# Chapitre 1

# Structures algébriques usuelles

## 1.1 Groupes et sous-groupes

**Définition 1.1 (Groupe)** *Un groupe $(G,\star)$ est un ensemble $G$ munie d'une loi de composition interne notée $\star$ vérifiant les trois propriétés suivantes :*

- *la loi $\star$ est associative : $\forall x,y,z \in G$, on a $x \star (y \star z) = (x \star y) \star z$ ;*
- *elle est muni d'un élément neutre $e \in G$ : $x \star e = e \star x$, $\forall x \in G$ ;*
- *tout élément $a \in G$ possède son symétrique dans $G$ : $\exists a' \in G$ tel que $a \star a' = a' \star a = e$.*

Si de plus $\star$ est commutative, on dit que $G$ est un groupe commutatif (ou abélien).

**Définition 1.2 (Sous-groupe)** *Soit $(G,\star)$ un groupe. Une partie $H \subset G$ est un sous-groupe de $G$ si:*

- *$e \in H$,*
- *pour tout $x,y \in H$, on a $x \star y \in H$,*
- *pour tout $x \in H$, on a $x^{-1} \in H$.*

**Théorème 1.1 (Caractérisation des sous-groupes)** *Soit $G$ un groupe et $H$ une partie de $G$. Les assertions suivantes sont équivalentes :*

*i) $H$ est un sous-groupe de $G$.*

*ii) $e_G \in H$ et $\forall h,h' \in H$, on a : $h^{-1}h' \in H$.*

**Définition 1.3 (Sous-groupe engendré par une partie)** *Soit $G$ un groupe et $S$ une partie de $G$. On appelle le sous-groupe de $G$ engendré par $S$, l'intersection de tous les sous-groupes de $G$ qui contiennent $S$. C'est le plus petit sous-groupe de $G$ contenant $S$, on le note $\langle S \rangle$.*

**Exemple 1.1** $\mathbb{Z} = \{n = n.1 \mid n \in \mathbb{Z}\} = \langle 1 \rangle$.
$U_n = \{z \in \mathbb{C} \mid z^n = 1\} = \langle e^{2i\pi/n} \rangle$.

**Théorème 1.2** *Toute intersection de sous-groupe de $G$ est un sous-groupe de $G$.*

## 1.2 Morphismes de groupes

**Définition 1.4** *Soient $G$ et $H$ deux sous-groupes. Une application $f : G \to H$ est un homomorphisme si la propriété suivante est vérifiée :*

$$\forall a,b \in G, \qquad f(ab) = f(a)f(b).$$

*Si en plus*

1) *l'application $f$ est injective, on l'appelle monomorphisme et on le note $f : G \hookrightarrow H$ ;*
2) *l'application $f$ est surjective, on l'appelle épimorphisme ;*
3) *l'application $f$ est bijective, on l'appelle isomorphisme et on dit que $G$ et $H$ sont isomorphes. Notation $G \simeq H$.*

Un homomorphisme (resp. isomorphisme) de $G$ dans $G$ s'appelle un endomorphisme (resp. automorphisme).

**Exemple 1.2** L'application exponentielle est un isomorphisme du groupe additif des nombres réels dans le groupe multiplicatif des nombres réels positifs. Son inverse est l'application logarithme.

**Définition 1.5** *Soit $f : G \to H$ un homomorphisme de groupes.*
*Le noyau de $f$ est l'ensemble $f^{-1}(\{e_H\}) = \{x \in G \mid f(x) = e_H\}$ noté* Ker $f$.
*L'image de $f$ est l'ensemble* $\operatorname{Im} f = \{y \in H \mid \exists x \in G : f(x) = y\} = f(G)$.

