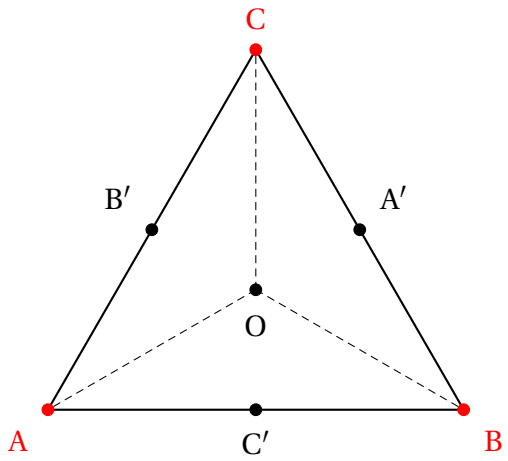
ALG 8 | Introduction aux structures algébriques

Dans ce chapitre, nous allons généraliser la notion d'opération à des ensembles quelconques, ainsi que les règles de calculs inhérentes (commutativité, associativité, distributivité, etc.). Nous introduirons progressivement les structures algébriques fondamentales : magmas, monoïdes, groupes, anneaux et corps. Il ne s'agit pas d'une étude exhaustive mais d'une première approche de ces objets, assortie de nombreux exemples et contre-exemples. En fin de parcours, les isomorphismes nous permettront de mieux appréhender ce qu'est une structure algébrique.

L'Agneau Mystique, Van Eyck

La notion de groupe est née de l'idée de symétrie. Considérons un ensemble X de points du plan. Déterminer les symétries de cet objet X, c'est rechercher les isométries affines planes f laissant globalement invariant la figure X, c'est-à-dire celles vérifiant $f(X) = X$.



Prenons le cas où X est un triangle équilatéral ABC. Notons O son centre de gravité et G l'ensemble des isométries laissant invariant X. On prouve facilement que G contient six transformations :

$$\begin{cases} f_1\ , & \text{l'identité} \\ f_2\ , & \text{la rotation de centre O et d'angle } 2\pi/3 \\ f_3\ , & \text{la rotation de centre O etvd'angle } 4\pi/3 \\ f_4\ , & \text{la réflection d'axe (AA}') \\ f_5\ , & \text{la réflection d'axe (BB}') \\ f_6\ , & \text{la réflection d'axe (CC}') \end{cases}$$

On vérifie de manière élémentaire que l'action d'un élément f de G sur le triangle ABC va entraîner une permutation des points A, B et C. En numérotant ceux-ci de 1 à 3 (dans l'ordre suivant : A, B puis C), l'action de f_i sur ABC se traduit donc par une permutation σ_i de l'ensemble $\{1,2,3\}$.

Notons $\mathfrak{S}_3$ l'ensemble des permutations de $\{1,2,3\}$.
Les ensembles G et $\mathfrak{S}_3$ ne sont pas les mêmes (car leurs éléments sont de natures différentes) mais agissent respectivement sur les ensembles X et $\{1,2,3\}$ de la même manière.

En faisant varier l'isométrie f dans G, on obtient toutes les permutations de l'ensemble $\{1,2,3:\}$, c'est-à-dire que l'on a $\mathfrak{S}_3 = \{\sigma_1, \ldots, \sigma_6\}$ où :

$$\begin{cases} \sigma_1\ , & \text{l'identité} \\ \sigma_2\ , & 1 \mapsto 2,\ 2 \mapsto 3 \text{ et } 3 \mapsto 1 \\ \sigma_3\ , & 1 \mapsto 3,\ 2 \mapsto 1 \text{ et } 3 \mapsto 2 \\ \sigma_4\ , & 1 \mapsto 1,\ 2 \mapsto 3 \text{ et } 3 \mapsto 2 \\ \sigma_5\ , & 1 \mapsto 3,\ 2 \mapsto 2 \text{ et } 3 \mapsto 1 \\ \sigma_6\ , & 1 \mapsto 2,\ 2 \mapsto 1 \text{ et } 3 \mapsto 3 \end{cases}$$

Ce qui se cache derrière ces actions analogues est *une structure commune* des ensembles G et $\mathfrak{S}_3$.

On dit que G et $\mathfrak{S}_3$ ont *des structures isomorphes*, ou encore qu'ils ont *la même structure*. Cela se traduit par le fait que leurs *tables*[1] sont « *les mêmes* » au nom-près des éléments.

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_3	f_1	f_6	f_4	f_5
f_3	f_3	f_1	f_2	f_5	f_6	f_4
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_6	f_4	f_3	f_1	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

$\circ$	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_3	σ_1	σ_6	σ_4	σ_5
σ_3	σ_3	σ_1	σ_2	σ_5	σ_6	σ_4
σ_4	σ_4	σ_5	σ_6	σ_1	σ_2	σ_3
σ_5	σ_5	σ_6	σ_4	σ_3	σ_1	σ_2
σ_6	σ_6	σ_4	σ_5	σ_2	σ_3	σ_1

Les premières traces de la théorie des groupes remontent aux travaux de 1832 d'**Évariste Galois** qui ne furent publiés qu'après sa mort, en 1846. Lors de son étude des équations algébriques, le jeune mathématicien s'intéressa particulièrement aux permutations de l'ensemble des racines d'un polynôme. Il mis en évidence de nombreuses propriétés de ce qui est de nos jours appelé le groupe symétrique à n éléments et noté $\mathfrak{S}_n$.

1. Par analogie avec les tables de multiplication de notre tendre enfance !

Évariste Galois

Vers la même époque, **Augustin Cauchy** s'intéressa également à cette structure. L'ensemble de la communauté scientifique pris conscience de l'importance de la notion de groupe au travers des nombreuses applications à la géométrie mises en évidence au cours du XIX^{e} siècle.

Ce n'est cependant qu'au début du XX^{e} siècle que la notion de groupe actuelle vit le jour après les mises au points successives de mathématiciens comme **Cayley**, **Weber**, **Frobenius** ou encore **Burnside**.

Les groupes ont permis de donner un sens plus précis à la notion de symétrie (un carré possède plus de symétries qu'un losange : le groupe des isométries d'un carré possède plus d'éléments que celui d'un losange).

Cette théorie suscite encore de nos jours de nombreux travaux. Ajoutons enfin que la théorie des groupes possède de nombreux champs d'application : la cristallographie en chimie[2], la physique des particules[3], la géométrie différentielle et la théorie de la relativité, la physique quantique, etc.

1. Magmas et monoïdes

Dans ce paragraphe, nous allons généraliser la notion d'opération, telle que l'addition sur $\mathbb{R}$ ou $\mathbb{C}$, le produit matriciel sur $\mathcal{M}_n(\mathbb{C})$, etc.

