11 | Structures algébriques usuelles

Ce chapitre vise à présenter le vocabulaire de base pour l'étude systématique des structures opératoires, nommées *structures algébriques*. Le but étant d'offrir une présentation unifiée de situations a priori distinctes.

1 Loi de composition interne

Dans l'ensemble de cette section, E désigne un ensemble.

1.1 Généralités

Définition 1 – Loi de composition interne, magma

On appelle *loi de composition interne sur* E toute application de $E \times E$ dans E. Dans ce contexte, on adopte la convention de notation suivante :

$$* : \left| \begin{array}{ccc} E \times E & \longrightarrow & E \\ (x,y) & \longmapsto & x * y. \end{array} \right.$$

Le couple $(E, *)$ formé d'un ensemble E et d'une loi de composition interne sur E est appelé un *magma*.

Exemple 2 Nous avons déjà rencontré les lois de composition internes suivantes :

- × L'addition dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$;
  × La soustraction dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ (mais pas dans $\mathbb{N}$) ;
  × La multiplication dans $\mathbb{N}$, $\mathbb{N}^*$, $\mathbb{Z}$, $\mathbb{Z}^*$, $\mathbb{Q}$, $\mathbb{Q}^*$, $\mathbb{Q}_+^*$, $\mathbb{R}$, $\mathbb{R}^*$, $\mathbb{R}_+^*$, $\mathbb{C}$ et $\mathbb{C}^*$ (mais pas dans $\mathbb{Q}_-^*$ ou $\mathbb{R}_-^*$) ;
  × La division dans $\mathbb{Q}^*$, $\mathbb{R}^*$ et $\mathbb{C}^*$ (mais pas dans $\mathbb{Z}^*$).
- L'intersection $\cap$, l'union $\cup$ et la différence symétrique Δ dans $\mathscr{P}(E)$.
- La composition des applications dans E^E et dans l'ensemble des bijections de E sur E (th. 76 du chapitre 3).

1.1.1 Propriétés éventuelles d'une loi de composition interne

Définition 3 – Associativité, commutativité

Une loi de composition interne $*$ dans E est dite

- *associative* lorsque $\forall (x,y,z) \in E^3, \quad (x*y)*z = x*(y*z)$.
- *commutative* lorsque $\forall (x,y) \in E^2, \quad x*y = y*x$.

Exemple 4

- Dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, l'addition et la multiplication sont associatives et commutatives.
- Dans $\mathscr{P}(E)$, l'intersection, l'union et la différence symétrique sont associatives et commutatives (théorème 22 du chapitre 3 et exercice 31).
- Dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, la soustraction n'est ni associative ni commutative.
- Dans E^E, la composition des applications est associative (théorème 52 du chapitre 3), mais non commutative dès que E possède au moins deux éléments.

Remarque 5 Par convention, la notation additive $+$ est utilisée exclusivement pour désigner une loi commutative.

Définition 6 – Distributivité

Soit $\square$ et $\star$ deux lois de composition internes dans E. La loi $\star$ est dite *distributive* par rapport à loi $\square$ lorsque

$$\forall (x,y,z) \in E^3, \quad x \star (y \square z) = (x \star y) \square (x \star z) \quad \text{et} \quad (x \square y) \star z = (x \star z) \square (y \star z).$$

Exemple 7

- Dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, la multiplication est distributive par rapport à l'addition.
- Dans $\mathscr{P}(E)$, l'intersection et l'union sont chacune distributive par rapport à l'autre (théorème 22 du chapitre 3), et l'intersection est distributive par rapport à la différence symétrique (exercice 31).

1.1.2 Propriétés éventuelles des éléments

Soit $*$ une loi de composition interne dans E.

Définition 8 – Élément régulier/simplifiable

Un élément a de E est dit *régulier* (ou *simplifiable*) pour $*$ lorsque

$$\forall (x,y) \in E^2, \quad a*x = a*y \implies x = y \quad \text{et} \quad x*a = y*a \implies x = y.$$

Exemple 9

- Dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$: × tous les éléments sont réguliers pour l'addition ; × tous les éléments NON NULS sont réguliers pour la multiplication.
- Dans $\mathscr{P}(E)$: × le seul élément régulier pour l'intersection (resp. l'union) est E (resp. $\varnothing$) ; × tous les éléments sont réguliers pour la différence symétrique (exercice 31).

Définition-théorème 10 – Élément neutre, magma unifère

- **Élément neutre.** Un élément e de E est un *élément neutre pour* $*$ lorsque

$$\forall x \in E, \quad x*e = e*x = x.$$

  Un tel élément, quand il existe, est unique et régulier pour $*$.
- **Magma unifère.** Un magma $(E,*)$ est dit *unifère* lorsqu'il possède un élément neutre.

Démonstration. Si e et e' sont deux éléments neutres pour $*$, alors $e = e*e' = e'$. La régularité est triviale. ∎

Exemple 11

- Dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, 0 est l'élément neutre pour l'addition et 1 l'élément neutre pour la multiplication. En particulier, $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$, $(\mathbb{Q}^*,\times)$, $(\mathbb{Q}_+^*,\times)$, $(\mathbb{R}^*,\times)$, $(\mathbb{R}_+^*,\times)$ et $(\mathbb{C}^*,\times)$ sont des magmas unifères.
- Dans $\mathscr{P}(E)$, E est l'élément neutre pour l'intersection et $\varnothing$ l'élément neutre pour l'union et la différence symétrique.
- Dans E^E, Id_E est l'élément neutre pour la composition (théorème 52 du chapitre 3).
- Le magma $\mathbb{N}^*$ n'a pas d'élément neutre pour l'addition.

