Groupes

Cornou Jean-Louis

22 septembre 2023

Évariste Galois (1811-1832) est à l'origine de la notion de groupe. Cette notion fondamentale irrigue toutes les mathématiques, ainsi qu'une bonne part de la physique et même de la chimie. Alexandre Grothendieck n'hésite pas à parler de l'invention du zéro et de l'idée de groupe comme des deux plus grandes innovations mathématiques de tous les temps. On retiendra surtout l'aspect structuraliste de ces notions : ce qui compte n'est pas tant les objets manipulés que les relations entre ces objets.

1 Loi de composition interne

1.1 Magmas

Définition 1 *Soit* E *un ensemble. On appelle loi de composition interne (en abrégé l.c.i) sur* E *toute application de* $\mathsf{E}\times\mathsf{E}$ *dans* E*, i.e un élément de* $\mathcal{F}(\mathsf{E}\times\mathsf{E},\mathsf{E})$*.*

Exemple 1 $f:\mathbb{R}\times\mathbb{R}\to\mathbb{R},(x,y)\mapsto x+y$ *est un loi de composition interne sur l'ensemble des réels.*

Notation
Soit $\dashv$ *une loi de composition interne sur* E*,* x,y *deux éléments de* E*. L'élément* $\dashv(x,y)$ *de* E *est plutôt noté* $x\dashv y$ *dans le cadre de l'algèbre générale. Dans le cadre d'un ensemble fini, il peut être commode de représenter la loi de composition interne sous forme d'un tableau à double entrée. Si l'ensemble* E *est constitué par exemple de trois éléments distincts* a,b,c*, on peut représenter la loi* $\dashv$ *sous la forme :*

	a	b	c
a	$a\dashv a$	$a\dashv b$	$a\dashv c$
b	$b\dashv a$	$b\dashv b$	$b\dashv c$
c	$c\dashv a$	$c\dashv b$	$c\dashv c$

Ce genre de tableau à doubles entrées s'appelle une table de Cayley.

Exemple 2 *On considère un ensemble* E *à deux éléments, notons-les* a *et* b*. On définit une loi de composition interne* $\dashv$ *sur* E *via la table de Cayley suivante :*

	a	b
a	a	b
b	b	a

Gardez cet exemple en tête pour les prochaines définitions.

Définition 2 *Soit* E *un ensemble et* $\star$ *une loi de composition interne sur* E*. Le couple* $(\mathsf{E},\star)$ *est appelé un magma.*

Dans tout la fin de cette partie, on fixe $(\mathsf{E},\star)$ un magma.

Définition 3 *On dit que la loi de composition interne* $\star$ *est* ***associative*** *lorsque*

$$\forall(x,y,z)\in\mathsf{E}^3,(x\star y)\star z=x\star(y\star z)$$

Exemple 3 *L'addition des entiers naturels* $\mathbb{N}^2\to\mathbb{N},(n,p)\mapsto n+p$ *est associative. L'opération d'exponentiation sur* $\mathbb{N}$*, i.e* $(n,p)\mapsto n^p$ *est une loi de composition interne sur* $\mathbb{N}$ *non associative. La soustraction d'entiers relatifs* $\mathbb{Z}^2\to\mathbb{Z},(n,p)\mapsto n-p$ *n'est pas associative.*

Exercice 1 *Vérifier que la loi $\dashv$ définie sur l'ensemble $E = \{a, b\}$ dans l'exemple précédent est associative.*

☞ **Remarque**
L'associativité permet de faire une suite d'opérations internes sans se soucier de l'ordre dans lequel on effectue les opérations.

Notation
Lorsqu'on dispose d'une lci associative, on peut effectuer un nombre d'opérations fini dans le sens que l'on souhaite, ce qui permet d'écrire $x \star y \star z \star t$ sans qu'il y ait d'ambiguïté. On écrit plus généralement $\bigstar_{i=1}^{n} x_i$ à la place de $x_1 \star x_2 \star \cdots \star x_n$. On note également $x^{\star n} = \underbrace{x \star x \star \cdots \star x}_{n \text{ termes}}$ pour tout n dans $\mathbb{N}^*$.

Définition 4 *Soit e un élément de E. On dit que e est un élément neutre de la lci $\star$ lorsque*

$$\forall x \in E, x \star e = e \star x = x$$

Lorsqu'une lci possède un élément neutre, on dit qu'elle est unifère.

⚠ **Attention**
Ne pas oublier de vérifier les deux égalités !

Propriété 1 *Il y a au plus un élément neutre dans $(E, \star)$.*

Démonstration. Soit e_1, e_2 deux neutres pour la lci $\star$. Alors $e_1 = e_1 \star e_2$ puisque e_2 est un neutre. D'autre part, $e_1 \star e_2 = e_2$ puisque e_1 est un neutre. Conclusion, $e_1 = e_2$.

Définition 5 *On suppose que $(E, \star)$ est unifère et on note e l'élément neutre de E. Soit $x \in E$. On dit que x est inversible (ou symétrisable) lorsque*

$$\exists y \in E, x \star y = y \star x = e$$

Dans ce cas, les éléments y de E satisfaisant $x \star y = y \star x = e$ sont appelés inverses ou symétriques de x.

Exemple 4 *Le neutre de E est inversible et e est un inverse de e.*

⚠ **Attention**
Ne pas oublier de vérifier les deux égalités !

Exemple 5 *Le magma $(\{a, b\}, \dashv)$ en exemple précédent est unifère de neutre a. Quel sont les inverses de b dans cette structure ?*

Définition 6 *Soit $(x, y) \in E^2$. On dit que x et y commutent lorsque $x \star y = y \star x$. Lorsque tous les éléments de E commutent, on dit que la lci $\star$ est commutative.*

⚠ **Attention**
Ne pas confondre associativité et commutativité ! L'associativité porte sur l'ordre des opérations, tandis que la commutativité porte sur l'ordre des éléments dans une unique opération.

Exercice 2 *Démontrer que l'exemple de structure $(\{a, b\}, \dashv)$ est commutatif.*

Définition 7 *Soit F une partie de E. On dit que F est stable par $\star$ lorsque*

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

Dans ce cas, on note $\star_F : F \times F \to F, (x, y) \mapsto x \star y$. Cette application est appelée loi induite par $\star$ sur F.

☞ **Remarque**
Dans la pratique, il est rare de différencier les notations de la lci $\star$ sur E et la loi induite sur une partie stable.

Exemple 6 *Si $(E, \star)$ est unifère de neutre e, la partie $F = \{e\}$ est stable par $\star$. Dans $(\mathbb{Z}, +)$, la partie $\mathbb{N}$ est stable par $+$ ou plus généralement, tout intervalle d'entiers de la forme $[\![a, +\infty[\![$ avec $a \in \mathbb{N}$ est stable par $+$. La partie $[\![-1, +\infty[\![$ ne l'est pas.*

1.2 Monoïdes

Dans cette partie, on fixe $(E,\star)$ un **magma associatif unifère**. Ces structures sont également appelées monoïdes.