1.1. Loi de composition interne sur un ensemble

L'idée d'une opération interne sur un ensemble E se formalise simplement : c'est une application qui à tout couple (x, y) d'éléments de E associe un élément de E, résultat de « *l'opération* » de x par y.

Définition 8.0. Loi de composition interne et structure de magma (↯ 8.1)

Soit E un ensemble.

- ⇛ On appelle loi de composition interne (LCI) sur E toute application ϕ de $E \times E$ dans E.
- ⇛ Plutôt que $\phi(x, y)$, on note souvent le résultat de l'opération ϕ de x par y au moyen d'un symbole dit opératoire, par exemple $\star$: on écrira $x \star y$ au lieu de $\phi(x, y)$.
- ⇛ On appelle magma tout ensemble E muni d'une loi de composition interne $\star$.
- ⇛ On écrira plus simplement que $(E, \star)$ est un magma pour signifier que l'ensemble E est muni d'une loi de composition interne $\star$.

Nous sommes de longue date familiarisés avec cette écriture au travers des signes + et × utilisés pour l'addition et la multiplication des nombres complexes. Le choix de la *notation opérationnelle* plutôt que *fonctionnelle* pour une loi de composition interne allégera considérablement la rédaction. À l'instar des tables d'addition et de multiplication de notre enfance, on peut dresser la table d'une loi de composition.

2. Les propriéts optique d'un cristal dépendant de la structure de son groupe de symétrie.
3. Dans cette théorie, chaque particule est représentée par un groupe !

Notation 8.1. Table de Cayley d'une LCI

Soit $(E,\star)$ un magma.

⇛ On construit un tableau dans lequel figurent sur la première ligne et la première colonne les éléments de E.

⇛ Pour tout couple (x,y) d'éléments de E, la case correspondant à la ligne de x et à la colonne de y contient le produit $x\star y$. Ce tableau est appelé table de Cayley de la loi de composition $\star$.

⇛ Il y a unicité de la table de la loi $\star$ sur E à permutation près des éléments de E.

$\star$	a	b	c	…
a	$a\star a$	$a\star b$	$a\star c$	…
b	$b\star a$	$b\star b$	$b\star c$	…
c	$c\star a$	$c\star b$	$c\star c$	…
⋮	⋮	⋮	⋮	⋱

Δ	$\varnothing$	$\{0\}$	$\{1\}$	E
$\varnothing$	$\varnothing$	$\{0\}$	$\{1\}$	E
$\{0\}$	$\{0\}$	$\varnothing$	E	$\{1\}$
$\{1\}$	$\{1\}$	E	$\varnothing$	$\{0\}$
E	E	$\{1\}$	$\{0\}$	$\varnothing$

Réciproquement, on peut définir une loi sur E par la donnée d'une table de cette forme.

Nous avons dressé ci-contre la table de Cayley de la loi Δ sur $A=\mathscr{P}(E)$, où $E=\{0,1\}$.

On rappelle que la différence symétrique de deux parties A et B de E est définie par $A\Delta B := (A\cup B)\setminus(A\cap B)$. On a

Nous terminerons ce paragraphe par la notion de partie stable d'un magma $(E,\star)$.

Définition 8.2. Partie stable par une une loi de composition et loi induite (↯ 8.2)

Soit $(E,\star)$ un magma et F une partie de E.

⇛ La partie F est dite stable par $\star$ si $\forall (x,y)\in F^2,\ x\star y\in F$.

⇛ Si F est stable par $\star$, alors l'application de $F\times F$ dans F définie par $(x,y)\mapsto x\star y$ est correctement définie et est appelée loi de composition interne induite par $\star$ sur F.

Par exemple, $\mathbb{R}_+^*$ est une partie de $\mathbb{R}$ stable par l'addition et la multiplication usuelles. De même, l'ensemble $\mathscr{T}_n^+(\mathbb{K})$ des matrices triangulaires supérieures de $\mathscr{M}_n(\mathbb{K})$ est stable par l'addition et la multiplication matricielles. Il en est de même de $\mathscr{T}_n^-(\mathbb{K})$.

1.2. Associativité, commutativité, distributivité et élément neutre

En imposant des règles de calcul à nos magma $(E,\star)$, des premiers théorèmes vont apparaître.

Définition 8.3. Élément neutre, commutativité et associativité d'une LCI (↯ 8.3)

Soit un magma $(E,\star)$ et $e\in E$. On dit que :

⇛ la loi $\star$ est commutative lorsque $\forall (x,y)\in E^2,\ x\star y = y\star x$;

⇛ deux éléments x et y de E commutent si $x\star y = y\star x$;

⇛ la loi $\star$ est associative lorsque $\forall (x,y,z)\in E^3,\ x\star(y\star z) = (x\star y)\star z$;

⇛ e est un élément neutre pour la loi $\star$ lorsque $\forall x\in E,\ x\star e = e\star x = x$.

Il est clair qu'en cas d'existence, un élément neutre est unique.

Les lois + et × définies sur $\mathscr{M}_2(\mathbb{K})$ sont associatives, + et × étant respectivement commutative et non commutative, et admettent 0_n et I_n pour éléments neutres.

On peut facilement construire des exemples et des contre-exemples en s'aidant des tables de Cayley.

$\star$	a	b	c	d
a	b	a	a	d
b	a	b	c	d
c	c	c	b	a
d	b	d	a	b

Considérons, par exemple, la LCI $\star$ définie sur un ensemble $\{a,b,c,d\}$ de cardinal quatre par la table de Cayley ci-contre. On déduit de la ligne et la colonne deux que b est un élément neutre pour $\star$. On voit que c et d commutent mais pas a et d (la loi $\star$ n'est donc pas commutative). L'associativité (ou son défaut) ne se voit pas *directement* sur la table : il faut l'appliquer deux fois, bref faire des calculs intermédiaires, pour conclure. Ici, on obtient $(d\star a)\star c = c$ et $d\star(a\star c) = b$. La loi $\star$ n'est donc pas associative.

Définition 8.4. Structure de monoïde

On appelle monoïde tout magma $(E,\star)$ tel que $\star$ soit associative et admette un élément neutre.

On rencontre la sgtructure de monoïde dans de nombreux domaines. Par exemple, l'ensemble $\mathscr{P}(E)$ muni de la différence symétrique et $(\mathscr{M}_n(\mathbb{K}),\times)$ sont des monoïdes. Pour un ensemble E, la composition $\circ$ définit sur l'ensemble E^E une loi de composition interne. Elle est associative et admet l'identité de E pour élément neutre.

La structure de monoïde est *le bon cadre* pour définir les puissances d'un élément.

Définition 8.5. Exponentiation a^n

Soit $(E,\star)$ un monoïde neutre e, $a\in E$ et $n\in\mathbb{N}$. On définit par récurrence $a^{\star n}$ par $a^0 = e$ et pour tout $n\geqslant 1$, $a^n = a\star a^{n-1}$. On note plus simplement a^n lorsqu'il n'y a pas d'ambiguité sur la loi $\star$.