Définition-théorème 12 – Élément inversible

Soit $(E,*)$ un magma associatif et unifère, de neutre e. Un élément x de E est dit *inversible* lorsque

$$\exists y \in E, \quad x*y = y*x = e.$$

Le cas échéant, il y a unicité d'un tel élément y que l'on appelle l'*inverse de* x et que l'on note x^{-1}.

Démonstration. Soit x un élément inversible de $(E,*)$. Si y et y' sont deux inverses de x, alors

$$y' = y'*e = y'*(x*y) = (y'*x)*y = e*y = y.$$

∎

Notation 13 Pour les lois notées additivement, l'inverse d'un élément x se note $-x$ et est appelé l'*opposé de* x.

Exemple 14

- Pour l'addition dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, tout élément admet un opposé. En revanche, seul le neutre 0 admet un opposé pour l'addition dans $\mathbb{N}$.
- Pour la multiplication dans $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, tout élément non nul admet un inverse. En revanche, seul 1 et -1 admettent un inverse pour la multiplication dans $\mathbb{Z}$.
- Dans $(\mathscr{P}(E), \cap)$ (resp. $(\mathscr{P}(E), \cup)$) seul l'élément neutre E (resp. $\varnothing$) est inversible. En revanche, tout élément est son propre inverse dans $(\mathscr{P}(E), \Delta)$ (exercice 31).

Théorème 15 – Propriétés des éléments inversibles

Soit $(E, *)$ un magma associatif et unifère, de neutre e.

(i) L'élément neutre e est inversible et est son propre inverse.

(ii) Si x est un élément inversible de $(E, *)$, alors x^{-1} est inversible et $\left(x^{-1}\right)^{-1} = x$.

(iii) Si x et y sont deux éléments inversibles de $(E, *)$, alors $x * y$ est inversible et

$$(x * y)^{-1} = y^{-1} * x^{-1}.$$

(iv) Tout élément inversible de $(E, *)$ est régulier.

Démonstration. ... ∎

Exemple 16 Dans $\left(E^E, \circ\right)$, les éléments inversibles sont les bijections (théorème 72 du chapitre 3), qui admettent pour inverse leur bijection réciproque. Par ailleurs, nous avions déjà établi (théorème 76 du chapitre 3) que si f et g sont deux bijections de E sur E, alors il en va de même de $g \circ f$ et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

✖ **Attention !** ✖ La réciproque du point **(iv)** du théorème 15 est fausse en géneral. Un élément régulier de $(E, *)$ peut ne pas être inversible, *e.g.* dans $(\mathbb{N}, +)$ tout élément est régulier alors que seul le neutre 0 est inversible.

1.1.3 Itérés d'un élément

Soit $(E, *)$ un magma associatif et unifère, de neutre e. Pour $x \in E$ et $n \in \mathbb{N}^*$, l'élément

$$x^n = \underbrace{x * x * \cdots * x}_{n \text{ fois}}$$

appelé n^e *itéré de* x est défini par récurrence :

$$x^0 = e \qquad \text{et} \qquad \forall n \in \mathbb{N}, \quad x^{n+1} = x * x^n = x^n * x.$$

En outre, si x est inversible, alors, pour tout $n \in \mathbb{N}$, x^n est inversible et son inverse est $\left(x^{-1}\right)^n$ que l'on note x^{-n}.

Exemple 17 Dans le magma $\left(E^E, \circ\right)$, on note f^n la composée n fois de l'application f avec elle-même.

Théorème 18

Pour tous $x \in E$ et $(p, q) \in \mathbb{N}^2$,

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

Ces relations restent vraies pour $(p, q) \in \mathbb{Z}^2$ lorsque x est inversible.

Démonstration. Pour $(p, q) \in \mathbb{N}^2$, fixer p et procéder par récurrence sur $q \in \mathbb{N}$. Par passage à l'inverse, on en déduit les résultats pour p et q entiers relatifs quelconques lorsque x est inversible. ∎

Notation 19 – Notation additive Lorsque la loi est commutative et notée additivement :

- l'élément neutre est noté 0_E ;
- le n^{e} itéré d'un élément x est noté $n.x$ ou nx, en lieu et place de x^n, et lorsque x admet un opposé, on note $-nx$ l'opposé de nx ;
- les règles de calcul du théorème 18 s'écrivent alors, pour tout $(p,q) \in \mathbb{N}^2$ (ou $\mathbb{Z}^2$ si x admet un opposé),

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

1.2 Construction de lois

Définition 20 – Partie stable, loi induite

Soit $(E,*)$ un magma. Une partie F de E est dite *stable par* $*$ lorsque

$$\forall (x,y) \in F^2, \quad x * y \in F.$$

Le cas échéant, la loi de composition interne définie dans F par $\left|\begin{array}{ccc} F^2 & \longrightarrow & F \\ (x,y) & \longmapsto & x*y \end{array}\right.$ est appelée *loi induite* par $*$ dans F, on la note $*$ aussi.