Propriété 2 *Soit $x \in E$. On suppose que x est inversible, alors x possède un unique inverse. On le note classiquement $x^{\star(-1)}$ ou x^{-1}.*

Démonstration. Notons e l'élément neutre de E (on sait qu'il existe puisque E est supposé unifère, et qu'il est unique d'après ce qui précède). Soit y_1, y_2 deux inverses de x. Alors

$$\begin{aligned} y_1 &= y_1 \star e && \text{car } e \text{ est le neutre de E} \\ &= y_1 \star (x \star y_2) && \text{car } y_2 \text{ est un inverse de } x \\ &= (y_1 \star x) \star y_2 && \text{associativité de } \star \\ &= e \star y_2 && \text{car } y_1 \text{ est un inverse de } x \\ &= y_2 && \text{car } e \text{ est le neutre de E} \end{aligned}$$

Propriété 3 *Soit $(x,y) \in E^2$. On suppose que x et y sont tous deux inversibles. Alors $x \star y$ est également inversible. De plus,*

$$(x \star y)^{-1} = y^{-1} \star x^{-1}$$

Démonstration. Notez bien la structure de la preuve ici.

$$(x \star y) \star (y^{-1} \star x^{-1}) = x \star (y \star y^{-1}) \star x^{-1} = x \star e \star x^{-1} = x \star x^{-1} = e$$

$$(y^{-1} \star x^{-1}) \star (x \star y) = y^{-1} \star (x^{-1} \star x) \star y = y^{-1} \star e \star y = y^{-1} \star y = e$$

Cela démontre que $x \star y$ est inversible et que $y^{-1} \star x^{-1}$ est un inverse de $x \star y$. D'après ce qui précède, c'est l'inverse de $x \star y$.

Propriété 4 *Soit $x \in E$. On suppose que x est inversible. Alors x^{-1} est inversible d'inverse x, ce qui s'écrit encore $\left(x^{-1}\right)^{-1} = x$.*

Démonstration. Notons e le neutre de $(E,\star)$. L'inverse x^{-1} est bien défini de manière unique, puisque x est supposé inversible et l'inverse est unique puisqu'on travaille dans un monoïde. Ces éléments de E vérifient

$$x^{-1} \star x = x \star x^{-1} = e$$

L'élément x satisfait alors les critères pour que x^{-1} soit inversible. C'est un inverse de x^{-1}. Comme $(E,\star)$ est un monoïde, c'est l'inverse de x, ce que l'on écrit $\left(x^{-1}\right)^{-1} = x$.

2 Structure de groupe

2.1 Notion de groupe

Définition 8 *Soit $(G,\star)$ un magma. On dit que $(G,\star)$ (ou G en abrégé) est un groupe lorsque*

- *La loi $\star$ est associative.*
- *La loi $\star$ est unifère.*
- *Tout élément de G est inversible.*

En abrégé, un groupe est un magma associatif unifère dont tous les éléments sont inversibles, ou encore un monoïde dont tous les éléments sont inversibles.

Exemple 7 *$(\mathbb{N},+)$ est un monoïde, mais n'est pas un groupe. L'élément 1 ne possède pas d'inverse pour la loi $+$. $(\mathbb{Z},+)$ est un groupe.*

⚠ **Attention**
Parfois, un énoncé donne une structure $(G,\star)$, mais l'application $\star : G \times G \to X$ n'est pas strictement une loi de composition interne, il faut alors vérifier que $\forall (g,h) \in G^2, g \star h \in G$.

Définition 9 *Un groupe $(G,\star)$ dont la loi est commutative est appelé groupe commutatif ou encore groupe abélien.*

Exercice 3 *Montrer que l'exemple de structure $(\{a,b\},\dashv)$ est un groupe commutatif.*

Roger Godement : *Le débutant aura soin de* ne pas *dire qu'un groupe « est un ensemble* G *sur lequel* il existe *une loi de composition vérifiant les conditions a), b), c) ci-dessus », car on peut facilement démontrer que, sur tout ensemble, il existe une telle loi de composition, et même qu'on peut en construire une infinité pour peu que l'ensemble donné soit lui-même infini : en disant qu'un groupe est « un ensemble sur lequel il existe » une loi de composition, on ne dit donc rien d'autre que ceci : « un groupe est un ensemble » – définition dont la stupidité est particulièrement claire ...*

☞ **Remarque**
Toutes les propriétés précédentes sur les monoïdes et les magmas sont encore valides pour les groupes : unicité du neutre, unicité des inverses, $(x\star y)^{-1}=y^{-1}\star x^{-1}$, $(x^{-1})^{-1}=x$.

Notation
Il est fréquent d'utiliser des notations « additives » pour les groupes abéliens, c'est-à-dire de noter la lci $+$. Dans ce cadre, on note plutôt $-x$ le symétrique de x pour la lci $+$, le neutre est souvent noté 0_G ou 0. On note également $nx=\underbrace{x+x+\cdots+x}_{n\text{ termes}}$ pour $n\in\mathbb{N}^*$, $0x=0$, puis $nx=\underbrace{(-x)+(-x)+\cdots+(-x)}_{-n\text{ termes}}$ pour $n\in\mathbb{Z}\backslash\mathbb{N}$.
Lorsque le groupe n'est pas abélien, on utilise souvent des notations « multiplicatives », en notant la lci $\times$. Le neutre alors souvent noté 1_G ou 1, et les puissances $x^n=\underbrace{x\times x\times\cdots\times x}_{n\text{ termes}}$ pour $n\in\mathbb{N}^*$, $x^0=1$, puis $x^n=\underbrace{x^{-1}\times x^{-1}\times\cdots\times x^{-1}}_{-n\text{ termes}}$ pour $n\in\mathbb{Z}\backslash\mathbb{N}$.

2.2 Exemples de groupes

Exemple 8 *$(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ sont des groupes commutatifs. $(\mathbb{Q}^*,\times)$, $(\mathbb{Q}_+^*,\times)$, $(\mathbb{R}^*,\times)$, $(\mathbb{R}_+^*,\times)$, $(\mathbb{U},\times)$, $(\mathbb{C}^*,\times)$ sont des groupes commutatifs. $(\mathbb{Q},\times)$, $(\mathbb{Q}_+,\times)$, $(\mathbb{R},\times)$, $(\mathbb{R}_+,\times)$, $(\mathbb{C},\times)$ ne sont pas des groupes commutatifs car 0 n'admet pas d'inverse multiplicatif. $(\mathbb{N}^*,\times)$ et $(\mathbb{Z}^*,\times)$ ne sont pas des groupes car 2 n'admet pas d'inverse.*

Exercice 4 *On considère un ensemble E, puis l'ensemble de ses parties $\mathcal{P}(E)$. On munit cet ensemble de la loi de composition interne découlant de la différence symétrique. Montrer que $(\mathcal{P}(E),\Delta)$ est un groupe.*

Propriété 5 *Soit $n\in\mathbb{N}^*$. L'ensemble des racines n-ièmes de l'unité $\mathbb{U}_n$, muni de la multiplication est un groupe.*

Démonstration. — La multiplication est a priori une loi de composition interne de $\mathbb{C}$ dans $\mathbb{C}$. Il faut vérifier qu'elle stabilise $\mathbb{U}_n$. Soit donc z,z' deux racines n-ièmes de l'unité. Alors la commutativité de la multiplication complexe entraîne $(zz')^n=z^nz'^n=1\times1=1$. Ainsi, $zz'\in\mathbb{U}_n$, on peut donc bien parler de structure $(\mathbb{U}_n,\times)$.