**Théorème 1.3** *Un homomorphisme est injectif si et seulement si son noyau est réduit à l'élément neutre.*

## 1.3 Groupes monogènes et cycliques

**Définition 1.6** *S'il existe un élément $x$ de $G$ tel que $G = \langle x \rangle$,on dit que $G$ est un groupe monogène.*

**Définition 1.7** *Un groupe cyclique est un groupe monogène fini. Il est engendré par un seul élément.*

**Théorème 1.4** *Les générateurs de $\mathbb{Z}/p\mathbb{Z}$ sont les $\bar{k}$ avec $k \wedge n = 1$.*

## 1.4 Ordre d'un élément dans un groupe

**Théorème 1.5** *Si $x$ est d'ordre fini, l'ordre de $x$ est le cardinal du sous-groupe de $G$ engendré par $x$.*

**Théorème 1.6** *Si $x$ est d'ordre fini $d$ et si $e$ désigne l'élément neutre de $G$, alors, pour $n$ dans $\mathbb{Z}$, on a : $x^n = e \Leftrightarrow d \mid n$.*

**Théorème 1.7** *L'ordre d'un élément d'un groupe fini divise le cardinal du groupe.*

**Définition 1.8 (Permutation, groupe symétrique)** *On appelle permutation de* $\{1,\ldots,n\}$ *toute bijection de* $\{1,\ldots,n\}$ *dans lui-même.*

On note $S_n$ l'ensemble des permutations de $\{1,\ldots,n\}$. Alors $(S_n,\circ)$ est un groupe, appelé le groupe symétrique de degré $n$.

**Définition 1.9 (Cycle, transposition)** • *Soit* $p \in [\![2,n]\!]$. *On appelle p-cycle de* $\{1,\ldots,n\}$ *ou cycle de longueur p de* $\{1,\ldots,n\}$ *toute permutation* $\sigma$ *de* $\{1,\ldots,n\}$ *pour laquelle il existe des éléments deux à deux distincts* $a_1,a_2,\ldots,a_p$ *de* $\{1,\ldots,n\}$ *tels que :*

$$\sigma(a_1) = a_2,\ \sigma(a_2) = a_3,\quad \sigma(a_{p-1}) = a_p \quad et \quad \sigma(a_p) = a_1$$
$$et \quad \sigma(a) = a \quad si\ a\ n'est\ aucun\ des\ éléments\ a_1,a_2,\ldots,a_p.$$

*un tel p-cycle est alors noté* $(a_1\ a_2\ \ldots\ a_p)$.

• *Un 2-cycle de* $\{1,\ldots,n\}$ *est aussi appelé une transposition de* $\{1,\ldots,n\}$.

**Théorème 1.8 (Décomposition d'une permutation)** *Toute permutation de* $S_n$ *se décompose en composition de cycles à supports disjoints. De plus cette décomposition est unique.*

**Théorème 1.9 ($S_n$ est engendré par ses transpositions)** *Toute permutation de* $\{1,\ldots,n\}$ *peut être décomposée comme un produit de transpositions.*

**Théorème 1.10 (Signature)** *Il existe une et une seule application* $\varepsilon$ *de* $S_n$ *dans* $\{-1,1\}$ *telle que* $\varepsilon(\tau) = -1$ *pour toute transposition* $\tau$ *et* $\varepsilon(\sigma\sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$ *pour toues permutations* $\sigma$ *et* $\sigma'$.

## 1.5 Anneaux

**Définition 1.10** *Un anneau est un triplet* $(A,+,.)$ *où A est un ensemble non-vide et* $+$ *et* $.$ *sont des lois de composition internes telles que :*

*1)* $(A,+)$ *est un groupe abélien ;*
$(A,.)$ *est un sous-groupe ;*

*ii) la multiplication est distributive par rapport à l'addition. Ce qui signifie que pour tout triplet* $(x,y,z)$ *d'éléments de A, on a :* $x.(y+z) = x.y + x.z$ *et* $(x+y).z = x.z + y.z$.

*2) L'élément neutre de l'addition est noté* $0_A$ *ou* $0$.

*3) Si de plus la multiplication est commutative, l'anneau est dit commutatif.*

*4) On dit que A est unitaire s'il est non nul et que* $(A,.)$ *admet un élément neutre noté* $1_A$ *ou* $1$ *ou* $e$.

*5) Deux éléments x et y de A commutent (ou sont permutables) si on a* $x.y = y.x$.