La loi induite dans F hérite naturellement des propriétés de $*$ (associativité, commutativité, ...). En particulier, si $(E,*)$ possède un élément neutre e ET si $e \in F$, alors e est le neutre du magma induit $(F,*)$.

✖ ATTENTION ! ✖ Un élément x du magma induit $(F,*)$ peut être un élément inversible dans $(E,*)$ mais dont l'inverse n'est pas dans F, auquel cas x n'est pas inversible dans $(F,*)$.

Exemple 21

- Dans $\mathbb{C}$, l'ensemble $\mathbb{U}$ des nombres complexes de module 1 est stable par $\times$.
- Dans $\mathbb{Z}$, $\mathbb{N}$ est stable par $+$ et $\times$, mais pas par $-$. Par ailleurs, les entiers naturels non nuls sont inversibles dans $(\mathbb{Z},+)$ mais pas dans le magma induit $(\mathbb{N},+)$.
- Dans $\mathbb{N}$, $\mathbb{N}^*$ est stable par $+$, mais le magma $(\mathbb{N}^*,+)$ n'est pas unifère.
- Soit $A \subsetneq E$ une partie stricte de E. Dans $(\mathscr{P}(E),\cap)$, E est l'élément neutre, en revanche le neutre pour la loi induite sur la partie stable $\mathscr{P}(A)$ est A.

Définition 22 – Loi produit

Soit $(E,*_E)$ et $(F,*_F)$ deux magmas. La *loi produit* $*_{E\times F}$ *dans* $E\times F$ est définie par

$$\forall (x,y),(x',y') \in E\times F, \quad (x,y) *_{E\times F} (x',y') = (x *_E x', y *_F y').$$

À nouveau, la loi produit $*_{E\times F}$ hérite des propriétés communes des lois $*_E$ et $*_F$ (associativité, commutativité, ...). En particulier, si $(E,*_E)$ et $(F,*_F)$ sont unifères, de neutres respectifs e et f, alors (e,f) est le neutre du magma produit $(E\times F, *_{E\times F})$. En outre, un élément (x,y) de $E\times F$ est inversible si et seulement si x et y le sont dans $(E,*_E)$ et $(F,*_F)$ respectivement et, le cas échant, $(x,y)^{-1} = \left(x^{-1},y^{-1}\right)$.

Exemple 23

- On peut ainsi définir une addition dans $\mathbb{R}^2$ à partir de celle dans $\mathbb{R}$ en posant

$$(x_1,x_2)+(y_1,y_2) = (x_1+y_1, x_2+y_2).$$

- La loi produit dans $\mathbb{R}_+^* \times \mathbb{R}$, avec $\left(\mathbb{R}_+^*,\times\right)$ et $(\mathbb{R},+)$, est donnée par $\quad (r,\theta) * (r',\theta') = (rr', \theta+\theta')$.

Le procédé de la définition 22 se généralise à un produit fini quelconque de magmas, ce qui permet par exemple de définir une addition dans $\mathbb{R}^n$ $(n \geqslant 2)$:

$$(x_1,\dots,x_n)+(y_1,\dots,y_n) = (x_1+y_1,\dots,x_n+y_n).$$

Définition 24 – Loi dans E^X

Soit $(E, *)$ un magma et X un ensemble. On définit dans E^X une loi de composition interne, encore notée $*$ par abus, par

$$\forall f, g \in E^X, \quad \forall x \in X, \quad (f * g)(x) = f(x) * g(x).$$

La loi $*$ dans E^X hérite alors des propriétés de la loi $*$ dans E (associativité, commutativité, ...). Par exemple, si $(E, *)$ est unifère, de neutre e, alors $\left(E^X, *\right)$ possède un élément neutre donné par

$$X \longrightarrow E, x \longmapsto e.$$

En outre, un élément $f \in E^X$ est inversible si et seulement si $f(x)$ est inversible dans $(E, *)$, pour tout $x \in X$, et, le cas échéant, son inverse est donné par

$$X \longrightarrow E, x \longmapsto f(x)^{-1}.$$

La définition précédente généralise le cas bien connu des fonctions numériques (définition 2 du chapitre 4) rappelée ci-après.

Exemple 25 – Opérations sur les fonctions numériques

Les lois d'addition et de multiplication dans $\mathbb{K}$, avec $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$, permettent de définir la somme et le produit de deux éléments de $\mathbb{K}^X$:

$$\forall x \in X, \quad (f + g)(x) = f(x) + g(x) \quad \text{et} \quad (f \times g)(x) = f(x)g(x).$$

- Les lois $+$ et $\times$ sont associatives et commutatives et $\times$ est distributive par rapport à $+$, à l'instar des lois dans $\mathbb{K}$.
- L'élément neutre pour l'addition est la fonction nulle et tout élément f admet pour opposé l'application

$$-f : x \longmapsto -f(x).$$

- L'élément neutre pour la multiplication est la fonction constante égale à 1 et une fonction f est inversible pour la multiplication si et seulement si elle ne s'annule pas sur X, le cas échéant son inverse est l'application

$$\frac{1}{f} : x \longmapsto \frac{1}{f(x)}.$$

2 Structure de groupes

Cette section est dévolue à la présentation de la première structure algébrique fondamentale : la structure de groupe.

