20

# Structure de groupe

On suppose construits les ensembles usuels $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ avec les quatre opérations classiques. Nous reviendrons plus loin sur les constructions de $\mathbb{Z}$ à partir de $\mathbb{N}$, de $\mathbb{Q}$ à partir de $\mathbb{Z}$, de $\mathbb{R}$ à partir de $\mathbb{Q}$ et de $\mathbb{C}$ à partir de $\mathbb{R}$.

L'étude préliminaire de l'algèbre linéaire a nécessité l'utilisation des notions de groupe, anneau et corps sans une étude très approfondie.

On se propose dans ce chapitre et les deux suivants d'étudier plus en détail ces structures algébriques de base.

Les résultats de base en algèbre linéaire sont supposés acquis.

Les espaces de matrices (réelles ou complexes) ainsi que les espaces de fonctions polynomiales (à coefficients réels ou complexes) nous seront utiles pour illustrer certaines notions.

Nous supposerons également acquises les notions basiques d'arithmétique (division euclidienne, pgcd, ppcm, ...). Pour $a, b$ entiers relatifs, on note respectivement $a \wedge b$ et $a \vee b$ le pgcd et le ppcm de $a$ et $b$.

## 20.1 Loi de composition interne

**Définition 20.1** *On appelle loi de composition interne sur un ensemble non vide $G$ toute application $\varphi$ définie sur $G \times G$ et à valeurs dans $G$.*

Si $\varphi$ est loi de composition interne sur $G$, on notera souvent :

$$\forall\, (a,b) \in G^2,\ a \star b = \varphi\,(a,b)\,.$$

Il sera parfois commode de noter une telle loi sous la forme additive $(a,b) \mapsto a+b$ ou sous la forme multiplicative $(a,b) \mapsto a \cdot b$ ou plus simplement $(a,b) \mapsto ab$.

On notera $(G, \star)$ l'ensemble non vide $G$ muni de la loi de composition interne $\star$.

**Exemple 20.1** *L'addition et la multiplication usuelles sont des lois de composition interne sur* $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ *et* $\mathbb{C}$.

**Exemple 20.2** *Si $E$ est un ensemble non vide et $\mathcal{P}(E)$ l'ensemble de toutes les parties de $E$, les applications :*

$$(A,B) \mapsto A \cap B,\ (A,B) \mapsto A \cup B,\ (A,B) \mapsto A \triangle B = (A \cup B) \setminus (A \cap B)$$

*sont des lois de composition interne sur $\mathcal{P}(E)$ ($\triangle$ est l'opérateur de différence symétrique).*

**Exemple 20.3** *Si $E$ est un ensemble non vide et $\mathcal{F}(E)$ l'ensemble de toutes les applications de $E$ dans $E$, alors l'application de composition $(f,g) \mapsto f \circ g$ est une loi de composition interne sur $\mathcal{F}(E)$.*

**Exemple 20.4** *Dans l'ensemble $\mathcal{M}_n(\mathbb{R})$ des matrices carrées d'ordre $n$ à coefficients réels les opérations usuelles d'addition $(A,B) \mapsto A+B$ et de multiplication $(A,B) \mapsto AB$ sont des lois de composition interne.*

**Exemple 20.5** *Dans l'ensemble $GL_n(\mathbb{R})$ des matrices carrées d'ordre $n$ à coefficients réels inversibles l'addition n'est pas une loi interne (si $A$ est inversible, il en est de même de $B=-A$ et la somme $A+B=0$ ne l'est pas) et la multiplication est une loi interne.*

**Définition 20.2** *Soit $G$ un ensemble non vide muni d'une loi de composition interne $(a,b) \mapsto a \star b$. On dit que :*

1. *cette loi est associative si :*

$$\forall (a,b,c) \in G^3,\ (a \star b) \star c = a \star (b \star c)$$

2. *cette loi est commutative si :*

$$\forall (a,b) \in G^2,\ a \star b = b \star a$$

3. *$e$ est un élément neutre pour cette loi si :*

$$\forall a \in G,\ a \star e = e \star a = a$$

4. *un élément $a$ de $G$ est dit régulier (ou simplifiable) si :*

$$\forall (b,c) \in G^2,\ \begin{cases} a \star b = a \star c \Rightarrow b = c, \\ b \star a = c \star a \Rightarrow b = c. \end{cases}$$

**Remarque 20.1** *Dire qu'un élément $a \in G$ est régulier à gauche [resp. à droite] signifie que l'application $g \mapsto a \star g$ [resp. $g \mapsto g \star a$] est injective.*

Si $\star$ est une loi de composition interne associative sur $G$, on écrira $a \star b \star c$ pour $(a \star b) \star c$ ou $a \star (b \star c)$.

De manière plus générale, toujours dans le cas d'une loi associative, on peut effectuer les opérations $a_1 \star a_2 \star \cdots \star a_n$ où les $a_j$ sont des éléments de $G$, ce que l'on notera $\prod_{j=1}^{n} a_j$ dans le cas d'une loi multiplicative ou $\sum_{j=1}^{n} a_j$ dans le cas d'une loi additive. Ce produit (ou cette somme) est donc défini par $a_1 \in G$ et supposant $\prod_{j=1}^{n-1} a_j$ construit pour $n \geq 2$, on a :

$$\prod_{j=1}^{n} a_j = \prod_{j=1}^{n-1} a_j \star a_n$$

le parenthésage étant sans importance du fait de l'associativité.

Pour $n=0$, il sera commode de noter $\prod_{j=1}^{n} a_j = 1$ (ou $\sum_{j=1}^{n} a_j = 0$ dans le cas d'une loi additive).

Dans le cas où tous les $a_j$ sont égaux à un même élément $a$, ce produit est noté $a^n$ et on dit que c'est la puissance $n$-ième de $a$. On retiendra que ces éléments de $G$ sont donc définis par la relation de récurrence :

$$\begin{cases} a^0 = 1 \\ \forall n \in \mathbb{N},\ a^{n+1} = a^n \star a \end{cases}$$

Dans le cas où la loi est notée additivement, on note plutôt $na$ au lieu de $a^n$.

On vérifie facilement que $a^n \star a^m = a^m \star a^n = a^{n+m}$ [resp. $(na) + (ma) = (ma) + (na) = (n+m)\,a$ pour une loi additive] pour tous $n, m$ dans $\mathbb{N}^*$ (voir le théorème 20.9).

**Exemple 20.6** *Les opérations usuelles d'addition et de multiplication sont commutatives et associatives sur $G = \mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$. 0 est un élément neutre pour l'addition et 1 est un élément neutre pour la multiplication pour chacun de ces ensembles. Tous les éléments de $G$ sont simplifiables pour l'addition et tous les éléments de $G^* = G \setminus \{0\}$ sont simplifiables pour la multiplication.*

**Exemple 20.7** *Si $E$ est un ensemble non vide, les opérations $\cap$ et $\cup$ sont commutatives et associatives sur $\mathcal{P}(E)$. L'ensemble vide $\emptyset$ est un élément neutre pour $\cup$ et $E$ est un élément neutre pour l'intersection $\cap$.*

**Exemple 20.8** *Si $E$ est un ensemble non vide la composition des applications est associative et non commutative dans $\mathcal{F}(E)$. L'identité est un élément neutre pour cette loi.*

**Exemple 20.9** *Dans $\mathcal{M}_n(\mathbb{R})$ l'addition est associative et commutative et la multiplication est associative et non commutative.*

**Exercice 20.1** *Montrer que le produit vectoriel est une loi de composition interne non associative sur $\mathbb{R}^3$.*

**Solution 20.1** *On rappelle que ce produit vectoriel est la loi interne définie par :*

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \wedge \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} yz' - y'z \\ x'z - xz' \\ xy' - x'y \end{pmatrix}.$$

*En désignant par $\left(\overrightarrow{\imath}, \overrightarrow{\jmath}, \overrightarrow{k}\right)$ la base canonique de $\mathbb{R}^3$, on a :*

$$\overrightarrow{\jmath} \wedge \left(\overrightarrow{\jmath} \wedge \overrightarrow{k}\right) = \overrightarrow{\jmath} \wedge \overrightarrow{\imath} = -\overrightarrow{k},\ \left(\overrightarrow{\jmath} \wedge \overrightarrow{\jmath}\right) \wedge \overrightarrow{k} = \overrightarrow{0} \wedge \overrightarrow{k} = \overrightarrow{0}.$$

*Cette loi n'est donc pas associative.*
*Comme $\overrightarrow{u} \wedge \overrightarrow{v} = -\overrightarrow{v} \wedge \overrightarrow{u}$, cette loi n'est pas commutative (il existe des vecteurs tels que $\overrightarrow{v} \wedge \overrightarrow{u} \neq \overrightarrow{0}$).*

**Théorème 20.1** *Soit $(G, \star)$ un ensemble non vide muni d'une loi de composition interne. Si $G$ admet un élément neutre, alors ce dernier est unique.*

**Démonstration.** Soient $e, e'$ deux éléments neutres. On a alors $e = e \star e'$ puisque $e'$ est neutre et $e' = e \star e'$ puisque $e$ est neutre, ce qui implique $e = e'$. ∎

**Définition 20.3** *Soit $(G, \star)$ un ensemble non vide muni d'une loi de composition interne et admettant un élément neutre $e$. On dit qu'un élément $a$ de $G$ est inversible s'il existe un élément $a'$ dans $G$ tel que $a \star a' = a' \star a = e$. On dit alors que $a'$ est un inverse (ou un symétrique) de $a$ dans $G$.*

**Théorème 20.2** *Soit $(G,\star)$ un ensemble non vide muni d'une loi de composition interne associative et admettant un élément neutre $e$. Si $a\in G$ admet un inverse dans $G$, alors ce dernier est unique.*

**Démonstration.** Supposons que $a\in G$ admette deux inverses $a'$ et $a''$. On a alors :

$$a'\star a\star a''=(a'\star a)\star a''=e\star a''=a''$$

puisque la loi est associative et $a'$ est inverse de $a$ et :

$$a'\star a\star a''=a'\star(a\star a'')=a'\star e=a'$$

puisque $a''$ est inverse de $a$, ce qui implique $a'=a''$. ■

**Remarque 20.2** *Pour une loi non associative, l'unicité du symétrique n'est pas assurée. Par exemple dans l'ensemble $G=\{0,-1,1\}$ muni de la loi définie par la table :*

| $\star$ | 0 | $-1$ | 1 |
|---|---|---|---|
| 0 | 0 | $-1$ | 1 |
| $-1$ | $-1$ | 0 | 0 |
| 1 | 1 | 0 | 0 |

*0 est neutre et $1\star 1=1\star(-1)=0$.*

En cas d'existence, on notera $a^{-1}$ un inverse de $a$ dans $(G,\star)$, la loi $\star$ étant associative.

Dans le cas d'une loi de composition interne notée de façon additive, on notera plutôt $-a$ un inverse de $a$ et on l'appellera opposé.

**Exemple 20.10** *Dans $(\mathbb{N},+)$ seul 0 a un opposé et dans $(\mathbb{N},\cdot)$ seul 1 a un inverse.*

**Exemple 20.11** *Dans $(\mathbb{Z},+)$ tout élément admet un opposé et dans $(\mathbb{Z},\cdot)$ les seuls éléments inversibles sont 1 et $-1$.*

**Exemple 20.12** *Dans $(\mathbb{R}[x],+)$ tout élément admet un opposé et dans $(\mathbb{R}[x],\cdot)$ les seuls éléments inversibles sont les polynômes constants non nuls.*

**Exemple 20.13** *Le cours d'algèbre linéaire nous dit que l'ensemble des éléments inversibles de $(\mathcal{M}_n(\mathbb{R}),\cdot)$ est $GL_n(\mathbb{R})$.*

## 20.2 Groupes

**Définition 20.4** *Un groupe est un ensemble non vide $G$ muni d'une loi de composition interne $\star$ possédant les propriétés suivantes :*

- *la loi $\star$ est associative ;*
- *il existe un élément neutre $e$ pour la loi $\star$ ;*
- *tout élément de $G$ admet un symétrique.*

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

En général, s'il n'y pas de confusion possible, on dira tout simplement que $G$ est un groupe pour $(G,\star)$ est un groupe et on notera $ab$ ou $a+b$ le résultat de l'opération $a\star b$. Avec la première notation, on dit que $G$ est un groupe multiplicatif et on notera 1 l'élément neutre, $a^{-1}$ le symétrique d'un élément $a$ de $G$ et avec la seconde notation, on dit que $G$ est un groupe additif et on notera 0 l'élément neutre, $-a$ le symétrique qu'on appelle opposé.

**Exemple 20.14** *Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de l'addition usuelle sont des groupes abéliens.*

**Exemple 20.15** *L'ensemble $\mathbb{N}$ muni de l'addition usuelle n'est pas un groupe du fait qu'un élément non nul de $\mathbb{N}$ n'a pas d'opposé dans $\mathbb{N}$ (l'équation $a+x=0$ avec $a\neq 0$ dans $\mathbb{N}$ n'a pas de solution dans $\mathbb{N}$).*

**Exemple 20.16** *Les ensembles $\mathbb{Q}^*$, $\mathbb{R}^*$ et $\mathbb{C}^*$ munis de la multiplication usuelle sont des groupes abéliens.*

**Exemple 20.17** *L'ensemble $\mathbb{Z}^*$ muni de la multiplication usuelle n'est pas un groupe du fait qu'un élément de $\mathbb{Z}\backslash\{-1,0,1\}$ n'a pas d'inverse dans $\mathbb{Z}$ (l'équation $ax=1$ avec $a\in\mathbb{Z}\backslash\{-1,0,1\}$ n'a pas de solution dans $\mathbb{Z}$).*

**Exemple 20.18** *Si $E$ est un ensemble non vide, l'ensemble $\mathcal{P}(E)$ est alors un groupe pour l'opération de différence symétrique : $(A,B)\mapsto A\triangle B=(A\cup B)\setminus(A\cap B)$.*

**Exemple 20.19** *Si $E$ est un ensemble non vide, l'ensemble des bijections de $E$ dans lui même muni de la composition des applications est un groupe (en général non abélien). Ce groupe est le groupe des permutations de $E$, il est noté $S(E)$ ou $\mathfrak{S}(E)$.*

**Exemple 20.20** *L'ensemble $\mathcal{M}_n(\mathbb{R})$ des matrices carrées d'ordre $n$ à coefficients réels est un groupe additif, mais non multiplicatif.*

**Exemple 20.21** *L'ensemble $GL_n(\mathbb{R})$ des matrices carrées d'ordre $n$ à coefficients réels et inversibles est un groupe multiplicatif, mais non additif.*

**Théorème 20.3** *Dans un groupe $(G,\star)$ tout élément est simplifiable.*

**Démonstration.** Soient $a,b,c$ dans $G$. Si $a\star b=a\star c$, on a alors $a^{-1}\star a\star b=a^{-1}\star a\star c$, soit $b=c$. De même si $b\star a=c\star a$, alors $b\star a\star a^{-1}=c\star a\star a^{-1}$, soit $b=c$. ■

**Exercice 20.2** *Montrer que si $(G,\star)$ est un groupe, alors pour tout $a\in G$, la translation à gauche $g_a:x\mapsto a*x$ [resp. à droite $d_a:x\mapsto x*a$] est une bijection de $G$ d'inverse $g_{a^{-1}}$ [resp. $d_{a^{-1}}$].*

**Solution 20.2** *L'égalité $g_a(x)=g_a(y)$ équivaut à $a*x=a*y$ et multipliant à gauche par $a^{-1}$, on en déduit que $x=y$. L'application $g_a$ est donc injective.*
*Pour $y\in G$, l'équation $g_a(x)=y$ équivaut à $a*x=y$, ce qui entraîne $x=a^{-1}*y$. L'application $g_a$ est donc surjective.*
*En fait comme, pour tout $y\in G$, l'équation $g_a(x)=y$ a pour unique solution $x=a^{-1}*y$, on déduit immédiatement que $g_a$ est bijective d'inverse $g_{a^{-1}}$.*

**Exercice 20.3** *Montrer que si $(G,\star)$ est un groupe et $E$ un ensemble non vide, alors l'ensemble $G^E$ des applications de $E$ dans $G$ muni de la loi $\cdot$ définie par :*

$$\forall (f,g)\in G^E\times G^E,\ \forall x\in E,\ (f\cdot g)(x)=f(x)\star g(x)$$

*est un groupe et que ce groupe est commutatif si $G$ l'est.*

**Solution 20.3** *Pour $f, g$ dans $G^E$, $f \cdot g$ est bien une application de $E$ dans $G$, donc un élément de $G^E$.*
*L'application $1 : x \mapsto e$ est le neutre pour cette loi.*
*Si $f \in G^E$, l'application $f' : x \mapsto (f(x))^{-1}$ est l'inverse de $f$.*
*Pour $f, g, h$ dans $G^E$ et $x \in E$, on a :*

$$\begin{aligned}(f \cdot (g \cdot h))(x) &= f(x) * (g \cdot h)(x) = f(x) * (g(x) \star h(x)) \\ &= (f(x) * g(x)) \star h(x) = (f \cdot g)(x) * h(x) \\ &= ((f \cdot g) \cdot h)(x)\end{aligned}$$

*et donc $f \cdot (g \cdot h) = (f \cdot g) \cdot h$.*
*L'ensemble $G^E$ muni de la loi $\cdot$ est donc un groupe.*
*Si $G$ est commutatif, on a alors pour $f, g$ dans $G^E$ et tout $x \in E$, $(f \cdot g)(x) = f(x) \star g(x) = g(x) \star f(x) = (g \cdot f)(x)$, ce qui revient à dire que $f \cdot g = g \cdot f$. Le groupe $\left(G^E, \cdot\right)$ est donc commutatif si $G$ l'est.*

**Exercice 20.4** *Soient $G, H$ deux groupes multiplicatifs. Montrer que le produit direct $G \times H$ muni de la loi :*

$$((a_1, a_2), (b_1, b_2)) \mapsto (a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2)$$

*est un groupe.*

**Solution 20.4** *Laissée au lecteur.*

De manière plus générale, si $H_1, \cdots, H_n$ sont des groupes multiplicatifs, alors le produit direct $H_1 \times \cdots \times H_n$ muni de la loi :

$$((a_1, \cdots, a_n), (b_1, \cdots, b_n)) \mapsto (a_1 b_1, \cdots, a_n b_n)$$

est un groupe et ce groupe est commutatif si, et seulement si, tous les $H_i$ le sont.

Si $(G, \star)$ est un groupe tel que $G$ ait un nombre fini $n \geq 1$ d'éléments, on dira alors que $G$ est un groupe fini d'ordre (ou de cardinal) $n$. Pour un tel groupe fini d'ordre petit, on peut dresser sa table de composition. Cette table est appelée table de Pythagore.

**Exercice 20.5** *Montrer que l'ensemble $G = \{e, a, b, c\}$ muni de la loi $\star$ définie par la table suivante :*

| $\star$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $b$ | $a$ | $e$ |

*est un groupe commutatif ($a \star b$ est situé à l'intersection de la ligne de $a$ et de la colonne de $b$). Ce groupe est le groupe de Klein. Une représentation géométrique est donnée par l'ensemble $\{Id, \sigma_x, \sigma_y, \sigma_z\}$, où $Id$ est l'identité de l'espace $\mathbb{R}^3$ et $\sigma_x, \sigma_y, \sigma_z$ sont les symétries orthogonales par rapport aux trois axes $O_x$, $O_y$ et $O_z$, en munissant cet ensemble de la composition des applications.*

**Solution 20.5** *Laissée au lecteur.*

**Exercice 20.6** *La table suivante :*

| $\star$ | $e$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ | $d$ |
| $a$ | $a$ | $e$ | $d$ | $b$ | $c$ |
| $b$ | $b$ | $c$ | $e$ | $d$ | $a$ |
| $c$ | $c$ | $d$ | $a$ | $e$ | $b$ |
| $d$ | $d$ | $b$ | $c$ | $a$ | $e$ |

*définit-elle un groupe ?*

**Solution 20.6** *La loi n'est pas associative puisque :*

$$\begin{cases} a \star (b \star c) = a \star d = c \\ (a \star b) \star c = d \star c = a \neq c \end{cases}$$

**Exercice 20.7** *Soit $(G, \star)$ un ensemble non vide muni d'une loi de composition interne associative, admettant un élément neutre $e$ à gauche, c'est-à-dire que :*

$$\forall a \in G,\ e \star a = a$$

*et telle que tout élément de $G$ admette un symétrique à gauche, c'est-à-dire que :*

$$\forall a \in G,\ \exists a' \in G \mid a' \star a = e.$$

*Montrer alors que $(G, \star)$ est un groupe ($e$ est alors le neutre de $(G, \star)$ et $a'$ le symétrique de $a$).*

**Solution 20.7** *Soient $a \in G$ et $a' \in G$ tel que $a' \star a = e$. En désignant par $a''$ un inverse à gauche de $a'$, on a :*

$$a \star a' = a'' \star a' \star a \star a' = a'' \star (a' \star a) \star a' = a'' \star a' = e,$$

*ce qui signifie que $a'$ est aussi un inverse à droite de $a$. Et avec :*

$$a \star e = a \star (a' \star a) = (a \star a') \star a = e \star a = a,$$

*on déduit que $e$ est aussi un neutre à droite. En définitive, $e$ est un élément neutre dans $(G, \star)$ et $a'$ est le symétrique de $a$. Avec l'associativité de $\star$, il en résulte que $(G, \star)$ est un groupe.*

L'exercice précédent nous dit que pour une loi associative la vérification de l'existence d'un neutre à gauche et d'un inverse à gauche est suffisante pour affirmer qu'on a une structure de groupe.

