
2. Tout sous-groupe de G, distinct de $\{ e \}$ et G est appelé **sous-groupe propre** de G.
3. Chacun des groupes $(\mathbb{Q}^\star, .), (\mathbb{R}^\star, .), (\mathbb{C}^\star, .)$ est un sous-groupe de tous les suivants.
4. L'ensemble $\mathbb{U}$ des nombres complexes de module un est un sous-groupe de $\mathbb{C}^\star$. En effet, 1 est de module un ($1 \in \mathbb{U}$), si z est de module un, alors $1/z$ est de module un (car $|1/z| = 1/|z|$), et si z, w sont de module un, alors zw aussi (car $|zw| = |z|\,|w|$).
5. La géométrie élémentaire fournit de nombreux exemples de sous-groupes du groupe des permutations : le groupe des translations sur la droite, ou dans le plan, ou dans l'espace ; le groupe des rotations autour d'un point dans le plan ou dans l'espace ; le groupe des déplacements dans le plan, ou dans l'espace ; le groupe des homothéties de centre donné et de rapport *non nul* dans le plan ou dans l'espace, etc, etc,...

Remarque

En notation additive, une partie H d'un groupe $(G, +)$ est un sous-groupe de G si, et seulement si

- $0_G \in H$,
- $\forall (x, y) \in H^2, x + y \in H$,
- $\forall x \in H, -x \in H$.

Ou encore, de manière équivalente

$$H \neq \emptyset \quad \text{et} \quad \forall (x, y) \in H^2, x - y \in H.$$

Exemples 29

1. Chacun des groupe $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ est un sous-groupe de tous les suivants.
2. $\mathbb{R}_+^*$ est un sous-groupe de $(\mathbb{R}^*, .)$ mais n'est pas un sous-groupe de $(\mathbb{R}, +)$.

§2 Sous-groupes de $(\mathbb{Z}, +)$

Théorème 30 *Pour $a \in \mathbb{Z}$, l'ensemble*

$$a\mathbb{Z} = \{\, ka \mid k \in \mathbb{Z} \,\}$$

est un sous-groupe de $(\mathbb{Z}, +)$.

Démonstration. En effet, $a\mathbb{Z} \neq \emptyset$ car $0 \in a\mathbb{Z}$.

Soient $x, y \in a\mathbb{Z}$. Il existe donc $x', y' \in \mathbb{Z}$ tel que $x = ax'$ et $y = ay'$. On a donc

$$x - y = (ax') - (ay') = a\left(x' - y'\right) \text{ et } x' - y' \in \mathbb{Z},$$

c'est-à-dire, $x - y \in a\mathbb{Z}$.

∎

Réciproquement,

Théorème 31 *Soit H un sous-groupe de de $(\mathbb{Z}, +)$. Il existe un entier $a \geq 0$ et un seul tel que $H = a\mathbb{Z}$.*

Démonstration.

- Si $H = \{\, 0 \,\}$, on a $H = 0\mathbb{Z}$.
- Supposons $H \neq \{\, 0 \,\}$. Le sous-groupe H possède un élément $x \neq 0$. On a $x > 0$ ou $-x > 0$, et par suite H possède des éléments > 0. Posons

  $$a = \min\left(H \cap \mathbb{N}^\star\right)$$

  le plus petit élément > 0 de H.
- Le sous-groupe H contient a, donc il contient tous les itérés (les multiples) de a:

  $$\forall k \in \mathbb{Z}, ka \in H.$$

  Autrement dit, on a l'inclusion

  $$a\mathbb{Z} \subset H.$$
- Montrons $H \subset a\mathbb{Z}$. Soit $y \in H$. Effectuons la division euclidienne de y par a : il existe des entiers q et r tels que $y = aq + r$ et $0 \leq r < a$. On a donc

  $$r = y - aq \in H$$

  car y et aq appartiennent au sous-groupe H. Mais ceci n'est possible que si $r = 0$ par définition de a, et par suite $y \in a\mathbb{Z}$.

∎

§3 Intersection de sous-groupes

Proposition 32 *Soient $(G, \star)$ un groupe, H et K deux sous-groupes de G. Alors $H \cap K$ est un sous-groupe de G.*

Cette proposition se généralise à une intersection quelconque de sous-groupes d'un groupe G.