2.1 Définitions et exemples fondamentaux

Définition 26 – Groupe (abélien)

On appelle groupe tout magma associatif, unifère et dans lequel tout élément est inversible.
Un groupe est dit *commutatif* (ou *abélien*[†]) lorsque sa loi est commutative.

Remarque 27

- L'ensemble sous-jacent à un groupe est nécessairement non vide, puisqu'il contient au moins l'élément neutre.
- Dans un groupe, tout élément est régulier, dans la mesure où il est inversible (point **(iv)** du théorème 15) !
- Par abus de langage et lorsqu'il n'y a pas d'ambiguïté, on dit souvent « soit G un groupe » sans préciser la notation de sa loi. Par convention, on note alors généralement multiplicativement la loi de G et on se contente même de noter xy le produit de deux éléments x et y.

Exemple 28 – Exemples usuels Les magmas additifs $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, et les magmas multiplicatifs $(\mathbb{Q}^*, \times)$, $(\mathbb{Q}_+^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{R}_+^*, \times)$ et $(\mathbb{C}^*, \times)$ sont des groupes abéliens.

†. Niels Henrik Abel (1802 à Finnoy – 1829 à Froland) est un mathématicien norvégien. Il est connu pour ses travaux en analyse mathématique sur la semi-convergence des séries numériques, des suites et séries de fonctions, sur la notion d'intégrale elliptique, et en algèbre sur la résolution des équations.

Exemple 29 – Groupe des permutations d'un ensemble Soit E un ensemble non vide.
On appelle *permutation de* E toute bijection de E sur E et on note $\mathfrak{S}(E)$ (ou S_E) l'ensemble des permutations de E. Le magma $(\mathfrak{S}(E), \circ)$ des permutations d'un ensemble E non vide est un groupe. Il est abélien si et seulement si le cardinal de E est inférieur ou égal à 2.

Les théorèmes suivants énoncent que certains ensembles héritent naturellement d'une structure de groupe.

Théorème 30 – Groupe produit

Si G et G' sont deux groupes, alors $G \times G'$ muni de la loi produit est un groupe (cf. définition 22). Par ailleurs, le groupe $G \times G'$ est abélien si et seulement si G et G' le sont.
Cette notion de groupe produit s'étend naturellement à un produit d'un nombre fini de groupes.

Démonstration. L'élément neutre est (e, e'), avec e et e' les neutres respectifs de G et G', et l'inverse de $(x, y) \in G \times G'$ est (x^{-1}, y^{-1}). ■

Théorème 31 – Structure de groupe sur l'ensemble des fonctions à valeurs dans un groupe

Si G est un groupe et X un ensemble non vide, alors G^X est un groupe pour la loi induite par celle de G (cf. définition 24). Par ailleurs, le groupe G^X est abélien si et seulement si G l'est.

Démonstration. Le neutre est l'application constante $x \longmapsto e$, où e est le neutre de G, et l'inverse de $f \in G^X$ est l'application $x \longmapsto f(x)^{-1}$. ■

Théorème 32 – Groupe des éléments inversibles

Soit $(E, *)$ un magma associatif et unifère, de neutre e. Le sous-ensemble I des éléments inversibles de $(E, *)$ est un groupe pour la loi induite par $*$.

Démonstration. Le point **(iii)** du théorème 15 signifie que I est stable par $*$, le magma $(I, *)$ muni de la loi induite est alors associatif, à l'instar de $(E, *)$. Par ailleurs, $e \in I$ (point **(i)** du théorème 15) et est donc l'élément neutre de $(I, *)$. Enfin, le point **(ii)** du théorème 15 montre que tout élément de I admet un inverse DANS I. ■

Exemple 33

- $(\mathbb{N}, +)$, $(\mathbb{R}, \times)$ et $(\mathbb{Z}^*, \times)$ ne sont pas des groupes, car ils possèdent des éléments non inversibles.
- Le magma $(E^E, \circ)$ n'est pas un groupe dès que E possède au moins deux éléments, dans la mesure où une application constante ne saurait être inversible (*i.e.* bijective). En revanche, $(\mathfrak{S}(E), \circ)$ en est le groupe des éléments inversibles (cf. exemple 29) !
- $(\mathscr{P}(E), \cap)$ (resp. $(\mathscr{P}(E), \cup)$) n'est pas un groupe dès que E est non vide, dans la mesure où $\varnothing$ (resp. E) n'est pas inversible. En revanche, $(\mathscr{P}(E), \Delta)$ est un groupe abélien de neutre $\varnothing$ (exercice 31).

2.2 Sous-groupes

Définition 34 – Sous-groupe

Soit $(G, *)$ un groupe et H une partie de G stable par la loi $*$. On dit que H est un sous-groupe de G lorsque H est un groupe pour la loi induite par celle de G.

Par définition, un sous-groupe est un groupe dans un autre groupe, pour la même loi.

Théorème 35 – Élément neutre et inverse dans un sous-groupe

Soit G un groupe d'élément neutre e et H un sous-groupe de G.

(i) $e \in H$. **(ii)** H est stable par inversion : $\forall h \in H, \quad h^{-1} \in H$.

Démonstration. ... ■

Ainsi un groupe et l'un quelconque de ses sous-groupes ont le même élément neutre et tout élément du sous-groupe a le même inverse dans le groupe et dans le sous-groupe.

Remarque 36 La relation « être un sous-groupe » est une relation transitive sur tout ensemble de groupes.