— La multiplication complexe est associative, elle l'est donc sur $\mathbb{U}_n$.

— On propose 1 comme neutre. En effet, $1^n=1$, et $\forall z\in\mathbb{U}_n, z\times1=1\times z=z$.

— Soit $z\in\mathbb{U}_n$. Alors $|z|=1$, donc $z\neq0$. On sait alors qu'on peut manipuler le complexe $1/z$ qui vérifie $z\times\frac{1}{z}=\frac{1}{z}\times z=1$. Il faut toutefois vérifier que $1/z\in\mathbb{U}_n$. On remarque alors $\left(\frac{1}{z}\right)^n=1=\frac{1^n}{z^n}=\frac{1}{1}=1$, i.e $1/z\in\mathbb{U}_n$.

Définition 10 *Soit X un ensemble. L'ensemble des applications bijectives de X dans X est appelé ensemble des permutations de X, noté S_X ou $\mathfrak{S}(X)$. Il est muni de la loi de composition interne de composition des applications, i.e*

$$\forall(f,g)\in(\mathfrak{S}(X))^2,\forall x\in X,(f\circ g)(x)=f(g(x))$$

Le fait que $f\circ g$ est encore bijective de X dans X a été prouvé au chapitre trois, c'est donc bien une loi de composition interne.

Propriété 6 *Pour tout ensemble* X*, la structure* $(\mathfrak{S}(X), \circ)$ *est un groupe.*

Démonstration. — Montrons l'associativité, soit f, g, h trois applications bijectives de X dans X et montrons que $(f \circ g) \circ h = f \circ (g \circ h)$. Soit donc $x \in X$.

$$\begin{aligned}((f \circ g) \circ h)(x) &= (f \circ g)(h(x)) \\ &= f(g(h(x)) \\ &= f((g \circ h)(x)) \\ &= (f \circ (g \circ h))(x)\end{aligned}$$

— On note $e = \mathrm{Id}_X$ l'application identité de X dans X. On sait qu'elle vérifie

$$\forall f \in \mathfrak{S}(X), f \circ e = e \circ f = f$$

Par conséquent, e est bien un neutre pour la loi $\circ$.

— Soit $f \in \mathfrak{S}(X)$. On note alors g l'application réciproque de f, définition légitime puisque f est bijective. On sait que g vérifie $g \circ f = f \circ g = \mathrm{Id}_X = e$. Ainsi, tout élément f de $\mathfrak{S}(X)$ possède un inverse pour la loi $\circ$, à savoir sa réciproque.

Exercice 5 *On note* $X = \{1, 2, 3\}$*. Montrer que le groupe* $(\mathfrak{S}(X), \circ)$ *n'est pas commutatif. Que vaut son cardinal ?*

2.3 Construction de groupes

Comme souvent, on doit commencer par construire des groupes « par l'extérieur », ce qui peut être fastidieux, notamment l'étape d'associativité.

Définition 11 *Soit* X *un ensemble et* $(G, \star)$ *un groupe. Pour toutes applications* f, g *de* X *dans* G*, on définit l'application* $f \star g$ *de* X *dans* G *via*

$$f \star g : X \to G, x \mapsto f(x) \star g(x)$$

☞ **Remarque**
Il est incorrect en toute rigueur de noter avec le même symbole la lci $\star$ *du groupe* G *et la lci* $\star$ *de l'ensemble* $\mathcal{F}(X, G)$*.*

Propriété 7 *Avec les notations précédentes, la structure* $(\mathcal{F}(X, G), \star)$ *est un groupe.*

Démonstration. L'application $\star$ est bien une loi de composition interne.

— Associativité : soit $(f, g, h) \in \mathcal{F}(X, G)^3$ Montrons que $(f \star g) \star h = f \star (g \star h)$. Soit $x \in X$. Alors

$$\begin{aligned}[(f \star g) \star h](x) &= (f \star g)(x) \star h(x) && \text{définition de la loi } \star \text{ sur } \mathcal{F}(X, G) \\ &= (f(x) \star g(x)) \star h(x) && \text{définition de la loi } \star \text{ sur } \mathcal{F}(X, G) \\ &= f(x) \star (g(x) \star h(x)) && \text{associativité de la loi } \star \text{ sur G} \\ &= f(x) \star (g \star h)(x) && \text{définition de la loi } \star \text{ sur } \mathcal{F}(X, G) \\ &= [f \star (g \star h)](x) && \text{définition de la loi } \star \text{ sur } \mathcal{F}(X, G)\end{aligned}$$

— Notons e le neutre de $(G, \star)$. On propose alors $E : X \to G, x \mapsto e$ l'application constante égale à e comme neutre de la loi $\star$ sur $\mathcal{F}(X, G)$. Montrons que cela est bien le cas. Soit $f \in \mathcal{F}(X, G)$ et $x \in X$.

$$\begin{aligned}(f \star E)(x) &= f(x) \star E(x) && \text{définition de la loi } \star \text{ sur } \mathcal{F}(X, G) \\ &= f(x) \star e && \text{définition de l'application E} \\ &= f(x) && e \text{ est le neutre de } (G, \star)\end{aligned}$$

Comme cela est vrai pour tout x dans X, on a bien l'égalité d'applications $f \star E = f$. De plus,

$$\begin{aligned}(E \star f)(x) &= E(x) \star f(x) && \text{définition de la loi } \star \text{ sur } \mathcal{F}(X, G) \\ &= e \star f(x) && \text{définition de l'application E} \\ &= f(x) && e \text{ est le neutre de } (G, \star)\end{aligned}$$

D'où l'égalité $E \star f = f$. Conclusion, E est bien le neutre de $(\mathcal{F}(X, G), \star)$.

