Chapitre 2
Introduction à la théorie des groupes

Les groupes font partie des structures abstraites les plus fondamentales en algèbre générale.

Ils sont en lien étroit avec la notion de symétrie, et ont donc un rôle important dans de nombreuses sciences fondamentales : algèbre (théorie des nombres, théorie de Galois, théorie des représentations, ...), géométrie (symétries, géométrie algébrique, ...), sciences physiques (relativité restreinte, mécanique quantique, ...), chimie (cristallographie, symétrie moléculaire, ...), informatique (cryptographie, ...), sciences de l'information (codes correcteurs, ...), etc.

Le but de ce deuxième chapitre est d'introduire le vocabulaire de base à la théorie des groupes et de présenter des algorithmes en lien avec la notion de groupe.

1 Définitions et premières propriétés

1.1 La structure de groupe

Définition 1

*Un **groupe** $(G, \star)$ est la donnée*

— *d'un ensemble G*

— *et d'une application de G^2 vers G notée $(x, y) \mapsto x \star y$ appelée **loi de composition interne***

qui vérifient les trois axiomes suivants :

(i) ***associativité*** *:* $\boxed{\forall (x, y, z) \in G^3,\ (x \star y) \star z = x \star (y \star z)}$ *(qu'on peut donc écrire $x \star y \star z$),*

(ii) *existence d'un **élément neutre** :* $\boxed{\exists e \in G,\ \forall x \in G,\ x \star e = e \star x = x}$,

(iii) *existence de **symétriques** :* $\boxed{\forall x \in G,\ \exists \overline{x} \in G,\ x \star \overline{x} = \overline{x} \star x = e}$.

Exemple. $(\mathbb{N}, +)$ n'est pas un groupe : l'addition est bien associative et 0 est un élément neutre, mais 1 n'a pas de symétrique. Par contre, $(\mathbb{Z}, +)$ est un groupe. De même, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes.

Exemple. $(\mathbb{Z}, \times)$ n'est pas un groupe : la multiplication est bien associative et 1 est un élément neutre, mais 2 n'a pas de symétrique. De même, $(\mathbb{Q}, \times)$ n'est pas un groupe : 2 a bien un symétrique mais 0 n'en a pas. Par contre, $(\mathbb{Q}^*, \times)$ est un groupe. De même, $(\mathbb{R}^*, \times)$, $(\mathbb{R}_+^*, \times)$ et $(\mathbb{C}^*, \times)$ sont des groupes.

Définition 2

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

— *Si $\forall (x, y) \in G^2,\ x \star y = x \star y$ alors on dit que la loi de composition interne $\star$ est **commutative** et que $(G, \star)$ est un **groupe abélien** (ou un **groupe commutatif**).*

— *Si G est un ensemble fini, alors on dit que $(G, \star)$ est un **groupe fini**. Dans ce cas, on note $|G|$ le cardinal de G qu'on appelle l'**ordre** de $(G, \star)$. Sinon, on dit que $(G, \star)$ est d'**ordre infini**.*

Exemple. Pour $n \in \mathbb{N}^*$, on note $\mathbb{U}_n$ l'ensemble des racines complexes n-èmes de l'unité, c'est-à-dire :

$$\mathbb{U}_n = \left\{ z \in \mathbb{C} \mid z^n = 1 \right\} = \left\{ e^{i2k\pi/n} \mid k \in [\![0, n-1]\!] \right\}.$$

$(\mathbb{U}_n, \times)$ est un groupe abélien fini d'ordre n.

La loi de composition interne d'un groupe fini peut être présentée sous forme d'un tableau appelé **table de Cayley** dont chaque case à l'intersection de la ligne x et de la colonne y contient le résultat de $x \star y$. Par exemple pour le groupe $(\mathbb{U}_4 = \{1, i, -1, -i\}, \times)$:

$\overset{\star}{\downarrow}$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

On remarque que, pour cet exemple, la table de Cayley est symétrique car le groupe $(\mathbb{U}_n, \times)$ est abélien.

Remarque. Le plus petit groupe fini est d'ordre 1 : c'est le groupe contenant seulement l'élément neutre.

1.2 Propriétés de calculs dans les groupes

Propriété 1

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

- *L'élément neutre de $(G, \star)$ est unique.*
- *Pour tout $x \in G$, le symétrique de x dans $(G, \star)$ est unique.*
- $\overline{e} = e$.
- $\forall x \in G,\ \overline{\overline{x}} = x$.
- $\forall (x, y) \in G^2,\ \overline{x \star y} = \overline{y} \star \overline{x}$.

Démonstration.

- On suppose qu'il existe deux éléments neutres $(e_1, e_2) \in G^2$. En particulier, on a :

$$\begin{aligned} &\forall x \in G,\ e_1 \star x = x \quad \text{donc } e_1 \star e_2 = e_2 \quad \text{pour } x = e_2 \\ \text{et}\quad &\forall x \in G,\ x \star e_2 = x \quad \text{donc } e_1 \star e_2 = e_1 \quad \text{pour } x = e_1. \end{aligned}$$

  On en déduit que $e_1 = e_2$, d'où l'unicité de l'élément neutre.
- Soit $x \in G$. On suppose qu'il existe deux symétriques $(x_1, x_2) \in G^2$ de x. Alors :

$$\begin{aligned} x_1 &= x_1 \star e \quad \text{car } e \text{ est l'élément neutre} \\ &= x_1 \star (x \star x_2) \quad \text{car } x_2 \text{ est un symétrique de } x \\ &= (x_1 \star x) \star x_2 \quad \text{par associativité} \\ &= e \star x_2 \quad \text{car } x_1 \text{ est un symétrique de } x \\ &= x_2 \quad \text{car } e \text{ est l'élément neutre.} \end{aligned}$$