Exemple 37 – Sous-groupes triviaux G et $\{e\}$ sont des sous-groupes du groupe $(G,*)$, qualifiés de *triviaux*.

Exemple 38

- $(\mathbb{Z},+)$ est un sous-groupe de $(\mathbb{Q},+)$, qui lui-même un sous-groupe de $(\mathbb{R},+)$, qui lui-même un sous-groupe de $(\mathbb{C},+)$. De même $(\mathbb{Q}^*,\times)$ est un sous-groupe de $(\mathbb{R}^*,\times)$, qui lui-même un sous-groupe de $(\mathbb{C}^*,\times)$.
- En revanche, $(\mathbb{N},+)$ n'est pas un sous-groupe de $(\mathbb{Z},+)$.
- $\mathbb{R}_+^*$ est un sous-groupe de $(\mathbb{R}^*,\times)$ mais pas de $(\mathbb{R},+)$.
- Pour toute partie A d'un ensemble E, $(\mathscr{P}(A),\Delta)$ est un sous-groupe de $(\mathscr{P}(E),\Delta)$.

Théorème 39 – Caractérisations des sous-groupes

Soit G un groupe d'élément neutre e et H une partie de G. Les assertions suivantes sont équivalentes :

(i) H est un sous-groupe de G.

(ii) $e\in H$, H est stable par produit et H est stable par passage à l'inverse, *i.e.*

$$\forall x,y\in H,\quad xy\in H \qquad \text{et} \qquad \forall x\in H,\quad x^{-1}\in H.$$

(iii) H est non vide et, pour tous $x,y\in H$, $xy^{-1}\in H$.

En notation additive, l'assertion **(iii)** s'écrit « H est non vide et, pour tous $x,y\in H$, $x-y\in H$ ».

Démonstration. ... ∎

✎ **En pratique** ✎

- Pour montrer qu'une partie d'un groupe en est un sous-groupe, on utilisera toujours l'une des caractérisations précédentes, en lieu et place de la définition qui nous obligerait à revenir sur l'associativité et l'inversibilité.
- Pour montrer qu'un ensemble peut être muni d'une structure de groupe, il est commode de montrer qu'il s'agit d'un sous-groupe d'un groupe connu. D'où l'importance des groupes usuels de l'exemple 28 et de l'exemple ci-après.

Exemple 40 – Exemples usuels (suite)

- L'ensemble $\mathbb{U}$ des nombres complexes de module 1 et l'ensemble $\mathbb{U}_n$ des racines n^{es} de l'unité sont des sous-groupes de $(\mathbb{C}^*,\times)$ et donc des groupes. Remarquons que les groupes $\mathbb{U}_n$ sont aussi des sous-groupes de $\mathbb{U}$.
- En particulier, $\mathbb{U}_2=\{\pm 1\}$ est un sous-groupe de $(\mathbb{Q}^*,\times)$, $(\mathbb{R}^*,\times)$ et $(\mathbb{C}^*,\times)$

Exemple 41 – Sous-groupes de $\mathbb{Z}$ (à connaître) Les sous-groupes de $\mathbb{Z}$ sont exactement les $a\mathbb{Z}$, avec $a\in\mathbb{Z}$.

2.3 Morphismes de groupes

Définition 42 – Morphisme de groupes

Soit $(G,*)$ et $(G',*')$ deux groupes. On appelle *morphisme (de groupes) de G dans G'* toute application $f:G\longrightarrow G'$ telle que

$$\forall (x,y)\in G^2,\quad f(x*y)=f(x)*'f(y).$$

Lorsque $G'=G$, on dit plutôt que f est un *endomorphisme (de groupe) de G*.

Exemple 43 Toute phrase du genre « le machin des trucs est égal au bidule des machins » signale la présence d'un morphisme de groupes.

- La fonction module $z\longmapsto |z|$ est un endomorphisme du groupe $(\mathbb{C}^*,\times)$, car le module d'un produit est égal au produit des modules.
- L'exponentielle complexe est un morphisme de groupes de $(\mathbb{C},+)$ dans $(\mathbb{C}^*,\times)$ (et aussi de $(\mathbb{R},+)$ dans $\left(\mathbb{R}_+^*,\times\right)$), dans la mesure où l'exponentielle d'une somme est égal au produit des exponentielles. De la même manière, le logarithme est un morphisme de groupes de $(\mathbb{R}_+^*,\times)$ dans $(\mathbb{R},+)$, puisque le logarithme d'un produit est égal à la somme des logarithmes.

Exemple 44

- L'application qui envoie tous les éléments d'un groupe G sur l'élément neutre d'un groupe G' est un morphisme de groupes, dit *morphisme trivial*.
- Pour tout groupe G, l'application identité Id_G est un endomorphisme de G.
- Soit $n \in \mathbb{Z}$. L'application $x \longmapsto nx$ est un endomorphisme du groupe $\mathbb{Z}$.
- Plus généralement, pour tous groupe abélien $(G,+)$ et $n \in \mathbb{N}$, l'application $x \longmapsto nx$ est un endomorphisme du groupe G.
- Soit $(G,*)$ un groupe et $x \in G$. La règle de calcul $x^p * x^q = x^{p+q}$ sur les itérés (cf. théorème 18) équivaut à dire que l'application $n \longmapsto x^n$ est un morphisme de $(\mathbb{Z},+)$ dans $(G,*)$.