L'associativité de $\star$ nous permet d'écrire

$$\forall (m,n)\in\mathbb{N}^2,\ \forall (a,b)\in E^2,\ a^{n+m} = a^n\star a^m,\ \left(a^n\right)^m = a^{nm} \text{ et } a^nb^n = (ab)^n \text{ si } a \text{ et } b \text{ commutent}$$

Afin d'être cohérents avec nos usages précédents, nous adopterons la convention suivante :

Notation multiplicative Vs. notation additive

Dans le cas d'une loi notée additivement (i.e. le symbole opératoire est +), on note

$$nx := \underbrace{x+\cdots+x}_{n \text{ fois}} \text{ plutôt que multiplicativement } x^n$$

Nous terminons ce paragraphe par la distributivité d'une LCI sur une autre.

Définition 8.6. Distributivité

Soit E un ensemble muni de deux LCI $\star$ et $\bullet$. On dit que $\star$ est distributive sur $\bullet$ si

$$\forall (x,y,z)\in E^2,\ x\star(y\bullet z) = (x\star y)\bullet(x\star z) \text{ et } (x\star y)\bullet z = (x\star z)\bullet(y\star z)$$

1.3. Inversibilité

Nous avons déjà rencontré dans le cours sur les matrices la problématique suivante : afin de résoudre des équations de la forme $a \star x = b$ ou encore $y_1 \star a = y_2 \star a$, nous allons introduire la notion d'inversibilité à gauche et à droite.

Définition 8.7. Inverses à droite et à gauche

Soit E un ensemble muni d'une LCI $\star$ et admettant un neutre e. Un élément x de E est dit inversible :

- à gauche lorsqu'il existe $y \in E$ tel que $y \star x = e$.
- à droite lorsqu'il existe $y \in E$ tel que $x \star y = e$.
- inversible lorsqu'il existe $y \in E$ tel que $y \star x = x \star y = e$.

Sous réserve d'existence, un tel élément y est appelé respectivement un inverse à gauche, un inverse à droite et un inverse de x pour la loi $\star$,

En général, l'existence d'un inverse à droite et d'un inverse à gauche n'implique pas l'existence d'un inverse en général. L'unicité d'un éventuel inverse n'est pas assurée en général. On parlera donc *d'un inverse* et non de *l'inverse* d'un élément x du magma $(E, \star)$.

$\star$	a	b	c	d
a	a	b	c	d
b	b	d	a	b
c	c	a	b	a
d	d	a	a	b

- Il n'est pas difficile de produire des contre-exemples. Il suffit de définir des LCI via leurs tables de Cayley en remplissant les cases de façon à obtenir les bonnes propriétés.
- Par exemple, dans le magma $(E, \star)$ défini par la table de Cayley ci-contre, l'élément a est neutre, b et c sont inverses l'un de l'autre, d est un inverse à gauche de b mais pas à droite (et donc b est un inverse à droite de d mais pas à gauche), c admet deux inverses (b et d).

Un inverse latéral ne sera vraiment utile que dans le cadre des monoïdes. Par exemple, dans un monoïde $(E, \star)$, considérons a d'inverse à gauche a'. Pour x_1 et x_2 dans E, la relation $a \star x_1 = a \star x_2$ est équivalente à $x_1 = x_1$. En effet,

$$a \star x_1 = a \star x_2 \implies a' \star (a \star x_1) = a' \star (a \star x_2) \overset{\text{associativité}}{\implies} (a' \star a) \star x_1 = (a' \star a) \star x_2 \overset{a' \star a = e}{\implies} x_1 = x_2$$

La réciproque est claire. Considérons à présent l'équation $a \star x = b$ d'inconnue x. Si x est solution, alors $a' \star (a \star x) = a' \star b$ i.e. $x = a' \star b$ par associativité de $\star$. Ainsi cette équation admet au plus une solution. Si a' est aussi un inverse à droite, alors $a \star (a' \star b) = b$ et donc $a \star x = b$ équivaut à $x = a' \star b$. Comme nous le voyons ici, ces calculs reposent sur l'associativité sans laquelle on ne peut rien faire.

Proposition 8.8. Unicité de l'inverse dans un monoïde (↯ 8.4)

Soit $(E, \star)$ un monoïde. Si $x \in E$ admet un inverse, alors celui-ci est unique. On le note alors x^{-1} voire $-x$ en cas de notation additive de la loi de E, et parle plutôt d'opposé dans ce cas.

- Revenons au monoïde $(E^E, \circ)$ déjà évoqué ci-dessus. Comme E^E est réduit à l'application vide si E est vide, on peut supposer que E est non vide dans ce qui suit. Soit f et g deux applications de E dans lui-même.

✔ *L'injectivité de f* équivaut à *l'inversibilité à gauche de f* dans le monoïde $\left(\mathrm{E}^{\mathrm{E}}, \circ\right)$:

$$\text{Pour } g : \mathrm{E} \to \mathrm{E} \ , \ g \circ f = \mathrm{id}_{\mathrm{E}} \iff \forall x \in \mathrm{E},\ g\big(f(x)\big) = x$$

- En effet, supposons f inversible à gauche : il existe alors $g : \mathrm{E} \to \mathrm{E}$ tel que $g \circ f = \mathrm{id}_{\mathrm{E}}$. Comme id_{E} est injective, on en déduit qu'il en est de même de f. Réciproquement, supposons f injective. Pour tout y dans $f\langle \mathrm{E} \rangle$, il existe un unique x dans E tel que $y = f(x)$. On pose $g(y) := x$. Pour $y \in \mathrm{E} \setminus f\langle \mathrm{E} \rangle$, on pose $g(y) := x_0$ où x_0 est un élément quelconque de E. On a bien $g \circ f = \mathrm{id}_{\mathrm{E}}$.
- En particulier, il y a plusieurs inverses à gauche si f est injective mais non surjective. D'après le cours de dénombrement, cela ne peut se produire que dans le cas où l'ensemble E est de cardinal infini. Par exemple, pour la fonction définie de $\mathbb{N}$ dans $\mathbb{N}$ par $f : n \mapsto 2n$, toute fonction $g : \mathbb{N} \to \mathbb{N}$ vérifiant $g(2n) := n$ pour tout entier naturel n convient et il en existe une infinité.