— Soit $f \in \mathcal{F}(X,G)$. Construisons un inverse de f dans $\mathcal{F}(X,G)$ pour la loi $\star$. On propose l'application $g : X \to G, x \mapsto f(x)^{-1}$, bien définie puisque G est un groupe, et pour tout x dans X, $f(x) \in G$ possède un inverse, noté $f(x)^{-1}$. Montrons que cette application est bien un inverse de f dans $\mathcal{F}(X,G)$ pour la loi $\star$. Soit $x \in X$.

$$\begin{aligned}(f \star g)(x) &= f(x) \star g(x) && \text{définition de la loi } \star \text{ sur } \mathcal{F}(X,G)\\ &= f(x) \star f(x)^{-1} && \text{définition de } g \text{ proposée}\\ &= e && e \text{ est le neutre de G}\end{aligned}$$

Comme cela est vrai pour tout x dans X, on a l'égalité d'applications $f \star g = E$. De plus

$$\begin{aligned}(g \star f)(x) &= g(x) \star f(x) && \text{définition de la loi } \star \text{ sur } \mathcal{F}(X,G)\\ &= f(x)^{-1} \star f(x) && \text{définition de } g \text{ proposée}\\ &= e && e \text{ est le neutre de G}\end{aligned}$$

ce qui prouve $g \star f = E$. Conclusion, g est bien l'inverse de f dans $\mathcal{F}(X,G)$ pour la loi $\star$.

Définition 12 *Soit* $(G,\star)$ *et* $(H,\sharp)$ *deux groupes. On définit l'application* $\flat : G \times H \to G \times H$ *via*

$$\forall (x_1,y_1,x_2,y_2) \in G^2 \times H^2, (x_1,x_2)\flat(y_1,y_2) = (x_1 \star y_1, x_2 \sharp y_2)$$

Propriété 8 *Avec les notations précédentes, la structure* $(G \times H, \flat)$ *est un groupe. Il est appelé groupe produit de* $(G,\star)$ *et* $(H,\sharp)$.

Démonstration. Notons tout d'abord que l'application $\flat$ est bien une lci sur l'ensemble $G \times H$.

— Montrons l'associativité : soit $(x_1,x_2,x_3) \in G^3, (y_1,y_2,y_3) \in H^3$. Alors

$$\begin{aligned}((x_1,y_1)\flat(x_2,y_2))\flat(x_3,y_3) &= (x_1 \star x_2, y_1 \sharp y_2)\flat(x_3,y_3) && \text{définition de la loi } \flat\\ &= ((x_1 \star x_2) \star x_3, (y_1 \sharp y_2)\sharp y_3) && \text{définition de la loi } \flat\\ &= (x_1 \star (x_2 \star x_3), (y_1 \sharp y_2)\sharp y_3) && \text{associativité de la loi } \star\\ &= (x_1 \star (x_2 \star x_3), y_1 \sharp (y_2 \sharp y_3)) && \text{associativité de la loi } \sharp\\ &= (x_1,y_1)\flat(x_2 \star x_3, y_2 \sharp y_3) && \text{définition de la loi } \flat\\ &= (x_1,y_1)\flat((x_2,y_2)\flat(x_3,y_3)) && \text{définition de la loi } \flat\end{aligned}$$

— Notons e_G et e_H les neutres respectifs de $(G,\star)$ et $(H,\sharp)$. On propose comme neutre pour $(G \times H, \flat)$ l'élément (e_G, e_H). Vérifions que c'est bien le cas. Soit $(x,y) \in G \times H$.

$$(x,y)\flat(e_G,e_H) = (x \star e_G, y \sharp e_H) = (x,y)$$

D'autre part,

$$(e_G,e_H)\flat(x,y) = (e_G \star x, e_H \sharp y) = (x,y)$$

— Soit $(x,y) \in G \times H$. Comme G et H sont des groupes, on dispose de x^{-1} l'inverse de x pour la loi $\star$ et de y^{-1} l'inverse de y pour la loi $\sharp$. On pense alors à l'élément (x^{-1},y^{-1}). Celui-ci vérifie

$$(x^{-1},y^{-1})\flat(x,y) = (x^{-1} \star x, y^{-1} \sharp y) = (e_G,e_H)$$

et

$$(x,y)\flat(x^{-1},y^{-1}) = (x \star x^{-1}, y \sharp y^{-1}) = (e_G,e_H)$$

Ainsi, (x,y) est bien inversible pour la loi $\flat$ d'inverse (x^{-1},y^{-1}).

On généralise ces constructions à des nombres finis de groupes $(G_1 \star_1),\dots(G_n,\star_n)$.

Exercice 6 *Soit* $(G,\star)$ *et* $(H,\sharp)$ *deux groupes commutatifs. Montrer que le groupe produit* $G \times H$ *est commutatif.*

☞ **Remarque**

L'un des grands enjeux de la classification des groupes est le « dévissage » des groupes. Soit G *un groupe, on se pose souvent la question de savoir si on peut voir* G *comme un groupe produit* $H \times K$ *avec* H *et* K *plus petits. L'étude de la structure de* G *se ramènerait alors à celles de* H *et* K. *C'est ce genre d'idées, qui a amené Galois à démontrer que les équations polynomiales d'ordre 5 ne sont pas résolubles par radicaux.*

2.4 Petits groupes

Etudions les groupes finis de cardinal 2 et 3, via des tables de Cayley.

Exemple 9 *Soit* $(G,\star)$ *un groupe de cardinal 2. On note e son neutre, puis a l'autre élément de* G. *On souhaite établir la table de Cayley de ce groupe. Comme e est le neutre, on a déjà le tableau partiel :*

	e	a
e	e	a
a	a	?

Il reste à déterminer $a\star a$. *Comme* $\star$ *est un loi de composition interne, il n'y a que deux possibilités :* $a\star a=e$ *ou* $a\star a=a$. *Supposons par l'absurde que* $a\star a=a$. *Alors on peut multiplier à droite par l'inverse de a (puisque* $(G,\star)$ *est un groupe). Cela donne* $a\star a\star a^{-1}=a\star a^{-1}$, *soit encore* $a\star e=e$, *donc* $a=e$. *Or a est l'unique élément de* G *distinct de e, donc* $a\neq e$. *Cette absurdité entraîne que* $a\star a=e$. *En conclusion, la table de Cayley est nécessairement la suivante :*

	e	a
e	e	a
a	a	e

On constate que dans ce groupe tout élément est son propre inverse et que ce groupe est commutatif.

Etablissons une propriété simple avant d'aborder les groupes de cardinal 3.

Propriété 9 *Soit* $(G,\star)$ *un groupe et* $g\in G$. *Alors les applications* $L_g : G\to G, x\mapsto g\star x$ *(la multiplication à gauche par g) et* $R_g : G\to G, x\mapsto x\star g$ *(la multiplication à droite par g) sont des bijections de réciproques respectives* $L_{g^{-1}}$ *et* $R_{g^{-1}}$.