**Exercice 20.8** *Montrer que l'ensemble $G = ]-1, 1[$ muni de la loi $\star$ définie par :*

$$x \star y = \frac{x + y}{1 + xy}$$

*est un groupe commutatif.*

**Solution 20.8** *Pour $x, y$ dans $]-1,1[$, on a $|xy|<1$, donc $1+xy>0$ et $x\star y$ est bien défini. De plus avec :*

$$\begin{aligned}(x+y)^2-(1+xy)^2 &= x^2+y^2-1-x^2y^2\\ &= \left(x^2-1\right)\left(1-y^2\right)<0\end{aligned}$$

*on déduit que $|x\star y|<1$ et $\star$ défini bien une loi interne sur $G$.*
*De la commutativité de la somme et du produit sur $\mathbb{R}$ on déduit que $\star$ est commutative.*
*Pour tout $x\in G$, on a $x\star 0=x$ et $x\star(-x)=0$, donc $0$ est neutre et tout élément de $G$ est inversible.*
*Enfin pour $x, y, z$ dans $G$, on a :*

$$\begin{aligned}x\star(y\star z) &= \frac{x+y\star z}{1+x\cdot y\star z}=\frac{x+\frac{y+z}{1+yz}}{1+x\frac{y+z}{1+yz}}\\ &= \frac{x+y+z+xyz}{xy+xz+yz+1}\end{aligned}$$

*et :*

$$\begin{aligned}(x\star y)\star z &= \frac{x\star y+z}{1+x\star y\cdot z}=\frac{\frac{x+y}{1+xy}+z}{1+\frac{x+y}{1+xy}z}\\ &= \frac{x+y+z+xyz}{xy+xz+yz+1}\end{aligned}$$

*donc $\star$ est associative.*

**Exercice 20.9** *Montrer que l'ensemble $G=\left]-\frac{\pi}{2},\frac{\pi}{2}\right[$ muni de la loi $\star$ définie par :*

$$x\star y=\arctan\left(\tan(x)+\tan(y)\right)$$

*est un groupe commutatif.*

**Solution 20.9** *La fonction* arctan *étant bijective de $\mathbb{R}$ sur $\left]-\frac{\pi}{2},\frac{\pi}{2}\right[$ l'application $\star$ défini bien une loi interne sur $G$.*
*De la commutativité de la somme sur $\mathbb{R}$ on déduit que $\star$ est commutative.*
*Pour tout $x\in G$, on a $x\star 0=x$ et $x\star(-x)=0$ (la fonction* tan *est impaire), donc $0$ est neutre et tout élément de $G$ est inversible.*
*Enfin pour $x, y, z$ dans $G$, on a :*

$$\begin{aligned}x\star(y\star z) &= \arctan\left(\tan(x)+\tan(y\star z)\right)\\ &= \arctan\left(\tan(x)+(\tan(y)+\tan(z))\right)\end{aligned}$$

*et :*

$$\begin{aligned}(x\star y)\star z &= \arctan\left(\tan(x\star y)+\tan(z)\right)\\ &= \arctan\left(\tan(x)+(\tan(y)+\tan(z))\right)\end{aligned}$$

*ce qui montre que $\star$ est associative.*

Les deux exercices précédents ne sont que des cas particuliers de l'exercice 20.34.

**Théorème 20.4** *Soit $(G,\star)$ un groupe. Pour tous $a,b$ dans $G$, on a $(a^{-1})^{-1}=a$ et $(a\star b)^{-1}=b^{-1}\star a^{-1}$.*

**Démonstration.** La première égalité se déduit immédiatement de la définition de $a^{-1}$ et la deuxième résulte de :

$$b^{-1}\star a^{-1}\star a\star b=b^{-1}\star e\star b=b^{-1}\star b=e$$

■

Plus généralement, on vérifie facilement par récurrence sur $p\geq 2$ que si $a_1,\cdots,a_p$ sont des éléments d'un groupe $G$, on a alors :

$$(a_1\star\cdots\star a_p)^{-1}=a_p^{-1}\star\cdots\star a_1^{-1}.$$

**Exercice 20.10** *Soit $G$ un groupe multiplicatif d'élément neutre 1. Montrer que si on a $a^2=1$ pour tout $a$ dans $G$, alors $G$ est commutatif.*

**Solution 20.10** *Pour $a,b$ dans $G$, de $abab=(ab)^2=1$, on déduit que $a(abab)b=ab$, soit $a^2bab^2=ab$ ou encore $ba=ab$.*

**Exercice 20.11** *Soit $G$ un groupe multiplicatif d'élément neutre 1.*

1. *Montrer que $G$ est commutatif si, et seulement si, on a $(ab)^2=a^2b^2$ pour tous $a,b$ dans $G$ (ce qui revient à dire que l'application $a\mapsto a^2$ est un morphisme de groupes, cette notion étant définie au paragraphe 20.7).*
2. *Montrer que $G$ est commutatif si, et seulement si, on a $(ab)^{-1}=a^{-1}b^{-1}$ pour tous $a,b$ dans $G$ (ce qui revient à dire que l'application $a\mapsto a^{-1}$ est un morphisme de groupes).*

**Solution 20.11**

1. *Dans le cas où $G$ est commutatif, on a pour tous $a,b$ dans $G$ :*

   $$(ab)^2=abab=aabb=a^2b^2.$$

   *Réciproquement, si $(ab)^2=a^2b^2$ pour tous $a,b$ dans $G$, de $abab=(ab)^2=a^2b^2=aabb$, on déduit par simplification à gauche par $a$ et à droite par $b$ que $ba=ab$.*
   *On peut retrouver le résultat de l'exercice précédent avec ce résultat. Si $a^2=1$ pour tout $a$ dans $G$, on a alors pour tous $a,b$ dans $G$, $(ab)^2=1=a^2b^2$ et $G$ est commutatif.*
2. *Dans le cas où $G$ est commutatif, on a pour tous $a,b$ dans $G$ :*

   $$a^{-1}b^{-1}ab=a^{-1}b^{-1}ba=1$$

   *donc $a^{-1}b^{-1}=(ab)^{-1}$.*
   *Réciproquement, si $(ab)^{-1}=a^{-1}b^{-1}$ pour tous $a,b$ dans $G$, on a alors $ab=\left((ab)^{-1}\right)^{-1}=(a^{-1}b^{-1})^{-1}=ba$ et $G$ est commutatif.*

Dans $(GL_n(\mathbb{R}),\cdot)$ qui est non commutatif, on a en général $(AB)^n\neq A^nB^n$ pour $n\geq 2$ dans $\mathbb{N}$. Par exemple, pour $A=\begin{pmatrix}1&2\\3&4\end{pmatrix}$ et $B=\begin{pmatrix}1&1\\0&1\end{pmatrix}$, on a $(AB)^2=\begin{pmatrix}10&24\\24&58\end{pmatrix}$ et $A^2B^2=\begin{pmatrix}7&24\\15&52\end{pmatrix}$.

On peut aussi remarquer que les éléments de $\mathcal{M}_n(\mathbb{R})$ ne sont pas tous simplifiables pour le produit. Par exemple, pour $A=\begin{pmatrix}1&0\\0&0\end{pmatrix}$ et $B=\begin{pmatrix}0&0\\1&0\end{pmatrix}$, on a $AB=0=A\cdot 0$ avec $B\neq 0$.

## 20.3 Sous-groupes

**Définition 20.5** *Soit $(G, \star)$ un groupe. Un sous-groupe de $G$ est un sous-ensemble $H$ de $G$ tel que :*
- *$H$ est non vide ;*
- *pour tous $a, b$ dans $H$, $a \star b^{-1}$ est dans $H$.*

Le résultat qui suit nous donne une définition équivalente de la notion de sous-groupe.

**Théorème 20.5** *Soit $(G, \star)$ un groupe. Un sous-ensemble $H$ de $G$ est sous-groupe si, et seulement si :*
- *$H$ contient l'élément neutre $e$ de $G$ ;*
- *$H$ est stable pour la loi $\star$, c'est-à-dire que :*

$$\forall\, (a, b) \in H^2,\ a \star b \in H$$

- *$H$ est stable par passage à l'inverse, c'est-à-dire que :*

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

**Démonstration.** Soit $H$ un sous-groupe de $G$.
Pour $a \in H$, on a $e = a \star a^{-1} \in H$, $a^{-1} = e \star a^{-1} \in H$ et pour $b \in H$, $a \star b = a \star (b^{-1})^{-1} \in H$.
Réciproquement si $H$ contient $e$, il est non vide et s'il est stable par multiplication et passage à l'inverse, on a pour $a, b$ dans $H$, $b^{-1} \in H$ et $a \star b^{-1} \in H$. ∎
On vérifie facilement qu'un sous-groupe $H$ d'un groupe $G$ est lui même un groupe et $H$ est commutatif si $G$ l'est.

**Exemple 20.22** *Si $(G, \star)$ est un groupe d'élément neutre $e$, alors $H = \{e\}$ et $G$ sont des sous-groupes de $G$. On dit que ce sont les sous-groupes triviaux de $G$.*

**Exemple 20.23** *L'ensemble $\Gamma$ des nombres complexes de module égal à 1 (le cercle unité) est un sous-groupe du groupe multiplicatif $\mathbb{C}^*$.*

**Exemple 20.24** *Pour tout entier $n \geq 1$, l'ensemble $\Gamma_n = \{z \in \mathbb{C} \setminus z^n = 1\}$ des racines $n$-èmes de l'unité est un sous-groupe de $\Gamma$.*

**Exemple 20.25** *Pour tout entier naturel $n$, l'ensemble $n\mathbb{Z} = \{q \cdot n \mid q \in \mathbb{Z}\}$ des multiples de $n$ est un sous groupe de $(\mathbb{Z}, +)$ . En réalité ce sont les seuls, comme le montre le théorème suivant qui est une conséquence du théorème de division euclidienne dans $\mathbb{Z}$ (théorème 23.1).*

**Théorème 20.6** *Si $G$ est un sous-groupe de $(\mathbb{Z}, +)$ , il existe alors un unique entier naturel $n$ tel que*

$$G = n\mathbb{Z} = \{qn \mid q \in \mathbb{Z}\}$$

*Cet entier $n$ est le plus petit élément de $G \cap \mathbb{N}^*$.*

**Démonstration.** Si $G = \{0\}$ , on a $G = 0\mathbb{Z}$.
Si $G \neq \{0\}$ , il existe dans $G$ un entier $a$ non nul et comme $G$ est un sous-groupe de $(\mathbb{Z}, +)$ $-a$ est aussi dans $G$ et l'un des entiers $a$ ou $-a$ est dans $G^+ = G \cap \mathbb{N}^*$. L'ensemble $G^+$ est donc une partie non vide de $\mathbb{N}^*$ et en conséquence admet un plus petit élément $n \geq 1$. Comme $n \in G$ et $G$ est un groupe additif, on a $n\mathbb{Z} \subset G$. D'autre part, pour tout $m \in G$, la division

euclidienne par $n$ donne $m = qn + r$ avec $r = m - nq \in G^+$ et $r \leq n-1$, ce qui impose $r = 0$ par définition de $n$. On a donc $G \subset n\mathbb{Z}$ et $G = n\mathbb{Z}$.

L'unicité provient du fait que $n\mathbb{Z} = m\mathbb{Z}$ si, et seulement si, $n = \pm m$ et pour $n, m$ positifs, on a nécessairement $n = m$. ■

Nous verrons avec le chapitre sur les anneaux, que le résultat précédent peut se traduire en disant que l'anneau $\mathbb{Z}$ est principal et il a de nombreuses applications.

La notion de sous-groupe est commode pour montrer qu'un ensemble est un groupe : on peut essayer de le voir comme sous-groupe d'un groupe connu, ce qui évite de prouver l'associativité. Les exercices qui suivent illustrent cette idée.

**Exercice 20.12** *Soit $i$ dans $\mathbb{C}$ tel que $i^2 = -1$. Montrer que $G = \{1, -1, i, -i\}$ est un groupe multiplicatif.*

**Solution 20.12** *On montre que c'est un sous-groupe de $\mathbb{C}$, ce qui se déduit de la table de multiplication :*

| $\cdot$ | $1$ | $-1$ | $i$ | $-i$ |
|---|---|---|---|---|
| $1$ | $1$ | $-1$ | $i$ | $-i$ |
| $-1$ | $-1$ | $1$ | $-i$ | $i$ |
| $i$ | $i$ | $-i$ | $-1$ | $1$ |
| $-i$ | $-i$ | $i$ | $1$ | $-1$ |

**Exercice 20.13** *Montrer que l'ensemble $T_n(\mathbb{R})$ des matrices carrées d'ordre $n$ à coefficients réels triangulaires supérieures à termes diagonaux non nuls est un groupe multiplicatif.*

**Solution 20.13** *On a $T_n(\mathbb{R}) \subset GL_n(\mathbb{R})$ puisque le déterminant d'une matrice triangulaire est égal au produit de ces termes diagonaux. La matrice identité $I_n$ est dans $T_n(\mathbb{R})$ et pour $A, B$ dans $T_n(\mathbb{R})$ de diagonales respectives $(\lambda_1, \cdots, \lambda_n)$ et $(\mu_1, \cdots, \mu_n)$, l'inverse de $B$ est une matrice triangulaire de diagonale $\left(\frac{1}{\mu_1}, \cdots, \frac{1}{\mu_n}\right)$ et le produit $AB^{-1}$ est une matrice triangulaire de diagonale $\left(\frac{\lambda_1}{\mu_1}, \cdots, \frac{\lambda_n}{\mu_n}\right)$, c'est donc un élément de $T_n(\mathbb{R})$. En définitive, $T_n(\mathbb{R})$ est un sous-groupe de $GL_n(\mathbb{R})$.*

**Exercice 20.14** *Montrer que l'ensemble $TU_n(\mathbb{R})$ des matrices carrées d'ordre $n$ à coefficients réels triangulaires supérieures à termes diagonaux tous égaux à $1$ est un groupe multiplicatif (le groupe des matrices triangulaires unipotentes).*

**Solution 20.14** *On procède comme pour l'exercice précédent.*

**Exercice 20.15** *Montrer que l'ensemble $SL_n(\mathbb{R})$ des matrices carrées réelles d'ordre $n$ de déterminant égal à $1$ est un sous-groupe de $GL_n(\mathbb{R})$.*

**Solution 20.15** *Comme les matrices de $SL_n(\mathbb{R})$ ont un déterminant non nul, elles sont inversibles. On a donc $SL_n(\mathbb{R}) \subset GL_n(\mathbb{R})$.*
*La matrice identité $I_n$ est dans $SL_n(\mathbb{R})$ et pour $A, B$ dans $SL_n(\mathbb{R})$, on a $\det(AB^{-1}) = \dfrac{\det(A)}{\det(B)} = 1$, donc $AB^{-1} \in SL_n(\mathbb{R})$.*

**Exercice 20.16** *Montrer que l'ensemble $\mathcal{O}_2^+(\mathbb{R})$ des matrices de rotation défini par :*

$$\mathcal{O}_2^+(\mathbb{R}) = \left\{ R_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \mid \theta \in \mathbb{R} \right\}$$

*est un groupe multiplicatif commutatif.*

**Solution 20.16** *On vérifie que c'est un sous-groupe du groupe multiplicatif* $SL_2(\mathbb{R})$.
*Pour tout réel* $\theta$, *on a* $\det(R_\theta) = 1$, *donc* $R_\theta \in SL_2(\mathbb{R})$. *On vérifie facilement que* $R_\theta R_{-\theta} = I_n$, *ce qui signifie que* $R_\theta^{-1} = R_{-\theta}$.
*On a* $I_n = R_0 \in \mathcal{O}_2^+(\mathbb{R})$ *et pour* $R_{\theta_1}$, $R_{\theta_2}$ *dans* $\mathcal{O}_2^+(\mathbb{R})$, $R_{\theta_1} R_{\theta_2^{-1}} = R_{\theta_1 - \theta_2} \in \mathcal{O}_2^+(\mathbb{R})$.
*Donc* $\mathcal{O}_2^+(\mathbb{R})$ *est un sous-groupe de* $SL_2(\mathbb{R})$.
*Avec* $R_{\theta_1} R_{\theta_2} = R_{\theta_1+\theta_2}$, *on déduit que* $\mathcal{O}_2^+(\mathbb{R})$ *est commutatif.*

**Exercice 20.17** *L'ensemble* $\mathcal{O}_2^-(\mathbb{R})$ *des matrices de réflexion défini par :*

$$\mathcal{O}_2^-(\mathbb{R}) = \left\{ S_\theta = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix} \mid \theta \in \mathbb{R} \right\}$$

*est-il un groupe multiplicatif ? Que dire du produit de deux réflexions ?*

**Solution 20.17** *Pour tout réel* $\theta$, *on a* $\det(R_\theta) = -1 \neq 0$, *donc* $\mathcal{O}_2^-(\mathbb{R}) \subset GL_2(\mathbb{R})$.
*Comme* $I_n \notin \mathcal{O}_2^-(\mathbb{R})$, *cet ensemble n'est pas un sous-groupe de* $GL_2(\mathbb{R})$.
*Pour* $\theta_1, \theta_2$ *dans* $\mathbb{R}$, *on a :*

$$\begin{aligned} S_{\theta_1} S_{\theta_2} &= \begin{pmatrix} \cos(\theta_1) & \sin(\theta_1) \\ \sin(\theta_1) & -\cos(\theta_1) \end{pmatrix} \begin{pmatrix} \cos(\theta_2) & \sin(\theta_2) \\ \sin(\theta_2) & -\cos(\theta_2) \end{pmatrix} \\ &= \begin{pmatrix} \cos\theta_1\cos\theta_2 + \sin\theta_1\sin\theta_2 & \cos\theta_1\sin\theta_2 - \cos\theta_2\sin\theta_1 \\ -\cos\theta_1\sin\theta_2 + \cos\theta_2\sin\theta_1 & \cos\theta_1\cos\theta_2 + \sin\theta_1\sin\theta_2 \end{pmatrix} \\ &= \begin{pmatrix} \cos(\theta_1 - \theta_2) & -\sin(\theta_1 - \theta_2) \\ \sin(\theta_1 - \theta_2) & \cos(\theta_1 - \theta_2) \end{pmatrix} = R_{\theta_1 - \theta_2} \in \mathcal{O}_2^+(\mathbb{R}) \end{aligned}$$

*c'est-à-dire que le produit de deux réflexions est une rotation.*

**Exercice 20.18** *Montrer que l'ensemble* $G$ *des matrices réelles de la forme* $M_{(a,b)} = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$ *avec* $a^2 \neq b^2$ *est un groupe multiplicatif. Est-il commutatif.*

**Solution 20.18** *On vérifie que c'est un sous-groupe du groupe multiplicatif* $GL_2(\mathbb{R})$.
*On a* $I_n = M_{(1,0)} \in G$ *et pour tous réels* $a, b$, *on a* $\det\left(M_{(a,b)}\right) = a^2 - b^2 \neq 0$, *donc* $M_{(a,b)} \in GL_2(\mathbb{R})$, *l'inverse de* $M_{(a,b)}$ *étant :*

$$M_{(a,b)}^{-1} = \frac{1}{a^2 - b^2} \begin{pmatrix} a & -b \\ -b & a \end{pmatrix} = M_{\frac{a}{a^2-b^2}, \frac{-b}{a^2-b^2}} \in G.$$

*Pour* $M_{(a_1,b_1)}$, $M_{(a_2,b_2)}$ *dans* $G$, *on a :*

$$M_{(a_1,b_1)} M_{(a_2,b_2)} = M_{(a_1a_2+b_1b_2, a_1b_2+a_2b_1)} \in G$$

*Donc* $G$ *est un sous-groupe de* $GL_2(\mathbb{R})$.
*Avec*

$$\begin{aligned} M_{(a_1,b_1)} M_{(a_2,b_2)} &= M_{(a_1a_2+b_1b_2, a_1b_2+a_2b_1)} \\ &= M_{(a_2a_1+b_2b_1, a_2b_1+a_1b_2)} = M_{(a_2,b_2)} M_{(a_1,b_1)} \end{aligned}$$

*on déduit que ce groupe est commutatif.*

**Exercice 20.19** *L'ensemble des matrices carrées d'ordre* $n$ *à coefficients réels symétriques et inversibles est-il un groupe multiplicatif ?*

**Solution 20.19** *Le produit de deux matrices symétriques n'étant pas nécessairement symétrique, la réponse est négative. Par exemple, pour* $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ *et* $A' = \begin{pmatrix} a' & b' \\ b' & c' \end{pmatrix}$, *on a* $AA' = \begin{pmatrix} aa' + bb' & ab' + bc' \\ ba' + cb' & bb' + cc' \end{pmatrix}$ *et en général,* $ba' + cb' \neq ab' + bc'$. *En effet l'égalité revient à* $b(a' - c') = b'(a - c)$ *qui n'est pas réalisée pour* $a = c$, $b \neq 0$ *et* $a' \neq c'$.