✔ *La surjectivité de f* équivaut à *l'inversibilité à droite de f* dans le monoïde $\left(\mathrm{E}^{\mathrm{E}}, \circ\right)$:

$$\text{Pour } g : \mathrm{E} \to \mathrm{E} \ , \ f \circ g = \mathrm{id}_{\mathrm{E}} \iff \forall x \in \mathrm{E},\ f\big(g(x)\big) = x$$

- En effet, supposons f inversible à droite : il existe alors $g : \mathrm{E} \to \mathrm{E}$ tel que $f \circ g = \mathrm{id}_{\mathrm{E}}$. Comme id_{E} est surjective, on en déduit qu'il en est de même de f. Réciproquement, supposons f surjective. Pour $y \in \mathrm{E}$, il existe au moins un antécédent x de f, on pose $g(y) := x$ (on utilise ici l'axiome du choix). On a bien $f \circ g = \mathrm{id}_{\mathrm{E}}$. En particulier, il y a plusieurs inverses à droite si f est surjective mais non injective.
- À nouveau, pour un exemple de fonction surjective admettant plusieurs inverses à droite, il faut choisir un ensemble E de cardinal infini. Par exemple, pour la fonction définie de $\mathbb{N}$ dans $\mathbb{N}$ par $f(0) = 0$ et $f(n) := n - 1$ pour tout $n \in \mathbb{N}^*$, les fonctions $g : \mathbb{N} \to \mathbb{N}$ vérifiant $g(0) \in \{0, 1\}$ et $g(n) := n + 1$ pour tout n dans $\mathbb{N}^*$ convient et il en existe deux.

✔ *la bijectivité de f* et *inversibilité de f* dans le monoïde $\left(\mathrm{E}^{\mathrm{E}}, \circ\right)$.

✘ Revenons à l'exemple de la différence symétrique Δ sur $\mathscr{P}(\mathrm{E})$ où E est un ensemble quelconque (cf. la page 4. pour la définition de Δ). Toute partie X de E est inversible et $\mathrm{X}^{-1} = \mathrm{X}$ car $\mathrm{X}\Delta\mathrm{X} = \varnothing$.

Le lecteur pourra s'entraîner grâce au test (↯ **8.5**).

Les propriétés suivantes expriment la stabilité par la loi d'un monoïde E et par passage à l'inverse de l'ensemble des éléments inversibles[4] de E.

Proposition 8.9. Règles de calcul dans un monoïde

Soit $(\mathrm{E}, \star)$ un monoïde.

⇛ **Simplification à gauche** : pour a inversible à gauche, x_1, x_2 dans E, $a \star x_1 = a \star x_2 \implies x_1 = x_2$;

⇛ **Simplification à droite** : pour a inversible à droite, x_1, x_2 dans E, $x_1 \star a = x_2 \star a \implies x_1 = x_2$;

⇛ **Inverse d'un inverse** : pour x dans E inversible, x^{-1} est inversible et $\left(x^{-1}\right)^{-1} = x$;

⇛ **Puissances de l'inverse** : pour x dans E inversible et $n \in \mathbb{N}$, x^n est inversible et $(x^n)^{-1} = \left(x^{-1}\right)^n$;

On note x^{-n} l'inverse de x^n.

⇛ **Inverse d'un produit** : pour x et y dans E inversibles, $x \star y$ est inversible et $(x \star y)^{-1} = y^{-1} \star x^{-1}$.

⇛ **Puissance d'un conjugué** : pour a et x dans E, avec a inversible, $\left(a^{-1} x a\right)^n = a^{-1} x^n a$ pour tout n dans $\mathbb{N}$ (et même dans $\mathbb{Z}$ si x est inversible).

4. On dira que l'ensemble des inversibles de E, noté $\mathrm{E}^\times$, a une structure de groupe (voir la section 2 à la page 8)

2. Groupes

La structure de groupe a été introduite par **Évariste Galois** lors de ses travaux sur la résolution des équations polynomiales. Elle est liée à l'idée de symétrie (cf. l'exemple du groupe des symétries du triangles équilatéral étudié ci-dessus).

On appelle groupe un monoïde E dans lequel tous les éléments sont inversibles. On peut donc résumer la structure de groupe en quatre axiomes :

Définition 8.10. Structure de groupe

Un magma $(G, \star)$ est appelé groupe s'il vérifie les propriétés suivantes :

a. La loi $\star$ est assocative sur G ;

b. La loi $\star$ admet un élément neutre dans G ;

c. Tout élément de G est inversible pour la loi $\star$.

Un groupe $(G, \star)$ sera dit abélien[5] (ou encore commutatif) si la loi $\star$ est commutative.

En l'absence d'ambiguité, il est d'usage d'abandonner le symbole opératoire $\star$ et de noter xy au lieu de $x \star y$. On parlera ainsi simplement d'un groupe G.

Les règles de calcul 1.3 (cf. la page 7) dans un monoïde sont toutes appliquables dans un groupe.
De nombreux exemples de groupes sont issus d'une structure de monoïde.

- ✗ Pour tout ensemble non vide X, l'ensemble $\mathfrak{S}_X$ des bijections de X sur X (on dit également *permutations* de X) muni de la composition des applications. Cet ensemble est appelé *groupe symétrique de* X. Lorsque $X = [\![1, n]\!]$, on le notre plus simplement $\mathfrak{S}_n$.
- ✗ L'ensemble $E^\times$ des éléments inversibles d'un monoïde $(E, \star)$ est un groupe pour la loi de composition $\star$. En effet, d'après les règles de calcul dans un monoïde :
  - ✔ Le produit de deux éléments inversibles étant inversible, $E^\times$ est stable par la loi $\star$;
  - ✔ Le neutre de E appartient à $E^\times$ et la loi $\star$ est associative sur E donc aussi sur $E^\times$;
  - ✔ Pour x dans $E^\times$, x^{-1} est inversible (d'inverse x) donc x^{-1} appartient à $E^\times$: ainsi x admet bien un inverse dans $E^\times$.

  Ainsi, $(\mathbb{K}^*, \times)$ et $(\mathrm{GL}_n(\mathbb{K}), \times)$ sont les groupes des inversibles des monoïdes $(\mathbb{K}, \times)$ et $(\mathscr{M}_n(\mathbb{K}), \times)$.

Il s'agit d'étudier les sous-ensembles d'un groupe G qui *héritent* d'une structure de groupe par restriction de la loi de composition de G.

Définition 8.11. Sous-groupe

Soit $(G, \star)$ un groupe et $H \subset G$. On dit que H est un sous-groupe de G si $(H, \star)$ est un groupe.

Par exemple, les sous-ensembles $\{e\}$ et G d'un groupe G (de neutre e) sont des sous-groupes de G. Il s'agit en quelque sorte des sous-groupes *extrêmes*[6] de G, on les appelle *sous-groupes triviaux* de G. On retiendra la caractérisation suivante des sous-groupes :

5. En hommage à Niels Abel, mathématicien danois du milieu du XIXième siècle.
6. Respectivement le plus grand et le plus petit sous-groupes de G au sens de l'inclusion.