  D'où l'unicité du symétrique de x.
- L'unique symétrique de $\overline{e}$ de e vérifie $e * \overline{e} = \overline{e} * e = e$. Or $e * e = e$ car e est l'élément neutre. Donc $\overline{e} = e$ par unicité du symétrique de e.
- Soit $x \in G$. L'unique symétrique $\overline{\overline{x}}$ de $\overline{x}$ vérifie $\overline{x} \star \overline{\overline{x}} = \overline{\overline{x}} \star \overline{x} = e$. Or $\overline{x} \star x = x \star \overline{x} = e$ car $\overline{x}$ est le symétrique de x. Donc $\overline{\overline{x}} = x$ par unicité du symétrique de $\overline{x}$.
- Soient $x \in G$ et $y \in G$. On a :

$$\begin{aligned} (x \star y) \star (\overline{y} \star \overline{x}) &= x \star (y \star \overline{y}) \star \overline{x} \quad \text{par associativité} \\ &= x \star e \star \overline{x} \quad \text{car } \overline{y} \text{ est le symétrique de } y \\ &= x \star \overline{x} \quad \text{car } e \text{ est l'élément neutre} \\ &= e \quad \text{car } \overline{x} \text{ est le symétrique de } x. \end{aligned}$$

  De même, on a $(\overline{y} \star \overline{x}) \star (x \star y) = e$. Donc $\overline{x \star y} = \overline{y} \star \overline{x}$ par unicité du symétrique de $x \star y$.

□

Propriété 2 (*Résolution d'équations dans un groupe*)

Soit $(G, \star)$ un groupe. Alors pour tout $(a, b, x) \in G^3$:

$$a \star x = b \iff x = \overline{a} \star b \qquad \text{et} \qquad x \star a = b \iff x = b \star \overline{a}.$$

Démonstration. Si $a \star x = b$ alors $\overline{a} \star b = \overline{a} \star (a \star x) = (\overline{a} \star a) \star x = e \star x = x$. Réciproquement, si $x = \overline{a} \star b$ alors $a \star x = a \star (\overline{a} \star b) = (a \star \overline{a}) \star b = e \star b = b$. On montre de même la deuxième équivalence.

□

Propriété 3 (*Simplifications dans un groupe*)

Soit $(G, \star)$ un groupe. Alors pour tout $(a, b, x) \in G^3$:

$$x \star a = x \star b \iff a = b \iff a \star x = b \star x.$$

Démonstration. Si $x \star a = x \star b$, alors $\overline{x} \star (x \star a) = \overline{x} \star (x \star b)$. Or $\overline{x} \star (x \star a) = (\overline{x} \star x) \star a = e \star a = a$ et de même $\overline{x} \star (x \star b) = b$. On en déduit que $a = b$. La réciproque est évidente, puis on montre de même la deuxième équivalence.

□

Remarque. La propriété précédente implique que chaque ligne et chaque colonne d'une table de Cayley contient des résultats deux à deux différents, donc tous les éléments du groupe fini.

Exemple. La table de Cayley d'un groupe fini $(G = \{e, a\}, \star)$ d'ordre 2 est nécessairement de la forme :

$\vec{\star}$	e	a
e	e	a
a	a	e

De même, pour un groupe fini $(G = \{e, a, b\}, \star)$ d'ordre 3, il n'y a qu'une seule forme possible de table de Cayley, et donc qu'une seule loi de composition interne possible :

$\vec{\star}$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Par contre, il y a quatre lois de composition interne possibles pour un groupe fini $(G = \{e, a, b, c\}, \star)$ d'ordre 4 (on peut vérifier qu'elles sont bien associatives) :

$\vec{\star}$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$\vec{\star}$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

$\vec{\star}$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$\vec{\star}$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

Dans tous les cas, on remarque que tout groupe fini d'ordre inférieur ou égal à 4 est abélien.

Définition 3

*Soit $(G, \star)$ un groupe. Pour tout $x \in G$, on définit la suite $(x^{\star n})_{n \in \mathbb{Z}}$ de ses **itérés** par les récurrences suivantes :*

$$x^{\star 0} = e \quad et \quad \begin{cases} \forall n \geqslant 0,\ x^{\star(n+1)} = x^{\star n} \star x \\ \forall n \leqslant 0,\ x^{\star(n-1)} = x^{\star n} \star \overline{x}. \end{cases}$$

Remarque. En particulier, pour tout $x \in G$ et tout $n \in \mathbb{N}^*$:

$$x^{\star n} = \underbrace{x \star x \star \cdots \star x}_{n \text{ fois}} \quad \text{et} \quad x^{\star -n} = \underbrace{\overline{x} \star \overline{x} \star \cdots \star \overline{x}}_{n \text{ fois}}.$$

Propriété 4

Soit $(G, \star)$ un groupe. On a pour tout $x \in G$:

- $\forall n \in \mathbb{Z},\ \overline{x^{\star n}} = (\overline{x})^{\star n} = x^{\star -n}$,
- $\forall (n,p) \in \mathbb{Z}^2,\ x^{\star n} \star x^{\star p} = x^{\star (n+p)} = x^{\star p} \star x^{\star n}$,
- $\forall (n,p) \in \mathbb{Z}^2,\ (x^{\star n})^{\star p} = x^{\star np} = (x^{\star p})^{\star n}$.

Démonstration. Par récurrences.

□

1.3 Notations et autres exemples

Définition 4

*La loi de composition interne $\star$ d'un groupe $(G, \star)$ est souvent notée $+$ ou $\times$. Dans ce cas, on adopte les notations **additives** ou **multiplicatives** suivantes.*

	not. générales	*not. additives*	*not. multiplicatives*
groupe	$(G, \star)$	$(G, +)$	$(G, \times)$
composition interne	$x \star y$	$x + y$	xy
élément neutre	e *(ou* e_G*)*	0 *(ou* 0_G*)*	1 *(ou* 1_G*)*
symétriques	$\overline{x} = x^{\star -1}$	$-x$	x^{-1}
itérés	$x^{\star n}$	nx	x^n

Exemple. L'ensemble des fonctions réelles ou complexes définies sur $I \subset \mathbb{R}$ muni de l'addition est un groupe abélien dont l'élément neutre est la fonction constante égale à 0. De même pour l'ensemble des suites réelles ou complexes.