**Exercice 20.20** *Montrer que pour tout groupe* $(G, \star)$ *et tout élément* $a$ *de* $G$, *le centralisateur de* $a$ *formé des éléments* $Z_a$ *de* $G$ *qui commutent avec* $a$, *soit :*

$$Z_a = \{b \in G \mid a \star b = b \star a\}$$

*est un sous-groupe de* $G$.

**Solution 20.20** *On a* $Z_a \neq \emptyset$ *puisque* $e \in Z_a$. *Pour* $b, c$ *dans* $Z_a$, *on a :*

$$\begin{aligned}(b \star c) \star a &= b \star (c \star a) = b \star (a \star c) \\ &= (b \star a) \star c = (a \star b) \star c = a \star (b \star c)\end{aligned}$$

*c'est-à-dire que* $b \star c \in Z_a$.
*Pour* $b$ *dans* $Z_a$, *de* $a \star b = b \star a$, *on déduit que*

$$b^{-1} \star a = b^{-1} \star a \star b \star b^{-1} = b^{-1} \star b \star a \star b^{-1} = a \star b^{-1}$$

*c'est-à-dire que* $b^{-1} \in Z_a$.
*En définitive,* $Z_a$ *est un sous-groupe de* $G$.
*Dans le cas où* $G$ *est commutatif, on a* $Z_a = G$ *pour tout* $a \in G$.

**Exercice 20.21** *Montrer que pour tout groupe* $(G, \star)$, *le centre (ou commutateur)* $Z(G)$ *de* $G$ *formé des éléments de* $G$ *qui commutent à tous les autres éléments de* $G$, *soit :*

$$Z(G) = \{a \in G \mid \forall b \in G,\ a \star b = b \star a\}$$

*est un sous-groupe de* $G$.

**Solution 20.21** *On a* $Z(G) \neq \emptyset$ *puisque* $e \in Z(G)$. *Pour* $a, b$ *dans* $Z(G)$, *on a pour tout* $c \in G$ *:*

$$\begin{aligned}\left(a \star b^{-1}\right) \star c &= a \star \left(c^{-1} \star b\right)^{-1} = a \star \left(b \star c^{-1}\right)^{-1} \\ &= (a \star c) \star b^{-1} = c \star \left(a \star b^{-1}\right)\end{aligned}$$

*c'est-à-dire que* $a \star b^{-1} \in Z(G)$.
*En définitive,* $Z(G)$ *est un sous-groupe de* $G$.
*On peut remarquer que* $Z(G) = G$ *si, et seulement si,* $G$ *est commutatif.*

**Exercice 20.22** *Déterminer les centres des groupes multiplicatifs* $GL_n(\mathbb{R})$ *et* $SL_n(\mathbb{R})$.

**Solution 20.22** *Le centre de* $GL_n(\mathbb{R})$ *est formé des homothéties de rapport non nul.*
*Soit* $A = ((a_{ij}))_{1 \leq i,j \leq n}$ *dans le centre de* $GL_n(\mathbb{R})$, *c'est-à-dire commutant avec toutes les matrices inversibles. En désignant par* $(E_{ij})_{1 \leq i,j \leq n}$ *la base canonique de* $\mathcal{M}_n(\mathbb{R})$, *on a* $A(I_n + E_{ij}) =$

*$(I_n + E_{ij})\,A$ pour tous $i \neq j$ compris entre 1 et $n$, ce qui équivaut à $AE_{ij} = E_{ij}A$ pour tous $i \neq j$. En désignant par $(e_i)_{1\leq i\leq n}$ la base canonique de $\mathbb{R}^n$, on a :*

$$\begin{cases} AE_{ij}e_j = Ae_i = \sum_{k=1}^{n} a_{ki}e_k \\ E_{ij}Ae_j = E_{ij}\left(\sum_{k=1}^{n} a_{kj}e_k\right) = a_{jj}e_i \end{cases}.$$

*pour tous $i \neq j$ et l'égalité $AE_{ij} = E_{ij}A$ impose $a_{ki} = 0$ pour $k \in \{1, \cdots, n\} - \{i\}$ et $a_{ii} = a_{jj}$. C'est-à-dire que $A = \lambda I_n$ avec $\lambda \in \mathbb{R}^*$. Réciproquement ces matrices d'homothéties sont bien dans le centre de $GL_n(\mathbb{R})$.*
*Comme les matrices $I_n + E_{ij}$ (pour $i \neq j$ compris entre 1 et $n$) sont aussi dans $SL_n(\mathbb{R})$, le raisonnement précédent nous montre que le centre de $SL_n(\mathbb{R})$ est $\{I_n\}$ pour $n$ impair et $\{-I_n, I_n\}$ pour $n$ pair.*

**Exercice 20.23** *Soit $H$ une partie finie non vide d'un groupe $(G, \star)$. Montrer que $H$ est un sous-groupe de $G$ si, et seulement si, il est stable pour la multiplication.*

**Solution 20.23** *Il est clair que la condition est nécessaire.*
*Supposons que $H$ soit fini et stable pour la multiplication. Il s'agit alors de montrer que pour tout $a \in H$, l'inverse $a^{-1}$ est aussi dans $H$.*
*La translation à gauche $g_a : x \mapsto a * x$ est une bijection de $G$ et comme $H$ est stable pour la multiplication, cette translation est injective de $H$ dans $H$ et donc bijective puisque $H$ est fini. Il existe donc $x \in H$ tel que $a * x = a$, ce qui entraîne $x = e$ (en multipliant à gauche par $a^{-1}$). On a donc $e \in H$ et il existe $x \in H$ tel que $a * x = e$, ce qui entraîne $x = a^{-1}$ et $a^{-1} \in H$.*

**Exercice 20.24** *Soient $H, K$ deux sous-groupes d'un groupe multiplicatif $G$. On définit les sous-ensembles $HK$ et $KH$ de $G$ par :*

$$HK = \{hk \mid (h,k) \in H \times K\},\ KH = \{kh \mid (k,h) \in K \times H\}.$$

*Montrer que :*

$$(HK \text{ est un sous-groupe de } G) \Leftrightarrow (HK = KH)$$

**Solution 20.24** *Supposons que $HK$ soit un sous-groupe de $G$.*
*Si $g \in HK$, alors $g^{-1}$ est aussi dans $HK$ puisque $HK$ est un groupe, il existe donc $(h,k)$ dans $H \times K$ tel que $g^{-1} = hk$ et $g = (g^{-1})^{-1} = k^{-1}h^{-1} \in KH$ ($H$ et $K$ sont des groupes). On a donc $HK \subset KH$.*
*Si $g \in KH$, il existe alors $(h,k)$ dans $H \times K$ tel que $g = kh$ et $g^{-1} = h^{-1}k^{-1} \in HK$ et comme $HK$ est un groupe, il en résulte que $g = (g^{-1})^{-1} \in HK$. On a donc $KH \subset HK$ et l'égalité $HK = KH$.*
*Réciproquement supposons que $HK = KH$.*
*On a $1 = 1 \cdot 1 \in HK$.*
*Si $g_1 = h_1k_1$ et $g_2 = h_2k_2$ sont dans $HK$ avec $h_1, h_2$ dans $H$ et $k_1, k_2$ dans $K$, alors $g_1g_2^{-1} = h_1k_1k_2^{-1}h_2^{-1}$ avec $h_1 \in H$, $k_1k_2^{-1} \in K$ ($K$ est un groupe), donc $h_1\left(k_1k_2^{-1}\right) \in HK = KH$ et il existe $(k_3, h_3) \in K \times H$ tel que $h_1\left(k_1k_2^{-1}\right) = k_3h_3$, ce qui donne $g_1g_2^{-1} = k_3\left(h_3h_2^{-1}\right) \in KH = HK$. On a donc prouvé que $HK$ est un sous-groupe de $G$.*
*Dans le cas où $G$ est commutatif, on a toujours $HK = KH$ et $HK$ est un sous-groupe de $G$ si $H$ et $K$ le sont.*

**Exercice 20.25** *Soient $G$ un groupe fini, $H, K$ deux sous-groupes de $G$ et $\varphi$ l'application :*

$$\begin{array}{rccc} \varphi : & H \times K & \to & HK \\ & (h,k) & \mapsto & hk \end{array}$$

1. *Montrer que pour tout $g \in HK$, on a :*
$$\operatorname{card}\left(\varphi^{-1}(g)\right) = \operatorname{card}(H \cap K)$$
2. *En déduire que :*
$$\operatorname{card}(H)\operatorname{card}(K) = \operatorname{card}(HK)\operatorname{card}(H \cap K)$$
*puis que :*
$$(HK \text{ est un sous-groupe de } G) \Leftrightarrow (HK \subset KH) \Leftrightarrow (HK = KH)$$

**Solution 20.25**

1. *Soit $g = h_1k_1 \in HK$. L'égalité $g = hk$ avec $(h,k) \in H \times K$ équivaut à $h_1k_1 = hk$, ce qui entraîne $h = h_1k_1k^{-1} = h_1g$ avec $g = k_1k^{-1} = h_1^{-1}h \in H \cap K$ et $k = h^{-1}h_1k_1 = g^{-1}k_1$. On a donc $\varphi^{-1}(g) \subset \{(h_1g, g^{-1}k_1) \mid g \in H \cap K\}$. Réciproquement si $(h,k) = (h_1g, g^{-1}k_1)$ avec $g \in H \cap K$, on a alors $(h,k) \in H \times K$ et $hk = h_1gg^{-1}k_1 = g$. Donc :*
$$\varphi^{-1}(g) = \left\{\left(h_1g, g^{-1}k_1\right) \mid g \in H \cap K\right\}$$
*et* $\operatorname{card}(\varphi^{-1}(g)) = \operatorname{card}(H \cap K)$.
2. *En écrivant qu'on a la partition :*
$$H \times K = \bigcup_{g \in HK} \varphi^{-1}(g)$$
*on déduit que :*
$$\begin{aligned} \operatorname{card}(H)\operatorname{card}(K) = \operatorname{card}(H \times K) &= \sum_{g \in HK} \operatorname{card}\left(\varphi^{-1}(g)\right) = \sum_{g \in HK} \operatorname{card}(H \cap K) \\ &= \operatorname{card}(HK)\operatorname{card}(H \cap K) \end{aligned}$$
*Il en résulte que* $\operatorname{card}(HK) = \operatorname{card}(KH) = \dfrac{\operatorname{card}(H)\operatorname{card}(K)}{\operatorname{card}(H \cap K)}$.
3. *On en déduit que $(HK \subset KH) \Leftrightarrow (HK = KH)$ et l'exercice précédent permet de conclure.*

**Exercice 20.26** *Soient $a, b$ deux éléments d'un groupe multiplicatif $G$ tels que $(ab)^{-1} = a^{-1}b$ et $(ba)^{-1} = b^{-1}a$. Montrer que $(a^2)^{-1} = b^2 = a^2$ et $a^4 = b^4 = 1$.*
*Donner un exemple non trivial (i. e. avec $a$ et $b$ distincts de 1) d'une telle situation.*

**Solution 20.26** *De $b^{-1}a^{-1} = (ab)^{-1} = a^{-1}b$, on déduit après multiplication à gauche et à droite par $a$ que $ab^{-1} = ba$ et :*

$$b^2a^2 = b(ba)a = b\left(ab^{-1}\right)a = (ba)\left(b^{-1}a\right) = (ba)(ba)^{-1} = 1,$$

*ce qui signifie que $(a^2)^{-1} = b^2$.*
*On en déduit que :*

$$\begin{aligned} b^4 = b^2b^2 = \left(a^2\right)^{-1}b^2 &= \left(a^{-1}\right)^2b^2 = a^{-1}\left(a^{-1}b\right)b \\ &= a^{-1}(ab)^{-1}b = \left(a^{-1}b^{-1}\right)\left(a^{-1}b\right) = (ba)^{-1}\left(a^{-1}b\right) \\ &= \left(b^{-1}a\right)\left(a^{-1}b\right) = 1 \end{aligned}$$

*et de* $(a^2)^{-1} = b^2$, *on déduit que* $a^2b^2 = 1$, *donc* $a^2b^4 = b^2$, *soit* $a^2 = b^2$ *et* $a^4 = 1$.
*Les conditions* $(ab)^{-1} = a^{-1}b$ *et* $(ba)^{-1} = b^{-1}a$ *reviennent à dire que* $b^{-1}a^{-1} = a^{-1}b$, *soit* $b = ab^{-1}a^{-1}$ *et* $a^{-1}b^{-1} = b^{-1}a$, *soit* $a = ba^{-1}b^{-1}$. *Dans le cas où* $a$ *et* $b$ *commutent, celà donne* $b = b^{-1}$ *et* $a = a^{-1}$, *soit* $a^2 = b^2 = 1$. *Il suffit donc de prendre deux éléments d'ordre* 2 *qui commutent.*
*On peut considérer, par exemple, le groupe de Klein* $G = \{Id, \sigma_x, \sigma_y, \sigma_y\}$ *(isomorphe à* $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^2$*),* *où* $\sigma_x, \sigma_y, \sigma_y$ *désignent les symétries orthogonales par rapport aux axes dans l'espace euclidien* $\mathbb{R}^3$.

## 20.4 Sous-groupe engendré par une partie d'un groupe

**Théorème 20.7** *Soit* $(G, \star)$ *un groupe. L'intersection d'une famille quelconque* $(H_i)_{i\in I}$ *de sous-groupes de* $G$ *est un sous-groupe de* $G$.

**Démonstration.** Soit $H = \bigcap_{i\in I} H_i$. Comme l'élément neutre $e$ est dans tous les $H_i$, il est aussi dans $H$ et $H \neq \emptyset$. Si $a, b$ sont dans $H$, ils sont alors dans tous les $H_i$, donc $a \star b^{-1} \in H_i$ pour tout $i \in I$, ce qui signifie que $a \star b^{-1} \in H$. On a donc montré que $H$ un sous-groupe de $G$. ■

**Remarque 20.3** *La réunion d'une famille de sous-groupes de* $G$ *n'est pas nécessairement un sous-groupe. Par exemple* $2\mathbb{Z}$ *et* $3\mathbb{Z}$ *sont des sous groupes de* $(\mathbb{Z}, +)$, *mais la réunion* $H$ *ne l'est pas puisque* 2 *et* 3 *sont dans* $H$ *alors que* $2 + 3 = 5 \notin H$.

**Exercice 20.27** *Soient* $H, K$ *deux sous-groupes d'un groupe* $G$. *Montrer que* $H \cup K$ *est un sous-groupe de* $G$ *si, et seulement si,* $H \subset K$ *ou* $K \subset H$.

**Solution 20.27** *Si* $H \subset K$ *ou* $K \subset H$, *on a alors* $H \cup K = K$ *ou* $H \cup K = H$ *et c'est un sous-groupe de* $G$.
*Réciproquement, supposons que* $H \cup K$ *soit un sous-groupe de* $G$. *Si* $H \subset K$ *c'est terminé, sinon il existe* $g \in H \setminus K$. *Pour tout* $k \in K \subset H \cup K$, $gk$ *est dans* $H \cup K$ *(c'est un groupe) et* $gk$ *ne peut être dans* $K$ *(sinon* $g = (gk)\, k^{-1} \in K$, *ce qui n'est pas), donc* $gk \in H$ *et* $k = g^{-1}\,(gk) \in H$. *On a donc* $K \subset H$.

**Corollaire 20.1** *Si* $X$ *est une partie d'un groupe* $(G, \star)$, *l'intersection de tous les sous-groupes de* $G$ *qui contiennent* $X$ *est un sous-groupe de* $G$.

**Démonstration.** L'ensemble des sous-groupes de $G$ qui contiennent $X$ est non vide puisque $G$ en fait partie et le théorème précédent nous dit que l'intersection de tous ces sous-groupes est un sous-groupe de $G$. ■

**Définition 20.6** *Si* $X$ *est une partie d'un groupe* $(G, \star)$, *le sous-groupe de* $G$ *engendré par* $X$ *est l'intersection de tous les sous-groupes de* $G$ *qui contiennent* $X$.

On note $\langle X\rangle$ le sous-groupe de $G$ engendré par $X$ et ce sous-groupe $\langle X\rangle$ est le plus petit (pour l'ordre de l'inclusion) des sous-groupes de $G$ qui contiennent $X$.
Dans le cas où $X$ est l'ensemble vide, on a $\langle X\rangle = \{e\}$.

**Définition 20.7** *Si* $X$ *est une partie d'un groupe* $(G, \star)$, *on dit que* $X$ *engendre* $G$ *si* $G = \langle X\rangle$.

**Théorème 20.8** *Soient $(G,\star)$ un groupe et $X,Y$ deux parties de $G$.*

1. *On a $X\subset\langle X\rangle$ et l'égalité est réalisée si, et seulement si $X$ est un sous-groupe de $G$.*
2. *Si $X\subset Y$, on a alors $\langle X\rangle\subset\langle Y\rangle$.*
3. *En notant, pour $X$ non vide, $X^{-1}$ l'ensemble formé des symétriques des éléments de $X$, soit $X^{-1}=\{x^{-1}\mid x\in X\}$, les éléments de $\langle X\rangle$ sont de la forme $x_1\star\cdots\star x_n$ où $n\in\mathbb{N}^*$ et les $x_k$ sont dans $X\cup X^{-1}$ pour tout $k$ compris entre 1 et $n$.*

**Démonstration.** Les points **1.** et **2.** se déduisent immédiatement des définitions.
Pour le point **3.** on montre tout d'abord que l'ensemble :

$$H=\left\{x_1\star\cdots\star x_n\mid n\in\mathbb{N}\text{ et }x_k\in X\cup X^{-1}\text{ pour }1\leq k\leq n\right\}$$

est un sous-groupe de $G$.
Pour $x_1\in X$, on a $e=x_1\star x_1^{-1}\in H$ et pour $x=x_1\star\cdots\star x_n$, $y=y_1\star\cdots\star y_m$ dans $H$, on a :

$$x\star y^{-1}=x_1\star\cdots\star x_n\star y_m^{-1}\star\cdots\star y_1^{-1}\in H$$

Donc $H$ est bien un sous-groupe de $G$.
Comme $X\subset H$, il nous suffit de monter que $H$ est contenu dans tout sous-groupe de $G$ qui contient $X$. Si $K$ est un tel sous-groupe, tout produit $x_1\star\cdots\star x_n$ de $H$ est un produit d'éléments de $X\cup X^{-1}\subset K$, donc dans $K$, ce qui prouve que $H\subset K$. On a donc bien $\langle X\rangle=H$. ∎

**Remarque 20.4** *Le point **3.** du théorème précédent nous dit aussi que $\langle X\rangle=\langle X^{-1}\rangle=\langle X\cup X^{-1}\rangle$.*

## 20.5 Groupes monogènes

Pour ce paragraphe, on se donne un groupe multiplicatif $(G,\cdot)$.
Si $X$ est une partie de $G$ formée d'un nombre fini d'éléments, $x_1,\cdots,x_n$, on note alors $\langle X\rangle=\langle x_1,\cdots,x_n\rangle$.
Pour $n=1$, on dit que $\langle x_1\rangle$ est un sous-groupe monogène de $G$.