Proposition 8.12. Caractérisation des sous-groupes (↯ 8.6)

Soit G un groupe de neutre e et $H \subset G$. Les trois propositions suivantes sont équivalentes :

a. H est un sous-groupe de G ;

b. $e \in H$ et $\forall (h_1, h_2) \in H^2$, h_1^{-1} et $h_1 h_2$ appartiennent à H ;

c. $e \in H$ et $\forall (h_1, h_2) \in H^2$, $h_1^{-1} h_2$ appartient à H.

Une partie H de G vérifiant $\forall h \in H$, $h^{-1} \in H$ est dite stable par inversion. Un sous-groupe de G est donc un partie de G contenant le neutre de G, stable par produit et inversion.

✗ Le cercle unité $(\mathbb{U}, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$. Tout d'abord $\mathbb{U} \subset \mathbb{C}^*$. De plus, $1 \in \mathbb{U}$ et pour z_1 et z_2 dans $\mathbb{U}$, on a

$$\left|z_1^{-1} z_2\right| = \frac{|z_2|}{|z_1|} = 1 \text{ donc } z_1^{-1} z_2 \in \mathbb{U}$$

Pour $n \in \mathbb{N}^*$, on démontre de même que l'ensemble $\mathbb{U}_n$ des racines n-ème de l'unité est un sous-groupe de $(\mathbb{U}, \times)$.

✗ L'ensemble $a\mathbb{Z}$ des multiples d'un entier a est un sous-groupe de $(\mathbb{Z}, +)$. On a $a\mathbb{Z} \subset \mathbb{Z}$. De plus, $0 \in a\mathbb{Z}$ et pour (k_1, k_2) dans $\mathbb{Z}^2$, on a $-k_1 a + k_2 a \in a\mathbb{Z}$.

Il est évident que toute intersection de sous-groupe est un sous-groupe. Par exemple, dans le groupe $(\mathbb{Z}, +)$, on a $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$. Le cas d'une réunion est plus délicat. On voit que $2\mathbb{Z} \cup 3\mathbb{Z}$ n'est pas un sous-groupe de $(\mathbb{Z}, +)$ car $2+3$ n'appartient ni à $2\mathbb{Z}$, ni à $3\mathbb{Z}$. Considérons deux sous-groupes H et K d'un groupe G. Nous allons établir que

$$H \cup K \text{ est un sous-groupe de G} \iff H \subset K \text{ ou } K \subset H$$

Il est clair que si $H \subset K$ ou $K \subset H$, alors $H \cup K$ est un sous-groupe (car $H \cup K = K$ ou $H \cup K = H$). On démontre la réciproque par contraposition. Supposons que $H \not\subset K$ et $K \not\subset H$. Il existe (h_0, k_0) dans $H \times K$ tel que $h_0 \in H \setminus K$ et $k_0 \in K \setminus H$. Afin d'établir que $H \cup K$ n'est pas un sous-groupe de G, nous allons vérifier que $h_0 k_0$ n'appartient pas à $H \cup K$ par l'absurde[7]. Supposons que $h_0 k_0 \in H \cup K$. Supposons que $h_0 k_0 \in H$. On a alors $k_0 = h_0^{-1} h_0 k_0 \in H$ car H est stable par passage à l'inverse et par produit, c'est absurde. On prouve de même l'absurdité de la proposition $h_0 k_0 \in K$.

Proposition 8.13. Opérations sur les sous-groupes

Soit G un groupe.

a. Toute intersection de sous-groupes de G est un sous-groupe de G.

b. Soit H et K deux sous-groupes de G ; $H \cup K$ est un sous-groupe de G $\iff$ $H \subset K$ ou $K \subset H$.

Le lecteur pourra aborder avec profit le test (↯ 8.7).

3. Anneaux et corps

Dans ce paragraphe, nous allons définir et étudier deux structures comportant chacune deux lois internes :

7. Nous reprenons ici la même stratégie qu'avec $(h_0, k_0) := (2, 3)$ dans l'exemple de $2\mathbb{Z} \cup 3\mathbb{Z}$.

- les anneaux : c'est dans ce type de structure que l'on pourra généraliser l'arithmétique développée dans $(\mathbb{Z},+,\times)$;
- les corps qui généralisent les ensembles bien connus $(\mathbb{K},+,\times)$.

3.1. La structure d'anneau

Définition 8.14. Structure d'anneau (8.8)

On appelle anneau tout ensemble $(\mathbb{A},+,\times)$ muni de deux lois de compositions internes telles que :

- $(\mathbb{A},+)$ est un groupe abélien et $(\mathbb{A},\times)$ un monoïde d'éléments neutres notés 0 et 1 ;
- La multiplication $\times$ est distributive sur l'addition $+$.
- L' anneau $(\mathbb{A},+,\times)$ est dit commutatif lorsque $\times$ est commutative. On notera xy au lieu de $x\times y$.
- On note $\mathbb{A}^* := \mathbb{A}\setminus\{0\}$.
- On note $\mathbb{A}^\times$ le groupe des inversibles du monoïde $(\mathbb{A},\times)$ (cf. la page 8).

Il ne faut pas confondre $\mathbb{A}^*$ et $\mathbb{A}^\times$. Par exemple, $\mathbb{Z}^\times = \{-1,1\}$ et $\mathscr{M}_n(\mathbb{K})^\times$ sont distincts de $\mathbb{Z}^*$ et $\mathscr{M}_n(\mathbb{K})\setminus\{0\}$ pour $n\geqslant 2$.

La loi de groupe d'un anneau est traditionnellement notée additivement ; pour la loi $+$, l'inverse d'un élément a s'écrira donc $-a$ et les puissances de a seront notées na pour $n\in\mathbb{Z}$, la notation a^n étant réservée aux puissances pour loi $\times$ pour $n\in\mathbb{N}$. Ainsi,

$$\forall (a,n)\in\mathbb{A}\times\mathbb{N},\ na := \underbrace{a+\cdots+a}_{n \text{ fois si } n\in\mathbb{N}} \quad\text{et}\quad na := \underbrace{(-a)+\cdots+(-a)}_{-n \text{ fois si } n<0}$$

Nous connaissons déjà de nombreux exemples d'anneaux : l'anneau $(\mathbb{Z},+,\times)$ de l'arithmétique des entiers, celui du calcul matriciel $(\mathscr{M}_n(\mathbb{K}),+,\times)$ pour les cours les plus récents. L'ensemble des suites de réels $(\mathbb{R}^{\mathbb{N}},+,\times)$ muni des opérations suivantes

$$\forall u := (u_n)_{n\in\mathbb{N}}\in\mathbb{R}^{\mathbb{N}},\ \forall v := (v_n)_{n\in\mathbb{N}}\in\mathbb{R}^{\mathbb{N}},\ u+v := (u_n+v_n)_{n\in\mathbb{N}} \quad\text{et}\quad u\times v := (u_nv_n)_{n\in\mathbb{N}}$$

que nous avons rencontré dans le cours sur les suites – il faut se souvenir des opérations sur les limites par exemple – a une structure d'anneau avec pour éléments neutres respectifs la suite nulle et celle constante de valeur un.