Exemple. Soient $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, et $(n,p) \in (\mathbb{N}^*)^2$. L'ensemble $\mathscr{M}_{n,p}(\mathbb{K})$ des matrices rectangulaires de taille (n,p) à coefficients dans $\mathbb{K}$ a une structure de groupe (abélien) pour l'addition de matrices, mais pas pour la multiplication de matrices. Alors que l'ensemble $\mathscr{GL}_n(\mathbb{K})$ des matrices carrés inversibles d'ordre n à coefficients dans $\mathbb{K}$ a une structure de groupe (non-abélien) pour la multiplication de matrices, mais pas pour l'addition de matrices. De même, les sous-ensembles de $\mathscr{M}_n(\mathbb{K})$ des matrices symétriques et des matrices hermitiennes ont une structure de groupe additif, alors que ceux des matrices orthogonales et des matrices unitaires ont une structure de groupe multiplicatif.

Exemple. On peut vérifier que le cercle trigonométrique $\mathbb{S}^1 = \{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ a une structure de groupe abélien pour la loi de composition interne définie par :

$$\forall (x_1,y_1) \in \mathbb{S}^1,\ \forall (x_2,y_2) \in \mathbb{S}^1,\ (x_1,y_1) \star (x_2,y_2) = \Big(x_1x_2 - y_1y_2, x_1y_2 + x_2y_1\Big).$$

L'élément neutre est $(1,0)$ et l'inverse de chaque $(x,y) \in \mathbb{S}^1$ est $(x,-y)$. On peut identifier $\mathbb{S}^1$ à l'ensemble $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\} = \{e^{i\theta} = \cos(\theta) + i\sin(\theta) \mid \theta \in \mathbb{R}\}$ qui a aussi une structure de groupe abélien pour la multiplication des nombres complexes.

Définition 5

*L'ensemble des bijections d'un ensemble E dans lui-même, appelées **permutations** de E, muni de la composition des applications est un groupe noté $(\mathscr{S}(E), \circ)$ appelé le **groupe symétrique** de E.*
Pour $n \in \mathbb{N}^*$, l'ensemble des permutations de $[\![1,n]\!] = \{1,2,\dots,n\}$ est simplement noté $\mathscr{S}_n$ et a donc une structure de groupe fini d'ordre $|\mathscr{S}_n| = n!$. De plus, chaque permutation $\varphi \in \mathscr{S}_n$ est notée :

$$\varphi = \begin{pmatrix} 1 & 2 & \dots & n \\ \varphi(1) & \varphi(2) & \dots & \varphi(n) \end{pmatrix}.$$

Exemple. Les 6 permutations du groupe symétrique $(\mathscr{S}_3, \circ)$ sont :

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = \mathrm{Id},\ \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \tau_{1,2},\ \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = \tau_{1,3},\ \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \tau_{2,3},\ \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \sigma_+ \text{ et } \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \sigma_-.$$

On obtient la table de Cayley suivante :

$\circlearrowleft$	Id	$\tau_{1,2}$	$\tau_{1,3}$	$\tau_{2,3}$	σ_+	σ_-
Id	Id	$\tau_{1,2}$	$\tau_{1,3}$	$\tau_{2,3}$	σ_+	σ_-
$\tau_{1,2}$	$\tau_{1,2}$	Id	σ_-	σ_+	$\tau_{2,3}$	$\tau_{1,3}$
$\tau_{1,3}$	$\tau_{1,3}$	σ_+	Id	σ_-	$\tau_{1,2}$	$\tau_{2,3}$
$\tau_{2,3}$	$\tau_{2,3}$	σ_-	σ_+	Id	$\tau_{1,3}$	$\tau_{1,2}$
σ_+	σ_+	$\tau_{1,3}$	$\tau_{2,3}$	$\tau_{1,2}$	σ_-	Id
σ_-	σ_-	$\tau_{2,3}$	$\tau_{1,2}$	$\tau_{1,3}$	Id	σ_+

On remarque que $(\mathscr{S}_3, \circ)$ n'est pas un groupe abélien.

Cette remarque se généralise à tout entier $n \geqslant 3$. En effet, si $(a, b, c) \in [\![1, n]\!]^3$ sont deux à deux distincts, alors on a par exemple $(\tau_{a,b} \circ \tau_{a,c})(a) = c \neq b = (\tau_{a,c} \circ \tau_{a,b})(a)$ donc $(\mathscr{S}_n, \circ)$ n'est pas abélien. D'autre part pour $\mathscr{S}_3$, on remarque que le sous-ensemble de permutations $\{\mathrm{Id}, \sigma_+, \sigma_-\}$ a également une structure de groupe pour la composition (groupe abélien fini d'ordre 3), mais pas le sous-ensemble $\{\mathrm{Id}, \tau_{1,2}, \tau_{1,3}, \tau_{2,3}\}$ (car par exemple $\tau_{1,3} \circ \tau_{1,2} = \sigma_+$ n'appartient pas à ce sous-ensemble).

2 Sous-groupes

2.1 Définition et exemples

Définition 6

*Soit $(G, \star)$ un groupe. On dit qu'une partie $H \subset G$ est un **sous-groupe** de $(G, \star)$ lorsque :*

(i) *H contient l'élément neutre : $e \in H$,*

(ii) *H est **stable par la loi de composition interne** : $\forall (x, y) \in H^2,\ x \star y \in H$,*

(iii) *H est **stable par passage au symétrique** : $\forall x \in H,\ \overline{x} \in H$.*

Propriété 5

Soient $(G, \star)$ un groupe et $H \subset G$. Alors H est un sous-groupe de $(G, \star)$ si et seulement si

$$e \in H \quad \text{et} \quad \forall (x, y) \in H^2,\ x \star \overline{y} \in H.$$

Et dans ce cas $(H, \star)$ est un groupe.

Démonstration. L'implication directe est évidente. Pour la réciproque, le point (i) de la définition 6 est immédiat. Puis, on a pour tout $x \in H$: $\overline{x} = e \star \overline{x} \in H$ d'où la stabilité par passage au symétrique (iii). Enfin, on en déduit la stabilité par la loi de composition interne (ii) car on a pour tout $(x, y) \in H^2$: $x \star y = x \star (\overline{\overline{y}}) \in H$. Ainsi, la restriction de la loi de composition interne de $(G, \star)$ au sous-groupe H définit bien une application de H^2 dans H. Il suffit ensuite de vérifier les axiomes (i), (ii) et (iii) de la définition 1, ce qui est immédiat.