**Définition 20.8** *On dit que $G$ est un groupe monogène s'il existe $x_1\in G$ tel que $G=\langle x_1\rangle$. Si de plus, $G$ est fini, on dit alors qu'il est cyclique (ce terme sera justifié après avoir défini la notion d'ordre d'un élément d'un groupe).*

Pour tout $a\in G$ nous avons déjà défini les puissances entières positives de $a$ (paragraphe 20.1). Dans un groupe, on définit les puissances entières, positives ou négatives, de $a\in G$ par :

$$\begin{cases}a^0=1\\ \forall n\in\mathbb{N},\ a^{n+1}=a^na\\ \forall n\in\mathbb{N}^*,\ a^{-n}=\left(a^n\right)^{-1}\end{cases}$$

On peut remarquer que pour $n\in\mathbb{N}^*$, on a aussi $a^{-n}=\left(a^{-1}\right)^n$, ce qui résulte de :

$$\left(a^{-1}\right)^n a^n=a^{-1}\cdots a^{-1}a\cdots a=1$$

En notation additive, $a^n$ est noté $na$ pour $n\in\mathbb{Z}$.

**Théorème 20.9** *Pour $a$ dans $G$ et $n, m$ dans $\mathbb{Z}$, on a :*

$$a^n a^m = a^{n+m}$$

*et pour $b \in G$ qui commute avec $a$, on a :*

$$(ab)^n = a^n b^n = b^n a^n$$

**Démonstration.** On montre tout d'abord le résultat pour $n, m$ dans $\mathbb{N}$ par récurrence sur $m \geq 0$ à $n$ fixé. Le résultat est évident pour $m = 0$ et le supposant acquis pour $m \geq 0$, on a :

$$a^n a^{m+1} = a^n a^m a = a^{n+m} a = a^{n+m+1}.$$

On en déduit que pour $n', m'$ dans $\mathbb{N}$, on a :

$$a^{-n'} a^{-m'} = \left(a^{n'}\right)^{-1} \left(a^{m'}\right)^{-1} = \left(a^{m'} a^{n'}\right)^{-1} = \left(a^{m'+n'}\right)^{-1} = \left(a^{n'+m'}\right)^{-1} = a^{-n'-m'}$$

c'est-à-dire que le résultat est valable pour $n \leq 0$ et $m \leq 0$.

Pour $n, m'$ dans $\mathbb{N}$ tels que $n \geq m'$ on a :

$$a^{n-m'} a^{m'} = a^n \Rightarrow a^n \left(a^{m'}\right)^{-1} = a^n a^{-m'} = a^{n-m'}$$

et pour $n \leq m'$, on a :

$$a^{n-m'} = \left(a^{m'-n}\right)^{-1} = \left(a^{m'} a^{-n}\right)^{-1} = a^n a^{-m'}$$

donc le résultat est valable pour $n \geq 0$ et $m \leq 0$.

On procède de manière analogue pour $n \leq 0$ et $m \geq 0$.

En définitive, c'est valable pour tous $n, m$ dans $\mathbb{Z}$.

En supposant que $a$ et $b$ commutent, on montre par récurrence sur $n \geq 0$ que $(ab)^n = a^n b^n$ et $ab^{n+1} = b^{n+1} a$. C'est clair pour $n = 0$ et supposant le résultat acquis pour $n \geq 0$, on a :

$$\begin{aligned}(ab)^{n+1} &= (ab)^n ab = a^n b^n ab = a^n b^n ba \\ &= a^n b^{n+1} a = a^n a b^{n+1} = a^{n+1} b^{n+1}.\end{aligned}$$

Et avec $ab = ba$, on déduit que $(ab)^n = (ba)^n = b^n a^n$.

Ensuite, pour $n' \geq 0$, on a :

$$(ab)^{-n'} = \left((ab)^{n'}\right)^{-1} = \left(a^{n'} b^{n'}\right)^{-1} = \left(b^{n'} a^{n'}\right)^{-1} = a^{-n'} b^{-n'} = b^{-n'} a^{-n'}$$

et le résultat est valable pour $n \leq 0$. ∎

On vu que la relation $(ab)^n = a^n b^n$ est fausse si $a$ et $b$ ne commutent pas, des exemples simples étant donnés dans $GL_2(\mathbb{R})$.

**Théorème 20.10** *Pour tout $a \in G$, le sous-groupe de $G$ engendré par $a$ est :*

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$$

**Démonstration.** En notant $H = \{a^n \mid n \in \mathbb{Z}\}$, on a $\{a\} \subset H$, $1 = a^0 \in H$ et pour $n, m$ dans $\mathbb{Z}$, $a^n (a^m)^{-1} = a^{n-m} \in H$, donc $H$ est un sous-groupe de $G$ qui contient $\{a\}$ et c'est le plus petit du fait que pour tout sous-groupe $K$ de $G$ qui contient $\{a\}$, on a $a^n \in K$ pour tout $n \in \mathbb{Z}$, ce qui implique $H \subset K$. On a donc bien $H = \langle a \rangle$. ∎

**Exercice 20.28** *Soit $G$ un groupe. Montrer que pour tout $n$-uplet $(x_1, \cdots, x_n)$ d'éléments de $G$ qui commutent deux à deux (avec $n \geq 1$), on a :*

$$\langle x_1, \cdots, x_n \rangle = \left\{ \prod_{k=1}^{n} x_k^{\alpha_k} \mid (\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}^n \right\}$$

**Solution 20.28** *En notant $X = \{x_1, \cdots, x_n\}$, on a $X^{-1} = \left\{x_1^{-1}, \cdots, x_n^{-1}\right\}$ et comme les $x_k$ commutent, on déduit que :*

$$\begin{aligned}\langle x_1, \cdots, x_n \rangle &= \left\{ \prod_{k=1}^{m} y_k \mid m \in \mathbb{N} \text{ et } y_k \in X \cup X^{-1} \text{ pour } 1 \leq k \leq m \right\} \\ &= \left\{ \prod_{k=1}^{n} x_k^{\alpha_k} \mid (\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}^n \right\}\end{aligned}$$

*($x_k x_j = x_j x_k$ entraîne $x_j^{-1} x_k x_j x_j^{-1} = x_j^{-1} x_j x_k x_j^{-1}$, soit $x_j^{-1} x_k = x_k x_j^{-1}$ et les éléments de $X \cup X^{-1}$ commutent).*

Pour une loi de groupe notée additivement, on a, dans le cas où $G$ est commutatif :

$$\langle x_1, \cdots, x_n \rangle = \left\{ \sum_{k=1}^{n} \alpha_k x_k \mid (\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}^n \right\}$$

Par exemple pour le groupe additif $G = \mathbb{Z}$, on a :

$$\langle x_1, \cdots, x_n \rangle = \sum_{k=1}^{n} x_k \mathbb{Z} = \delta \mathbb{Z}$$

où $\delta \in \mathbb{N}$ est pgcd de $x_1, \cdots, x_n$. Cette notion est étudiée au paragraphe 23.4.2.

**Exercice 20.29** *Montrer qu'un groupe $G$ engendré par deux éléments $a$ et $b$ qui commutent est commutatif.*

**Solution 20.29** *Comme $ab = ba$, on a $G = \langle a, b \rangle = \left\{a^\alpha b^\beta \mid (\alpha, \beta) \in \mathbb{Z}^2\right\}$ et ce groupe est commutatif.*

**Exercice 20.30** *Soit $X = \{r_1, \cdots, r_n\}$ une partie finie de $\mathbb{Q}$ et $G = \langle X \rangle$ le sous groupe de $(\mathbb{Q}, +)$ engendré par $X$. Montrer que $G$ est monogène.*

**Solution 20.30** *En désignant par $\mu$ le* ppcm *des dénominateurs de $r_1, \cdots, r_n$, il existe des entiers relatifs $a_1, \cdots, a_n$ tels que $r_k = \dfrac{a_k}{\mu}$ pour tout $k$ compris entre 1 et $n$ et en désignant par $\delta$ le* pgcd *de $a_1, \cdots, a_n$, on a :*

$$\begin{aligned}G &= \left\{ \sum_{k=1}^{n} \alpha_k \frac{a_k}{\mu} \mid (\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}^n \right\} \\ &= \left\{ \frac{\delta}{\mu} \sum_{k=1}^{n} \alpha_k b_k \mid (\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}^n \right\}\end{aligned}$$

*où $b_1, \cdots, b_n$ sont des entiers relatifs premiers entre eux dans leur ensemble. On a donc $G = \dfrac{\delta}{\mu}\mathbb{Z}$, ce qui signifie que $G$ est monogène engendré par $\dfrac{\delta}{\mu}$.*

## 20.6 Groupes finis. Théorème de Lagrange

Pour ce paragraphe, on se donne un groupe multiplicatif $(G, \cdot)$.

**Théorème 20.11** *Pour tout sous-groupe $H$ de $G$, la relation $\sim$ définie sur $G$ par :*

$$x \sim y \Leftrightarrow x^{-1}y \in H$$

*est une relation d'équivalence.*

**Démonstration.** Pour tout $x \in G$, on a $x^{-1}x = 1 \in H$, donc $\sim$ est réflexive.

Si $x, y$ dans $G$ sont tels que $x^{-1}y \in H$, on a alors $(x^{-1}y)^{-1} = y^{-1}x \in H$, ce qui signifie que $y \sim x$. Cette relation est donc symétrique.

Si $x, y, z$ dans $G$ sont tels que $x^{-1}y \in H$ et $y^{-1}z \in H$, on a alors $x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$, ce qui signifie que $x \sim z$. Cette relation est donc transitive. ■

Avec les notations du théorème précédent, on note, pour tout $g \in G$, $\overline{g}$ la classe d'équivalence de $g$ et on dit que $\overline{g}$ est la classe à gauche modulo $H$ de $g$.

On a, pour $g \in G$ :

$$h \in \overline{g} \Leftrightarrow g \sim h \Leftrightarrow k = g^{-1}h \in H \Leftrightarrow \exists k \in H \mid h = gk \Leftrightarrow h \in gH$$

soit $\overline{g} = gH$.

L'ensemble de toutes ces classes d'équivalence est noté $G/H$ et on l'appelle l'ensemble des classes à gauche modulo $H$.

On a donc :

$$G/H = \{\overline{g} \mid g \in G\} = \{gH \mid g \in G\}.$$

L'application :

$$\begin{array}{rccc} \pi : & G & \to & G/H \\ & g & \mapsto & \overline{g} = gH \end{array}$$

est surjective. On dit que c'est la surjection canonique de $G$ sur $G/H$.

Dans le cas où $G$ est le groupe additif $\mathbb{Z}$ tout sous-groupe de $G$ est de la forme $n\mathbb{Z}$ où $n$ est un entier naturel et cette construction aboutit au groupe $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ des classes résiduelles modulo $n$ (ces groupes seront étudiés plus en détails au chapitre 25).

**Définition 20.9** *Si $G$ est un groupe ayant un nombre fini d'éléments son cardinal est appelé l'ordre de $G$.*

**Théorème 20.12 (Lagrange)** *Soient $G$ un groupe fini d'ordre $n \geq 2$ et $H$ un sous-groupe de $G$.*

1. *Les classes à gauche modulo $H$ forment une partition de $G$.*
2. *Pour tout $g \in G$ on a $\operatorname{card}(\overline{g}) = \operatorname{card}(H)$.*
3. *L'ordre du sous-groupe $H$ divise l'ordre du groupe $G$.*

**Démonstration.**

1. Comme $G$ est fini, il en est de même de $G/H$. Notons :
$$G/H = \{\overline{g_1}, \cdots, \overline{g_p}\}$$
où $1 \leq p \leq n$ et $\overline{g_j} \neq \overline{g_k}$, pour $1 \leq j \neq k \leq p$. Pour tout $g \in G$, il existe un unique indice $j$ tel que $\overline{g} = \overline{g_j}$ et $g \in \overline{g_j}$. On a donc $G = \bigcup_{j=1}^{p} \overline{g_j}$. Dire que $g$ est dans $\overline{g_j} \cap \overline{g_k}$ signifie que $g$ est équivalent modulo $H$ à $g_j$ et $g_k$ et donc par transitivité $g_j$ et $g_k$ sont équivalent, ce qui revient à dire que $\overline{g_j} = \overline{g_k}$. Les classes à gauche modulo $H$ forment donc bien une partition de $G$.
2. Pour $g \in G$, l'application $h \mapsto gh$ est injective (dans un groupe tout élément est simplifiable) et en restriction à $H$ elle réalise une bijection de $H$ sur $gH = \overline{g}$. Il en résulte que $\overline{g}$ est de même cardinal que $H$.
3. Avec la partition $G = \bigcup_{j=1}^{p} \overline{g_j}$ et $\operatorname{card}(\overline{g_j}) = \operatorname{card}(H)$ pour tout $j$, on déduit que $\operatorname{card}(G) = p \operatorname{card}(H)$ et $\operatorname{card}(H)$ divise $\operatorname{card}(G)$.

■

Le cardinal $p$ de l'ensemble $G/H$ est noté $[G : H]$ et on l'appelle l'indice de $H$ dans $G$. Le théorème de Lagrange peut aussi se traduire par :
$$[G : H] = \operatorname{card}(G/H) = \frac{\operatorname{card}(G)}{\operatorname{card}(H)}.$$

**Exercice 20.31** *Montrer qu'un groupe fini d'ordre $p$ un nombre premier est cyclique (et donc commutatif).*

**Solution 20.31** *Si $G$ est d'ordre $p \geq 2$ premier, il a au moins deux éléments et il existe $a \neq 1$ dans $G$. Le sous-groupe cyclique $\langle a \rangle$ de $G$ est alors d'ordre un diviseur de $p$ supérieur ou égal à 2, il est donc égal à $p$ et $G = \langle a \rangle$ est cyclique.*

**Exercice 20.32** *Soient $G$ un groupe et $H, K$ deux sous-groupes distincts de $G$ d'ordre un même nombre premier $p \geq 2$. Montrer que $H \cap K = \{1\}$.*

**Solution 20.32** *$H \cap K$ est un sous groupe de $H$, il est donc d'ordre 1 ou $p$. S'il est d'ordre $p$, il est égal à $H$ et $H = H \cap K \subset K$ entraîne $H = K$, puisque ces deux ensembles ont le même nombre d'éléments. On a donc, pour $H \neq K$, $p = 1$ et $H \cap K = \{1\}$.*

**Exercice 20.33** *Soient $G$ un groupe, $H$ un sous-groupe de $G$ et $K$ un sous-groupe de $H$. Montrer que si l'indice de $K$ dans $G$ est fini, alors l'indice de $H$ dans $G$ et celui de $K$ dans $H$ sont aussi finis et on a :*
$$[G : K] = [G : H]\,[H : K]$$

**Solution 20.33** *On note respectivement $(g_i H)_{i \in I}$ et $(h_j K)_{j \in J}$ les classes à gauches modulo $H$ dans $G$ et modulo $K$ dans $H$ deux à deux distinctes.*
*Nous allons alors montrer que la famille des classes à gauches modulo $K$ dans $G$ deux à deux distinctes est $(g_i h_j K)_{(i,j) \in I \times J}$. Dans le cas où $[G : K]$ est fini, il n'y a qu'un nombre fini de telles classes, ce qui impose que $I$ et $J$ sont finis et on a :*
$$[G : K] = \operatorname{card}(I \times J) = \operatorname{card}(I) \operatorname{card}(J) = [G : H]\,[H : K]$$

*Montrons le résultat annoncé.*
*Si $g$ est un élément de $G$, il existe un unique indice $i \in I$ tel que $gH = g_iH$ et il existe $h \in H$ tel que $g = g_ih$. De même il existe un unique indice $j \in J$ tel que $hK = h_jK$ et $h$ s'écrit $h = h_jk$ avec $k \in K$, ce qui donne $g = g_ih_jk \in g_ih_jK$ et $gK = g_ih_jK$. Les classes à gauche dans $G$ modulo $K$ sont donc les $g_ih_jK$ pour $(i,j) \in I \times J$. Il reste à montrer que ces classes sont deux à deux distinctes.*
*Si $(i,j)$ et $(i',j')$ dans $I \times J$ sont tels que $g_ih_jK = g_{i'}h_{j'}K$, il existe $k \in K$ tel que $g_ih_j = g_{i'}h_{j'}k$ et $g_i = g_{i'}\left(h_{j'}kh_j^{-1}\right)$ avec $h_{j'}kh_j^{-1} \in H$, ce qui impose $g_iH = g_{i'}H$ et $i = i'$. Il en résulte que $h_j = h_{j'}k$ et $h_jK = h_{j'}K$, qui équivaut à $j = j'$.*

## 20.7 Morphismes de groupes

On désigne par $(G, \star)$ et $(H, \cdot)$ deux groupes et on note respectivement $e$ et 1 les éléments neutres de $(G, \star)$ et $(H, \cdot)$.

**Définition 20.10** *On dit que $\varphi$ est un morphisme de groupes de $G$ dans $H$ si $\varphi$ est une application de $G$ dans $H$ telle que : :*

$$\forall (a,b) \in G^2,\ \varphi(a \star b) = \varphi(a) \cdot \varphi(b).$$

*Dans le cas où $\varphi$ est de plus bijective, on dit que $\varphi$ est un isomorphisme du groupe $G$ sur le groupe $H$.*
*Dans le cas où $H = G$, on dit que $\varphi$ est un endomorphisme du groupe $(G, \star)$ et que c'est un automorphisme du groupe $(G, \star)$ si $\varphi$ est de plus bijective.*

Si $G$ et $H$ sont deux groupes isomorphes, on notera $G \backsimeq H$.

**Théorème 20.13** *Soient $G, H, K$ trois groupes, $\varphi$ un morphisme de groupes de $G$ dans $H$ et $\psi$ un morphisme de groupes de $H$ dans $K$. L'application $\psi \circ \varphi$ est un morphisme de groupes de $G$ dans $K$.*
*Si $\varphi$ est un automorphisme de $G$, alors $\varphi^{-1}$ est également un automorphisme de $G$.*

**Démonstration.** En notant les lois de chacun des groupes sous forme multiplicative, on a pour tout $(a,b) \in G^2$ :

$$\begin{aligned}(\psi \circ \varphi)(a \cdot b) &= \psi(\varphi(a \cdot b)) = \psi(\varphi(a) \cdot \varphi(b)) \\ &= \psi(\varphi(a))\,\psi(\varphi(b)) = \psi \circ \varphi(a)\,\psi \circ \varphi(b).\end{aligned}$$

Si $\varphi$ est un automorphisme de $G$, on a alors pour tous $a', b'$ dans $G$, en notant $a = \varphi^{-1}(a')$, $b = \varphi^{-1}(b')$ :

$$\begin{aligned}\varphi^{-1}(a' \star b') &= \varphi^{-1}(\varphi(a) \star \varphi(b)) = \varphi^{-1}(\varphi(a \star b)) \\ &= a \star b = \varphi^{-1}(a') \star \varphi^{-1}(b')\end{aligned}$$

ce qui signifie que $\varphi^{-1}$ est un morphisme de groupe. Et on sait déjà qu'il est bijectif, c'est donc un automorphisme de $G$ ∎

On déduit du théorème précédent que l'ensemble $(\mathrm{Aut}(G), \circ)$ des automorphismes de $G$ dans lui même est un sous-groupe du groupe symétrique $(S(G), \circ)$ formé des bijections (ou permutations) de $G$.

**Exemple 20.26** *La fonction exponentielle est un isomorphisme de groupes de* $(\mathbb{R},+)$ *sur* $(\mathbb{R}^{+,*},\cdot)$.

**Exemple 20.27** *La fonction logarithme népérien est un isomorphisme de groupes de* $(\mathbb{R}^{+,*},\cdot)$ *sur* $(\mathbb{R},+)$.

**Exemple 20.28** *L'application* $\mathrm{tr} : A = ((a_{ij}))_{1\leq i,j\leq n} \mapsto \sum_{i=1}^{n} a_{ii}$ *qui associe à une matrice sa trace est un morphisme du groupe additif* $(\mathcal{M}_n(\mathbb{R}),+)$ *dans* $(\mathbb{R},+)$.

**Exemple 20.29** *L'application* $\det : A \mapsto \det(A)$ *qui associe à une matrice son déterminant est un morphisme du groupe multiplicatif* $(GL_n(\mathbb{R}),\cdot)$ *dans* $(\mathbb{R}^*,\cdot)$.