**Exemple 1.3** $(\mathbb{Z},+,\times)$ est un anneau commutatif.

**Définition 1.11 (Sous-anneau)** *Un sous-anneau de $A$ est une partie de $B$ de $A$ qui vérifie les propriétés suivants :*

*1)* $(-1_A) \in B$

*2)* *$B$ est stable pour les opérations $+$ et $-$.*

**Définition 1.12 (Morphisme d'anneaux)** *Soient $(A,+,.)$ et $(B,+,.)$ deux anneaux.*

*1) On appelle homomorphisme d'anneaux de $A$ dans $B$ une application $f$ de $A$ dans $B$ vérifiant les trois assertions suivantes :*

$$f(x+y) = f(x) + f(y) \quad f(xy) = f(x)f(y) \quad et \quad f(1_A) = 1_B.$$

*2) Le même vocabulaire concernant les monomorphismes, les épimorphismes et les isomorphismes vu en théorie des groupes se conserve pour les homomorphismes d'anneaux.*

*3) On dit que $A$ et $B$ sont deux anneaux isomorphes s'il existe un isomorphisme d'anneaux de $A$ sur $B$.*

**Théorème 1.11** *Soit $f$ un homomorphisme d'anneaux de $(A,+,.)$ vers $(B,+,.)$.*

*1) L'image par $f$ de tout sous-anneau de $A$ est un sous-anneau de $B$.*

*2) L'image de $f$ est un sous-anneau de $B$.*

*3) L'image par $f$ de tout idéal de $A$ est un idéal de $f(A)$.*

*4) L'image réciproque par $f$ de tout idéal de $B$ est un idéal de $A$.*

*5) Le noyau, $\mathrm{Ker}(f) = \{x \in A \mid f(x) = 0_B\} = f^{-1}(\{0_B\})$, de $f$ est un idéal de $A$.*

*6) Si $f$ est un isomorphisme d'anneaux, alors $f^{-1}$ l'est aussi.*

*7) Si $I$ est un idéal de $A$, alors la surjection canonique de $A$ sur $A/I$ est un homomorphisme d'anneaux.*

**Définition 1.13 (Anneau intègre)** *L'anneau $A$ est dit intègre s'il est non-nul, commutatif, unitaire et ne contient aucun diviseur de zéro.*

**Définition 1.14 (Corps)** *Un corps est un anneau unitaire dans lequel tout élément non-nul est inversible. Il est dit commutatif si sa loi multiplicative est commutative.*

**Exemple 1.4** 1) Les anneaux $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des corps commutatifs.

2) $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : (a,b) \in \mathbb{Q}^2\}$, $\mathbb{Q}[\mathrm{i}] = \{a + b\mathrm{i} \mid (a,b) \in \mathbf{Q}^2\}$ munis des lois induites par celles de $\mathbb{C}$ sont des corps commutatifs.

## 1.6 Idéaux d'un anneau commutatif

**Définition 1.15 (Idéal)** *Un idéal d'un anneau $A$ est un sous-groupe additif $I$ de $A$ vérifiant pour tout $a$ dans $I$ et tout $x$ dans $A$, on a : $a.x$ et $x.a$ sont dans $I$.*

**Exemple 1.5** Soit $A$ un anneau.

1) $\{0_A\}$ et $A$ sont deux idéaux, appelés idéaux **triviaux** de $A$.

2) En outre si $A$ est commutatif, alors pour tout $a$ dans $A$, $aA = \{ax \mid a \in A\}$ est un idéal de $A$.
   Un idéal propre de $A$ est un idéal non-trivial.
3) Si $A$ est unitaire et $I$ un idéal de $A$, alors $I = A$ si et seulement si $1_A \in I$.

**Définition 1.16** *Soit $A$ un anneau intègre. Soit $a \neq 0$ et $b$ deux éléments de $A$.*

*1) On dit que $a$ divise $b$ (ou que $a$ est un diviseur de $b$ ou que $b$ est un multiple de $a$) s'il existe $c$ dans $A$ tel que : $b = ac$ et on écrit $a \mid b$ et $c = \frac{b}{a}$.*

*2) Les éléments $a$ et $b$ sont dits associés si $a$ divise $b$ et $b$ divise $a$ ; c'est à dire s'il existe $u$ inversible dans $A$ tel que $a = ub$.*