□

Exemple. $\mathbb{Z}$ est un sous-groupe de $(\mathbb{Q}, +)$, donc aussi de $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ car $\mathbb{Q}$ est un sous-groupe de $(\mathbb{R}, +)$ et $\mathbb{R}$ est un sous-groupe de $(\mathbb{C}, +)$. De même, pour $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$.

Exemple. Pour tout $n \in \mathbb{N}$, $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ est un sous-groupe additif de $\mathbb{Z}$. En particulier, le sous-ensemble $2\mathbb{Z}$ des entiers pairs est un sous-groupe de $(\mathbb{Z}, +)$, mais pas le sous-ensemble des entiers impairs (car il ne contient pas 0 et n'est pas stable par addition).

Exemple. Le sous-ensemble des fonctions réelles continues sur $I \subset \mathbb{R}$ est un sous-groupe additif de l'ensemble des fonctions réelles définies sur I, mais pas le sous-ensemble des fonctions réelles positives sur I (car il n'est pas stable par passage à l'opposé). De même, le sous-ensemble des suites réelles croissantes n'est pas un sous-groupe additif de l'ensemble des suites réelles, alors que le sous-ensemble des suites réelles nulles à partir d'un certain rang en est un.

Exemple. Pour tout $n \in \mathbb{N}^*$, $\mathbb{U}_n$ est un sous-groupe multiplicatif de $\mathbb{U}$ qui est lui-même un sous-groupe multiplicatif de $\mathbb{C}^*$. De même, $\mathbb{R}^*$ et $\mathbb{R}_+^*$ sont des sous-groupes multiplicatifs de $\mathbb{C}^*$, mais pas $i\mathbb{R}^*$.

Exemple. $\{\mathrm{Id}, \sigma_+, \sigma_-\}$ est un sous-groupe de $(\mathscr{S}_3, \circ)$ mais pas $\{\mathrm{Id}, \tau_{1,2}, \tau_{1,3}, \tau_{2,3}\}$.

Exemple. Soit $n \in \mathbb{N}^*$. On fixe une partie $A \subset [\![1, n]\!]$ et on considère $H = \{\varphi \in \mathscr{S}_n \mid \varphi(A) \subset A\}$, c'est-à-dire le sous-ensemble des permutations de $[\![1, n]\!]$ qui laissent A **invariant**. Alors H est un sous-groupe du groupe symétrique. En effet, si $\varphi \in H$ alors $\varphi(A) = A$ car φ est bijective et A est un ensemble fini, donc $\varphi^{\circ -1}(A) = A$ d'où la stabilité par passage à la bijection réciproque. La stabilité par composition et le fait que $\mathrm{Id} \in H$ sont évidents.

Exemple. Soit $(G, \star)$ un groupe. L'ensemble $\mathscr{Z}(G)$ des éléments de G qui **commutent** avec tous les autres, c'est-à-dire $\mathscr{Z}(G) = \{x \in G \mid \forall y \in G,\ x \star y = y \star x\}$ est un sous-groupe abélien de $(G, \star)$. La stabilité par passage au symétrique se déduit de $\forall (x, y) \in \mathscr{Z}(G) \times G,\ \overline{x} \star y = \overline{\overline{y} \star x} = \overline{x \star \overline{y}} = y \star \overline{x}$.

Remarque. Le plus petit sous-groupe d'un groupe $(G, \star)$ est $\{e\}$, et le plus grand est G. Ces deux sous-groupes de $(G, \star)$ sont appelés ses **sous-groupes triviaux**.

Propriété 6

Toute intersection de sous-groupes d'un groupe $(G, \star)$ est un sous-groupe de $(G, \star)$.

Démonstration. C'est immédiat d'après la propriété 5.

□

Exemple. $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$.

Attention. C'est en général faux pour l'union. Par exemple, $2\mathbb{Z} \cup 3\mathbb{Z}$ n'est pas un sous-groupe de $(\mathbb{Z}, +)$ car $2.1 + 3.1 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$ ce qui contredit la stabilité par addition.

2.2 Sous-groupes engendrés

Définition 7

Soient $(G, \star)$ un groupe et $A \subset G$. Le plus petit sous-groupe de $(G, \star)$ contenant A, c'est-à-dire l'intersection de tous les sous-groupes de $(G, \star)$ contenant A, est appelé le ***sous-groupe engendré*** *par A. On le note :*

$$\langle A \rangle = \bigcap_{\substack{H \text{ sous-groupe de } (G,\star) \\ \text{et } A \subset H}} H.$$

Propriété 7

Soient $(G, \star)$ un groupe et $A \subset G$. Alors :

$$\langle A \rangle = \left\{ a_1^{\star n_1} \star a_2^{\star n_2} \star \cdots \star a_p^{\star n_p} \;\middle|\; p \in \mathbb{N},\ (a_1, a_2, \ldots, a_p) \in A^p \text{ et } (n_1, n_2, \ldots, n_p) \in \mathbb{Z}^p \right\}.$$

En particulier, chaque élément du sous-groupe engendré par A peut s'écrire comme une composée interne d'un nombre fini d'éléments de A ou de leur symétrique.

Démonstration. On note H l'ensemble des éléments de G qui peuvent s'écrire comme une composée interne d'un nombre fini d'itérés d'éléments de A. D'après les propriétés de calculs dans les groupes, H contient l'élément neutre, est stable par la loi de composition interne et par passage au symétrique. Donc H est bien un sous-groupe contenant A. Et c'est le plus petit car tout sous-groupe contenant A doit contenir les composées internes d'un nombre fini d'itérés d'éléments de A (par stabilité).

□

Exemple. Dans $(\mathbb{Z},+)$, on a $\langle\{2\}\rangle = 2\mathbb{Z}$ car si un sous-groupe contient 2 alors il contient tous ses itérés (par stabilité de l'addition et par passage à l'opposé), c'est-à-dire le sous-groupe des entiers pairs. Par ailleurs, $\langle\{2,3\}\rangle = \mathbb{Z}$. En effet, si $n \in \mathbb{Z}$ est pair alors $\exists k \in \mathbb{Z},\ n = 2k \in \langle\{2,3\}\rangle$ (en tant qu'itéré de 2) et si $n \in \mathbb{Z}$ est impair alors $\exists k \in \mathbb{Z},\ n = 2k+1 = 2(k-1)+3 \in \langle\{2,3\}\rangle$ (par stabilité de l'addition). Donc $\mathbb{Z} \subset \langle\{2,3\}\rangle$ et l'inclusion réciproque est évidente.