**Théorème 20.14** *Si* $\varphi$ *est un morphisme de groupes de* $G$ *dans* $H$*, on alors :*

1. $\varphi(e) = 1$ ;
2. *pour tout* $a \in G$, $\varphi(a)^{-1} = \varphi(a^{-1})$.

**Démonstration.**

1. Pour tout $a \in G$, on a :
$$\varphi(a) = \varphi(a \star e) = \varphi(a) \cdot \varphi(e)$$
et multipliant par $\varphi(a)^{-1}$, on obtient $1 = \varphi(e)$.
2. Pour tout $a \in G$, on a :
$$1 = \varphi(e) = \varphi\left(a \star a^{-1}\right) = \varphi(a) \cdot \varphi\left(a^{-1}\right)$$
et multipliant par $\varphi(a)^{-1}$, on obtient $\varphi(a)^{-1} = \varphi(a^{-1})$.

■

**Définition 20.11** *Soit* $\varphi$ *un morphisme de groupes de* $G$ *dans* $H$.

1. *Le noyau de* $\varphi$ *est l'ensemble :*
$$\ker(\varphi) = \{x \in G \mid \varphi(x) = 1\}.$$
2. *L'image de* $\varphi$ *est l'ensemble :*
$$\mathrm{Im}(\varphi) = \{\varphi(x) \mid x \in G\}.$$

**Théorème 20.15** *Si* $\varphi$ *est un morphisme de groupes de* $G$ *dans* $H$*, alors :*

1. $\ker(\varphi)$ *est un sous-groupe de* $G$.
2. $\varphi$ *est injectif si, et seulement si,* $\ker(\varphi) = \{e\}$.
3. $\mathrm{Im}(\varphi)$ *est un sous-groupe de* $H$.
4. $\varphi$ *est surjectif si, et seulement si,* $\mathrm{Im}(\varphi) = H$.
5. *Pour tout sous-groupe* $G'$ *de* $G$, $\varphi(G')$ *est un sous-groupe de* $H$.
6. *Pour tout sous-groupe* $H'$ *de* $H$, $\varphi^{-1}(H')$ *est un sous-groupe de* $G$.

**Démonstration.**

1. On a $\ker(\varphi) \neq \emptyset$ puisque $e \in \ker(\varphi)$ ($\varphi(e) = 1$) et pour $x, y$ dans $\ker(\varphi)$ :
$$\varphi\left(x \star y^{-1}\right) = \varphi(x) \cdot \varphi\left(y^{-1}\right) = \varphi(x) \cdot \varphi(y)^{-1} = 1$$
c'est-à-dire que $x \star y^{-1} \in \ker(\varphi)$ et $\ker(\varphi)$ est un sous-groupe de $G$.
2. Si $\varphi$ est injectif, on a alors :
$$\forall x \in \ker(\varphi),\ \varphi(x) = 1 = \varphi(e) \Rightarrow x = e$$
et donc $\ker(\varphi) = \{e\}$.
Réciproquement si $\ker(\varphi) = \{e\}$, pour $x, y$ dans $G$ tels que $\varphi(x) = \varphi(y)$, on a :
$$1 = \varphi(x)^{-1} \cdot \varphi(x) = \varphi\left(x^{-1}\right) \cdot \varphi(y) = \varphi\left(x^{-1} \star y\right)$$
donc $x^{-1} \star y \in \ker(\varphi)$ et $x^{-1} \star y = e$, ce qui équivaut à $x = y$.
3. On a $\mathrm{Im}(\varphi) \neq \emptyset$ puisque $\varphi(e) \in \mathrm{Im}(\varphi)$ et pour $\varphi(x), \varphi(y)$ dans $\mathrm{Im}(\varphi)$ avec $x, y$ dans $G$ :
$$\varphi(x) \cdot \varphi(y)^{-1} = \varphi(x) \cdot \varphi\left(y^{-1}\right) = \varphi\left(x \star y^{-1}\right) \in \mathrm{Im}(\varphi)$$
et $\mathrm{Im}(\varphi)$ est un sous-groupe de $H$.
4. C'est la définition de la surjectivité.
5. On a $e \in G'$, donc $1 = \varphi(e) \in \varphi(G')$ et pour $a' = \varphi(a)$, $b' = \varphi(b)$ dans $\varphi(G')$ avec $a, b$ dans $G'$, on a :
$$\begin{aligned} a' \star (b')^{-1} &= \varphi(a) \star (\varphi(b))^{-1} = \varphi(a) \star \varphi\left(b^{-1}\right) \\ &= \varphi\left(a \star b^{-1}\right) \in \varphi(G') \end{aligned}$$
Prenant $G' = G$, on retrouve le fait que $\mathrm{Im}(\varphi)$ est un sous-groupe de $H$.
6. On a $1 = \varphi(e) \in H'$, donc $e \in \varphi^{-1}(H')$ et pour $a, b$ dans $\varphi^{-1}(H')$, on a :
$$\varphi\left(a \star b^{-1}\right) = \varphi(a) \star \varphi\left(b^{-1}\right) = \varphi(a) \star (\varphi(b))^{-1} \in H'$$
donc $a \star b^{-1} \in \varphi^{-1}(H')$.
Prenant $H' = \{1\}$, on retrouve le fait que $\ker(\varphi)$ est un sous-groupe de $G$.

■

**Exemple 20.30** *L'application* $\varphi : \theta \mapsto R_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$ *est un morphisme de groupes de* $(\mathbb{R}, +)$ *dans* $(SL_2(\mathbb{R}), \cdot)$ *et son image* $\mathrm{Im}(\varphi) = \mathcal{O}_2^+(\mathbb{R})$ *est un sous-groupe commutatif de* $(SL_2(\mathbb{R}), \cdot)$ *(exercice 20.16).*

**Exercice 20.34**

1. *Soient* $(G, \cdot)$ *un groupe,* $E$ *un ensemble non vide et* $f : G \to E$ *une application bijective. Montrer que l'ensemble* $E$ *muni de la loi* $\star$ *définie par :*
$$x \star y = f\left(f^{-1}(x) \cdot f^{-1}(y)\right)$$
*est un groupe isomorphe à* $(G, \cdot)$ *(on dit qu'on a transporté la structure de groupe de* $G$ *sur* $E$*).*
2. *Retrouver les résultats des exercices 20.8 et 20.9.*

3. *Montrer que pour tout entier $n \geq 1$ impair l'application $(x,y) \mapsto x \star y = \sqrt[n]{x^n + y^n}$ défini une structure de groupe commutatif sur $\mathbb{R}$.*

**Solution 20.34**

1. *La fonction $f$ étant bijective de $G$ sur $E$ l'application $\star$ défini bien une loi interne sur $E$. Pour tout $x \in E$, on a $x \star f(1) = f(1) \star x = x$ et $x \star f\left(\left(f^{-1}(x)\right)^{-1}\right) = f\left(\left(f^{-1}(x)\right)^{-1}\right) \star x = f(1)$ donc $f(1)$ est neutre et tout élément de $E$ est inversible.*
   *Enfin pour $x, y, z$ dans $E$, on a :*

$$\begin{aligned} x \star (y \star z) &= f\left(f^{-1}(x) \cdot f^{-1}(y \star z)\right) \\ &= f\left(f^{-1}(x) \cdot f^{-1}(y) \cdot f^{-1}(z)\right) \end{aligned}$$

   *et :*

$$\begin{aligned} (x \star y) \star z &= f\left(f^{-1}(x \star y) \cdot f^{-1}(z)\right) \\ &= f\left(f^{-1}(x) \cdot f^{-1}(y) \star f^{-1}(z)\right) \end{aligned}$$

   *ce qui montre que $\star$ est associative.*
   *Avec $f^{-1}(x \star y) = f^{-1}(x) \cdot f^{-1}(y)$, on déduit que $f^{-1}$ est un morphisme de groupes de $(E, \star)$ sur $(G, \cdot)$ et $f$ est un morphisme de groupes de $(G, \cdot)$ sur $(E, \star)$.*
   *on dit qu'on a transporté la structure de groupe de $(G, \cdot)$ sur $E$ par la bijection $f$.*
2. *Les exercices 20.8 et 20.9 sont des exemples de telle situation avec le groupe $(\mathbb{R}, +)$, $f(x) = \operatorname{th}(x) = \dfrac{e^x - e^{-x}}{e^x + e^{-x}}$ pour $x \in \mathbb{R}$ qui réalise une bijection de $\mathbb{R}$ sur $]-1, 1[$ avec pour bijection réciproque* argth *et $f(x) = \arctan(x)$ pour $x \in \mathbb{R}$ qui réalise une bijection de $\mathbb{R}$ sur $\left]-\dfrac{\pi}{2}, \dfrac{\pi}{2}\right[$ avec pour bijection réciproque* tan*. Dans le premier cas, on a :*

$$\begin{aligned} x \star y &= f\left(f^{-1}(x) + f^{-1}(y)\right) \\ &= \operatorname{th}(\operatorname{argth}(x) + \operatorname{argth}(y)) \\ &= \frac{\operatorname{th}(\operatorname{argth}(x)) + \operatorname{th}(\operatorname{argth}(y))}{1 + \operatorname{th}(\operatorname{argth}(x)) \operatorname{th}(\operatorname{argth}(y))} = \frac{x + y}{1 + xy} \end{aligned}$$

   *et dans le second, on a :*

$$\begin{aligned} x \star y &= f\left(f^{-1}(x) + f^{-1}(y)\right) \\ &= \arctan(\tan(x) + \tan(y)) \end{aligned}$$

3. *L'application $f : x \mapsto \sqrt[n]{x}$ est bijective de $\mathbb{R}$ sur $\mathbb{R}$ pour $n$ impair, son inverse étant l'application $x \mapsto x^n$ et on a :*

$$x \star y = \sqrt[n]{x^n + y^n} = f\left(f^{-1}(x) + f^{-1}(y)\right)$$

**Exercice 20.35** *Soit $G$ un groupe multiplicatif.*

1. *Montrer que pour tout $a \in G$, l'application $f_a : x \mapsto axa^{-1}$ est un automorphisme de $G$. On dit que $f_a$ est un automorphisme intérieur de $G$.*
2. *Montrer que l'application $f : a \mapsto f_a$ est un morphisme de groupes de $G$ dans $\operatorname{Aut}(G)$ et que l'ensemble $\operatorname{Int}(G)$ des automorphismes intérieurs de $G$ est un sous-groupe de $\operatorname{Aut}(G)$.*
3. *Déterminer le noyau de $f$.*

4. *Déterminer ce noyau dans le cas où* $G = GL_n(\mathbb{R})$.
5. *Vérifier que si on prend pour définition d'automorphisme intérieur les applications* $g_a : x \mapsto a^{-1}xa$, *l'application* $a \mapsto g_a$ *n'est pas nécessairement un morphisme de groupes.*

**Solution 20.35**

1. *Pour* $x, y$ *dans* $G$, *on a :*

$$f_a(xy) = axya^{-1} = \left(axa^{-1}\right)\left(aya^{-1}\right) = f_a(x) f_a(y)$$

*ce qui signifie que* $f_a$ *est un endomorphisme de* $G$. *Pour* $y \in G$, *l'égalité* $y = f_a(x)$ *équivaut à* $x = a^{-1}ya = f_{a^{-1}}(y)$, *ce qui revient à dire que* $f_a$ *est bijective d'inverse* $f_a^{-1} = f_{a^{-1}}$.

2. *On vient de voir que l'application* $f$ *est une application du groupe* $G$ *dans le groupe* $(\mathrm{Aut}(G), \circ)$.
*Pour* $a, b$ *dans* $G$ *et* $x$ *dans* $G$, *on a :*

$$f_{ab}(x) = abx(ab)^{-1} = a\left(bxb^{-1}\right)a^{-1} = (f_a \circ f_b)(x)$$

*donc* $f(ab) = f_{ab} = f_a \circ f_b$ *et* $f$ *est un morphisme de groupes. Donc* $Int(G)$ *qui est l'image de* $f$ *est un sous-groupe de* $\mathrm{Aut}(G)$.

3. *Le noyau de* $f$ *est formé des* $a \in G$ *tels que* $f_a = Id_G$, *c'est-à-dire des* $a \in G$ *tels que* $axa^{-1} = x$ *pour tout* $x \in G$, *ce qui équivaut à* $ax = xa$ *pour tout* $x \in G$. *Le noyau est donc le commutateur (ou le centre)* $Z(G)$ *de* $G$.

4. *Pour* $G = GL_n(\mathbb{R})$, *ce noyau est formé des homothéties de rapport non nul. Soit* $A = ((a_{ij}))_{1\leq i,j\leq n}$ *dans le centre de* $GL_n(\mathbb{R})$, *c'est-à-dire commutant avec toutes les matrices inversibles. En désignant par* $(E_{ij})_{1\leq i,j\leq n}$ *la base canonique de* $\mathcal{M}_n(\mathbb{R})$, *on a* $A(I_n + E_{ij}) = (I_n + E_{ij})A$ *pour tous* $i, j$ *compris entre* $1$ *et* $n$, *ce qui équivaut à* $AE_{ij} = E_{ij}A$ *pour tous* $i, j$. *En désignant par* $(e_i)_{1\leq i\leq n}$ *la base canonique de* $\mathbb{R}^n$, *on a :*

$$AE_{ij}e_j = Ae_i = \sum_{k=1}^{n} a_{ki}e_k = E_{ij}Ae_j = E_{ij}\left(\sum_{k=1}^{n} a_{kj}e_k\right) = a_{jj}e_i.$$

*Donc* $a_{ki} = 0$ *pour* $k \in \{1, \cdots, n\} - \{i\}$ *et* $a_{ii} = a_{jj}$. *C'est-à-dire que* $A = \lambda I_n$ *avec* $\lambda \in \mathbb{R}^*$. *Réciproquement ces matrices d'homothéties sont bien dans le centre de* $GL_n(\mathbb{R})$.

5. *Si on prend pour définition d'automorphisme intérieurs les applications* $g_a : x \mapsto a^{-1}xa$, *on a* $g_{ab} = g_b \circ g_a \neq g_a \circ g_b$ *en général et* $a \mapsto g_a$ *n'est pas un morphisme de groupes.*
*Par exemple pour le groupe multiplicatif* $G = GL_2(\mathbb{R})$, *soient* $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ *et* $B = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$. *On a* $A^{-1} = A$, $B^{-1} = \begin{pmatrix} 0 & \frac{1}{2} \\ 1 & 0 \end{pmatrix}$ *et pour tout matrice* $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R})$, *on a :*

$$A^{-1}M = \begin{pmatrix} c & d \\ a & b \end{pmatrix},\ B^{-1}M = \begin{pmatrix} \frac{c}{2} & \frac{d}{2} \\ a & b \end{pmatrix}$$

*de sorte que :*

$$g_A(M) = A^{-1}MA = AMA = \begin{pmatrix} d & c \\ b & a \end{pmatrix}$$

*et :*

$$g_B(M) = B^{-1}MB = \begin{pmatrix} d & \frac{c}{2} \\ 2b & a \end{pmatrix}$$

*ce qui donne :*

$$g_A \circ g_B(M) = \begin{pmatrix} a & 2b \\ \frac{c}{2} & d \end{pmatrix} \neq g_B \circ g_A(M) = \begin{pmatrix} a & \frac{b}{2} \\ 2c & d \end{pmatrix}$$

*en général.*

**Exercice 20.36** *Déterminer tous les endomorphismes du groupe additif $\mathbb{Z}$ puis tous les automorphismes de ce groupe.*

**Solution 20.36** *Soit $\varphi$ un endomorphisme du groupe additif $\mathbb{Z}$. En notant $n = \varphi(1)$, on vérifie facilement par récurrence que pour tout entier $k \in \mathbb{N}$ on a $\varphi(k) = nk$ et avec $\varphi(-k) = -\varphi(k)$, on déduit que cette égalité est valable sur tout $\mathbb{Z}$. L'endomorphisme $\varphi$ est donc de la forme $\varphi : k \mapsto nk$. Réciproquement de telles applications définissent bien des endomorphismes de $\mathbb{Z}$. On a donc :*

$$End(\mathbb{Z}) = \{\varphi : k \mapsto nk \mid n \in \mathbb{Z}\} \approx \mathbb{Z}$$

*Si $\varphi : k \mapsto nk$ est un automorphisme de $\mathbb{Z}$, son inverse est aussi de la forme $\varphi^{-1} : k \mapsto mk$ et l'égalité $\varphi^{-1} \circ \varphi(k) = k$ pour tout $k \in \mathbb{Z}$ s'écrit $mnk = k$ pour tout $k \in \mathbb{Z}$, ce qui est réalisée si, et seulement si, $n = m = \pm 1$. On a donc :*

$$\mathrm{Aut}(\mathbb{Z}) = \{Id, -Id\} \approx \frac{\mathbb{Z}}{2\mathbb{Z}}$$

*(les groupe $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ sont définis au chapitre 25).*

**Exercice 20.37**

1. *Montrer que si $f$ est un endomorphisme du groupe additif $\mathbb{R}$, alors :*

$$\forall a \in \mathbb{R},\ \forall r \in \mathbb{Q},\ f(ra) = rf(a).$$

2. *Montrer que les seuls endomorphismes du groupe additif $\mathbb{R}$ qui sont monotones sont les homothéties (i. e. les applications $x \mapsto \lambda x$, où $\lambda$ est une constante réelle).*

**Solution 20.37** *Un endomorphisme du groupe additif $\mathbb{R}$ est une application $f : \mathbb{R} \to \mathbb{R}$ qui vérifie l'équation fonctionnelle de Cauchy :*

$$\forall (x, y) \in \mathbb{R}^2,\ f(x + y) = f(x) + f(y). \tag{20.1}$$

1. *En prenant $(x, y) = (0, 0)$ dans (20.1), on obtient $f(0) = 2f(0)$, ce qui équivaut à $f(0) = 0$ (un morphisme de groupes transforme le neutre en neutre).*
   *En prenant $(x, y) = (x, -x)$ dans (20.1), on obtient $f(x) + f(-x) = 0$. On a donc $f(-x) = -f(x)$ pour tout $x \in \mathbb{R}$, c'est-à-dire que la fonction $f$ est impaire (un morphisme de groupes transforme l'opposé en opposé).*
   *De (20.1) on déduit par récurrence que pour tout $a \in \mathbb{R}$ on a :*

$$\forall n \in \mathbb{N},\ f(na) = nf(a).$$

   *En effet, le résultat est vrai pour $n = 0$ et le supposant vrai pour $n \geq 0$, on a :*

$$f((n+1)a) = f(na) + f(a) = nf(a) + f(a) = (n+1)f(a),$$

*il est donc vrai pour tout* $n \in \mathbb{N}$.
*En écrivant, pour tout* $n \in \mathbb{N} \setminus \{0\}$, *que* $f(a) = f\left(n\frac{a}{n}\right) = nf\left(\frac{a}{n}\right)$, *on déduit que* $f\left(\frac{a}{n}\right) = \frac{1}{n}f(a)$ *pour tout* $a \in \mathbb{R}$ *et tout* $n \in \mathbb{N} \setminus \{0\}$. *Il en résulte que pour tout rationnel positif* $r = \frac{p}{q}$, *avec* $p \in \mathbb{N}$ *et* $q \in \mathbb{N} \setminus \{0\}$, *on a :*

$$f(ra) = f\left(p\frac{a}{q}\right) = pf\left(\frac{a}{q}\right) = \frac{p}{q}f(a) = rf(a).$$

*Enfin avec l'imparité de* $f$, *on déduit que ce dernier résultat est encore vrai pour les rationnels négatifs. On a donc* $f(ra) = rf(a)$ *pour tout* $a \in \mathbb{R}$ *et tout* $r \in \mathbb{Q}$.

2. *Soit* $f$ *un endomorphisme croissant du groupe additif* $\mathbb{R}$. *En particulier, on a* $\lambda = f(1) \geq f(0) = 0$.
*En désignant, pour* $x \in \mathbb{R}$, *par* $(r_n)_{n\in\mathbb{N}}$ *et* $(s_n)_{n\in\mathbb{N}}$ *des suites d'approximations décimales par défaut et par excès de ce réel, on a pour tout* $n \in \mathbb{N}$ *:*

$$\lambda r_n = f(r_n) \leq f(x) \leq f(s_n) = \lambda s_n$$

*et faisant tendre* $n$ *vers l'infini, on en déduit que* $f(x) = \lambda x$.
*On procède de manière analogue pour* $f$ *décroissante.*

**Exercice 20.38** *Soient* $G, H$ *deux sous-groupes du groupe additif* $\mathbb{R}$ *et* $\varphi$ *un morphisme de groupes croissant de* $G$ *vers* $H$. *On suppose que* $G$ *n'est pas réduit à* $\{0\}$.