Démonstration. Notons e le neutre de $(G,\star)$ et vérifions directement $L_g\circ L_{g^{-1}}=L_{g^{-1}}\circ L_g=\mathrm{Id}_G$, puis $R_g\circ R_{g^{-1}}=R_{g^{-1}}\circ R_g=\mathrm{Id}_G$. Soit $h\in G$, alors $(L_g\circ L_{g^{-1}})(h)=g\star(g^{-1}\star h)=(g\star g^{-1})\star h=e\star h=h$. De même, $(L_{g^{-1}}\circ L_g)(h)=g^{-1}\star(g\star h)=(g^{-1}\star g)\star h=e\star h=h$. Ainsi, L_g est bijective de réciproque $L_{g^{-1}}$.
De même, $(R_g\star R_{g^{-1}})(h)=(h\star g^{-1})\star g=h\star(g^{-1}\star g)=h\star e=h$ et $(R_{g^{-1}}\star R_g)(h)=(h\star g)\star g^{-1}=h\star(g\star g^{-1})=h\star e=h$, ce qui démontre le second point.

Exemple 10 *Soit* $(G,\star)$ *un groupe de cardinal 3. On note e son neutre, puis a et b ses deux autres éléments. Comme précédemment, on a une table de Cayley incomplète*

	e	a	b
e	e	a	b
a	a	?	?
b	b	?	?

On doit alors déterminer $a\star a, a\star b, b\star a$ *et* $b\star b$. *Notons que la deuxième ligne donne l'image de l'application* L_a, *donc que tous ses éléments doivent être distincts. Par conséquent,* $\{a\star a, a\star b\}=\{e,b\}$. *On continue à la manière d'un sudoku. Or, si* $a\star b=b$, *alors la troisième colonne contient deux fois l'élément b, ce qui contredit l'injectivité de* R_b. *Une autre façon de le démontrer est la suivante : si* $a\star b=b$, *alors en multipliant à droite par l'inverse de b, on obtient* $a=e$, *ce qui contredit la définition de a. Par conséquent,* $a\star b=e$, *puis* $a\star a=b$. *On complète alors les deuxième et troisième colonne par les seules possibilités restantes, et on obtient la table :*

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Dans cette structure, on constate que $a^{-1}=b$, *que* $b^{-1}=a$, *et que* $(G,\star)$ *est commutatif.*

Exercice 7 *L'ensemble* $\{L_g | g\in G\}$ *est-il un groupe ? Pour quelle loi ?*

3 Sous-groupes

On va exploiter une notion un peu plus maniable que les groupes : les sous-groupes. En contrepartie, il faut disposer d'un groupe « cadre » dans lequel travailler.

3.1 Notion de sous-groupe

Définition 13 *Soit* $(G,\star)$ *un groupe et* H *une partie de* G*. On dit que* H *est un sous-groupe de* G *lorsque*

- H *est stable par* $\star$*.*
- $(H,\star_H)$ *est un groupe.*

Afin d'alléger la démonstration du prochain théorème, on énonce et démontre un petit lemme qui permet de vérifier votre maîtrise du calcul dans les groupes.

Lemme 1 *Soit* $(G,\star)$ *un groupe et* H *un sous-groupe de* G*. Alors le neutre de* $(G,\star)$ *et le neutre de* $(H,\star_H)$ *sont égaux.*

Démonstration. On les note respectivement e_G et e_H. Comme e_H est le neutre de $\star_H$, on a $e_H \star_H e_H = e_H$. D'après la définition de $\star_H$, cela signifie $e_H \star e_H = e_H$. On multiplie à droite par e_H^{-1} l'inverse de e_H pour la loi $\star$ de G, ce qui entraîne $e_H \star e_G = e_G$. Comme e_G est le neutre de $\star$, on obtient $e_H = e_G$.

Théorème 1 (Première caractérisation des sous-groupes) *Soit* $(G,\star)$ *un groupe et* H *une partie de* G*. On a la caractérisation suivante :* H *est un sous-groupe de* G *si et seulement si*

- H *est non vide,*
- $\forall (x,y) \in H^2, x \star y \in H$*, (stabilité par* $\star$*)*
- $\forall x \in H, x^{-1} \in H$*. (stabilité par inverse)*

☞ **Remarque**
Pour certains auteurs, cette première caractérisation des sous-groupes est leur définition. La démarche proposée dans ce cours a l'avantage de se généraliser à d'autres structures que les groupes.

Démonstration. Supposons que H est un sous-groupe de G. Montrons qu'il vérifie les trois critères ci-dessus :

- $(H,\star_H)$ est un groupe, donc possède un neutre. Par conséquent, H est non vide.
- H est stable par $\star$, donc $\forall (x,y) \in H^2, x \star y \in H$.
- Soit $x \in H$, L'inverse x^{-1} est bien défini puisque $x \in G$ et $(G,\star)$ est un groupe. Tout l'enjeu est de montrer que x^{-1} l'inverse pour la loi $\star$ de G appartient à H. Comme $(H,\star_H)$ est un groupe, on dispose d'un élément z de H tel que z soit l'inverse de x pour la loi $\star_H$. On a alors les égalités

$$x \star z = x \star_H z = e_H = e_G$$

  En multipliant à gauche par x^{-1}, on obtient $e_G \star z = x^{-1} \star e_G$, i.e $z = x^{-1}$. Comme $z \in H$, cela prouve que x^{-1} appartient à H.

Réciproquement, supposons que H vérifie les trois critères ci-dessous, et montrons qu'il s'agit d'un sous-groupe de G. Le deuxième critère donne la stabilité, il reste à montrer que $(H,\star_H)$ est un groupe.

- Soit $(h_1,h_2,h_3) \in H^3$. Alors

$$\begin{aligned}
(h_1 \star_H h_2) \star_H h_3 &= (h_1 \star h_2) \star h_3 && \text{définition de } \star_H \\
&= h_1 \star (h_2 \star h_3) && \text{associativité de } \star \text{ dans G} \\
&= h_1 \star_H (h_2 \star_H h_3) && \text{définition de } \star_H
\end{aligned}$$

  Ceci démontre l'associativité de $\star_H$.

- Démontrons que le neutre de G appartient à H. H est non vide, notons h un élément de H. Comme h est stable par passage à l'inverse et stable par la loi $\star$, $h \star h^{-1} \in H$, i.e $e_G \in H$. On propose alors e_G comme neutre de $(H,\star_H)$. Vérifions que c'est bien le cas : soit $h' \in H$.

$$h \star_H e_G = h \star e_G = h \quad \text{et} \quad e_G \star_H h = e_G \star h = h$$

  Ainsi, $(H,\star_H)$ est unifère de neutre e_G.

— Soit $x \in H$. On propose x^{-1} l'inverse de x dans $(G,\star)$ comme inverse de x dans $(H,\star_H)$. Notons que x^{-1} appartient bien à H d'après la stabilité de H par passage à l'inverse. D'autre part,

$$x^{-1} \star_H x = x^{-1} \star x = e_G \quad \text{et} \quad x \star_H x^{-1} = x \star x^{-1} = e_G$$

Ainsi, $(H,\star_H)$ est bien un groupe, ce qui conclut la démonstration du théorème.