**Théorème 1.12** *Soient $a$ et $b$ deux éléments de $A$. Alors, on a :*

*1) $a$ divise $b$ si et seulement si $(b)$ est inclu dans $(a)$ .*

*2) $a$ et $b$ sont associés si et seulement si $(a) = (b)$.*

*3) $a$ est inversible dans $A$ si et seulement si $(a) = A$.*

*4) $a$ est inversible si et seulement si $a$ divise tout élément de $A$.*

## 1.7 L'anneau $\mathbb{Z}/n\mathbb{Z}$

**Théorème 1.13** *Pour tout entier naturel $n$, $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si $n$ est premier.*

**Théorème chinois**
*Si $m$ et $n$ sont deux entiers premiers entre eux, les ensembles $\mathbb{Z}/mn\mathbb{Z}$ sur $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes.*

## 1.8 Anneaux de polynômes à une indéterminée

**Définition 1.17** *Soient $n \in \mathbb{N}^*$, $(P_1, \ldots, P_n) \in (\mathbb{K}[X] - \{0\})^n$, il existe un polynôme et un seul $D$, unitaire, non nul, diviseur commun de $P_1, \ldots, P_n$ ; $D$ est appelé le plus grand commun diviseur de $P_1, \ldots, P_n$ et noté* $\mathrm{PGCD}(P_1, \ldots, P_n)$.

**Théorème 1.14 (Identité de Bézout)** *Soit $P$ et $Q$ deux polynômes, $P$ et $Q$ sont premiers entre eux si et seulement s'il existe deux polynômes $M$ et $N$ tels que :*

$$PM + QN = 1.$$

**Lemme de Gauss**
*Etant donné trois polynômes $P$, $Q$ et $R$ tels que*

$$P \mid QR \quad P \wedge Q = 1 \text{ alors } \quad P \mid R.$$

**Définition 1.18 (Polynôme irréductible)** *Un polynôme $P$ de $\mathbb{K}[X]$ est dit irréductible sur le corps $\mathbb{K}$ s'il est non inversible et si les seuls diviseurs dans $\mathbb{K}[X]$ sont les polynômes associés à $P$, et les éléments de $\mathbb{K}\backslash\{0\}$.*

**Théorème de décomposition**
*Tout polynôme non-constant $P$ (non-inversible) peut s'écrire d'une manière unique sous la forme :*

$$P = \lambda P_1^{\alpha_1} P_2^{\alpha_2} \dots P_r^{\alpha_r}$$

*avec $\lambda \in \mathbb{K}^* = \mathbb{K}\backslash\{0\}$ ; $P_1$,$P_2$,...,$P_r$ des polynômes irréductibles et $\alpha_1,\dots,\alpha_r$ des entiers naturels.*

**Corollaire 1.1** *Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré un et les polynômes de degré deux de discriminant srictement négatif.*

**Théorème 1.15** *Les seuls polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré* 1.

## 1.9 Algèbres

**Définition 1.19** *Soit $E$ un ensemble, muni de deux lois internes $+$, $\times$ et d'une loi externe à opérateurs dans $\mathbb{K}$, .. Alors $(E,+,\times,.)$ est un $\mathbb{K}-$algèbre lorsque :*

*1) $(E,+,\times,.)$ est un $\mathbb{K}-$espace vectoriel.*
*2) La loi $\times$ est associative et admet un élément neutre (qu'on note $1_E$).*
*3) La loi $\times$ est distributive sur la loi $+$.*
*4) Pour tous $u$,$v \in E$, et tout $\lambda \in \mathbb{K}$, $(\lambda u) \times v = u \times (\lambda v) = \lambda(u \times v)$*

**Définition 1.20 (Sous-algèbre)** *Un sous-algèbre d'un $\mathbb{K}-$algèbre $(E,+,\times,.)$, est une partie $F$ de $E$ qui contient $1_E$ et qui est stable pour chacune des trois lois, c'est-à-dire :*

*1) $1_E \in F$*
*2) $\forall(u,v) \in F^2$, $u+v \in F$ et $u \times v \in F$*
*3) $\forall u \in \mathbb{K}$, $\forall \lambda \in \mathbb{K}$, $\lambda u \in F$.*