1. *Montrer que l'ensemble* $G \cap \mathbb{R}^{+,*}$ *est non vide.*
2. *Montrer que s'il existe* $a$ *dans* $G \cap \mathbb{R}^{+,*}$ *tel que* $\varphi(a) = 0$, *alors* $\varphi$ *est le morphisme nul.*
3. *On suppose que pour tout* $x$ *dans* $G \cap \mathbb{R}^{+,*}$, *on a* $\varphi(x) \neq 0$.
   (a) *Montrer que* $\varphi(x) > 0$ *pour tout* $x$ *dans* $G \cap \mathbb{R}^{+,*}$.
   (b) *Montrer que la fonction* $x \mapsto \frac{\varphi(x)}{x}$ *est constante sur* $G \cap \mathbb{R}^{+,*}$.
   (c) *En déduire qu'il existe un réel positif* $\lambda$ *tel que* $\varphi(x) = \lambda x$ *pour tout* $x$ *dans* $G$.

**Solution 20.38** *Si* $G = \{0\}$ *alors* $\varphi(0) = 0$.

1. *Si* $G$ *n'est pas réduit à* $\{0\}$, *alors l'ensemble* $G \cap \mathbb{R}^{+,*}$ *est non vide du fait que pour tout* $x$ *non nul dans* $G$, $-x$ *est aussi dans* $G$.
2. *Supposons qu'il existe* $a$ *dans* $G \cap \mathbb{R}^{+,*}$ *tel que* $\varphi(a) = 0$. *Pour tout* $x$ *dans* $G \cap \mathbb{R}^{+,*}$ *on peut trouver un entier naturel* $n$ *tel que* $x < na$ ($\mathbb{R}$ *est archimédien) et avec la croissance de* $\varphi$, *on déduit que :*
$$0 \leq \varphi(x) \leq \varphi(na) = n\varphi(a) = 0,$$
*c'est-à-dire que* $\varphi$ *est nul sur* $G \cap \mathbb{R}^{+,*}$. *Avec* $\varphi(-x) = -\varphi(x)$ *pour tout* $x$ *dans* $G$, *on déduit que* $\varphi$ *est le morphisme nul.*
3. (a) *Si pour tout* $x$ *dans* $G \cap \mathbb{R}^{+,*}$, *on a* $\varphi(x) \neq 0$, *avec la croissance de* $\varphi$ *on déduit que* $\varphi(x) > 0$ *pour tout* $x$ *dans* $G \cap \mathbb{R}^{+,*}$.

*(b) Supposons qu'il existe* $a \neq b$ *dans* $G \cap \mathbb{R}^{+,*}$ *tels* $\dfrac{a}{b} \neq \dfrac{\varphi(a)}{\varphi(b)}$. *On peut supposer que* $\dfrac{a}{b} < \dfrac{\varphi(a)}{\varphi(b)}$ *et avec la densité de* $\mathbb{Q}$ *dans* $\mathbb{R}$ *on déduit qu'il existe un nombre rationnel* $\dfrac{p}{q}$ *tel que* $\dfrac{a}{b} < \dfrac{p}{q} < \dfrac{\varphi(a)}{\varphi(b)}$. *On a alors* $qa < pb$ *et avec la croissance de* $\varphi$ *on déduit que* $q\varphi(a) \leq p\varphi(b)$, *ce qui est en contradiction avec* $\dfrac{p}{q} < \dfrac{\varphi(a)}{\varphi(b)}$. *La fonction* $x \mapsto \dfrac{\varphi(x)}{x}$ *est donc constante sur* $G \cap \mathbb{R}^{+,*}$.

*(c) En notant* $\lambda$ *cette constante on a* $\lambda \geq 0$ *et* $\varphi(x) = \lambda x$ *pour tout* $x$ *dans* $G \cap \mathbb{R}^{+,*}$, *ce qui entraîne* $\varphi(x) = \lambda x$ *pour tout* $x$ *dans* $G$ *puisque* $\varphi$ *est un morphisme de groupes. On peut remarquer que* $\lambda$ *est nulle si, et seulement si,* $\varphi$ *est le morphisme nul. Pour* $G = H = \mathbb{R}$ *on retrouve le résultat de l'exercice précédent.*

**Exercice 20.39** *Soient* $G, H$ *deux sous-groupes du groupe multiplicatif* $\mathbb{R}^{+,*}$ *et* $\sigma$ *un morphisme de groupes croissant de* $G$ *vers* $H$. *Montrer qu'il existe un réel positif* $\lambda$ *tel que* $\sigma(x) = x^{\lambda}$ *pour tout* $x$ *dans* $G$.

**Solution 20.39** *Si* $G = \{1\}$, *alors* $\sigma(1) = 1$ *et* $\lambda = 1$ *convient.*
*Sinon* $\ln(G) = \{\ln(x) \mid x \in G\}$ *est un sous-groupe du groupe additif* $\mathbb{R}$ *non réduit à* $\{0\}$ *et* $\varphi : t \mapsto \ln(\sigma(e^t))$ *est un morphisme de groupes croissant de* $\ln(G)$ *vers* $\ln(H)$ *(la fonction logarithme est un morphisme de groupes strictement croissant de* $(\mathbb{R}^{+,*}, \times)$ *sur* $(\mathbb{R}, +)$*). Il existe donc un réel* $\lambda \geq 0$ *tel que* $\varphi(t) = \lambda t$ *pour tout* $t$ *dans* $\ln(G)$. *On a donc* $\sigma(e^t) = e^{\lambda t}$ *pour tout* $t$ *dans* $\ln(G)$ *et pour tout* $x$ *dans* $G$, *on a* $\sigma(x) = \sigma\left(e^{\ln(x)}\right) = e^{\lambda \ln(x)} = x^{\lambda}$.
*On peut remarquer que* $\lambda$ *est nulle si, et seulement si,* $\sigma$ *est l'application constante égale à* 1.

## 20.8 Sous-groupes distingués, groupes quotients

Pour ce paragraphe, on se donne un groupe multiplicatif $(G, \cdot)$.

Si $H$ est une partie non vide de $G$, on note, pour tout $g \in G$, $gH = \{g \cdot h \mid h \in H\}$ et $Hg = \{h \cdot g \mid h \in H\}$. Dans le cas où $G$ est commutatif, on a $gH = Hg$.

**Définition 20.12** *On dit qu'un sous-groupe* $H$ *de* $G$ *est distingué (ou normal) si on a* $gH = Hg$ *pour tout* $g \in G$.

On note parfois $H \lhd G$ pour signifier que $H$ est un sous-groupe distingué de $G$.

Si le groupe $G$ est commutatif, alors tous ses sous-groupes sont distingués.

**Théorème 20.16** *Un sous-groupe* $H$ *de* $G$ *est distingué si, et seulement si, on a* $ghg^{-1} \in H$ *pour tout* $(h, g) \in H \times G$, *ce qui équivaut encore à dire que* $H$ *est stable par tout automorphisme intérieur.*

**Démonstration.** Si $H$ est distingué dans $G$, on a alors $gH = Hg$ pour tout $g \in G$, ce qui équivaut à dire que pour tout $h \in H$ il existe $k \in H$ tel que $gh = kg$ et $ghg^{-1} = k \in H$. Le sous groupe $H$ est donc stable par tout automorphisme intérieur $a \mapsto gag^{-1}$.

Réciproquement si $H$ est stable par tout automorphisme intérieur, on a alors $ghg^{-1} \in H$ pour tout $(h, g) \in H \times G$, ce qui entraîne que $gh = (ghg^{-1})\, g \in Hg$ et $hg = g\,(g^{-1}hg) \in gH$ pour tout $(h, g) \in H \times G$, encore équivalent à dire que $gH = Hg$. ∎

**Exercice 20.40** *Montrer que :*

$$(H \lhd G) \Leftrightarrow (\forall g \in G,\ gH \subset Hg) \Leftrightarrow \left(\forall g \in G,\ gHg^{-1} \subset H\right)$$

**Solution 20.40** *On a :*

$$\begin{aligned}(H \lhd G) &\Leftrightarrow (\forall g \in G,\ gH = Hg) \Rightarrow (\forall g \in G,\ gH \subset Hg)\\ &\Rightarrow \left(\forall g \in G,\ gHg^{-1} \subset H\right) \Leftrightarrow (H \lhd G)\end{aligned}$$

*(si $gH \subset Hg$, alors pour $k \in H$, $gk \in Hg$, donc il existe $k' \in H$ tel que $gk = k'g$ et $gkg^{-1} = k' \in H$, donc $gHg^{-1} \subset H$).*

**Exercice 20.41** *Soient $G, G'$ deux groupes et $\varphi$ un morphisme de groupes de $G$ dans $G'$. Montrer que* $\ker(\varphi)$ *est un sous-groupe distingué de $G$.*

**Solution 20.41** *Pour $(g,h) \in G \times \ker(\varphi)$, on a :*

$$\varphi\left(g^{-1}hg\right) = \varphi\left(g^{-1}\right)\varphi(h)\varphi(g) = \varphi(g)^{-1} \cdot 1 \cdot \varphi(g) = 1$$

*c'est-à-dire que $g^{-1}hg \in \ker(\varphi)$. Le sous-groupe* $\ker(\varphi)$ *de $G$ est donc distingué.*

**Exercice 20.42** *Montrer que le centre d'un groupe $G$ est distingué.*

**Solution 20.42** *On a vu que le centre $Z(G)$ est le noyau du morphisme de groupes $a \mapsto f_a : g \mapsto aga^{-1}$ de $G$ dans* $\mathrm{Aut}(G)$ *(exercice 20.35), c'est donc un sous-groupe distingué de $G$.*

**Exercice 20.43** *Soient $G, H$ deux groupes et $\varphi$ un morphisme de groupes de $G$ dans $H$.*

1. *Montrer que si $G_1$ est un sous-groupe distingué de $G$ et $\varphi$ est surjectif, alors $\varphi(G_1)$ est un sous-groupe distingué de $H$ (pour $\varphi$ non surjectif, $\varphi(G_1)$ est un sous-groupe distingué de $\varphi(G)$).*
2. *Montrer que si $H_1$ est un sous-groupe distingué de $H$, alors $\varphi^{-1}(H_1)$ est un sous-groupe distingué de $G$.*

**Solution 20.43** *On sait déjà que $\varphi(G_1)$ est un sous-groupe de $H$ (que $\varphi$ soit surjectif ou non) et que $\varphi^{-1}(H_1)$ est un sous-groupe de $G$.*

1. *Si $\varphi$ est surjectif, tout $h \in H$ s'écrit $h = \varphi(g)$ avec $g \in G$ et pour tout $h_1 = \varphi(g_1) \in \varphi(G_1)$ (avec $g_1 \in G_1$), on a $hh_1 = \varphi(g)\varphi(g_1) = \varphi(gg_1)$ avec $gg_1 \in gG_1 = G_1g$ et il existe alors $g_2 \in G_1$ tel que $gg_1 = g_2g$, ce qui donne $hh_1 = \varphi(g_2g) = \varphi(g_2)\varphi(g) = \varphi(g_2)h \in \varphi(G_1)h$. On a donc $h\varphi(G_1) \subset \varphi(G_1)h$, pour tout $h \in H$, ce qui signifie que $\varphi(G_1)$ est distingué dans $H$.*
2. *Pour $g \in G$ et $g_1 \in \varphi^{-1}(H_1)$, on a :*

$$\varphi\left(gg_1g^{-1}\right) = \varphi(g)\varphi(g_1)(\varphi(g))^{-1} \in \varphi(g)H_1(\varphi(g))^{-1} = H_1$$

*et $gg_1g^{-1} \in \varphi^{-1}(H_1)$. Donc $g\varphi^{-1}(H_1)g^{-1} \subset \varphi^{-1}(H_1)$ et $\varphi^{-1}(H_1)$ est distingué dans $G$.*

**Théorème 20.17** *Un sous-groupe $H$ de $G$ est distingué si, et seulement si, il existe une unique structure de groupe sur l'ensemble quotient $G/H$ des classes à gauche modulo $H$ telle que la surjection canonique $\pi : G \to G/H$ soit un morphisme de groupes.*

**Démonstration.** Si $G/H$ est muni d'une structure de groupe telle que $\pi$ soit un morphisme de groupe, on a alors nécessairement pour tous $g, g'$ dans $G$ :

$$\overline{g}\overline{g'} = \pi(g)\,\pi(g') = \pi(gg') = \overline{gg'}$$

Pour $(g,h)$ dans $G \times H$, on a alors $\overline{g^{-1}hg} = \overline{g^{-1}h}\,\overline{g} = \overline{g^{-1}}\,\overline{g} = \overline{g^{-1}g} = \overline{1} = H$, ce qui signifie que $g^{-1}hg \in H$ (on rappelle que $\overline{g} = gH = \overline{1} = H$ si, et seulement si, $g \in H$).

Supposons $H$ distingué. L'analyse que l'on vient de faire nous montre que la seule loi possible sur $G/H$ est définie par $\overline{g}\overline{g'} = \overline{gg'}$. Pour montrer qu'une telle définition est permise, il s'agit de montrer qu'elle ne dépend pas des choix des représentants de $\overline{g}$ et $\overline{g'}$. Si $\overline{g} = \overline{g_1}$ et $\overline{g'} = \overline{g'_1}$, on a alors $g^{-1}g_1 \in H$ et $(g')^{-1}g'_1 \in H$, ce qui entraîne :

$$(gg')^{-1}(g_1g'_1) = (g')^{-1}g^{-1}g_1g'_1 = \left((g')^{-1}\left(g^{-1}g_1\right)g'\right)\left((g')^{-1}g'_1\right) \in H$$

$\underline{((g')^{-1}(g^{-1}g_1)\,g'}$ est dans $H$ puisque $H$ est stable par automorphismes intérieurs), soit $\overline{gg'} = \overline{g_1g'_1}$.

Il reste à vérifier que $G/H$ muni de cette loi de composition interne est bien un groupe.

Avec :

$$\begin{aligned}\overline{g_1}\,(\overline{g_2}\ \overline{g_3}) &= \overline{g_1g_2g_3} = \overline{g_1\,(g_2g_3)} = \overline{(g_1g_2)\,g_3}\\ &= \overline{g_1g_2}\ \overline{g_3} = (\overline{g_1}\ \overline{g_2})\,\overline{g_3}\end{aligned}$$

on déduit que cette loi est associative.

Avec $\overline{g}\overline{1} = \overline{g \cdot 1} = \overline{g}$, on déduit que $\overline{1}$ est le neutre.

Avec $\overline{g}\overline{g^{-1}} = \overline{g \cdot g^{-1}} = \overline{1}$, on déduit que tout élément de $G/H$ est inversible avec $(\overline{g})^{-1} = \overline{g^{-1}}$.

Par définition de cette loi de composition interne, l'application $\pi$ est surjective. ■

**Remarque 20.5** *Pour $H$ distingué dans $G$, le noyau de la surjection canonique est :*

$$\ker(\pi) = \left\{g \in G \mid \overline{g} = \overline{1}\right\} = \overline{1} = H$$

*Comme on a vu que le noyau d'un morphisme de groupes est distingué, on déduit qu'un sous-groupe distingué de $G$ est le noyau d'un morphisme de groupes.*

**Remarque 20.6** *Dans le cas où $G$ est commutatif, pour tout sous-groupe $H$ de $G$, $G/H$ est un groupe puisque tous les sous-groupes de $G$ sont distingués.*

**Exemple 20.31** *Si $G$ est le groupe additif $\mathbb{Z}$, on sait alors que ces sous-groupes sont les $n\mathbb{Z}$ où $n$ est un entier naturel et comme $(\mathbb{Z},+)$ est commutatif, l'ensemble quotient $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est naturellement muni d'une structure de groupe.*
*D'autre part, le théorème de division euclidienne nous permet d'écrire tout entier relatif $k$ sous la forme $k = qn + r$ avec $0 \leq r \leq n-1$, ce qui entraîne $k - r \in n\mathbb{Z}$ et $\overline{k} = \overline{r}$. Et comme $\overline{r} \neq \overline{s}$ pour $0 \leq r \neq s \leq n-1$ (on a $0 < |r-s| < n$ et $r-s$ ne peut être multiple de $n$), on en déduit que :*

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \left\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\right\}$$

*a $n$ éléments. Ce groupe est cyclique d'ordre $n$ engendré par $\overline{1}$.*

**Exercice 20.44** *Montrer qu'un sous-groupe $H$ de $G$ d'indice 2 est distingué.*

**Solution 20.44** *On a* $\operatorname{card}(G/H) = 2$. *Pour* $(g,h) \in G \times H$, *on a soit* $g \in H$ *et* $ghg^{-1} \in H$, *soit* $g \notin H$, *donc* $\overline{g} = gH \neq \overline{1} = H$ *et* $G = gH \cup H$ *avec* $gH \cap H = \emptyset$ *(les classes d'équivalence forment une partition de* $G$*). Si, pour* $g \notin H$, $ghg^{-1}$ *n'est pas dans* $H$, *il est forcément dans* $gH$ *et il existe* $k \in H$ *tel que* $ghg^{-1} = gk$, *ce qui entraîne* $hg^{-1} = k$ *et* $g = hk^{-1} \in H$, *en contradiction avec* $g \notin H$.

**Théorème 20.18** *Si* $G, H$ *sont deux groupes et* $\varphi : G \to H$ *un morphisme de groupes, il existe alors un unique isomorphisme de groupes* $\overline{\varphi} : G/\ker(\varphi) \to \operatorname{Im}(\varphi)$ *tel que* $\varphi = i \circ \overline{\varphi} \circ \pi$, *où* $i : \operatorname{Im}(\varphi) \to H$ *est l'injection canonique (définie par* $i(h) = h$ *pour tout* $h \in \operatorname{Im}(\varphi)$*) et* $\pi : G \to G/\ker(\varphi)$ *la surjection canonique (définie par* $\pi(g) = \overline{g} = g\ker(\varphi)$ *pour tout* $g \in G$*).*

**Démonstration.** Comme $\ker(\varphi)$ est distingué dans $G$, $G/\ker(\varphi)$ est un groupe.

Si un tel isomorphisme $\overline{\varphi}$ existe, on a alors, pour tout $g \in G$ :

$$\varphi(g) = i \circ \overline{\varphi} \circ \pi(g) = i \circ \overline{\varphi}(\overline{g}) = \overline{\varphi}(\overline{g})$$

ce qui prouve l'unicité de $\overline{\varphi}$.

Vu l'analyse du problème, on montre d'abord que l'on peut définir $\overline{\varphi}$ par $\overline{\varphi}(\overline{g}) = \varphi(g)$ pour tout $\overline{g} \in G/\ker(\varphi)$. Pour justifier cette définition, on doit vérifier qu'elle ne dépend pas des choix du choix d'un représentant de $\overline{g}$. Si $\overline{g} = \overline{g'}$, on a alors $g'g^{-1} \in \ker(\varphi)$, donc $\varphi(g')(\varphi(g))^{-1} = \varphi(g'g^{-1}) = 1$ et $\varphi(g) = \varphi(g')$. L'application $\overline{\varphi}$ est donc bien définie et par construction, on a $\varphi = i \circ \overline{\varphi} \circ \pi$.

$\overline{\varphi}$ est à valeurs dans $\operatorname{Im}(\varphi) = \operatorname{Im}(\overline{\varphi})$, donc surjectif.

Avec :

$$\overline{\varphi}\left(\overline{g}\overline{g'}\right) = \overline{\varphi}\left(\overline{gg'}\right) = \varphi(gg') = \varphi(g)\varphi(g') = \overline{\varphi}(\overline{g})\overline{\varphi}\left(\overline{g'}\right)$$

on voit que c'est un morphisme de groupes.