✎ **Méthode**
Pour démontrer qu'une partie H *de* $(G,\star)$ *en est un sous-groupe. On démontre les trois points précédents. Pour le premier point, il est fréquent de démontrer que* H *contient le neutre de* G.

Exemple 11 *L'ensemble* $2\mathbb{Z}$ *est un sous-groupe de* $(\mathbb{Z},+)$, $\mathbb{U}_3$ *est un sous-groupe de* $(\mathbb{U}_{27},\times)$. $\mathbb{U}$ *est un sous-groupe de* $(\mathbb{C}^*,\times)$. $\mathbb{N}$ *contient* 0 *et est stable par* $+$*, mais n'est pas un sous-groupe de* $(\mathbb{Z},+)$ *car non stable par inverse. L'ensemble* $\{z \in \mathbb{C}, \Re\mathfrak{e}(z) > 0\}$ *contient* 1*, est stable par inverse, mais n'est pas stable par multiplication, donc n'est pas un sous-groupe de* $(\mathbb{C}^*,\times)$.

Théorème 2 (Deuxième caractérisation des sous-groupes) *Soit* $(G,\star)$ *un groupe et* H *une partie de* G. *On a la caractérisation suivante :* H *est un sous-groupe de* G *si et seulement si*

— H *est non vide*
— $\forall (x,y) \in H^2, x \star y^{-1} \in H$

☞ **Remarque**
Bien que plus synthétique que la première caractérisation, cette seconde caractérisation n'apporte pas d'avantages dans la pratique, à moins que la définition de la partie à étudier utilise spécifiquement des expressions $x \star y^{-1}$.

Démonstration. Supposons que H est un sous-groupe et démontrons qu'il vérifie ces deux critères. D'après la première caractérisation, H est non vide. Soit $(x,y) \in H^2$, alors d'après le troisième critère de la première caractérisation, $y^{-1} \in H$, puis en utilisant la stabilité, $x \star y^{-1} \in H$.
Réciproquement, supposons que H est non vide et $\forall (x,y) \in H^2, x \star y^{-1} \in H$. Démontrons que H vérifie la première caractérisation des sous-groupes. La non-vacuité est acquise. Considérons donc un élément h de H. D'après le second point, $e_G = h \star h^{-1} \in H$, donc H contient le neutre de $\star$. On en déduit que $h^{-1} = e_G \star h^{-1} \in H$, ce qui prouve la troisième point. Soit $(h_1,h_2) \in H^2$. Alors $h_2^{-1} \in H$, puis $h_1 \star h_2 = h_1 \star \left(h_2^{-1}\right)^{-1} \in H$, ce qui prouve la stabilité par la loi $\star$.

3.2 Sous-groupes engendrés par un élément

On fixe $(G,\star)$ un groupe de neutre e dans cette partie. On note la loi de composition interne multiplicativement pour alléger les notations

Propriété 10 *Soit* g *un élément de* G. *Alors la partie* $\{g^n | n \in \mathbb{Z}\}$ *est un sous-groupe de* G. *On l'appelle sous-groupe de* G *engendré par l'élément* g.

Démonstration. Notons $H = \{g^n | n \in \mathbb{Z}\}$ et démontrons qu'il vérifie la première caractérisation des sous-groupes.

— $\mathbb{Z}$ contient 0, donc $g^0 = e \in H$.
— Soit $(h_1,h_2) \in H^2$. On dispose d'entiers relatifs n_1 et n_2 tels que $h_1 = g^{n_1}$ et $h_2 = g^{n_2}$. Mais alors $h_1 \star h_2 = g^{n_1} \star g^{n_2} = g^{n_1+n_2}$. Comme $n_1 + n_2 \in \mathbb{Z}$, on en déduit que $h_1 \star h_2$ appartient à H.
— Soit $h \in H$. On dispose d'un entier relatif n tel que $h = g^n$. Mais alors $h^{-1} = g^{-n}$, puisque $g^{-n} \star g^n = g^n \star g^{-n} = g^{n-n} = g^0 = e$. Comme $-n \in \mathbb{Z}$, on a $h^{-1} \in H$.

Notation
Ce sous-groupe est souvent noté $\langle g \rangle$.

Exercice 8 *Démontrer qu'un tel sous-groupe est nécessairement commutatif (même si* G *ne l'est pas).*

Propriété 11 *Soit* g *un élément de* G. *Alors* $\langle g \rangle$ *est le plus petit sous-groupe de* G *(au sens de l'inclusion) contenant* g.

Démonstration. Soit H un sous-groupe de G contenant g. Alors H est stable par $\star$, on en déduit par récurrence que $\forall n \in \mathbb{N}^*, g^n \in H$. On a vu que H contient le neutre de G, i.e g^0. Enfin, H est stable par inverse, donc $\forall n \in Z\backslash\mathbb{N}, g^n \in H$. Ainsi, $\langle g \rangle \subset H$.
Réciproquement, $\langle g \rangle$ est un sous-groupe de G et il contient g.

Définition 14 *Soit $g \in G$. On dit que g engendre G ou est un générateur de G, lorsque $\langle g \rangle = G$. Il revient au même de dire que $\forall h \in G, \exists n \in \mathbb{Z}, h = g^n$. Lorsqu'un tel élément existe, on dit que G est monogène.*

Exemple 12 *Le groupe $(\mathbb{Z}, +)$ est engendré par 1. Le groupe $(\mathbb{U}_n, \times)$ est engendré par le complexe $\exp(2i\pi/n)$. Le groupe produit $(\mathbb{U}_2 \times \mathbb{U}_2, \times)$ est n'est pas monogène. Tout sous-groupe engendré par un élément dans ce groupe est strictement inclus dans $\mathbb{U}_2 \times \mathbb{U}_2$.*

4 Morphismes de groupes

La notion de morphisme traverse toutes les études de structures. Il s'agit d'applications qui « respectent » les lois des ensembles étudiés, ou sont « compatibles » avec ces lois.

4.1 Morphisme

Définition 15 *Soit $(G, \star)$ et $(H, \sharp)$ deux groupes, puis $f : G \to H$ une application de G vers H. On dit que f est un morphisme de groupes (ou homomorphisme de groupes) lorsque*

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

Exemple 13 *Soit $(G, \star)$ un groupe noté multiplicativement et $g \in G$. L'application $(\mathbb{Z}, +) \to (G, \star), n \to g^n$ est un morphisme de groupes. L'exponentielle est un morphisme de groupe de $(\mathbb{C}, +)$ dans $(\mathbb{C}^*, \times)$. Les homotéthies de rapport $a \in \mathbb{R}$, $h_a : \mathbb{R} \to \mathbb{R}, x \mapsto ax$ sont des morphismes de groupes de $(\mathbb{R}, +)$ dans $(\mathbb{R}, +)$.*

Propriété 12 *Soit $f : G \to H$ un morphisme de groupes. Alors en notant, e_G le neutre de G et e_H le neutre de H, on a $f(e_G) = e_H$. De plus,*

$$\forall x \in G, f(x^{-1}) = f(x)^{-1}$$

où l'on a noté de la même manière l'inverse dans G et l'inverse dans H.