**Définition 1.21 (Morphisme d'algèbre)** *Soient $(E,+,\times,.)$ et $(F,+,\times,.)$ deux $\mathbb{K}-$algèbres. Soit $\phi$: $E \to F$. On dit que $\phi$ est un morphisme de $\mathbb{K}-$algèbres si les assertions suivantes sont vérifiées :*

*1) $\forall(u,v) \in E^2$, $\phi(u+v) = \phi(u) + \phi(v)$*
*2) $\forall(u,v) \in E^2$, $\phi(u \times v) = \phi(u) \times \phi(v)$*
*3) $\forall u \in E$, $\forall \lambda \in \mathbb{K}$, $\phi(\lambda u) = \lambda \phi(u)$*
*4) $\phi(1_E) = 1_F$.*

## 1.10 Exercices résolus

**Exercice 1.1** *Soit $G = \mathbb{R}^\star \times \mathbb{R}$ et $\star$ la loi de composition interne définie sur $G$ par*

$$(x,y) \star (x',y') = (xx',xy'+y)$$

*1) Montrer que $(G,\star)$ est un groupe non commutatif.*

*2) Montrer que* $\mathbb{R}_+^\star \times \mathbb{R}$ *est un sous-groupe de* $(G,\star)$.

**Solution.**

1) La loi $\star$ est bien définie, on montre que $*$ est associative, (1,0) est l'élément neutre et $(\frac{1}{x}, -\frac{y}{x})$ est le symétrique de $(x,y)$. Soient $(x,y), (x',y'), (x'',y'') \in G$

a) Associativité :

$$\begin{aligned}(x,y)\star(x',y')\star(x'',y'') &= (xx',xy'+y)\star(x'',y'')\\ &= (xx'x'',xx'y''+xy'+y)\end{aligned}$$

et

$$\begin{aligned}(x,y)\star((x',y')\star(x'',y'')) &= (x,y)\star(x'x'',x'y''+y')\\ &= (xx'x'',xx'y''+xy'+y)\end{aligned}$$

donc $\star$ est associative.

b) Elément neutre :

$$(x,y)\star(1,0) = (x,y) \quad \text{et} \quad (1,0)\star(x,y) = (x,y)$$

donc (1,0) est élément neutre.

c) Symétrie :

$$(x,y)\star(1/x, -y/x) = (1,0) \quad \text{et} \quad (1/x, -y/x)\star(x,y) = (1,0)$$

donc tout élément est symétrisable.

Finalement d'après a), b) et c), on a : $(G,\star)$ est un groupe.

$(1,2)\star(3,4) = (3,6)$ et $(3,4)\star(1,2) = (3,10)$ donc le groupe n'est pas commutatif.

2) $H = \mathbb{R}_+^\star \times \mathbb{R}$ est inclus dans $G$.

$(1,0) \in H$.

$$\forall (x,y),\ (x',y') \in H,\ (x,y)\star(x',y') \in H$$

car $xx' > 0$

$$\forall (x,y) \in H,\ (x,y)^{-1} = (1/x, -y/x) \in H$$

car $1/x > 0$.

D'où $H$ est un sous groupe de $(G,\star)$.

**Exercice 1.2** *1) L'ensemble des matrices* $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ *avec* $a,b,c,d \in \mathbb{R}$ *tels que* $ad - bc \neq 0$ *et* $a^2 - b^2 - c^2 - d^2 \leq 1$ *est-il un sous-groupe de* $\mathcal{G}l_2(\mathbb{R})$ *?*

*2) L'ensemble des matrices* $\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$ *avec* $a \in \mathbb{R}^*$ *et* $b \in \mathbb{R}$ *est-il un sous-groupe de* $\mathcal{G}l_2(\mathbb{R})$ *?*

*3) Existe-t-il une valeur* $M \in \mathbb{R}$ *telle que l'ensemble des matrices* $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ *avec* $a,b,c,d \in \mathbb{R}$ *tels que* $ad - bc \neq 0$ *et* $a \leq M$ *forme un sous-groupe de* $\mathcal{G}l_2(\mathbb{R})$ *?*