L'égalité $\overline{\varphi}(\overline{g}) = 1$ équivaut à $\varphi(g) = 1$, soit à $g \in \ker(\varphi)$ ou encore à $\overline{g} = \overline{1}$. Ce morphisme est donc injectif. ∎

**Corollaire 20.2** *Soient* $G, H$ *deux groupes et* $\varphi : G \to H$ *un morphisme de groupes. Si* $G$ *est fini, on a alors :*

$$\operatorname{card}(G) = \operatorname{card}(\ker(\varphi))\operatorname{card}(\operatorname{Im}(\varphi))$$

**Démonstration.** Comme $G/\ker(\varphi)$ et $\operatorname{Im}(\varphi)$ sont isomorphes, dans le cas où $G$ est fini, on a :

$$\operatorname{card}(\operatorname{Im}(\varphi)) = \operatorname{card}(G/\ker(\varphi)) = \frac{\operatorname{card}(G)}{\operatorname{card}(\ker(\varphi))}.$$

∎

Le théorème précédent s'exprime aussi en disant qu'on a le diagramme commutatif :

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ \pi \downarrow & & \uparrow i \\ G/\ker(\varphi) & \xrightarrow{\overline{\varphi}} & \operatorname{Im}(\varphi) \end{array}$$

**Théorème 20.19** *Si* $n = \dim(E) \geq 2$, *alors* $\mathcal{O}^+(E)$ *[resp.* $\mathcal{O}_n^+(\mathbb{R})$*] est un sous-groupe distingué de* $\mathcal{O}(E)$ *[resp. de* $\mathcal{O}_n(\mathbb{R})$*] d'indice* 2.

**Démonstration.** $\mathcal{O}^+(E)$ est un sous-groupe distingué de $\mathcal{O}(E)$ comme noyau du morphisme de groupes $\det : \mathcal{O}(E) \to \{-1, 1\}$. Comme cette application est surjective ($Id \in \mathcal{O}^+(E)$ et en désignant par $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ une base orthonormée de $E$, l'application $u$ définie par $u(e_1) = -e_1$ et $u(e_i) = e_i$ pour $i$ compris entre 2 et $n$ est dans $\mathcal{O}^-(E)$), $\mathcal{O}(E)/\mathcal{O}^+(E)$ est isomorphe à $\{-1, 1\}$ et $[\mathcal{O}(E) : \mathcal{O}^+(E)] = 2$. ∎

**Exercice 20.45** *Soient $G, H$ deux groupes, $\varphi : G \to H$ un morphisme de groupes, $G'$ un sous-groupe distingué de $G$ et $H'$ un sous-groupe distingué de $H$ tel que $\varphi(G') \subset H'$. Montrer qu'il existe un unique morphisme de groupes $\overline{\varphi} = G/G' \to H/H'$ tel que $\pi_H \circ \varphi = \overline{\varphi} \circ \pi_G$, où $\pi_G : G \to G/G'$ et $\pi_H : H \to H/H'$ sont les surjections canoniques.*

**Solution 20.45** *En supposant que $\overline{\varphi}$, on a nécessairement $\pi_H \circ \varphi(g) = \overline{\varphi} \circ \pi_G(g)$ pour tout $g \in G$, ce qui assure l'unicité de $\overline{\varphi}$.*
*On définit donc $\overline{\varphi}$ par :*

$$\forall \overline{g} \in G/G',\ \overline{\varphi}(\overline{g}) = \widetilde{\varphi(g)}$$

*en notant $\overline{g} = gG'$ la classe de $g \in G$ modulo $G'$ et $\widetilde{h}$ la classe de $h \in H$ modulo $H'$. Pour justifier cette définition, on doit vérifier qu'elle ne dépend pas des choix du choix d'un représentant de $\overline{g}$. Si $\overline{g_1} = \overline{g_2}$, on a alors $g_2 g_1^{-1} \in G'$, donc $\varphi(g_2)(\varphi(g_1))^{-1} = \varphi\left(g_2 g_1^{-1}\right) \in \varphi(G') \subset H'$ et $\widetilde{\varphi(g_1)} = \widetilde{\varphi(g_2)}$. L'application $\overline{\varphi}$ est donc bien définie et par construction, on a $\pi_H \circ \varphi = \overline{\varphi} \circ \pi_G$.*
*Avec :*

$$\begin{aligned}\overline{\varphi}(\overline{g_1 g_2}) &= \overline{\varphi}(\overline{g_1 g_2}) = \widetilde{\varphi(g_1 g_2)} = \widetilde{\varphi(g_1)\,\varphi(g_2)} \\ &= \widetilde{\varphi(g_1)}\widetilde{\varphi(g_2)} = \overline{\varphi}(\overline{g_1})\,\overline{\varphi}(\overline{g_2})\end{aligned}$$

*on voit que c'est un morphisme de groupes.*

Si $\mathcal{R}$ est une relation d'équivalence sur $G$, on dit que cette relation est compatible avec la loi de $G$ si, pour tous $g, g', h, h'$ dans $G$, on a :

$$(g\mathcal{R}h \text{ et } g'\mathcal{R}h') \Rightarrow gg'\mathcal{R}hh'$$

Cette compatibilté de $\mathcal{R}$ avec la loi de $G$ est une condition nécessaire et suffisante pour définir naturellement une structure de groupe sur l'ensemble quotient $G/\mathcal{R}$ par :

$$\overline{g}\overline{g'} = \overline{gg'}$$

Précisément, on a le résultat suivant, où $G/\mathcal{R}$ est l'ensemble des classes d'équivalence modulo $\mathcal{R}$ et $\pi : g \mapsto \overline{g} = \{h \in G \mid g\mathcal{R}h\}$ est la surjection canonique de $G$ sur $G/\mathcal{R}$.

**Théorème 20.20** *Soit $\mathcal{R}$ une relation d'équivalence sur $G$. Cette relation est compatible avec la loi de $G$ si, et seulement si, il existe une unique structure de groupe sur l'ensemble quotient $G/\mathcal{R}$ telle que la surjection canonique $\pi : G \to G/\mathcal{R}$ soit un morphisme de groupes.*

**Démonstration.** Si $G/\mathcal{R}$ est muni d'une structure de groupe telle que $\pi$ soit un morphisme de groupe, on a alors nécessairement pour tous $g, g'$ dans $G$ :

$$\overline{g}\overline{g'} = \pi(g)\,\pi(g') = \pi(gg') = \overline{gg'}$$

On en déduit que pour $g, g', h, h'$ dans $G$ tels que $g\mathcal{R}h$ et $g'\mathcal{R}h'$, on a :

$$\overline{gg'} = \overline{g}\ \overline{g'} = \overline{h}\ \overline{h'} = \overline{hh'}$$

ce qui signifie que $gg'\mathcal{R}hh'$. La relation $\mathcal{R}$ est donc compatible avec la loi de $G$.

Réciproquement, supposons que $\mathcal{R}$ soit compatible avec la loi de $G$. L'analyse que l'on vient de faire nous montre que la seule loi possible sur $G/\mathcal{R}$ est définie par $\overline{g}\overline{g'} = \overline{gg'}$. Pour montrer qu'une telle définition est permise, il s'agit de montrer qu'elle ne dépend pas des choix des représentants de $\overline{g}$ et $\overline{g'}$. Si $\overline{g} = \overline{h}$ et $\overline{g'} = \overline{h'}$, on a alors $g\mathcal{R}h$ et $g'\mathcal{R}h'$, ce qui entraîne $gg'\mathcal{R}hh'$, soit $\overline{gg'} = \overline{hh'}$. ∎

**Exercice 20.46** *Soit $\mathcal{R}$ une relation d'équivalence sur $G$ compatible avec la loi de $G$. Montrer que :*

1. *pour tous $g, h$ dans $G$, on a $g\overline{h} = \overline{gh}$ et $\overline{h}g = \overline{hg}$ ;*
2. *$H = \overline{1}$ est un sous-groupe distingué de $G$ ;*
3. *pour tout $g \in G$, $\overline{g} = gH = Hg$ et $G/\mathcal{R} = G/H$.*

**Solution 20.46**

1. *On a :*

$$\left(k \in g\overline{h}\right) \Leftrightarrow \left(\exists h' \in G \mid h'\mathcal{R}h \text{ et } k = gh'\right) \Rightarrow \left(k = gh'\mathcal{R}gh\right) \Rightarrow \left(k \in \overline{gh}\right)$$

*donc $g\overline{h} \subset \overline{gh}$. Et réciproquement :*

$$\left(k \in \overline{gh}\right) \Leftrightarrow \left(k\mathcal{R}gh\right) \Rightarrow \left(g^{-1}k\mathcal{R}h\right) \Rightarrow \left(g^{-1}k \in \overline{h}\right) \Rightarrow \left(k \in g\overline{h}\right)$$

*soit $\overline{gh} \subset g\overline{h}$ et $g\overline{h} = \overline{gh}$.*
*On procède de manière analogue pour l'égalité $\overline{h}g = \overline{hg}$*

2. *On a $1 \in H = \overline{1}$, si $g, h$ sont dans $H$, on a $g\mathcal{R}1$ et $h\mathcal{R}1$, donc $gh\mathcal{R}1$ et pour $g \in H$, $1\mathcal{R}g$ et $g^{-1}\mathcal{R}g^{-1}$ entraîne $g^{-1}\mathcal{R}1$, soit $g^{-1} \in H$. Donc $H$ est bien un sous-groupe de $G$.*
*pour $g \in G$, on a $gH = g\overline{1} = \overline{g}$ et $Hg = \overline{1}g = \overline{g} = gH$, ce qui signifie que $H$ est distingué dans $G$.*
3. *On a aussi montré en **2.** que $G/\mathcal{R} = G/H$.*

L'exercice précédent nous dit en fait que les relations d'équivalence sur un groupe compatibles avec sa loi sont celles suivant un groupe distingué (à gauche ou à droite).

## 20.9 Ordre d'un élément dans un groupe

Pour ce paragraphe, on se donne un groupe multiplicatif $(G, \cdot)$ et pour tout $a \in G$, $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ est le sous-groupe de $G$ engendré par $a$.

**Définition 20.13** *L'ordre d'un élément $a$ de $G$ est l'élément $\theta(a) \in \mathbb{N}^* \cup \{+\infty\}$ défini par :*

$$\theta(a) = \operatorname{card}(\langle a \rangle).$$

*Si $\theta(a)$ est dans $\mathbb{N}^*$, on dit alors que $a$ est d'ordre fini, sinon on dit qu'il est d'ordre infini.*

**Remarque 20.7** *Seul l'unité $1 \in G$ est d'ordre 1 dans $G$. En effet, si $a = 1$, alors $\langle a \rangle = \{1\}$ et si $a \neq 1$, alors $a^0 \neq a^1$ et $\langle a \rangle$ a au moins deux éléments.*

**Remarque 20.8** *Pour tout $a \in G$, on a $\theta(a) = \theta(a^{-1})$ puisque :*

$$\begin{aligned}\left\langle a^{-1} \right\rangle &= \left\{\left(a^{-1}\right)^n \mid n \in \mathbb{Z}\right\} = \left\{a^{-n} \mid n \in \mathbb{Z}\right\} \\ &= \{a^n \mid n \in \mathbb{Z}\} = \langle a \rangle\end{aligned}$$

**Remarque 20.9** *Dans le cas où le groupe $G$ est fini, le théorème de Lagrange (théorème 20.12) nous dit que, pour tout $a \in G$, l'ordre de $a$ divise l'ordre de $G$.*
*Un groupe fini $G$ d'ordre $n$ est cyclique si, et seulement si, il existe dans $G$ un élément d'ordre $n$.*

**Exercice 20.47** *Déterminer l'ordre d'un élément du groupe multiplicatif* $\mathbb{C}^*$.

**Solution 20.47** *Tout nombre complexe non nul s'écrit* $z = \rho e^{i\alpha}$ *où* $\rho \in \mathbb{R}^{+,*}$ *et* $\alpha \in [0, 2\pi[$ *(avec un tel choix de* $\alpha$*, cette écriture est unique).*
*Si* $\rho \neq 1$*, on a* $\left|z^k\right| = \rho^k \neq 1$ *pour tout entier relatif* $k$*, donc* $z^k \neq z^j$ *pour* $k \neq j$ *dans* $\mathbb{Z}$ *et* $\langle z \rangle$ *est infini.*
*Si* $\rho = 1$*, on a alors, pour* $k$ *entier relatif non nul,* $z^k = e^{ik\alpha} = 1$ *si, et seulement si, il existe un entier relatif* $q$ *tel que* $k\alpha = 2q\pi$*, ce qui signifie que* $\dfrac{\alpha}{2\pi}$ *est rationnel. On en déduit donc que :*

- *pour* $\dfrac{\alpha}{2\pi}$ *irrationnel,* $z^k \neq 1$ *pour tout entier relatif* $k$ *et* $\langle z \rangle$ *est infini ;*
- *pour* $\dfrac{\alpha}{2\pi} = \dfrac{p}{q}$ *rationnel avec* $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ *et* $p \wedge q = 1$*, en effectuant la division euclidienne d'un entier relatif* $k$ *par* $q$*, on a* $k = mq + r$ *avec* $0 \leq r \leq q - 1$ *et :*

$$z^k = e^{ik\alpha} = \left(e^{iq\alpha}\right)^m e^{ir\alpha} = \left(e^{2ip\pi}\right)^m e^{ir\alpha} = e^{ir\alpha}$$

*et* $\langle z \rangle = \{e^{ir\alpha} \mid 0 \leq r \leq q - 1\}$ *a au plus* $q$ *éléments.*
*Pour* $0 \leq r \neq s \leq q - 1$ *l'égalité* $e^{ir\alpha} = e^{is\alpha}$ *équivaut à* $e^{i(s-r)\alpha} = 1$*, ce qui revient à dire* $(s - r)\,\alpha = 2m\pi$ *avec* $m \in \mathbb{Z}$*, qui tenant compte de* $\alpha = 2\pi\dfrac{p}{q}$*, donne* $(s - r)\,\dfrac{p}{q} = m$*, soit* $q$ *divise* $p\,(s - r)$ *sachant que* $q$ *est premier avec* $p$*, donc* $q$ *divise* $r - s$ *(théorème de Gauss) et nécessairement* $r = s$ *puisque* $|r - s| \leq q - 1$*. On a donc exactement* $q$ *éléments dans* $\langle z \rangle$ *et* $z$ *est d'ordre* $q$*.*
*En fait* $\langle z \rangle$ *est le groupe* $\Gamma_q$ *des racines* $q$*-èmes de l'unité.*

*En définitive :*

$$\theta\left(\rho e^{i\alpha}\right) = \begin{cases} +\infty \text{ si } \rho \neq 1 \text{ ou } \rho = 1 \text{ et } \dfrac{\alpha}{2\pi} \text{ irrationnel} \\ q \text{ si } \dfrac{\alpha}{2\pi} = \dfrac{p}{q} \in \mathbb{Q} \text{ avec } p \wedge q = 1 \end{cases}$$

**Exercice 20.48** *Déterminer l'ordre d'une matrice de rotation [resp. de réflexion] dans* $GL_2(\mathbb{R})$ *(exercices 20.16 et 20.17). En déduire qu'on peut trouver deux éléments d'ordre fini dans* $GL_2(\mathbb{R})$ *dont le produit est d'ordre infini.*

**Solution 20.48** *Pour tout réel* $\alpha$ *et tout entier* $n \geq 1$*, on a* $R_\alpha^n = R_{n\alpha}$ *et* $R_\alpha^n = I_n$ *équivaut à* $e^{-in\alpha} = 1$*, ce qui revient à dire qu'il existe un entier relatif* $q$ *tel que* $n\alpha = 2q\pi$*. Il en résulte qu'une matrice de rotation* $R_\alpha$ *est d'ordre fini si, et seulement si,* $\dfrac{\alpha}{2\pi} \in \mathbb{Q}$.
*Si* $S_\alpha$ *est une matrice de réflexion, on a* $S_\alpha^2 = R_{\alpha-\alpha} = I_n$ *et* $S_\alpha \neq I_n$*, donc* $S_\alpha$ *est d'ordre* 2.
*La composée de deux matrices de réflexions* $S_\alpha \circ S_{\alpha'} = R_{\alpha-\alpha'}$ *est d'ordre infini si* $\dfrac{\alpha - \alpha'}{2\pi} \notin \mathbb{Q}$.

Pour $a \in G$, le sous-groupe de $G$ engendré par $a$ peut être vu comme l'image du morphisme de groupes :

$$\begin{array}{rccc} \varphi_a : & \mathbb{Z} & \to & G \\ & k & \mapsto & a^k \end{array}$$

(pour $j, k$ dans $\mathbb{Z}$, on a $\varphi_a(j + k) = a^{j+k} = a^j a^k = \varphi_a(j)\,\varphi_a(k)$ et $\varphi_a$ est bien un morphisme de groupes).

En utilisant la connaissance des sous-groupes additifs de $\mathbb{Z}$, on a le résultat suivant.

**Théorème 20.21** *Pour* $a \in G$*, on a* $\theta(a) = +\infty$ *si, et seulement si,* $\varphi_a$ *est injective et pour* $a$ *d'ordre fini, on a* $\ker(\varphi_a) = \theta(a)\,\mathbb{Z}$.

**Démonstration.** Le noyau de $\varphi_a$ étant un sous-groupe de $\mathbb{Z}$, il existe un unique entier $n \geq 0$ tel que $\ker(\varphi_a) = n\mathbb{Z}$.

On aura $n = 0$ si, et seulement si, $\varphi_a$ est injective, ce qui revient à dire que $\varphi_a(k) = a^k \neq 1$ pour tout $k \in \mathbb{Z}^*$ ou encore que $\varphi_a(k) = a^k \neq \varphi_a(j) = a^j$ pour tous $j \neq k$ dans $\mathbb{Z}$ et le sous-groupe $\langle a \rangle = \mathrm{Im}(\varphi_a)$ est infini.

Si $n \geq 1$, en effectuant, pour $k \in \mathbb{Z}$, la division euclidienne de $k$ par $n$, on a $k = qn + r$ avec $0 \leq r \leq n-1$ et $a^k = (a^n)^q a^r = a^r$, ce qui nous donne :

$$\langle a \rangle = \mathrm{Im}(\varphi_a) = \{a^r \mid 0 \leq r \leq n-1\}$$

De plus pour $1 \leq r \leq n-1$, on a $a^r \neq 1$ puisque $n = \inf(\ker(\varphi_a) \cap \mathbb{N}^*)$, ce qui entraîne $a^r \neq a^s$ pour $0 \leq r \neq s \leq n-1$ (pour $s \geq r$, l'égalité $a^r = a^s$ équivaut à $a^{s-r} = 1$ avec $s - r$ compris entre 0 et $n-1$, ce qui équivaut à $r = s$). Le groupe $\langle a \rangle$ a donc exactement $n$ éléments. ∎

Une autre définition de l'ordre d'un élément d'un groupe est donnée par le résultat suivant.

**Corollaire 20.3** *Dire que $a \in G$ est d'ordre fini $n \geq 1$ équivaut à dire que $a^n = 1$ et $a^k \neq 1$ pour tout $k$ est compris entre 1 et $n-1$ ($\theta(a)$ est le plus petit entier naturel non nul tel que $a^n = 1$).*

**Démonstration.** Si $a$ est d'ordre $n \geq 1$, on a vu avec la démonstration du théorème précédent que $a^n = 1$ et $a^k \neq 1$ pour tout $k$ est compris entre 1 et $n-1$.

Réciproquement s'il existe un entier $n \geq 1$ tel que $a^n = 1$ et $a^k \neq 1$ pour $k$ est compris entre 1 et $n-1$, le morphisme de groupes $\varphi_a$ est non injectif, donc $a$ est d'ordre fini et $\ker(\varphi_a) = \theta(a)\,\mathbb{Z}$ avec $\theta(a) = \inf(\ker(\varphi_a) \cap \mathbb{N}^*) = n$. ∎

**Corollaire 20.4** *Dire que $a \in G$ est d'ordre fini $n \geq 1$ équivaut à dire que, pour $k \in \mathbb{Z}$, on a $a^k = 1$ si, et seulement si, $k$ est multiple de $n$.*

**Démonstration.** Si $a$ est d'ordre $n$, on a alors $a^n = 1$ et pour $k = qn + r \in \mathbb{Z}$ avec $q \in \mathbb{Z}$ et $0 \leq r \leq n-1$ (division euclidienne), on a $a^k = a^r = 1$ si, et seulement si $r = 0$.

