Groupes

Aperçu

D 1 Soit E un ensemble. On appelle **loi de composition interne** sur E une application

$$\mathsf{T} : E \times E \to E.$$

La valeur $\mathsf{T}(x, y)$ de T pour un couple $(x, y) \in E \times E$ s'appelle le **composé** de x et de y pour cette loi.

E 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 $\mathbb{Z}$.

D 3 Soit une loi de composition interne $(x, y) \mapsto x \star y$ sur un ensemble E.
On dit que $\star$ est **associative** si

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

D 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

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

E 5 La soustraction n'est pas associative dans $\mathbb{Z}$ car $7-(3-1) \neq (7-3)-1$ et n'est pas commutative car $8-4 \neq 4-8$.

E 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.

E 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 $(4 \star 4) \star 8 = 6$.

D 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 $e = e \star e' = e'$.

E 9 L'application Id_E est l'élément neutre de la loi de composition $\circ$ dans $\mathscr{F}(E, E)$.

E 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.

D 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.

D 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 $\star$.

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

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

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 $A\star\{\, a \,\}$.

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

E 13 L'addition sur $\mathbb{Z}$ induit une loi de composition interne sur $\mathcal{P}(\mathbb{Z})$, par exemple

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

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

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

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

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

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 $\mathscr{F}(X,E)$.

E 14 Soit $X = E = \mathbb{R}$, pour $f, g, s, p \in \mathscr{F}(\mathbb{R},\mathbb{R})$, on aura

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

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

D 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 $|G|$.

P 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.*

E 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 $+$.

E 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 $z \mapsto \frac{1}{a}z - \frac{b}{a}$.

E 19 Pour $n \in \mathbb{N}^\star$, $\left(\mathbb{U}_n, \cdot\right)$ est un groupe fini d'ordre n.

N 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**).

P 20 *Soit $(G, \star)$ un groupe. Alors, pour tous $x, y \in G$*

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

P 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

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

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.

N

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

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

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

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

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.

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

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

(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

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

D 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.

P 23 *Pour tout $x \in G$ et tout $(p, q) \in \mathbb{Z}^2$,*

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

N 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

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

On a aussi la relation
$$px + py = p(x+y).$$

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

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

est fausse en général. Par exemple

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

sauf si x et y commutent.

T 24 *Soient deux groupes $(G_1, \top)$ et $(G_2, \perp)$. On définit une loi $\star$ sur $G = G_1 \times G_2$ par*

$$\left(x_1, x_2\right) \star \left(y_1, y_2\right) = \left(x_1 \top y_1, x_2 \perp y_2\right).$$

1. *La loi $\star$ confère à $G_1 \times G_2$ une structure de groupe appelé* ***produit direct des groupes*** *$(G_1, \top)$ et $(G_2, \perp)$.*
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 $G_1, \ldots, G_n$.

D 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

$$\forall x \in H, x^{-1} \in H.$$

P 26 *Soit $(G, \star)$ un groupe et H une partie de G. Alors H est un sous-groupe de G si, et seulement si*

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

P 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*:*

$$\begin{array}{rcl} H \times H & \to & H \\ (x, y) & \mapsto & x \star y \end{array}.$$

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.

E 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,...

R 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

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

E 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 $(\mathbb{R},+)$.

T 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,

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

P 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.

T 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 $(G, \star)$.

T 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. ∎

D 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.

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

E 37

1. $\begin{array}{rcl} (\mathbb{R}_+^\star, .) & \to & (\mathbb{R}, +) \\ x & \mapsto & \ln x \end{array}$ est un isomorphisme de groupes.
2. $\begin{array}{rcl} (\mathbb{C}, +) & \to & (\mathbb{C}, +) \\ z & \mapsto & \bar{z} \end{array}$ est un automorphisme de groupes.
3. $\begin{array}{rcl} (\mathbb{Z}, +) & \to & (\mathbb{R}_+^\star, .) \\ n & \mapsto & 5^n \end{array}$ est un morphisme de groupes non-surjectif.
4. $\begin{array}{rcl} (\mathbb{Z}, +) & \to & (\{\,-1, 1\,\}, .) \\ n & \mapsto & (-1)^n \end{array}$ est un morphisme de groupes non-injectif.

E 38 L'application

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

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.

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

P 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. $\forall x \in G, \forall n \in \mathbb{Z}, f(x^n) = (f(x))^n$.

P 40 *La composée de deux morphismes de groupes est un morphisme de groupes.*

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

T 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*

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

   est un sous-groupe de G.

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

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

   est un sous-groupe de H.

D 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 $\ker(f)$.

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

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

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

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

P 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.*

E 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

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

E 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

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

E 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

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

T 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 $\operatorname{Im}(f) = H$.*

T 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,

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

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.

D 50 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.

T 51 *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.

E 52 Dans $(\mathbb{C}^\star, \cdot)$,

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

E 53 Dans $(\mathbb{Z}, +)$, le sous groupe engendré par n est $n\mathbb{Z}$.

E 54

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

T 55 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 $\langle a, b \rangle = \left\{ ia + jb \,\middle|\, (i,j) \in \mathbb{Z}^2 \right\}$.

T 56 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

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

D 57 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.

T 58 **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 $(\mathbb{U}_p, \cdot)$.*

C 59 *Soit $(G, \cdot)$ un groupe d'élément neutre e_G et $a \in G$.*
Les assertions suivantes sont équivalentes.

(i) *L'ensemble $\left\{ k \in \mathbb{N}^\star \mid a^k = e_G \right\}$ 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 $e_G, a, \dots, a^{p-1}$ et ils sont deux à deux distincts.*

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

Dans ce cas p est l'ordre de a.

T 60 **Lagrange**

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

C 61 *Soit G un groupe fini d'ordre n. On a alors*

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