Théorème 33 *Soit $(H_i)_{i\in I}$ une famille de sous-groupes d'un groupe $(G, \star)$. Alors l'intersection des H_i,*

$$H = \bigcap_{i\in I} H_i$$

est encore un sous-groupe de $(G, \star)$.

§4 Sous-groupes d'un groupe fini

Théorème 34 **Théorème de Lagrange**
Soit G un groupe fini et H un sous-groupe de G. Alors l'ordre de H divise l'ordre de G.

Démonstration. En exercice. ∎

13.4 Morphismes de groupes

§1 Définitions

Définition 35 Soit $(G, \star)$ et $(H, \top)$ deux groupes. On appelle **morphisme de groupes** ou **homomorphisme de groupes** une application $f : G \to H$ telle que

$$\forall (x, y) \in G^2, f(x \star y) = f(x) \top f(y).$$

- Lorsque l'application f est bijective, on dit que f est un **isomorphisme de groupes**.
- Lorsque $G = H$, on dit que f est un **endomorphisme** de G.
- Lorsque $G = H$ et que f est bijectif, on dit que f est un **automorphisme** de G.

Définition 36 S'il existe un isomorphisme de $(G, \star)$ dans $(H, \top)$, on dit que $(G, \star)$ et $(H, \top)$ sont **isomorphes**.

Exemples 37

1. $\begin{array}{ccccc} (\mathbb{R}_+^\star, .) & \to & (\mathbb{R}, +) \\ x & \mapsto & \ln x \end{array}$ est un isomorphisme de groupes.

2. $\begin{array}{ccc}(\mathbb{C},+) & \to & (\mathbb{C},+) \\ z & \mapsto & \bar{z}\end{array}$ est un automorphisme de groupes.

3. $\begin{array}{ccc}(\mathbb{Z},+) & \to & (\mathbb{R}_+^\star,.) \\ n & \mapsto & 5^n\end{array}$ est un morphisme de groupes non-surjectif.

4. $\begin{array}{ccc}(\mathbb{Z},+) & \to & (\{-1,1\},.) \\ n & \mapsto & (-1)^n\end{array}$ est un morphisme de groupes non-injectif.

Exemple 38

L'application

$$\begin{array}{ccc}\mathcal{P}(E) & \to & \mathcal{P}(E) \\ A & \mapsto & \complement_E A\end{array}$$

est un isomorphisme de $(\mathcal{P}(E),\cap)$ dans $(\mathcal{P}(E),\cup)$ et également un isomorphisme de $(\mathcal{P}(E),\cup)$ dans $(\mathcal{P}(E),\cap)$ (loi de Morgan). Ce n'est cependant pas un automorphisme car la loi n'est pas la même au départ et à l'arrivée.

Proposition 39

Soit f un morphisme du groupe G dans le groupe H. Alors

1. $f(e_G) = e_H$.
2. $\forall x \in G, f\left(x^{-1}\right) = (f(x))^{-1}$.
3. $\forall x \in G, \forall n \in \mathbb{Z}, f\left(x^n\right) = (f(x))^n$.

Démonstration.

1. On a $f(e_G) = f(e_G e_G) = f(e_G)f(e_G)$ d'où $e_H = f(e_G)$ en simplifiant par $f(e_G)$.

2. Soit $x \in G$. On a

$$f(x)f\left(x^{-1}\right) = f(xx^{-1}) = f(e_G) = e_H$$
$$\text{et } f\left(x^{-1}\right)f(x) = f(x^{-1}x) = f(e_G) = e_H$$

D'où $f(x)^{-1} = f\left(x\right)^{-1}$.

3. Soit $x \in G$. Pour $n = 0$, la propriété s'écrit $f(x^0) = f(x)^0$, c'est-à-dire $f(e_G) = e_H$ et est vraie pour d'après 1. Soit $n \in \mathbb{N}$ tel que $f(x^n) = (f(x))^n$. Alors

$$f(x^{n+1}) = f(x^n x) = f(x^n)f(x) = f(x)^n f(x) = f(x)^{n+1}.$$

Par récurrence, on a $f(x^n) = (f(x))^n$ pour tout $n \in \mathbb{N}$.