Exemple. $\mathbb{U}_4$ est le sous-groupe de $(\mathbb{C}^*,\times)$ engendré par i car si un sous-groupe multiplicatif contient i alors il contient $\{i^k \mid k \in \mathbb{Z}\} = \{1,i,-1,-i\} = \mathbb{U}_4$.

Exemple. $\{a+ib \mid (a,b) \in \mathbb{Z}^2\}$ est le sous-groupe de $(\mathbb{C},+)$ engendré par 1 et i. On le note $\mathbb{Z}[i]$.

Exemple. Dans $(\mathscr{S}_3,\circ)$, le sous-groupe $\{\mathrm{Id},\sigma_+,\sigma_-\}$ est engendré par σ_+ (car $\sigma_+^{\circ 2} = \sigma_-$ et $\sigma_+^{\circ 3} = \mathrm{Id}$) ou par σ_- (car $\sigma_-^{\circ -1} = \sigma_+$). D'autre part, puisque $\tau_{1,3}\circ\tau_{1,2} = \sigma_+$ et $\tau_{1,2}\circ\tau_{1,3} = \sigma_-$, on a $\langle\{\tau_{1,2},\tau_{1,3},\tau_{2,3}\}\rangle = \mathscr{S}_3$.

Théorème 1

*Soit $n \in \mathbb{N}^*$. Le groupe symétrique $(\mathscr{S}_n,\circ)$ est engendré par les **transpositions**, c'est-à-dire par les permutations de $[\![1,n]\!]$ qui échangent deux éléments distincts en laissant inchangés les autres :*

$$\tau_{i,j} : k \mapsto \begin{cases} j \text{ si } k = i \\ i \text{ si } k = j \\ k \text{ sinon} \end{cases} \quad \text{où} \quad (i,j) \in [\![1,n]\!]^2 \quad \text{et} \quad i \neq j.$$

Autrement dit, toute permutation de $\mathscr{S}_n$ peut s'écrire comme une composée d'un nombre fini de transpositions.

Remarque. Si $1 \leqslant i < j \leqslant n$, alors $\tau_{i,j} = \begin{pmatrix} 1 & \dots & i-1 & i & i+1 & \dots & j-1 & j & j+1 & \dots & n \\ 1 & \dots & i-1 & j & i+1 & \dots & j-1 & i & j+1 & \dots & n \end{pmatrix}$. En pratique, on note plus simplement $\tau_{i,j} = (i,j)$.

Démonstration. Soit $\varphi_0 \in \mathscr{S}_n$. Si $\varphi_0 = \mathrm{Id}$ alors φ_0 peut s'écrire comme une composée de 0 transposition. Sinon, on pose $k_0 = \min\{k \in [\![1,n]\!] \mid \varphi_0(k) \neq k\}$ et $\varphi_1 = \tau_{k_0,\varphi_0(k_0)} \circ \varphi_0 = (k_0,\varphi_0(k_0)) \circ \varphi_0 \in \mathscr{S}_n$. On remarque que $\forall k \in [\![1,k_0]\!],\ \varphi_1(k) = k$. On peut donc itérer le raisonnement en construisant une suite strictement croissante $1 \leqslant k_0 < k_1 < \cdots < k_{p-1} \leqslant n$ et des permutations $(\varphi_i)_{1\leqslant i\leqslant p}$ jusqu'à ce que $\{k \in [\![1,n]\!] \mid \varphi_p(k) \neq k\} = \emptyset$, c'est-à-dire $\varphi_p = \mathrm{Id}$. Alors :

$$\mathrm{Id} = \varphi_p = \Big(k_{p-1},\varphi_{p-1}(k_{p-1})\Big) \circ \varphi_{p-1} = \Big(k_{p-1},\varphi_{p-1}(k_{p-1})\Big) \circ \Big(k_{p-2},\varphi_{p-2}(k_{p-2})\Big) \circ \varphi_{p-2} = \dots$$
$$\dots = \Big(k_{p-1},\varphi_{p-1}(k_{p-1})\Big) \circ \Big(k_{p-2},\varphi_{p-2}(k_{p-2})\Big) \circ \cdots \circ \Big(k_0,\varphi_0(k_0)\Big) \circ \varphi_0.$$

On en déduit que $\varphi_0 = (k_0,\varphi_0(k_0)) \circ \Big(k_1,\varphi_1(k_1)\Big) \circ \cdots \circ (k_{p-1},\varphi_{p-1}(k_{p-1}))$ car toute transposition est égale à sa bijection réciproque. Finalement, on a montré que $\mathscr{S}_n$ est inclus dans le sous-groupe engendré par les transpositions et l'inclusion réciproque est évidente.

□

Remarque. La démonstration précédente prouve de plus que toute permutation de $\mathscr{S}_n$ peut s'écrire comme une composée d'au plus $n-1$ transpositions (car $k_{p-1} < n$ sinon φ_{p-1} laisse inchangés exactement $n-1$ éléments de $[\![1,n]\!]$ ce qui est absurde). D'autre part, puisque $\tau_{i,j} \circ \tau_{i,k} = \tau_{j,k} \circ \tau_{i,j}$ lorsque $(i,j,k) \in [\![1,n]\!]^3$ sont deux à deux distincts, cette écriture n'est en général pas unique.

Exemple. Pour $n = 10$, le groupe symétrique $(\mathscr{S}_{10},\circ)$ contient $10! \approx 3,6 \times 10^6$ permutations, dont seulement $\frac{10\times(10-1)}{2} = 45$ transpositions. La démonstration précédente fournit un algorithme efficace pour décomposer chacune des permutations de $[\![1,10]\!]$ en une composée d'au plus $10-1 = 9$ transpositions.

2.3 Sous-groupes monogènes

Définition 8

*Un groupe $(G, \star)$ est dit **monogène** s'il est engendré par un seul élément, c'est-à-dire lorsque :*

$$\exists g \in G,\ G = \langle \{g\} \rangle = \left\{ g^{\star k} \mid k \in \mathbb{Z} \right\}.$$

*Dans ce cas, g est appelé un **générateur** de G.*

Propriété 8

Tout groupe monogène est abélien.