En remplaçant $\mathbb{N}$ par une partie Ω de $\mathbb{R}$, on obtient l'anneau $(\mathbb{R}^\Omega,+,\times)$ des fonctions $f:\Omega\to\mathbb{R}$. On peut bien-sûr remplacer le corps $\mathbb{R}$ par $\mathbb{C}$ dans tous les exemples mentionnés ci-dessus.

Définition 8.14. Sous-anneau (8.9)

Soit $(\mathbb{A},+,\times)$ un anneau et $\mathbb{B}$ une partie de $\mathbb{A}$. On dit que $\mathbb{B}$ est un sous-anneau de $\mathbb{A}$ si

$$1\in\mathbb{B} \quad\text{et}\quad \forall (b_1,b_2)\in\mathbb{B}^2,\ b_1-b_2\in\mathbb{B} \text{ et } b_1b_2\in\mathbb{B}$$

Ainsi, un sous-anneau est une partie de $\mathbb{A}$ contenant 1 et qui est un anneau pour les lois de $\mathbb{A}$.

- La condition $1\in\mathbb{B}$ n'est pas superflue, par exemple, $(\{0\},+,\times)$ est un anneau mais pas un sous-anneau de $(\mathbb{A},+,\times)$ si $0\neq 1$.

✕ L'ensemble $\mathbb{Z}[i] := \{x+iy,\,(x,y)\in\mathbb{Z}^2\}$ est un sous-anneau de $(\mathbb{C},+,\times)$. En effet, $1 = 1+0\times i\in\mathbb{Z}[i]$ et pour tous entiers x, y, z, t, on a

$$x+iy-(z+it) = \underbrace{(x-z)}_{\in\mathbb{Z}} + i\underbrace{(y-t)}_{\in\mathbb{Z}} \in \mathbb{Z}[i] \quad\text{et}\quad (x+iy)(z+it) = \underbrace{xz-yt}_{\in\mathbb{Z}} + i\underbrace{(yz+xt)}_{\in\mathbb{Z}} \in \mathbb{Z}[i]$$

Nous conseillons au lecteur de poursuivre par le test (↯ 8.10).

3.2. Notations et règles de calcul dans les anneaux

Nous commençons par quelques conséquences des axiomes, comme par exemple le fait que multiplier par zéro dans un anneau donne toujours zéro.

Proposition 8.15. Règles de calcul

Soit $(\mathbb{A},+,\times)$ un anneau. Pour tous a et b dans $\mathbb{A}$ et n dans $\mathbb{Z}$:

- ⇛ **Zéro est absorbant pour la multiplication** : $a\times 0 = 0\times a = 0$;
- ⇛ **Opposés et produits** : $(-a)b = a(-b) = -(ab)$ et plus généralement $n(ab) = (na)b = a(nb)$;
- ⇛ **Produits d'opposés** : $(-1)^2 = 1$ et plus généralement $(-a)(-b) = ab$.

L'exemple de $\mathscr{M}_n(\mathbb{K})$ est instructif, certaines règles de calcul ne sont pas généralisables à tous les anneaux, comme par exemple :

$$a_1a_2 = 0 \implies a_1 = 0 \text{ ou } a_2 = 0$$

Diviseurs de zéro

Dans un anneau, on peut avoir $a_1a_2 = 0$ avec $a_1\neq 0$ et $a_2\neq 0$. Deux tels éléments a_1 et a_2 sont appelés des diviseurs de zéros.

On distingue les anneaux sans diviseurs de zéros, dans lesquels la résolution d'une équation peut de faire via une factorisation, comme dans $\mathbb{R}$ ou $\mathbb{C}$ (mais pas dans $\mathscr{M}_n(\mathbb{K})$ pour $n\geqslant 2$).

Définition 8.16. Anneaux intègres (↯ 8.11)

Un anneau $\mathbb{A}$ est dit intègre s'il n'admet aucun diviseur de zéro, i.e. si

$$\forall (a_1,a_2)\in\mathbb{A}^2,\ a_1a_2 = 0 \implies a_1 = 0 \text{ ou } a_2 = 0$$

L'anneau $\left(\mathbb{R}^{\mathbb{R}},+,\times\right)$ n'est pas intègre car $\chi_{\mathbb{Q}}\times\chi_{\mathbb{R}\setminus\mathbb{Q}} = 0$ alors que $\chi_{\mathbb{Q}}$ et $\chi_{\mathbb{R}\setminus\mathbb{Q}}$ sont non nulles. En revanche, l'anneau $\left(\mathscr{P},+,\times\right)$ des fonctions polynomiales de $\mathbb{R}$ dans $\mathbb{R}$ est intègre (ce résultat est assez intuitif, nous le démontrerons dans un chapitre dédié aux polynômes).

Notation 8.17. Sommes et produits finis dans un anneau

Pour $n\in\mathbb{N}^*$ et tous éléments $a_1,\dots,a_n$ d'un anneau $(\mathbb{A},+,\times)$, on notera

$$\sum_{k=1}^{n} a_k := a_1 + \cdots + a_n \text{ et } \prod_{k=1}^{n} a_k = a_1 \times \cdots \times a_n$$

Développement par distributivité dans un anneau

Dans un anneau, la relation $\left(\sum_{k=1}^{n} x_k\right)\left(\sum_{k=1}^{m} y_k\right) = \sum_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}} x_i y_j$ est valable.

Les anneaux sont le cadre le plus général dans lequel la démonstration de la formule du binôme (par récurrence ou au moyen de la formule de distributivité générale) est valable.

Proposition 8.18. Formulaire

Soit a et b deux éléments qui commutent d'un anneau $(\mathbb{A}, +, \times)$. On a

$$\forall n \in \mathbb{N},\ (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \quad \text{et} \quad \forall n \in \mathbb{N}^*,\ a^n - b^n = \sum_{k=0}^{n-1} a^k b^{n-1-k}$$

Cette formule de factorisation admet un cas particulier important, celui des sommes géométriques. En l'absence d'inversibilité, la formule des sommes géométriques s'écrit sans passage à l'inverse.

Sommes géométriques d'un anneau

Pour un anneau $(\mathbb{A}, +, \times)$, $a \in \mathbb{A}$ et $n \in \mathbb{N}^*$, on a $(a-1)\sum_{k=0}^{n-1} a^k = a^n - 1$.

3.3. La structure de corps

Définition 8.19. Structure de corps

On appelle corps tout anneau commutatif $\mathbb{k}$ tel que $\mathbb{k}^* = \mathbb{k}^\times$ et $0 \neq 1$.

Dans le cas où la loi $\times$ n'est pas commutative, la structure $(\mathbb{k}, +, \times)$ est appelée un corps gauche.