Si n est un entier < 0, on a

$$f(x^n) \underset{\text{déf.}}{=} f\left(\left(x^{-1}\right)^{-n}\right) \underset{-n>0}{=} f\left(x^{-1}\right)^{-n} \underset{2.}{=} \left(f(x)^{-1}\right)^{-n} \underset{\text{déf.}}{=} f(x)^n.$$

∎

Proposition 40

La composée de deux morphismes de groupes est un morphisme de groupes.

Démonstration. Soient $f : G \to H$ et $g : H \to K$ deux morphismes de groupes.
Pour $x, y \in G$,

$$(g \circ f)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))\, g(f(y)) = (g \circ f)(x)\,(g \circ f)(y).$$

Donc $g \circ f$ est un morphisme de groupes. ∎

Proposition 41 *Si un morphisme de groupes est bijectif, l'application réciproque est encore un morphisme de groupes.*

Démonstration. Soit $f : G \to H$ un morphisme de groupes bijectif.
Soit $u, v \in H$, montrons $f^{-1}(uv) = f^{-1}(u)f^{-1}(v)$. Puisque f est un morphisme de groupes,

$$f\left(f^{-1}(u)f^{-1}(v)\right) = f\left(f^{-1}(u)\right) f\left(f^{-1}(v)\right) = uv = f\left(f^{-1}(uv)\right).$$

Puisque f est bijectif (et en particulier injectif), on a $f^{-1}(u)f^{-1}(v) = f^{-1}(uv)$. f^{-1} est donc un morphisme de groupes.

∎

Théorème 42 *Soit f un morphisme du groupe G dans le groupe H.*

1. *Si H' est un sous-groupe de H, alors l'image réciproque*

$$f^{-1}\left(H'\right) = \left\{ x \in G \mid f(x) \in H' \right\}$$

est un sous-groupe de G.

2. *Si G' est un sous-groupe de G, alors l'image*

$$f\left(G'\right) = \left\{ f(x) \mid x \in G' \right\} = \left\{ y \in H \mid \exists x \in G', y = f(x) \right\}$$

est un sous-groupe de H.

Démonstration. **1.** Puisque $f(e_G) = e_H$ et $e_H \in H'$, alors $e_G \in f^{-1}(H')$. Soit $(x, y) \in \left(f^{-1}(H')\right)^2$, c'est-à-dire $f(x) \in H'$ et $f(y) \in H'$. Puisque H' est un sous-groupe de H, on a

$$f(xy) = f(x)f(y) \in H' \text{ et } f\left(x^{-1}\right) = f(x)^{-1} \in H',$$

c'est-à-dire, $xy \in f^{-1}(H')$ et $x^{-1} \in H'$. L'image réciproque de H' par f est donc un sous-groupe de G.

2. On a $e_G \in G'$ et l'égalité $f(e_G) = e_H$, d'où $e_H \in f(G')$. Soit $(a, b) \in \left(f(G')\right)^2$. Il existe $x, y \in G'$ tel que $a = f(x)$ et $b = f(y)$. Puisque f est un morphisme de groupes et G' un sous-groupe de G, on a

$$f(xy) = f(x)f(y) = ab \text{ et } xy \in G',$$

ceci montre que $ab \in f(G')$. De plus

$$f(x^{-1}) = f(x)^{-1} = a^{-1} \text{ et } x^{-1} \in G',$$

d'où $a^{-1} \in f(G')$. L'image directe de G' par f est donc un sous-groupe de H.

∎

§2 Noyau et image d'un morphisme de groupes

Définition 43

Soit f un morphisme du groupe G dans le groupe H. L'ensemble des antécédents de l'élément neutre de H par f est appelé **noyau** de f et se note $\ker(f)$.

$$\ker(f) = \left\{ x \in G \;\middle|\; f(x) = e_H \right\} = f^{-1}\left(\{ e_H \}\right).$$

L'**image** $f(G)$ de f se note $\mathrm{Im}(f)$.

$$\mathrm{Im}(f) = \{ f(x) \mid x \in G \} = \{ y \in H \mid \exists x \in G, y = f(x) \}.$$

$$x \in \ker f \iff x \in G \text{ et } f(x) = e_H.$$
$$y \in \mathrm{Im}(f) \iff \exists x \in G, y = f(x).$$

Proposition 44

Soit f un morphisme du groupe G dans le groupe H.

1. $\ker(f)$ *est un sous-groupe de* G.
2. $\mathrm{Im}(f)$ *est un sous-groupe de* H.