Exemple. Pour tout $n \in \mathbb{N}$, $(n\mathbb{Z}, +)$ est un groupe monogène dont les générateurs sont n et $-n$.

Théorème 2

Tout sous-groupe additif de $\mathbb{Z}$ est monogène, c'est-à-dire de la forme $n\mathbb{Z}$ où $n \in \mathbb{N}$ est unique.

Démonstration. Soit H un sous-groupe de $(\mathbb{Z}, +)$. Si $H = \{0\}$ alors $H = 0\mathbb{Z}$. Sinon, $H \cap \mathbb{N}^* \neq \emptyset$ car H est stable par passage à l'opposé. On pose $n = \min(H \cap \mathbb{N}^*)$. Montrons que $H = n\mathbb{Z}$. Puisque $n \in H$, on a déjà que $n\mathbb{Z} \subset H$ par stabilité. Pour l'inclusion réciproque, on fixe $h \in H$ et on pose $k = \max\{k \in \mathbb{Z} \mid kn \leqslant h\} = \lfloor h/n \rfloor$, donc $h - kn \in [\![0, n-1]\!]$. De plus, $h - kn \in H$ par stabilité. Or $H \cap [\![0, n-1]\!] = \{0\}$ car $n = \min(H \cap \mathbb{N}^*)$. On en déduit que $h = kn \in n\mathbb{Z}$, donc que $H = n\mathbb{Z}$. Enfin, $n \in \mathbb{N}$ est unique car $n\mathbb{Z} = \{0\} \iff n = 0$ et $\forall n \in \mathbb{N}^*,\ \min(n\mathbb{Z} \cap \mathbb{N}^*) = n$.

□

Remarque. Dans $(\mathbb{R}, +)$, il existe des sous-groupes non-monogènes. Par exemple $\mathbb{Q}$ n'est pas de la forme $x\mathbb{Z}$ où $x \in \mathbb{R}$ car le complémentaire de $x\mathbb{Z}$ contient des intervalles de $\mathbb{R}$ (par exemple $]0, |x|[\cap x\mathbb{Z} = \emptyset$) alors que $\mathbb{Q}$ est dense dans $\mathbb{R}$: $\forall a < b,\ ]a, b[\cap \mathbb{Q} \neq \emptyset$.

Théorème 3

Tout sous-groupe additif de $\mathbb{R}$ est de l'un des deux types suivants :

- *monogène, c'est-à-dire de la forme $x\mathbb{Z}$ où $x \in \mathbb{R}_+$ est unique ;*
- *ou bien dense dans $\mathbb{R}$, c'est-à-dire intersectant tout intervalle de $\mathbb{R}$.*

Démonstration. Soit H un sous-groupe de $(\mathbb{R}, +)$. Si $H = \{0\}$ alors $H = 0\mathbb{Z}$. Sinon, $H \cap \mathbb{R}_+^* \neq \emptyset$. On pose $x = \inf(H \cap \mathbb{R}_+^*)$.
1er cas : $x > 0$. Si $x \notin H$, alors il existe une suite strictement décroissante $(h_n)_{n\in\mathbb{N}} \in H^{\mathbb{N}}$ qui converge vers x, donc $(h_n - h_{n+1})_{n\in\mathbb{N}} \in (H \cap \mathbb{R}_+^*)^{\mathbb{N}}$ converge vers 0 ce qui contredit $x > 0$. Donc $x \in H$, puis on montre que $H = x\mathbb{Z}$ et que $x \in \mathbb{R}_+$ est unique en raisonnant comme dans la démonstration du théorème 2.
2e cas : $x = 0$. Soit $]a, b[\subset \mathbb{R}$. Puisque $\inf(H \cap \mathbb{R}_+^*) = 0$, il existe $h \in H$ tel que $0 < h < b - a$. On pose $k = \max\{k \in \mathbb{Z} \mid kh \leqslant a\} = \lfloor a/h \rfloor$, alors :

$$kh \leqslant a < (k+1)h < kh + b - a \leqslant b \quad \text{donc } (k+1)h \in]a, b[.$$

Or $(k+1)h \in H$ par stabilité, d'où $H \cap]a, b[\neq \emptyset$.

□

Exemple. Pour tout $x \in \mathbb{R}$, il existe deux suites d'entiers relatifs $(a_n)_{n\in\mathbb{N}} \in \mathbb{Z}^{\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}} \in \mathbb{Z}^{\mathbb{N}}$ telles que $\lim_{n\to+\infty} a_n + b_n\sqrt{2} = x$. En effet, $\mathbb{Z}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \mid (a, b) \in \mathbb{Z}^2\right\}$ est un sous-groupe de $(\mathbb{R}, +)$ (le sous-groupe engendré par 1 et $\sqrt{2}$) qui n'est pas monogène car sinon il serait de la forme $y\mathbb{Z}$ où $y \in \mathbb{R}_+^*$ et on aurait en particulier $\exists (k_1, k_2) \in \mathbb{Z}^2,\ 1 = k_1 y$ et $\sqrt{2} = k_2 y$, donc $\sqrt{2} = k_2/k_1 \in \mathbb{Q}$ ce qui est absurde. On en déduit bien que $\mathbb{Z}\left[\sqrt{2}\right]$ est une partie dense de $\mathbb{R}$.

Définition 9

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

- *Si $(G, \star)$ est monogène et fini alors on dit que $(G, \star)$ est un **groupe cyclique**.*
- *Soit $g \in G$. Si le sous-groupe engendré par g est cyclique, son ordre $|\langle\{g\}\rangle|$ est appelé l'**ordre** de g dans $(G, \star)$. Sinon, on dit que g est d'**ordre infini** dans $(G, \star)$.*

Exemple. Pour tout $n \in \mathbb{N}^*$, $(\mathbb{U}_n, \times)$ est un groupe cyclique et $e^{i2\pi/n}$ est d'ordre n.