**Solution.**

1) L'ensemble $G$ des matrices $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ avec $a,b,c,d \in \mathbb{R}$ tels que $ad - bc \neq 0$ et $a^2 - b^2 - c^2 - d^2 \leq 1$ n'est pas un sous-groupe de $\mathcal{G}l_2(\mathbb{R})$. En effet, les deux matrices $\begin{pmatrix} 1 & 1 \\ 0 & \frac{1}{2} \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ 1 & \frac{1}{2} \end{pmatrix}$ appartiennent à $G$ et leur produit $\begin{pmatrix} 2 & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{4} \end{pmatrix}$ n'appartient pas à $G$.
2) L'ensemble $H$ des matrices $\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$ avec $a \in \mathbb{R}^*$ et $b \in \mathbb{R}$ est un sous-groupe de $\mathcal{G}l_2(\mathbb{R})$. En effet,
   - $I_2$ élément neutre de $\mathcal{G}l_2(\mathbb{R})$ appartient à $H$.
   - Soient $M = \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$ et $M' = \begin{pmatrix} c & d \\ 0 & c^{-1} \end{pmatrix}$ deux éléments de $H$ alors $MM' = \begin{pmatrix} ac & ad + bc^{-1} \\ 0 & (ac)^{-1} \end{pmatrix}$ donc le produit de deux éléments de $H$ appartient à $H$.
   - Soit $M = \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$. Alors $M^{-1} = \begin{pmatrix} a^{-1} & -b \\ 0 & a \end{pmatrix}$ appartient à $H$.
3) Soit $K_M$ l'ensemble des matrices $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ avec $a,b,c,d \in \mathbb{R}$ tels que $ad - bc \neq 0$ et $a \leq M$. On montre, en raisonnant par l'absurde, qu'il n'existe pas de valeur $M \in \mathbb{R}$ telle que $K_M$ forme un sous-groupe de $\mathcal{G}l_2(\mathbb{R})$.
   Soit $M \in \mathbb{R}$ tel que $K_M$ forme un sous-groupe de $Gl_2(\mathbb{R})$. Alors $I_2$ appartient à $K_M$ donc $M \geq 1$. Ainsi, les matrices $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et, pour tout $n \in \mathbb{N}$, $A_n = \begin{pmatrix} 1 & 1 \\ n & 1 \end{pmatrix}$ appartiennent à $K_n$ donc le produit $AA_n = \begin{pmatrix} 1+n & 0 \\ 0 & 1 \end{pmatrix}$ appartient à $K_n$. En conséquence, pour tout $n \in \mathbb{N}$, on a : $1 + n \leq M$, ce qui est absurde.

**Exercice 1.3** *Soit $G$ un groupe, $H$ et $K$ deux sous-groupes de $G$. Montrer que $H \cup K$ est un sous-groupe de $G$ si et seulement si $H \subset K$ ou $K \subset H$.*

**Solution.**

- Si $H \subset K$ alors $H \cup K = K$, qui est un sous-groupe de $H$. Même chose si $K \subset H$.
- Réciproquement, supposons que $H \cup K$ est un sous-groupe de $G$. Par l'absurde supposons que $H \not\subset K$ et $K \not\subset H$. Alors il existe $x \in H \setminus K$ et $y \in K \setminus H$. Comme $x,y \in H \cup K$ et que $H \cup K$ est un groupe alors $x.y \in H \cup K$. Donc $x.y \in H$ ou $x.y \in K$. Par exemple supposons $x.y \in H$ alors comme $x \in H$, $x^{-1} \in H$ et donc comme $H$ est un groupe $x^{-1}.x.y \in H$ et donc $y \in H$. Ce qui est en contradiction avec l'hypothèse $y \in K \setminus H$. En conclusion, parmi les sous-groupes $H$ et $K$ l'un est inclus dans l'autre.

**Exercice 1.4** *Soit $H$ un groupe abélien. Un élément $x \in H$ est dit d'ordre fini lorsqu'il existe $n \in \mathbb{N}$ tel que la somme $x + \cdots + x$ ($n$-fois) soit égale à 0. Montrer que l'ensemble des éléments d'ordre fini de $H$ est un sous-groupe abélien de $H$.*