Démonstration. On remarque que $f(e_G) \sharp f(e_G) = f(e_G \star e_G)$ puisque f est un morphisme. Comme e_G est le neutre de G, on en déduit $f(e_G) \sharp f(e_G) = f(e_G)$. En multipliant à droite par l'inverse de $f(e_G)$ dans H, on obtient alors $f(e_G) \sharp f(e_G) \sharp (f(e_G))^{-1} = f(e_G) \sharp f(e_G)^{-1}$, soit encore $f(e_G) \sharp e_H = e_H$. Comme e_H est le neutre de H, on a finalement, $f(e_G) = e_H$.
Soit $x \in G$. Comme f est un morphisme de groupes et d'après l'égalité précédente, on a

$$f(x^{-1}) \sharp f(x) = f(x^{-1} \star x) = f(e_G) = e_H$$

$$f(x) \sharp f(x^{-1}) = f(x \star x^{-1}) = f(e_G) = e_H$$

On a ainsi démontré que $f(x^{-1})$ est l'inverse de $f(x)$ dans H, i.e $f(x^{-1}) = f(x)^{-1}$).

⚠ **Attention**
L'égalité $f(e_G) = e_H$ découle de la notion de morphisme de groupes. Il n'est pas nécessaire de la démontrer lorsqu'on vous demande de vérifier qu'une application est un morphisme de groupes.

Propriété 13 *Soit $(G, \star)$, $(H, \sharp)$, $(K, \flat)$ trois groupes. Soit $f : G \to H$ un morphisme de groupes, puis $g : H \to K$ un morphisme de groupes. Alors $g \circ f : G \to K$ est un morphisme de groupes.*

Démonstration. Soit $(x_1, x_2) \in G^2$.

$$\begin{aligned}
(g \circ f)(x_1 \star x_2) &= g(f(x_1 \star x_2)) && \text{définition de la composée d'applications} \\
&= g(f(x_1) \sharp f(x_2)) && \text{car } f \text{ est un morphisme de groupes} \\
&= g(f(x_1)) \flat g(f(x_2)) && \text{car } g \text{ est un morphisme de groupes} \\
&= (g \circ f)(x_1) \flat (g \circ f)(x_2) && \text{définition de la composée d'applications}
\end{aligned}$$

Définition 16 *On appelle isomorphisme de groupes entre G et H tout morphisme de groupes bijectif. Si une telle application existe, on dit que G et H sont isomorphes. Tout isomorphisme de groupes de G dans G est appelé automorphisme de groupes.*

Exemple 14 *Le logarithme népérien est un morphisme bijectif de groupes entre* $(\mathbb{R}_+^*, \times)$ *et* $(\mathbb{R}, +)$.

Propriété 14 *Soit* $f : G \to H$ *un isomorphisme de groupes. Alors sa réciproque* $f^{-1} : H \to G$ *est un morphisme de groupes.*

Démonstration. Soit $(h_1, h_2) \in H^2$. Montrons que $f^{-1}(h_1 \sharp h_2) = f^{-1}(h_1) \star f^{-1}(h_2)$. Notons $g_1 = f^{-1}(h_1)$ et $g_2 = f^{-1}(h_2)$. Comme f est un morphisme de groupes, on a $f(g_1 \star g_2) = f(g_1) \sharp f(g_2)$, ce qui s'écrit encore $f(g_1 \star g_2) = h_1 \sharp h_2$. En appliquant f^{-1}, on obtient $f^{-1}(f(g_1 \star g_2)) = f^{-1}(h_1 \sharp h_2)$. Comme $f^{-1} \circ f = \mathrm{Id}_G$, on obtient $g_1 \star g_2 = f^{-1}(h_1 \sharp h_2)$, soit encore $f^{-1}(h_1) \star f^{-1}(h_2) = f^{-1}(h_1 \sharp h_2)$.

Propriété 15 *Soit* $(G, \star)$ *un groupe. L'ensemble des automorphismes de* G *dans* G*, noté Aut*(G) *est un sous-groupe de* $(\mathfrak{S}(G), \circ)$.

Démonstration.
- Les automorphismes de G dans G sont des applications bijectives de G dans G, donc $\mathrm{Aut}(G) \subset \mathfrak{S}(G)$.
- On connaît le neutre de $(\mathfrak{S}(G), \circ)$, il s'agit de l'application Id_G, vérifions qu'elle appartient à $\mathrm{Aut}(G)$, i.e que c'est un morphisme de groupes. Soit $(g_1, g_2) \in G^2$.

$$\mathrm{Id}_G(g_1 \star g_2) = g_1 \star g_2 = \mathrm{Id}_G(g_1) \star \mathrm{Id}_G(g_2)$$

- On a démontré que la composée de morphisme de groupes est un morphisme de groupes. Par conséquent, $\mathrm{Aut}(G)$ est stable par composition.
- On a démontré que la réciproque d'un morphisme de groupes est un morphisme de groupes. Par conséquent, $\mathrm{Aut}(G)$ est stable par inverse de la composition.

Conclusion, $\mathrm{Aut}(G)$ est un sous-groupe de $(\mathfrak{S}(G), \circ)$.

Exercice 9 *Soit* $g \in G$*, on note* $i_g : G \to G, h \to ghg^{-1}$*. Montrer que* i_g *est un automorphisme de* G*. L'ensemble* $\{i_g | g \in G\}$ *est-il un sous-groupe de Aut*(G) *?*

Exercice 10 *On considère deux groupes isomorphes. Montrer que si l'un des deux est commutatif, l'autre l'est également.*

Exemple 15 *Notons* $X = \{1, 2, 3\}$*. On considère le groupe* $S_3 = \mathfrak{S}(\{1, 2, 3\})$ *muni de la loi de composition. Il comporte* 6 *éléments,*

- *l'application* $Id_X : 1 \mapsto 1, 2 \mapsto 2, 3 \mapsto 3$*,*
- *l'application* $\tau_1 : 1 \mapsto 1, 2 \mapsto 3, 3 \mapsto 2$*,*
- *l'application* $\tau_2 : 1 \mapsto 3, 2 \mapsto 2, 3 \mapsto 1$*,*
- *l'application* $\tau_3 : 1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 3$*,*
- *l'application* $\gamma_1 : 1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1$*,*
- *et enfin l'application* $\gamma_2 : 1 \mapsto 3, 2 \mapsto 1, 3 \mapsto 2$*.*