Réciproquement supposons que $a^k = 1$ si, et seulement si, $k$ est multiple de $n$. On a alors $a^n = 1$ et $a^k \neq 1$ si $k$ est compris entre 1 et $n-1$, ce qui signifie que $a$ est d'ordre $n$. ∎

En résumé, on retiendra que :

- $(\theta(a) = +\infty) \Leftrightarrow (\varphi_a \text{ injective}) \Leftrightarrow (\ker(\varphi_a) = \{0\}) \Leftrightarrow$
  $\big(\forall k \in \mathbb{Z}^*,\ a^k \neq 1\big) \Leftrightarrow (\langle a \rangle \text{ est infini isomorphe à } \mathbb{Z})$ ;
- $(\theta(a) = n \in \mathbb{N}^*) \Leftrightarrow (\ker(\varphi_a) = n\mathbb{Z}) \Leftrightarrow (\langle a \rangle = \{a^r \mid 0 \leq r \leq n-1\})$
  $\Leftrightarrow \big(k \in \mathbb{Z} \text{ et } a^k = 1 \text{ équivaut à } k \equiv 0 \mod(n)\big) \Leftrightarrow$
  ($n$ est le plus petit entier naturel non nul tel que $a^n = 1$).

Pour $a$ d'ordre fini, le groupe $\langle a \rangle$ est dit cyclique, ce qui est justifié par $a^{qn+r} = a^r$ pour $q \in \mathbb{Z}$ et $0 \leq r \leq n-1$.

**Théorème 20.22** *Si $G$ est un groupe cyclique d'ordre $n$, il est alors isomorphe au groupe $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.*

**Démonstration.** Si $G = \langle a \rangle$ est cyclique d'ordre $n$, alors l'application $\varphi_a : k \mapsto a^k$ est un morphisme de groupes surjectif de $(\mathbb{Z}, +)$ sur $G$ de noyau $\ker(\varphi_a) = n\mathbb{Z}$ et le théorème d'isomorphisme (théorème 20.18) nous dit $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est isomorphe à $G$. ∎

**Exemple 20.32** *Le groupe multiplication $\Gamma_n$ des racines $n$-èmes de l'unité, qui est cyclique d'ordre $n$, est isomorphe à $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ par l'application $\overline{k} \mapsto e^{\frac{2ik\pi}{n}}$.*

Dans le cas où le groupe $G$ est additif, l'ordre de $a \in G$ est défini comme le plus petit entier $n \geq 1$ tel que $na = 0$, quand cet ordre est fini. L'égalité $ma = 0$ équivaut alors à dire que $m$ est multiple de $n$. Le groupe engendré par $a$ est alors :

$$\langle a \rangle = \{ka \mid k \in \mathbb{Z}\} = \{ra \mid 0 \leq r \leq n-1\}.$$

**Corollaire 20.5** *Si $G$ est fini d'ordre $m$, on a alors $a^m = 1$ pour tout $a \in G$.*

**Démonstration.** $\theta(a)$ est fini et divise $m$. ∎

**Exercice 20.49** *Déterminer les sous-groupes finis du groupe multiplicatif $\mathbb{C}^*$.*

**Solution 20.49** *Si $G \subset \mathbb{C}^*$ est un groupe d'ordre $n \geq 1$, on a alors $z^n = 1$ pour $z \in G$ et $G$ est contenu dans l'ensemble $\Gamma_n = \left\{ e^{2i\frac{k\pi}{n}} \mid 0 \leq k \leq n-1 \right\}$ des racines $n$-èmes de l'unité qui est lui même un groupe d'ordre $n$. On a donc $G = \Gamma_n$.*

**Exercice 20.50** *Soit $G$ un groupe fini d'ordre $m$. Montrer que pour tout entier relatif $n$ premier avec $m$, l'application $g \mapsto g^n$ est une bijection de $G$ sur lui même (c'est donc une permutation de $G$).*

**Solution 20.50** *Comme $m \wedge n = 1$, le théorème de Bézout nous dit qu'il existe deux entiers relatifs $u$ et $v$ tels que $un + vm = 1$ et pour tout $g \in G$, on a $g = g^{un+vm} = (g^u)^n (g^m)^v = (g^u)^n$, ce qui signifie que l'application $g \mapsto g^n$ est surjective. Comme $G$ est fini, cette application est bijective.*

**Exercice 20.51**

1. *Soit $G$ un groupe fini dont tous les éléments sont d'ordre au plus égal à 2. Montrer que $G$ est commutatif et que son ordre est une puissance de 2.*
2. *Montrer que si $G$ est un groupe fini d'ordre $2p$ avec $p$ premier, il existe alors un élément d'ordre $p$ dans $G$.*

**Solution 20.51**

1. *Si tous les éléments de $G$ sont d'ordre au plus égal à 2, on a alors $a^2 = 1$ pour tout $a \in G$, et $G$ est commutatif (exercice 20.10).*
   *Si $G$ est réduit à $\{1\}$, on a alors $\operatorname{card}(G) = 1 = 2^0$.*
   *Si $G$ d'ordre $n \geq 2$ n'est pas réduit à $\{1\}$, il existe $a \in G \setminus \{1\}$ tel que $\langle a \rangle = \{1, a\}$ et le groupe quotient $\dfrac{G}{\langle a \rangle}$ est de cardinal strictement inférieur à $n = \operatorname{card}(G)$ avec tous ses éléments d'ordre au plus égal à 2. On conclut alors par récurrence sur l'ordre de $G$. En supposant le résultat acquis pour les groupes d'ordre strictement inférieur à $n$, on a $\operatorname{card}\left(\dfrac{G}{\langle a \rangle}\right) = 2^p$ et $\operatorname{card}(G) = 2^{p+1}$.*
   *On peut procéder de façon plus rapide (et plus astucieuse) comme suit. En notant la loi de $G$ sous forme additive, on a $2 \cdot a = 0$ pour tout $a \in G$ et on peut munir $G$ d'une structure de $\dfrac{\mathbb{Z}}{2\mathbb{Z}}$-espace vectoriel en définissant la loi externe par $\overline{0}a = 0$ et $\overline{1}a = a$ pour tout $a \in G$, la loi interne étant l'addition de $G$. Si $G$ est fini, il est nécessairement de dimension fini sur $\dfrac{\mathbb{Z}}{2\mathbb{Z}}$ et notant $p$ sa dimension, on a $\operatorname{card}(G) = \operatorname{card}\left(\left(\dfrac{\mathbb{Z}}{2\mathbb{Z}}\right)^p\right) = 2^p$.*

2. *Si $G$ est d'ordre $2p \geq 4$ avec $p$ premier, le théorème de Lagrange nous dit que les éléments de $G \setminus \{1\}$ sont d'ordre 2, $p$ ou $2p$. S'il n'y a aucun élément d'ordre $p$, il n'y en a pas d'ordre $2p$ (si $g \in G \setminus \{1\}$ est d'ordre $2p$, on a alors $g^2 \neq 1$, $g^p \neq 1$ et $(g^2)^p = g^{2p} = 1$, donc $g^2$ est d'ordre $p$), donc tous les éléments de $G \setminus \{1\}$ sont d'ordre 2 et $G$ est d'ordre $2^n = 2p$, d'où $p = 2^{n-1}$, $n = 2$ et $p = 2$ puisque $p$ est premier, soit une contradiction avec l'hypothèse qu'il n'y a pas d'élément d'ordre $p$ $(= 2)$. Il existe donc dans $G$ des éléments d'ordre $p$.*
   *Ce résultat est un cas particulier d'un théorème de Cauchy qui nous dit que si $G$ est un groupe fini de cardinal $n$, alors pour tout diviseur premier $p$ de $n$, il existe dans $G$ un élément d'ordre $p$ (théorème 20.1).*

**Exercice 20.52** *Montrer qu'un groupe $G$ est fini si et seulement si l'ensemble de ses sous-groupes est fini.*

**Solution 20.52** *Si $G$ est un groupe fini alors l'ensemble $\mathcal{P}(G)$ des parties de $G$ est fini (de cardinal $2^{\mathrm{card}(G)}$) et il en est de même de l'ensemble des sous-groupes de $G$.*
*Réciproquement soit $(G, \cdot)$ un groupe tel que l'ensemble de ses sous-groupes soit fini. On peut écrire $G = \bigcup_{g \in G} \langle g \rangle$ et cette réunion est finie, soit $G = \bigcup_{k=1}^{r} \langle g_k \rangle$. Si l'un de ces sous-groupes $\langle g_k \rangle$ est infini, alors les $\langle g_k^n \rangle$ où $n$ décrit $\mathbb{N}$ forment une famille infinie de sous-groupes de $G$ : en effet l'égalité $\langle g_k^n \rangle = \langle g_k^m \rangle$ entraîne $g_k^n = g_k^{jm}$, soit $g_k^{n-jm} = 1$ et $n - jm = 0$ ($g_k$ est d'ordre infini), c'est-à-dire que $m$ divise $n$. Comme $n$ et $m$ jouent des rôles symétriques, on a aussi $n$ qui divise $m$ et en définitive $n = m$ (on peut aussi dire que $\langle g_k \rangle$ est isomorphe à $\mathbb{Z}$ et de ce fait a une infinité de sous groupes). On a donc une contradiction si l'un des $\langle g_k \rangle$ est infini. Donc tous les $\langle g_k \rangle$ sont finis et aussi $G$.*

**Exercice 20.53** *Donner des exemples de groupes infinis dans lequel tous les éléments sont d'ordre fini.*

**Solution 20.53** *En désignant, pour tout entier $n \geq 1$, par $\Gamma_n$ le groupe des racines $n$-èmes de l'unité dans $\mathbb{C}^*$, la réunion $\Gamma = \bigcup_{n=1}^{+\infty} \Gamma_n$ est un sous-groupe de $\mathbb{C}^*$ ($1 \in \Gamma$, pour $z \in \Gamma$, il existe $n \geq 1$ tel que $z \in \Gamma_n$, donc $z^{-1} \in \Gamma_n \subset \Gamma$ et pour $z, z'$ dans $\Gamma$, il existe $n, m$ tels que $z \in \Gamma_n$ et $z' \in \Gamma_m$, donc $zz' \in \Gamma_{n \cdot m} \subset \Gamma$). Ce groupe $\Gamma$ est infini avec tous ses éléments d'ordre fini.*
*Le groupe additif $G = \dfrac{\mathbb{Z}}{p\mathbb{Z}}[X]$ avec $p$ premier est infini et tous ses éléments sont d'ordre 1 ou $p$.*
*Si on définit sur le corps $\mathbb{Q}$ des rationnels la relation d'équivalence $r \backsim s$ si et seulement si $r - s \in \mathbb{Z}$, alors le groupe quotient $\dfrac{\mathbb{Q}}{\mathbb{Z}}$ pour cette relation d'équivalence est infini et tous ses éléments sont d'ordre fini ($q\dfrac{\overline{p}}{q} = \overline{0}$).*
*Si $E$ est un ensemble infini, alors $(\mathcal{P}(E), \Delta)$ où $\Delta$ est l'opérateur de différence symétrique est infini et tous les éléments sont d'ordre 1 ou 2 puisque $A \Delta A = \emptyset$.*

**Théorème 20.23** *Soient $a, b \in G$ d'ordre fini et $k \in \mathbb{Z}^*$.*

1. *On a $\theta\left(a^k\right) = \dfrac{\theta(a)}{\theta(a) \wedge k}$ (en particulier $\theta(a^{-1}) = \theta(a)$).*
2. *Si $k$ divise $\theta(a)$, on a alors $\theta\left(a^k\right) = \dfrac{\theta(a)}{|k|}$.*

3. *Si $k$ est premier avec $\theta(a)$, on a alors $\theta\left(a^k\right) = \theta(a)$.*
4. *Si $ab = ba$, alors $ab$ est d'ordre fini divisant $\theta(a) \vee \theta(b)$.*
   *Dans le cas où $\langle a\rangle \cap \langle b\rangle = \{1\}$, on a $\theta(ab) = \theta(a) \vee \theta(b)$. Si $\theta(a)$ et $\theta(b)$ sont premiers entre eux, on a alors $\langle a\rangle \cap \langle b\rangle = \{1\}$ et $\theta(ab) = \theta(a) \vee \theta(b) = \theta(a)\theta(b)$.*

**Démonstration.**

1. Soit $\delta = \theta(a) \wedge k$ et $n', k'$ premiers entre eux tels que $\theta(a) = \delta n'$, $k = \delta k'$.
   Pour tout entier relatif $j$, on a :
   $$\begin{aligned}\left(a^k\right)^j = a^{kj} = 1 &\Leftrightarrow \exists q \in \mathbb{Z} \mid kj = q\theta(a) \Leftrightarrow \exists q \in \mathbb{Z} \mid k'j = qn' \\ &\Leftrightarrow n' \text{ divise } j \text{ (Gauss)}\end{aligned}$$
   et en conséquence $\theta\left(a^k\right) = n' = \dfrac{\theta(a)}{\theta(a) \wedge k}$.
2. Si $k$ divise $\theta(a)$, on a alors $\theta(a) \wedge k = |k|$ et $\theta\left(a^k\right) = \dfrac{\theta(a)}{|k|}$.
3. Si $k$ est premier avec $\theta(a)$, on a alors $\theta(a) \wedge k = 1$ et $\theta\left(a^k\right) = \theta(a)$.
4. Soit $\mu = \theta(a) \vee \theta(b)$. Dans le cas où $a$ et $b$ commutent, on a $(ab)^\mu = a^\mu b^\mu = 1$ avec $\mu \geq 1$ et $ab$ est d'ordre fini et cet ordre divise $\mu$. En désignant par $n = \theta(ab)$ l'ordre de $ab$, on a $a^n b^n = (ab)^n = 1$ et $a^n = b^{-n} \in \langle a\rangle \cap \langle b\rangle$.
   Si $\langle a\rangle \cap \langle b\rangle = \{1\}$, on a alors $a^n = b^n = 1$ et $n$ est multiple de $\theta(a)$ et $\theta(b)$, donc de $\theta(a) \vee \theta(b)$ et $n = \theta(a) \vee \theta(b)$.
   Si $\theta(a) \wedge \vee\theta(b) = 1$, on a alors $\theta(a) \vee \theta(b) = \theta(a)\theta(b)$. De plus avec $\langle a\rangle \cap \langle b\rangle \subset \langle a\rangle$ et $\langle a\rangle \cap \langle b\rangle \subset \langle b\rangle$, on déduit que $\operatorname{card}(\langle a\rangle \cap \langle b\rangle)$ divise $\theta(a) = \operatorname{card}(\langle a\rangle)$ et $\theta(b) = \operatorname{card}(\langle b\rangle)$, donc $\operatorname{card}(\langle a\rangle \cap \langle b\rangle) = 1$ et $\langle a\rangle \cap \langle b\rangle = \{1\}$, ce qui implique que $\theta(ab) = \theta(a) \vee \theta(b) = \theta(a)\theta(b)$.

■

**Remarque 20.10** *Si $\theta(a)$ et $\theta(b)$ ne sont pas premiers entre eux, avec $a, b$ commutant et d'ordre fini, l'ordre de $ab$ n'est pas nécessairement le* ppcm *de $\theta(a)$ et $\theta(b)$. En prenant par exemple $a$ d'ordre $n \geq 2$ dans $G$ et $b = a^{-1}$ qui est également d'ordre $n$, on $ab = ba = 1$ d'ordre $1 \neq \operatorname{ppcm}(n, n) = n$.*

**Remarque 20.11** *Pour $a$ et $b$ ne commutant pas, le produit $ab$ peut être d'ordre infini, même si $a$ et $b$ sont d'ordre fini.*

## 20.10 Sous-groupes des groupes cycliques

Pour ce paragraphe, $G = \langle a\rangle$ un groupe cyclique d'ordre $n \geq 2$.

Si $H$ est un sous-groupe de $G$, le théorème de Lagrange nous dit que l'ordre de $H$ est un diviseur de $n$. Le théorème qui suit nous dit que les sous-groupes d'un groupe cyclique sont cycliques et que pour tout diviseur $d$ de $n$, il existe un sous-groupe de $G$ d'ordre $d$. Ce résultat n'est pas vrai pour un groupe fini quelconque comme nous le verrons avec l'étude du groupe symétrique.

**Théorème 20.24** *Pour tout diviseur $d$ de $n$, il existe un unique sous groupe d'ordre $d$ du groupe cyclique $G = \langle a\rangle$, c'est le groupe cyclique $H = \left\langle a^{\frac{n}{d}}\right\rangle$.*

**Démonstration.** Pour tout diviseur $d$ de $n$, $H = \left\langle a^{\frac{n}{d}} \right\rangle$ est un sous-groupe cyclique de $G$ et le théorème 20.23 nous dit qu'il est d'ordre $\theta\left(a^{\frac{n}{d}}\right) = \dfrac{n}{n \wedge \frac{n}{d}} = d$.

Réciproquement soit $H$ un sous-groupe de $G$ d'ordre $d$, un diviseur de $n$.

Si $d = 1$, on a alors $H = \{1\} = \langle a^n \rangle$.

Si $d \geq 2$, $H$ n'est pas réduit à $\{1\}$, donc il existe un entier $k$ compris entre 1 et $n-1$ tel que $a^k \in H$ et on peut poser :

$$p = \min\left\{k \in \{1, \cdots, n-1\} \mid a^k \in H\right\}.$$

En écrivant, pour tout $h = a^k \in H$, $k = pq + r$ avec $0 \leq r \leq p-1$ (division euclidienne par $p$), on a $a^r = a^k \left(a^{pq}\right)^{-1} \in H$ et nécessairement $r = 0$. On a donc $H \subset \langle a^p \rangle \subset H$, soit $H = \langle a^p \rangle$. Avec $a^n = 1 \in H$, on déduit que $n$ est multiple de $p$ et l'ordre de $H$ est $d = \dfrac{n}{n \wedge p} = \dfrac{n}{p}$, c'est-à-dire que $H = \left\langle a^{\frac{n}{d}} \right\rangle$. Un tel sous-groupe d'ordre $d$ est donc unique. ∎

**Exemple 20.33** *Les sous groupes de* $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ *sont les* $\left\langle \dfrac{n}{d}\overline{1} \right\rangle = \left\langle \dfrac{\overline{n}}{d} \right\rangle$ *où* $d$ *est un diviseur de* $n$. *Un tel sous-groupe est isomorphe à* $\dfrac{\mathbb{Z}}{d\mathbb{Z}}$ *et il y en a autant que de diviseurs de* $n$.

**Exemple 20.34** *Les sous groupes de* $\Gamma_n = \{z \in C \mid z^n = 1\} = \left\langle e^{\frac{2i\pi}{n}} \right\rangle$ *sont les* $\left\langle \left(e^{\frac{2i\pi}{n}}\right)^{\frac{n}{d}} \right\rangle = \left\langle e^{\frac{2i\pi}{d}} \right\rangle = \Gamma_d$ *où* $d$ *est un diviseur de* $n$ *et il y en a autant que de diviseurs de* $n$.

**Lemme 20.1 (Cauchy)** *Soit* $G$ *un groupe commutatif fini d'ordre* $n \geq 2$. *Pour tout diviseur premier* $p$ *de* $n$ *il existe dans* $G$ *un élément d'ordre* $p$

**Démonstration.** On procède par récurrence sur l'ordre $n \geq 2$ de $G$.

Pour $n = 2$, le résultat est trivial ($G$ est le seul sous-groupe d'ordre 2).

Supposons le acquis pour les groupes commutatifs d'ordre $m < n$, où $n \geq 3$ et soient $G$ un groupe commutatif d'ordre $n$, $p$ un diviseur premier de $n$ et $g \in G \setminus \{1\}$.

Si $G = \langle g \rangle$, alors $G$ est cyclique et $g$ est d'ordre $n$. Pour tout diviseur premier $p$ de $n$, l'élément $h = g^{\frac{n}{p}}$ est alors d'ordre $p$ dans $G$.

Si $G \neq \langle g \rangle$ et $p$ divise $m = \operatorname{card}(\langle g \rangle) < n$, alors l'hypothèse de récurrence nous assure de l'existence d'un élément $h$ dans $\langle g \rangle$ qui est d'ordre $p$.

Supposons enfin que $G \neq \langle g \rangle$ et $p$ ne divise pas $m = \operatorname{card}(\langle g \rangle)$. Comme $p$ est premier ne divisant pas $m$, il est premier avec $m$ et le groupe quotient $\dfrac{G}{\langle g \rangle}$ est commutatif d'ordre $r = \dfrac{n}{m} < n$ divisible par $p$ ($p$ divise $n = rm$ et $p$ est premier avec $m$, le théorème de Gauss nous dit alors que $p$ divise $r$). L'hypothèse de récurrence nous assure alors de l'existence d'un élément $[h]$ d'ordre $p$ dans $\dfrac{G}{\langle g \rangle}$. Si $s$ est l'ordre de $h$ dans $G$, alors $[h]^s = [h^s] = [1]$ et $s$ est multiple de $p$. L'élément $k = h^{s/p}$ est alors d'ordre $p$ dans $G$. ∎