Théorème 45 – Propriétés des morphismes de groupes

- Soit G et G' deux groupes d'éléments neutres respectifs e et e' et $f : G \longrightarrow G'$ un morphisme de groupes. Alors
  (i) $f(e) = e'$. **(ii)** $\forall x \in G,\quad f\left(x^{-1}\right) = f(x)^{-1}$. **(iii)** $\forall x \in G,\quad \forall n \in \mathbb{Z},\quad f(x^n) = f(x)^n$.
- **Composition.** Soit G, G' et G" trois groupes. Si $f : G \longrightarrow G'$ et $g : G' \longrightarrow G''$ sont deux morphismes de groupes, alors $g \circ f$ est un morphismes de groupes de G dans G''.
- **Images directe et réciproque d'un sous-groupe.** Soit G et G' deux groupes et $f : G \longrightarrow G'$ un morphisme de groupes.
  × Pour tout sous-groupe H de G, $f(H)$ est un sous-groupe de G'.
  × Pour tout sous-groupe H' de G', $f^{-1}(H')$ est un sous-groupe de G.

Démonstration. ... ∎

✎ **En pratique** ✎ Avec les notations du théorème, si $f(e) \neq e'$, alors f ne saurait être un morphisme de groupes.

Exemple 46 Dans le cas particulier de la fonction logarithme, on obtient ses propriétés algébriques bien connues :

$$\ln 1 = 0, \qquad \forall x \in \mathbb{R}_+^*,\quad \ln\left(\frac{1}{x}\right) = -\ln x \qquad \text{et} \qquad \forall x \in \mathbb{R}_+^*,\quad \forall n \in \mathbb{Z},\quad \ln(x^n) = n \ln x.$$

Définition-théorème 47 – Image et noyau d'un morphisme de groupes

Soit G et G' deux groupes d'éléments neutres respectifs e et e' et $f : G \longrightarrow G'$ un morphisme de groupes.

- **Image.** L'image de f, notée $\mathrm{Im}\, f$, est le sous-groupe $f(G)$ de G'.
  En outre, f est surjectif de G sur G' si et seulement si $\mathrm{Im}\, f = G'$.
- **Noyau.** Le *noyau de* f est le sous-groupe de G défini par

$$\mathrm{Ker}\, f = f^{-1}\left(\{e'\}\right) = \left\{x \in G \;\middle|\; f(x) = e'\right\}.$$

  En outre, f est injectif sur G si et seulement si $\mathrm{Ker}\, f = \{e\}$, ce qui équivaut à

$$\forall x \in G,\quad f(x) = e' \implies x = e.$$

Démonstration. ... ∎

Exemple 48

- Le morphisme trivial $x \longmapsto e'$ de G dans G' a pour noyau G et pour image $\{e'\}$.
- Soit $(G,*)$ un groupe et $x \in G$. Puisque $f : n \longmapsto x^n$ est un morphisme de $(\mathbb{Z},+)$ dans $(G,*)$ (exemple 44), l'ensemble des itérés de x qui n'est autre que $\mathrm{Im}\, f$ est un sous-groupe de G.
- L'exponentielle imaginaire $\theta \longmapsto \mathrm{e}^{i\theta}$ est un morphisme surjectif de $\mathbb{R}$ sur $\mathbb{U}$ de noyau $\left\{\theta \in \mathbb{R} \;\middle|\; \mathrm{e}^{i\theta} = 1\right\} = 2\pi\mathbb{Z}$ (théorème 28 du chapitre 6).
- L'application $(\rho,\theta) \longmapsto \rho\,\mathrm{e}^{i\theta}$ est un morphisme surjectif du groupe $(\mathbb{R}_+^*,\times) \times (\mathbb{R},+)$ sur le groupe $(\mathbb{C}^*,\times)$, de noyau $\{1\} \times 2\pi\mathbb{Z}$ (théorème 39 du chapitre 6).

Exemple 48 – (suite)

- L'exponentielle complexe $z \longmapsto \mathrm{e}^z$ est un morphisme surjectif de $\mathbb{C}$ sur $\mathbb{C}^*$ de noyau $\{z \in \mathbb{C} \mid \mathrm{e}^z = 1\} = 2i\pi\mathbb{Z}$ (théorème 50 du chapitre 6).
- L'endomorphisme $z \longmapsto |z|$ de $\mathbb{C}^*$ a pour image $\mathbb{R}_+^*$ et pour noyau $\{z \in \mathbb{C}^* \mid |z| = 1\} = \mathbb{U}$, ce qui au passage donne une nouvelle démonstration du fait que $\mathbb{U}$ soit un sous-groupe de $\mathbb{C}^*$.
- Soit $n \in \mathbb{N}^*$. L'endomorphisme $z \longmapsto z^n$ de $\mathbb{C}^*$ est surjectif et a pour noyau $\{z \in \mathbb{C}^* \mid z^n = 1\} = \mathbb{U}_n$ (théorème 54 du chapitre 6), ce qui au passage donne une nouvelle démonstration du fait que $\mathbb{U}_n$ soit un sous-groupe de $\mathbb{C}^*$.
- Soit $n \in \mathbb{N}^*$ et $\zeta = \mathrm{e}^{2i\pi/n}$. Le morphisme de groupe $k \longmapsto \zeta^k$ de $\mathbb{Z}$ dans $\mathbb{C}^*$ a pour image $\mathbb{U}_n$ et pour noyau

$$\left\{k \in \mathbb{Z} \,\middle|\, \zeta^k = 1\right\} = \left\{k \in \mathbb{Z} \,\middle|\, \frac{2k\pi}{n} \equiv 0\,[2\pi]\right\} = \{k \in \mathbb{Z} \mid k \equiv 0\,[n]\} = n\mathbb{Z}.$$

Définition 49 – Isomorphisme de groupes

Soit G et G' deux groupes.