Exemple 45

L'application

$$\begin{array}{rccc} \varphi : & (\mathbb{R}, +) & \to & \left(\mathbb{C}^\star, \cdot\right) \\ & t & \mapsto & e^{it} \end{array}$$

est un morphisme de groupe. On a

$$\ker(\varphi) = 2\pi\mathbb{Z} = \{ k2\pi \mid k \in \mathbb{Z} \} \quad \text{et} \quad \mathrm{Im}(\varphi) = \mathbb{U} = \{ z \in \mathbb{C} \mid |z| = 1 \}.$$

Exemple 46

L'application

$$\begin{array}{rccc} f : & (\mathbb{C}^\star, .) & \to & (\mathbb{R}^\star, .) \\ & z & \mapsto & |z| \end{array}$$

est un morphisme de groupes. On a

$$\ker(f) = \left\{ z \in \mathbb{C}^\star \;\middle|\; |z| = 1 \right\} = \mathbb{U} \quad \text{et} \quad \mathrm{Im}(f) = \mathbb{R}_+^\star.$$

Exemple 47

L'application

$$\begin{array}{rccc} \pi : & (\mathbb{Z}, +) & \to & (\mathbb{U}_n, .) \\ & k & \mapsto & e^{2ik\pi/n} \end{array}$$

est un morphisme de groupes surjectif. On a

$$\ker(\pi) = n\mathbb{Z}.$$

Théorème 48

Soient G et H deux groupes et f un morphisme de G dans H.

1. *f est injectif si et seulement si* $\ker(f) = \{ e_G \}$.

2. *f est surjectif si et seulement si* $\mathrm{Im}(f) = H$.

Démonstration. **1.** Supposons que f soit injectif. L'égalité $f(e_G) = e_H$ montre que l'on a $\{ e_G \} \subset \ker(f)$. De plus, si $x \in \ker(f)$, alors $f(x) = e_H = f(e_G)$; l'injectivité de f assure que $x = e_G$, c'est-à-dire $\ker(f) \subset \{ e_G \}$. Par double inclusion, on a $\ker(f) = \{ e_G \}$.

Supposons maintenant $\ker(f) = \{ e_G \}$. Soient $x, y \in G$ tels que $f(x) = f(y)$. Puisque f est un morphisme de groupes, on a

$$f\left(xy^{-1}\right) = f(x)f(y)^{-1} = e_H,$$

c'est-à-dire $xy^{-1} \in \ker(f)$. Puisque $\ker(f) = \{ e_G \}$, on a $xy^{-1} = e_G$ c'est-à-dire $x = y$. L'application f est donc injective.

2. Rien de nouveau…

∎

Théorème 49

Soient G et H deux groupes et f un morphisme de G dans H. Soit $b \in H$.

1. *Si $b \notin \mathrm{Im}(f)$, l'équation $f(x) = b$ d'inconnue $x \in G$ n'a pas de solution.*

2. *Si $b \in \mathrm{Im}(f)$, alors en notant x_0 un antécédent de b par f, on a*

$$\{ x \in G \mid f(x) = b \} = x_0 \ker(f) = \left\{ x_0 h \;\middle|\; h \in \ker(f) \right\}.$$

Si la loi de G est notée comme une addition,

$$\{ x \in G \mid f(x) = b \} = x_0 + \ker(f) = \left\{ x_0 + h \;\middle|\; h \in \ker(f) \right\}.$$

Test 50

Soit $f : G \to H$ un morphisme de groupes. Supposons G *fini*. Alors $\mathrm{Im}(f)$ est finie, et l'on a

$$|G| = |\ker(f)| \times |\mathrm{Im}(f)|.$$

13.5 Générateurs

§1 Sous-groupe engendré par une partie

Soit A une partie d'un groupe G. Il existe des sous-groupes de G qui contiennent A (par exemple G lui-même); l'intersection de tous ces sous-groupes

$$\bigcap_{\substack{H \text{ sous-groupe de } G \\ A \subset H}} H.$$

est encore un sous-groupe et contient encore A, tout en étant contenue, par construction même, dans tout sous-groupe de G contenant A. Ce sous-groupe intersection est donc le «plus petit» de tous les sous-groupes de G contenant A.