Propriété 9

Soient $(G, \star)$ un groupe et $g \in G$. Si g est d'ordre fini dans $(G, \star)$, alors son ordre est égal au plus petit $n \in \mathbb{N}^*$ tel que $g^{\star n} = e$ et dans ce cas :

$$\langle\{g\}\rangle = \left\{g^{\star k} \mid k \in [\![0, n-1]\!]\right\}.$$

Démonstration. Puisque g est d'ordre fini, il existe $(k_1, k_2) \in \mathbb{Z}^2$ distincts tels que $g^{\star k_1} = a^{\star k_2}$. Quitte à échanger k_1 et k_2, on peut supposer que $k_1 < k_2$ alors $k_2 - k_1 \in \mathbb{N}^*$ et $g^{\star(k_2-k_1)} = g^{\star k_2} \star \overline{g^{\star k_1}} = e$ d'après les propriétés de calculs dans les groupes. Donc $n = \min\{n \in \mathbb{N}^* \mid g^{\star n} = e\}$ existe. On déduit d'un raisonnement similaire que $\text{card}\{g^{\star k} \mid k \in [\![0, n-1]\!]\} = n$. Il suffit donc de montrer que $\langle\{g\}\rangle = \{g^{\star k} \mid k \in [\![0, n-1]\!]\}$ pour conclure. Soit $k \in \mathbb{Z}$. On pose $\ell = \max\{\ell \in \mathbb{Z} \mid \ell n \leqslant k\} = \lfloor k/n \rfloor$. Alors $k - \ell n \in [\![0, n-1]\!]$ et $g^{\star k} = g^{\star k} \star (\overline{g^{\star n}})^{\star \ell} = g^{\star(k-\ell n)}$. Donc $\langle\{g\}\rangle \subset \{g^{\star k} \mid k \in [\![0, n-1]\!]\}$ et l'inclusion réciproque est immédiate.

□

Exemple. Soit $n \in \mathbb{N}^*$. Les transpositions sont d'ordre 2 dans le groupe symétrique. Alors que la permutation de $[\![1, n]\!]$ suivante :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 2 & 3 & 4 & \dots & n & 1 \end{pmatrix} \quad \text{est d'ordre } n \text{ dans } (\mathscr{S}_n, \circ).$$

3 Morphismes de groupes

3.1 Définition et propriétés

Définition 10

*Soient $(G, \star)$ et $(H, \diamond)$ deux groupes. On dit qu'une application $f : G \to H$ est un **homomorphisme de groupes** ou un **morphisme de groupes** lorsque :*

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

Exemple. Pour tout $a \in \mathbb{R}$, $f : x \mapsto ax$ est un homomorphisme de $(\mathbb{R}, +)$ vers $(\mathbb{R}, +)$.

Exemple. $\ln : x \mapsto \ln(x)$ est un homomorphisme de $(\mathbb{R}_+^*, \times)$ vers $(\mathbb{R}, +)$.

Exemple. $f : \theta \mapsto e^{i\theta}$ est un homomorphisme de $(\mathbb{R}, +)$ vers $(\mathbb{C}^*, \times)$ ou vers $(\mathbb{U}, \times)$.

Exemple. La dérivation est fonctions réelles dérivables sur $I \subset \mathbb{R}$ est un homomorphisme de groupes additifs. De même, l'application qui associe à une suite réelle ou complexe convergente sa limite est un homomorphisme de groupes additifs.

Exemple. Soient $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ et $n \in \mathbb{N}^*$. La transposée est un homomorphisme additif de $\mathscr{M}_n(\mathbb{K})$ vers lui-même, et le déterminant est un homomorphisme multiplicatif de $\mathscr{G}\ell_n(\mathbb{K})$ vers $\mathbb{K}^*$.

Exemple. Soient E un ensemble et $\sigma \in \mathscr{S}(E)$. On peut vérifier que l'application

$$\iota_\sigma : \mathscr{S}(E) \to \mathscr{S}(E), \varphi \mapsto \sigma \circ \varphi \circ \sigma^{\circ -1}$$

est un homomorphisme du groupe symétrique de E vers lui-même. De plus :

$$\forall \varphi \in \mathscr{S}(E),\ \forall x \in E,\ \iota_\sigma(\varphi)\Big(\sigma(x)\Big) = \sigma\Big(\varphi(x)\Big).$$

En particulier, $\iota_\sigma(\tau_{i,j}) = \tau_{\sigma(i),\sigma(j)}$ pour tout $(i,j) \in E^2$.

Propriété 10

Soit f un homomorphisme d'un groupe $(G,\star)$ vers un groupe $(H,\diamond)$. On a :

$$\forall x \in G,\ \forall n \in \mathbb{Z},\ f\left(x^{\star n}\right) = f(x)^{\diamond n}.$$

En particulier :

$$f(e_G) = e_H \quad et \quad \forall x \in G,\ f\left(\overline{x}\right) = \overline{f(x)}.$$

Démonstration. On a $f(e_G) = f(e_G \star e_G) = f(e_G) \diamond f(e_G)$ donc $f(e_G) = f(e_G) \diamond \overline{f(e_G)} = e_H$. On en déduit que pour tout $x \in G$, $f(x) \diamond f(\overline{x}) = f(x \star \overline{x}) = f(e_G) = e_H$ et de même $f(\overline{x}) \diamond f(x) = e_H$, donc $\overline{f(x)} = f(\overline{x})$ par unicité du symétrique de $f(x)$. Puis on généralise aux itérés par récurrences.

□

Propriété 11

Soit f un homomorphisme d'un groupe $(G,\star)$ vers un groupe $(H,\diamond)$.

- *Si G' est un sous-groupe de $(G,\star)$ alors $\{f(x) \mid x \in G'\}$ est un sous-groupe de $(H,\diamond)$.*
- *Si H' est un sous-groupe de $(H,\diamond)$ alors $\{x \in G \mid f(x) \in H'\}$ est un sous-groupe de $(G,\star)$.*

Démonstration. C'est immédiat d'après la propriété 5.

□

3.2 Image et noyau d'un homomorphisme de groupes

Définition 11

Soit f un homomorphisme d'un groupe $(G,\star)$ vers un groupe $(H,\diamond)$.

- *L'**image** de f est le sous-groupe de $(H,\diamond)$ défini par* $\mathrm{Im}(f) = \{f(x) \mid x \in G\}$.
- *Le **noyau** de f est le sous-groupe de $(G,\star)$ défini par* $\mathrm{Ker}(f) = \{x \in G \mid f(x) = e_H\}$.