- **Isomorphisme de groupes.** On appelle *isomorphisme (de groupes) de G sur G'* tout morphisme de groupes bijectif de G sur G'. Lorsque $G' = G$, un tel morphisme est appelé un *automorphisme (de groupe) de G*.
- **Groupes isomorphes.** Le groupe G' est dit *isomorphe* au groupe G lorsqu'il existe un isomorphisme de groupes de G sur G', ce que l'on note $G' \simeq G$.

Dans le contexte des structures algébriques, on s'intéresse aux relations qu'entretiennent les objets vis-à-vis de la loi de composition interne, tandis que la nature des objets eux-mêmes importe peu. Ainsi, deux groupes isomorphes sont totalement identiques du point de vue de leur structure de groupe : un isomorphisme entre ses deux groupes transforme toute relation entre des éléments de l'un des groupes en une relation identique entre des éléments de l'autre groupe. Deux groupes isomorphes peuvent donc être confondus, même si du point de vue ensembliste leurs éléments n'ont rien en commun.

Exemple 50

- Soit G un groupe, l'identité Id_G est un automorphisme du groupe G.
- L'application $(\rho, u) \longmapsto \rho u$ est un isomorphisme de groupes de $(\mathbb{R}_+^*, \times) \times (\mathbb{U}, \times)$ sur $(\mathbb{C}^*, \times)$, de réciproque $z \longmapsto (|z|, z/|z|)$.
- Pour tout $\alpha \in \mathbb{R}^*$, la fonction puissance $x \longmapsto x^\alpha$ est un automorphisme de $\mathbb{R}_+^*$, de réciproque $x \longmapsto x^{1/\alpha}$.

Théorème 51 – Propriétés des isomorphismes de groupes

- **Composition.** La composée de deux isomorphismes de groupes est un isomorphisme de groupes.
- **Réciproque.** La réciproque d'un isomorphisme de groupes est un isomorphisme de groupes.
- **Relation d'équivalence.** La relation d'isomorphisme $\simeq$ est une relation d'équivalence sur tout ensemble de groupes.†

Démonstration. ... ∎

La propriété de symétrie d'une relation d'équivalence nous autorise alors à écrire « G et G' sont isomorphes » en lieu et place de « G' est isomorphe à G ».

Exemple 52 La fonction logarithme est un isomorphisme de $\left(\mathbb{R}_+^*, \times\right)$ sur $(\mathbb{R}, +)$, de réciproque la fonction exponentielle qui est un isomorphisme de $(\mathbb{R}, +)$ sur $\left(\mathbb{R}_+^*, \times\right)$. En particulier, les groupes $\mathbb{R}$ et $\mathbb{R}_+^*$ sont isomorphes.

Exemple 53 – Groupe des automorphismes d'un groupe Soit G un groupe.
L'ensemble $\mathrm{Aut}(G)$ des automorphismes de groupe de G est un groupe pour la composition.

†. Les limitations de la théorie des ensembles n'autorisent pas à considérer « l'ensemble des groupes ».

3 Structures d'anneaux et de corps

Nous poursuivons notre périple parmi les structures algébriques avec deux nouvelles structures fondamentales : les structures d'anneaux et de corps.

3.1 Anneaux

Définition 54 – Anneau

On appelle *anneau* tout triplet $(A, +, \times)$ constitué d'un ensemble A et de deux lois de composition internes dans A (une loi $+$ appelée *addition* et une loi $\times$ appelée *multiplication*) vérifiant les conditions suivantes :

(i) $(A, +)$ est un groupe abélien, dont l'élément neutre est généralement noté 0_A ou 0 ;

(ii) $(A, \times)$ est un magma associatif unifère, dont l'élément neutre est généralement noté 1_A ou 1 ;

(iii) la multiplication $\times$ est distributive par rapport à l'addition $+$.

En outre, l'anneau $(A, +, \times)$ est dit *commutatif* lorsque le magma $(A, \times)$ l'est.

Notation 55

- À l'instar des groupes, on allège souvent les notations : quand on écrit « Soit A un anneau », il est sous-entendu que l'addition est notée $+$ et la multiplication $\times$, ce dernier symbole étant souvent omis dans les calculs.
- On note $n.a$ ou na, avec $a \in A$ et $n \in \mathbb{Z}$, l'itéré additif et a^n, avec $a \in A$ et $n \in \mathbb{N}$ (ou $\mathbb{Z}$ si a est inversible), l'itéré multiplicatif. On a donc $a^0 = 1$, pour tout $a \in A$, et en particulier $0^0 = 1$.

Exemple 56 – Exemples usuels $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des anneaux commutatifs.

À l'instar de la structure de groupe, certains ensembles héritent naturellement d'une structure d'anneau.