Définition 51

Soient $(G, \star)$ un groupe et A une partie de G.

- Le sous-groupe engendré par A est le plus petit sous-groupe contenant cette partie A. On le note souvent $\langle A \rangle$ ou $\mathbf{Gr}(A)$.
- On dit que G est un **groupe monogène** lorsqu'il existe $a \in G$ tel que $\langle a \rangle = G$.

  Un tel a est **un générateur** de G.
- On qualifie de **cyclique** tout groupe monogène fini.

Théorème 52

Soit G un groupe et $a \in G$.

- *En notation multiplicative, le sous-groupe de G engendré par l'élément a est*

$$\langle a \rangle = \left\{ a^k \;\middle|\; k \in \mathbb{Z} \right\}.$$

- *En notation additive, le sous-groupe de G engendré par l'élément a est*

$$\langle a \rangle = \{ ka \mid k \in \mathbb{Z} \}.$$

Un groupe monogène est donc toujours abélien.

Exemple 53

Dans $(\mathbb{C}^\star, \cdot)$,

- le sous-groupe engendré par i est $\mathbb{U}_4$;
- le sous-groupe engendré par -1 est $\mathbb{U}_2 = \{ -1, +1 \}$.

Exemple 54

Dans $(\mathbb{Z}, +)$, le sous groupe engendré par n est $n\mathbb{Z}$.

Exemple 55

1. $(\mathbb{Z}, +)$ est un groupe monogène, engendré par 1.
2. $(\mathbb{U}_n, \cdot)$ est un groupe cyclique, engendré par $\omega = e^{2i\pi/n}$.

Test 56

Soit G un groupe *commutatif* et $a, b \in G$. Montrer que

$$\langle a, b \rangle = \left\{ a^i b^j \;\middle|\; (i, j) \in \mathbb{Z}^2 \right\}.$$

En notation additive, cela s'écrirait $\langle a, b \rangle = \left\{ ia + jb \;\middle|\; (i, j) \in \mathbb{Z}^2 \right\}$.

Test 57

Montrer que $\langle A \rangle$ est l'ensemble de tous les produits que l'on peut former à partir des éléments de A et de leurs inverses

$$\langle A \rangle = \left\{ x_1 \dots x_n \;\middle|\; n \in \mathbb{N} \text{ et } \forall i \in [\![1, n]\!], x_i \in A \text{ ou } x_i^{-1} \in A \right\}.$$

§2 Description des groupes monogènes

Définition 58

Soit $a \in G$.

- Si le sous-groupe $\langle a \rangle$ est fini, on appelle **ordre** de a le cardinal de $\langle a \rangle$.
- Si le sous-groupe $\langle a \rangle$ est infini, on dit que a est d'**ordre infini**.

On peut noter $\omega(a)$ l'ordre de a.

Théorème 59

Description des groupes monogènes
Soit $G = \langle a \rangle$ un groupe monogène. Alors,

1. *Si a est d'ordre infini, alors G est isomorphe au groupe $(\mathbb{Z}, +)$.*
2. *Si a est d'ordre fini $p \in \mathbb{N}^\star$, alors G est isomorphe au groupe $(\mathbb{U}_p, \cdot)$.*

Corollaire 60

Soit $(G, \cdot)$ un groupe d'élément neutre e_G et $a \in G$.
Les assertions suivantes sont équivalentes.

(i) *L'ensemble $\left\{ k \in \mathbb{N}^\star \;\middle|\; a^k = e_G \right\}$ est non vide et son minimum est égal à p.*

(ii) *Pour tout $k \in \mathbb{Z}$, on a l'équivalence $\left(a^k = e_G \iff k \in p\mathbb{Z}\right)$.*

(iii) *Les éléments de $\langle a \rangle$ sont exactement $e_G, a, \ldots, a^{p-1}$ et ils sont deux à deux distincts.*

(iv) *Le sous-groupe $\langle a \rangle = \left\{ a^k \;\middle|\; k \in \mathbb{Z} \right\}$ est fini de cardinal p.*

Dans ce cas p est l'ordre de a.

Théorème 61

Lagrange
Soit a un élément d'un groupe fini G. Alors l'ordre de a divise l'ordre de G.

Corollaire 62

Soit G un groupe fini d'ordre n. On a alors

$$\forall x \in G, x^n = e_G.$$