Le lecteur connaît bien les corps de nombres $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$. En revanche, l'anneau commutatif $(\mathbb{Z}, +, \times)$ n'est pas un corps car $\mathbb{Z}^\times = \{-1, 1\}$.

Tout corps est un anneau intègre. Soit en effet un corps $\mathbb{k}$ et $(x, y) \in \mathbb{k}^2$ tel que $xy = 0$. Supposons $x \neq 0$. Comme $\mathbb{k}$ est un corps, x est inversible d'où

$$y = x^{-1}(xy) = x^{-1} \times 0 = 0$$

Définition 8.19. Notation fractionnaire

Pour un corps $\mathbb{k}$ et $(a,b) \in \mathbb{k} \times \mathbb{k}^*$, on note $\dfrac{a}{b} := ab^{-1} = b^{-1}a$ (par commutativité).

Définition 8.20. Sous-corps

Une partie $\mathbb{L}$ d'un corps $\mathbb{k}$ est appelée un sous-corps de $\mathbb{k}$ si elle est un sous-anneau de $\mathbb{k}$ stable par inversion.

Un sous-corps est donc toujours un corps pour les lois induites.

✗ Démontrons par exemple que $\mathbb{Q}(i) := \{x+iy ; (x,y) \in \mathbb{Q}^2\}$ est un sous-corps de $\mathbb{C}$. On démontre comme dans le cas de $\mathbb{Z}[i]$ à la page 11 que $\mathbb{Q}(i)$ est un sous-anneau de $\mathbb{C}$. Il reste à établir que $\mathbb{Q}(i)$ est stable par inversion. Pour $(x,y) \neq (0,0)$, on a

$$\frac{1}{x+iy} = \frac{x-iy}{x^2+y^2} = \underbrace{\frac{x}{x^2+y^2}}_{\in\mathbb{Q}} + i\underbrace{\frac{-y}{x^2+y^2}}_{\in\mathbb{Q}} \in \mathbb{Q}(i)$$

4. Morphismes de structures

Revenons un instant à l'exemple et aux notations de l'introduction de cette leçon (cf page **??**).

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_3	f_1	f_6	f_4	f_5
f_3	f_3	f_1	f_2	f_5	f_6	f_4
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_6	f_4	f_3	f_1	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

$\circ$	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_3	σ_1	σ_6	σ_4	σ_5
σ_3	σ_3	σ_1	σ_2	σ_5	σ_6	σ_4
σ_4	σ_4	σ_5	σ_6	σ_1	σ_2	σ_3
σ_5	σ_5	σ_6	σ_4	σ_3	σ_1	σ_2
σ_6	σ_6	σ_4	σ_5	σ_2	σ_3	σ_1

Les magmas $(G,\circ)$ et $(\mathfrak{S}_3,\circ)$ sont en fait des groupes et la similarité de leurs tables se traduit par

$$\forall (i,j) \in [\![1,6]\!]^2 \,,\ \phi(f_i \circ f_j) = \phi(f_i) \circ \phi(f_j)$$

où ϕ est la bijection de G dans $\mathfrak{S}_3$ définie par $\forall i \in [\![1,6]\!],\ \phi(f_i) := \sigma_i$.

On notera que bien notées identiquement au moyen du symbole $\circ$, les deux lois $\circ$ de cet exemple sont différentes, les éléments de G et de $\mathfrak{S}_3$ sont de nature différentes.

Définition 8.21. Morphismes de groupes

Soit $(G_1,\star)$ et $(G_2,\bullet)$ deux groupes. On appelle morphisme de G_1 dans G_2 toute application $\phi : G_1 \to G_2$ telle que

$$\forall (x,y) \in G_1^2 \,,\ \phi(x \star y) = \phi(x) \bullet \phi(y)$$

En pratique, on notera $\phi(xy) = \phi(x)\phi(y)$ si les lois des deux groupes de ne sont pas précisés.

✗ Le lecteur connaît déjà deux morphismes issus du cours d'Analyse : l'exponentielle est un morphisme de $(\mathbb{R},+)$ dans $(\mathbb{R}_+^*,\times)$ et le logarithme de $(\mathbb{R}_+^*,\times)$ dans $(\mathbb{R},+)$:

$$\forall (x,y) \in \mathbb{R}^2 \,,\ \exp(x+y) = \exp(x) \times \exp(y) \quad \text{et} \quad \forall (x,y) \in (\mathbb{R}_+^*)^2 \,,\ \ln x \times y = \ln x + \ln y$$

Définition 8.22. Morphismes d'anneaux et de corps

Soit $\mathbb{A}_1$ et $\mathbb{A}_2$ deux anneaux. On appelle morphisme de $\mathbb{A}_1$ dans $\mathbb{A}_2$ toute application $\phi : \mathbb{A}_1 \to \mathbb{A}_2$ telle que

$$\phi(1) = 1 \ , \ \forall (x, y) \in \mathbb{A}_1^2, \ \ \phi(xy) = \phi(x)\phi(y) \text{ et } \phi(x + y) = \phi(x) + \phi(y)$$

Un morphisme de corps est un morphisme d'anneaux entre deux corps.

La notion d'isomorphisme permet d'identifier une structure particulière au sein d'une catégorie.

Définition 8.23. Isomorphismes

On appelle isomorphisme tout morphisme bijectif. Deux structures sont dites isomorphes s'il existe un isomorphisme de l'une sur l'autre.

Les groupes G et $\mathfrak{S}_3$ de l'exemple introductif sont donc différentes mais de même structure.

On vérifie facilement que la bijection réciproque d'un isomorphisme est un isomorphisme.

L'idée de structure algébrique en mathématiques

En mathématique, une structure algébrique est un ensemble muni d'une ou plusieurs opérations internes et relations, vérifiant un jeu axiomes prédéfini. Ce sont en fait celles-ci qui structurent l'ensemble sous-jacent d'une certaine façon.

5. Énoncés des tests

8.1.

La formule $x \star y = x + y + xy$ définit-elle une loi de composition interne sur $\mathbb{R} \setminus \{-1\}$?

8.2.

Une réunion de parties stables d'un magma $(E, \star)$ est-elle stable ?

8.3.

Soit E un ensemble. Quelles sont les propriétés de la loi Δ sur $\mathscr{P}(E)$?

8.4.

Quels sont les inversibles du monoïde $(\mathscr{P}(E), \cup)$? $(\mathscr{P}(E), \cap)$?

8.5.

Soit E un ensemble. Quels sont les éléments inversibles de $(\mathscr{P}(E), \Delta)$?

8.6.

Soit l'ensemble $E = \left\{ \dfrac{2p}{2q+1} \;\middle|\; (p,q) \in \mathbb{Z}^2 \right\}$. Montrer que $(E, +)$ est un groupe.

8.7.