Propriété 12

Soit f un homomorphisme d'un groupe $(G,\star)$ vers un groupe $(H,\diamond)$.

- *$f : G \to H$ est surjective si et seulement si* $\mathrm{Im}(f) = H$.
- *$f : G \to H$ est injective si et seulement si* $\mathrm{Ker}(f) = \{e_G\}$.

Démonstration. La première équivalence est évidente. Pour la deuxième, si $f : G \to H$ est injective alors e_G est le seul antécédent de e_H. Réciproquement, on remarque que :

$$\forall (x_1,x_2) \in G^2,\ f(x_1) = f(x_2) \implies x_1 \star \overline{x_2} \in \mathrm{Ker}(f) \quad \text{car} \quad f\left(x_1 \star \overline{x_2}\right) = f(x_1) \diamond \overline{f(x_2)}.$$

□

3.3 Morphismes particuliers

Définition 12

— *Un **endomorphisme de groupe** est un homomorphisme d'un groupe vers lui-même.*

— *Un **isomorphisme de groupes** est un homomorphisme bijectif.*

— *Un **automorphisme de groupe** est un endomorphisme bijectif, donc un isomorphisme d'un groupe sur lui-même.*

Définition 13

*Deux groupes $(G, \star)$ et $(H, \diamond)$ sont dits **isomorphes** s'il existe un isomorphisme de groupes de l'un vers l'autre. Dans ce cas, on note $(G, \star) \approx (H, \diamond)$.*

Exemple. Si $(G, \star)$ est un groupe monogène de générateur g d'ordre infini, alors on peut vérifier que $k \mapsto g^{\star k}$ est un isomorphisme de $(\mathbb{Z}, +)$ vers $(G, \star)$. On en déduit que tout sous-groupe additif de $\mathbb{Z}$ est isomorphe à $(\mathbb{Z}, +)$, et que tout sous-groupe d'un groupe monogène d'ordre infini est nécessairement un sous-groupe monogène d'ordre infini.

Exemple. $(\mathbb{Z}, +)$ et $(\mathbb{Q}, +)$ ne sont pas isomorphes car $\mathbb{Q}$ n'est pas monogène.

Exemple. $(\mathbb{R}, +) \approx (\mathbb{R}_+^*, \times)$ par l'isomorphisme $\exp : x \mapsto e^x$.

Propriété 13

— *Toute composée d'homomorphismes de groupes est un homomorphisme de groupes.*

— *La bijection réciproque de tout homomorphisme de groupes bijectif est un homomorphisme.*

Démonstration. C'est immédiat d'après la définition d'un homomorphisme de groupes.

□

Corollaire 1

L'ensemble des automorphismes d'un groupe $(G, \star)$ a une structure de groupe pour la composition d'applications. On le note $(\mathrm{Aut}(G), \circ)$.

Définition 14

*Soit $(G, \star)$ un groupe. Pour tout $a \in G$, on définit l'**automorphisme intérieur** $\iota_a \in \mathrm{Aut}(G)$ par :*

$$\iota_a : x \mapsto a \star x \star \overline{a}.$$

On peut vérifier que $\iota : a \mapsto \iota_a$ définit un homomorphisme du groupe $(G, \star)$ vers $(\mathrm{Aut}(G), \circ)$.

— *Son image $\mathrm{Im}(\iota) = \{i_a \mid a \in G\}$ est appelé le **sous-groupe des automorphimes intérieurs** de $(G, \star)$ et noté $\mathrm{Int}(G)$.*

— *Son noyau $\mathrm{Ker}(\iota) = \{a \in G \mid \forall x \in G,\ a \star x = x \star a\}$ est un sous-groupe abélien de $(G, \star)$, appelé le **centre** de $(G, \star)$ et noté $\mathcal{Z}(G)$.*

4 Groupes quotients

4.1 L'exemple du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$

Tout groupe cyclique est isomorphe à Z/nZ. En particulier, tout sous-groupe d'un groupe cyclique est cyclique.

Tout groupe monogène est isomorphe à Z ou à Z/nZ. En particulier, tout sous-groupe d'un groupe monogène est monogène.

Lemme 1 (*Division euclidienne*)

Étant donnés deux entiers relatifs a et $b \neq 0$, il existe un unique entier relatif q et un unique entier naturel r tel que $a = bq + r$ et $0 \leqslant r < |b|$. Les entiers q et r sont respectivement appelés le ***quotient*** *et le* ***reste*** *de la* ***division euclidienne*** *de a par b.*

$$\forall (a,b) \in \mathbb{Z} \times \mathbb{Z}^*,\ \exists !(q,r) \in \mathbb{Z} \times [\![0, |b| - 1]\!],\ a = bq + r.$$

Démonstration du lemme 1. On fixe $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$.

Existence. Dans le cas où $b > 0$, on pose :

$$q = \max\left\{k \in \mathbb{Z} \mid bk \leqslant a\right\} = \left\lfloor \frac{a}{b} \right\rfloor \in \mathbb{Z} \quad \text{puis} \quad r = a - bq \in \mathbb{N}.$$

On a bien $r < b$ car sinon $b(q+1) \leqslant a$ ce qui est absurde. De même, dans le cas où $b < 0$, il suffit de poser :

$$q = \min\left\{k \in \mathbb{Z} \mid bk \leqslant a\right\} = -\left\lfloor \frac{a}{-b} \right\rfloor \in \mathbb{Z} \quad \text{puis} \quad r = a - bq \in \mathbb{N}.$$

On vérifie que $r < -b$ car sinon $b(q-1) \leqslant a$.

Unicité. On suppose qu'il existe $(q_1, r_1) \in \mathbb{Z} \times [\![0, |b| - 1]\!]$ et $(q_2, r_2) \in \mathbb{Z} \times [\![0, |b| - 1]\!]$ tels que $a = bq_1 + r_1 = bq_2 + r_2$. Alors $b(q_1 - q_2) = r_2 - r_1 \in [\![-|b| + 1, |b| - 1]\!]$. Or le seul multiple de b entre $-|b| + 1$ et $|b| - 1$ est 0. On en déduit que $b(q_1 - q_2) = 0$ donc $q_1 = q_2$ et $r_1 = r_2$.

□