On considère d'autre part, la partie $\mathbb{U}_3$ *de* $\mathbb{C}$*, et on note* G *l'ensemble des isométries (rotations ou réflexions) de* $\mathbb{C}$ *qui stabilisent* $\mathbb{U}_3$*. Notons* $j = \exp(2i\pi/3)$ *et donnons la liste des éléments de* G *pour vous éviter une migraine, il s'agit des applications*

- $Id_{\mathbb{C}} : z \mapsto z$*,*
- $r_1 : z \mapsto jz$*,*
- $r_2 : z \mapsto j^2 z$*,*
- $s_1 : z \mapsto \overline{z}$*,*
- $s_2 : z \mapsto j^2\overline{z}$*,*
- $s_3 : z \mapsto j\overline{z}$*.*

On peut alors créer un isomorphisme de groupes $\varphi : S_3 \to G$ *via*

- $\varphi(Id_X) = Id_{\mathbb{C}}$*,*
- $\varphi(\gamma_1) = r_1$*,*
- $\varphi(\gamma_2) = r_2$*,*
- $\varphi(s_1) = \tau_1$*,*
- $\varphi(s_2) = \tau_2$*,*
- $\varphi(s_3) = \tau_3$*.*

4.2 Morphismes et sous-groupes

Dans tout ce qui suit, on fixe $(G, \star)$ et $(H, \sharp)$ deux groupes, puis $f : G \to H$ un morphisme de groupes.

Propriété 16 *Soit* K *un sous-groupe de* G. *Alors* $f(K)$ *est sous-groupe de* H.
Soit L *un sous-groupe de* H. *Alors* $f^{-1}(L)$ *est un sous-groupe de* G.

Démonstration. — K est non vide comme sous-groupe de G, par conséquent, $f(K)$ est non vide. Soit $(y_1, y_2) \in f(K)^2$. Montrons que $y_1 \sharp y_2 \in f(K)$. On dispose de $x_1 \in K$ tel que $y_1 = f(x_1)$ et $y_2 \in K$ tel que $y_2 = f(x_2)$. Comme f est un morphisme de groupes, on a

$$y_1 \sharp y_2 = f(x_1) \sharp f(x_2) = f(x_1 \star x_2)$$

Or comme K est un sous-groupe de G, il est stable par $\star$, donc $x_1 \star x_2 \in K$. On a ainsi trouvé un antécédent de $y_1 \sharp y_2$ par f dans K, i.e $y_1 \sharp y_2 \in f(K)$. Soit $y \in f(K)$. Montrons que y^{-1} (inverse de y pour la loi $\sharp$) appartient à $f(K)$. On dispose de $x \in K$ tel que $y = f(x)$. Mais alors, comme vu dans les propriétés sur les morphismes de groupes,

$$y^{-1} = f(x)^{-1} = f(x^{-1})$$

On note qu'alors x^{-1} appartient à K car K est stable par passage à l'inverse, puisque c'est un sous-groupe de G. Ainsi, on a trouvé un antécédent de y^{-1} par f dans K, i.e $y^{-1} \in f(K)$. Conclusion, $f(K)$ est bien un sous-groupe de H.

— Comme f est un morphisme de groupes, $f(e_G) = e_H$. Or L contient e_H puisque c'est un sous-groupe de H. Par conséquent, $f(e_G) \in L$, i.e $e_G \in f^{-1}(L)$ et $f^{-1}(L)$ est non vide. Soit $(x_1, x_2) \in (f^{-1}(L))^2$. Montrons que $x_1 \star x_2 \in f^{-1}(L)$. On note que $f(x_1 \star x_2) = f(x_1) \sharp f(x_2)$ puisque f est un morphisme. Or $f(x_1) \in L$ et $f(x_2) \in L$. Comme L est un sous-groupe de H, il est stable par $\sharp$, donc $f(x_1) \sharp f(x_2) \in L$. On a ainsi montré que $f(x_1 \star x_2) \in L$, i.e $x_1 \star x_2 \in f^{-1}(L)$. Soit $x \in f^{-1}(L)$. Montrons que $x^{-1} \in f^{-1}(L)$. Comme f est un morphisme de groupes, $f(x^{-1}) = f(x)^{-1}$. Or $f(x) \in L$ et L est stable par passage à l'inverse, donc $f(x)^{-1} \in L$. Ainsi, $f(x^{-1}) \in L$, i.e $x^{-1} \in f^{-1}(L)$.

Exemple 16 $\mathbb{Q}$ *est un sous-groupe de* $(\mathbb{R}, +)$. *Son image par le morphisme* $\mathbb{R} \to \mathbb{U}, t \mapsto \exp(it)$ *est un sous-groupe de* $(\mathbb{U}, \times)$. *L'ensemble* $\{-1, 1\}$ *est un sous-groupe de* $(\mathbb{U}, \times)$, *son image réciproque par le morphisme* $\mathbb{R} \to \mathbb{U}, t \mapsto \exp(it)$ *est un sous-groupe de* $(\mathbb{R}, +)$, *ici il s'agit de l'ensemble* $\pi\mathbb{Z}$.

Définition 17 *L'image de* f *est l'ensemble* $f(G)$, *elle est notée* $\mathrm{Im}(f)$. *Le noyau de* f *est l'ensemble* $f^{-1}(\{e_H\})$, *il est noté* $\ker(f)$.

Propriété 17 *On a les équivalences suivantes :*

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

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

Démonstration. — Le premier point est la définition de la surjectivité.

— Supposons f injective et démontrons que $\ker(f) = \{e_G\}$. On remarque tout d'abord que $f(e_G) = e_H$ puisque f est un morphisme de groupes. On en déduit que $e_G \in \ker(f)$, i.e $\{e_G\} \subset \ker(f)$. Soit $x \in \ker(f)$, alors $f(x) \in \{e_H\}$, i.e $f(x) = e_H = f(e_G)$. Comme f est injective, on a alors $x = e_G$. Conclusion, $\ker(f) \subset \{e_G\}$ et l'égalité d'ensembles $\ker(f) = \{e_G\}$. Réciproquement, supposons $\ker(f) = \{e_G\}$ et démontrons que f est injective. Soit $(x_1, x_2) \in G^2$ tel que $f(x_1) = f(x_2)$. Cela entraîne $f(x_1) f(x_2)^{-1} = e_H$. Comme f est un morphisme de groupes, on a alors $f(x_1 x_2^{-1}) = e_H$, autrement dit $x_1 x_2^{-1} \in \ker(f)$. On en déduit $x_1 x_2^{-1} = e_G$, soit encore $x_1 = x_2$. On a donc bien démontré l'injectivité de f.

Exercice 11 *Soit* G *un groupe monogène et* H *un groupe. On note* $g \in G$ *tel que* $G = \langle g \rangle$. *On considère* $f : G \to H$ *un morphisme de groupes. Rechercher des conditions nécessaires et suffisantes*

— *pour que* f *soit surjective,*

— *pour que* f *soit injective.*