Démontrer que la réunion d'une famille filtrante $(H_i)_{i \in I}$ de sous-groupes d'un groupe G est un sous-groupe de G. Voici la définition d'une famille filtrante :

$$\forall (i,j) \in I^2, \exists k \in I, H_i \cup H_j \subset H_k$$

8.8.

Que dire d'un anneau $(\mathbb{A}, +, \times)$ dans lequel $1 = 0$?

8.9.

L'ensemble $2\mathbb{Z} = \{2n ; n \in \mathbb{Z}\}$ est-il un sous-anneau de $(\mathbb{Z}, +, \times)$?

8.10.

L'ensemble $\mathbb{Z}[i\sqrt{2}] = \left\{ a + ib\sqrt{2} ; (a,b) \in \mathbb{Z}^2 \right\}$ est-il un sous-anneau de $(\mathbb{C}, +, \times)$?

8.11.

L'anneau $\left(\mathscr{D}(\mathbb{R}, \mathbb{R}), +, \times\right)$ usuel est-il intègre ?

6. Solutions des tests

8.1.

La formule est bien définie pour tous x et y dans $\mathbb{R}$. L'équation $x \star y = -1$ est équivalente à $(x+1)(y+1) = 0$, ie $x = -1$ ou $y = -1$. On vient d'établir par contraposition que

$$\big(x \neq -1 \text{ et } y \neq -1\big) \Rightarrow \big(x \star y \neq -1\big)$$

Ainsi $\mathbb{R} \setminus \{-1\}$ est stable par $\star$ et la loi $\star$ est interne sur $\mathbb{R} \setminus \{-1\}$.

8.2.

Non. Reprenons l'exemple 1.1 de la page 4 Les parties $U = \{\varnothing, \{0\}\}$ et $V = \{\varnothing, \{1\}\}$ sont stables par la différence symétrique mais par leur réunion car $\{0\}\Delta\{1\} = E \notin U \cup V$.

8.3.

La loi Δ est commutative, associative et admet un élément neutre.

- ⇛ La commutativité de Δ est évidente.
- ⇛ Puisque $\forall A \in \mathscr{P}(E), A\Delta\varnothing = \varnothing\Delta A = A$, $\varnothing$ est un élément neutre pour Δ.
- ⇛ Prouvons l'associativité de Δ en utilisant les fonctions indicatrices. Soient A, B et C trois parties de E. On a

$$\begin{aligned}
\mathbb{1}_{A\Delta(B\Delta C)} &= \mathbb{1}_A + \mathbb{1}_{B\Delta C} - 2\cdot\mathbb{1}_A\cdot\mathbb{1}_{B\Delta C} \\
&= \mathbb{1}_A + \mathbb{1}_B + \mathbb{1}_C - 2\cdot\mathbb{1}_B\cdot\mathbb{1}_C \\
&\quad - 2\cdot\mathbb{1}_A\cdot(\mathbb{1}_B + \mathbb{1}_C - 2\mathbb{1}_B\mathbb{1}_C) \\
&= \mathbb{1}_A + \mathbb{1}_B + \mathbb{1}_C - 2\mathbb{1}_A\mathbb{1}_B - 2\mathbb{1}_B\mathbb{1}_C \\
&\quad - 2\mathbb{1}_C\mathbb{1}_A + 4\mathbb{1}_A\mathbb{1}_B\cdot\mathbb{1}_C
\end{aligned}$$

Comme cette expression est invariante par permutations de A, B et C, on a $\mathbb{1}_{(A\Delta B)\Delta C} = \mathbb{1}_{(B\Delta C)\Delta A}$ d'où $(A\Delta B)\Delta C = (B\Delta C)\Delta A$. On déduit le résultat de la commutativité de Δ.

8.4.

Seuls les neutres sont inversibles dans ces monoïdes. On trouve respectivement $\varnothing$ et E.

8.5.

On se souvient que $\varnothing$ est le neutre de la loi Δ. Pour tout $A \in \mathscr{P}(E)$, on a $A\Delta A = \varnothing$ donc A est inversible d'inverse égal à lui-même.

8.6.

On prouve que c'est un sous-groupe de $(\mathbb{Q}, +)$.

- ⇛ L'inclusion $E \subset \mathbb{Q}$ est évidente.
- ⇛ $0 \in E$.
- ⇛ Soit x et y dans E. Il existe $(p, q, r, s) \in \mathbb{Z}^2$ tels que $x = \dfrac{2p}{2q+1}$ et $y = \dfrac{2r}{2s+1}$. Ainsi

$$\begin{aligned}
x - y &= \frac{2\big(p(2s+1) - (2q+1)r\big)}{(2q+1)(2s+1)} \\
&= \frac{2\big(p(2s+1) - (2q+1)r\big)}{2(2rs+r+s)+1} \\
&= \frac{2\alpha}{2\beta+1}
\end{aligned}$$

avec $\alpha = p(2s+1) - (2q+1)r \in \mathbb{Z}$ et $\beta = 2rs + r + s \in \mathbb{Z}$. ainsi $x - y \in E$. L'ensemble $(E, +)$ est un sous-groupe de $(\mathbb{Q}, +)$.

8.7.

Soit $(H_i)_{i\in I}$ une famille filtrante de sous-groupes de G. Notons U leur réunion. U est non vide car contient e. Soient x et y dans U : il existe des indices i et j de I tels que $x \in H_i$ et $y \in H_j$. Comme la famille est filtrante, il existe $k \in I$ tel que $H_i \cup H_j \subset H_k$. Comme x et y appartiennent à H_k sous-groupe de G, on a aussi $xy^{-1} \in H_k$ donc $xy^{-1} \in U$. Ainsi U est un sous-groupe de G.

8.8.

On a $\mathbb{A} = \{0\}$ car $\forall a \in \mathbb{A}$, $a = a1 = a0 = 0$.

8.9.

Non : $1 \notin 2\mathbb{Z}$.

8.10.

Oui :

⇛ $1 = 1 + i0 \in \mathbb{Z}[i\sqrt{2}]$.

⇛ Soit $(a, b, a', b') \in \mathbb{Z}^4$. On a $a + ib\sqrt{2} - \left(a' + ib'\sqrt{2}\right) = \underbrace{(a - a')}_{\in \mathbb{Z}} + i\sqrt{2}\underbrace{(b - b')}_{\in \mathbb{Z}}$. Ainsi $a + ib\sqrt{2} - \left(a' + ib'\sqrt{2}\right) \in \mathbb{Z}[\sqrt{2}]$.

8.11.

Non. Par exemple, les fonctions f et g suivantes sont dérivables de $\mathbb{R}$ dans $\mathbb{R}$, non nulles et de produit nul :

$$f(x) := \begin{cases} 0 & \text{si } x \leqslant 0 \\ x & \text{sinon} \end{cases} \quad \text{et} \quad g(x) := \begin{cases} x & \text{si } x \leqslant 0 \\ 0 & \text{sinon} \end{cases}$$