Théorème 57 – Anneau produit, anneau A^X

- **Anneau produit.** Si A et B sont deux anneaux, alors $A \times B$ muni des lois produits est un anneau (cf. définition 22). En particulier, $(0_A, 0_B)$ (resp. $(1_A, 1_B)$) est le neutre pour l'addition (resp. la multiplication).
- **Anneau A^X.** Si A est un anneau et X un ensemble non vide, les propriétés des magmas $(A, +)$ et $(A, \times)$ se transmettent naturellement aux magmas $(A^X, +)$ et $(A^X, \times)$ (cf. définition 24 et théorème 31), ainsi A^X est muni d'une structure d'anneau.

Exemple 58

- $(\mathbb{K}^{\mathbb{R}}, +, \times)$ est un anneau, qui plus est commutatif, à l'instar de $\mathbb{K}$, avec $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$.
- Si E est un ensemble non vide, alors $(\mathscr{P}(E), \Delta, \cap)$ et $(\mathscr{P}(E), \Delta, \cup)$ sont des anneaux commutatifs (exercice 31).
- Si $(G, +)$ est un groupe abélien, alors l'ensemble des endomorphismes de G muni de l'addition et de la composition des applications est un anneau, non commutatif en général.

Théorème 59 – Règles de calcul dans un anneau

Soit A un anneau et $a, b \in A$.

(i) 0 est absorbant. $a \times 0_A = 0_A \times a = 0_A$.

(ii) Règles des signes. $-(ab) = (-a)b = a(-b)$ et $(-a)(-b) = ab$. En particulier, $(-1_A)^2 = 1_A$.

(iii) Itéré additif. Pour tout $n \in \mathbb{Z}$, $n(ab) = (na)b = a(nb)$.

(iv) Formule du binôme et identité de Bernoulli. Pour tout $n \in \mathbb{N}$, si a et b COMMUTENT, *i.e.* $ab = ba$,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \qquad \text{et} \qquad a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^k b^{n-k-1}.$$

En particulier, ces identités sont vraies pour tous éléments a et b d'un anneau commutatif.

Démonstration. ... ∎

✖ ATTENTION ! ✖ Dans **(iv)**, l'hypothèse $ab = ba$ est cruciale, comme le montre déjà le cas $n = 2$:

$$(a+b)^2 = (a+b)(a+b) = a^2 + ab + ba + b^2 \underset{ab=ba}{=} a^2 + 2ab + b^2 \quad \text{et} \quad (a-b)(a+b) = a^2 + ab - ba - b^2 \underset{ab=ba}{=} a^2 - b^2.$$

Anneaux intègres Peut-on avoir $0_A = 1_A$ dans un anneau ? Le cas échant, pour tout $a \in A$,

$$a = a \times 1_A = a \times 0_A = 0_A,$$

ainsi $A = \{0_A\}$ (on parle d'*anneau nul*) et cet anneau est d'un intérêt assez limité. †

Définition 60 – Diviseur de zéro, anneau intègre

- Soit A un anneau. Un élément a de A est appelé un *diviseur de* 0 lorsque

$$a \neq 0_A \qquad \text{et} \qquad \exists b \in A\backslash\{0_A\}, \quad ab = 0_A \quad \text{ou} \quad ba = 0_A.$$

- Un anneau A est dit *intègre* lorsqu'il est commutatif, différent de $\{0_A\}$ et sans diviseur de 0. Ce dernier point équivaut alors à chacune des assertions suivantes :

(i) $\forall a, b \in A, \quad ab = 0_A \implies (a = 0_A \text{ ou } b = 0_A)$; **(ii)** $\forall a, b \in A, \quad (a \neq 0_A \text{ et } b \neq 0_A) \implies ab \neq 0_A$.

Dans un anneau intègre, on retrouve ainsi la propriété usuelle de $\mathbb{R}$ et $\mathbb{C}$ énonçant qu'un produit ne peut être nul que si l'un de ses facteurs l'est.

✖ **Attention !** ✖ Tout anneau n'est pas intègre ! Ainsi, dans un anneau quelconque, on veillera à ne pas utiliser automatiquement les règles

$$ax = ay \implies a = 0_A \text{ ou } x = y \qquad \text{et} \qquad a^2 = b^2 \implies a = b \text{ ou } a = -b,$$

qui sont a priori fausses.

Exemple 61

- Les anneaux $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont intègres.
- L'anneau produit $\mathbb{R}^2$ n'est pas intègre, dans la mesure où $(1, 0) \times (0, 1) = (0, 0)$. Plus généralement, un produit d'anneaux intègres n'est pas intègre.
- Si X est un ensemble ayant au moins deux éléments, alors l'anneau $\left(\mathbb{R}^X, +, \times\right)$ n'est pas intègre, dans la mesure où l'on peut trouver deux applications non nulles de X dans $\mathbb{R}$ telles qu'en tout point de X l'une ou l'autre soit nulle. Nous avions notamment mentionné cette difficulté au chapitre 3 lors de la manipulation des fonctions indicatrices des parties d'un ensemble : l'implication « $\mathbb{1}_A \mathbb{1}_B = 0_{\mathbb{R}^X} \implies (\mathbb{1}_A = 0_{\mathbb{R}^X} \text{ ou } \mathbb{1}_A = 0_{\mathbb{R}^X})$ » est fausse.
- Les éléments réguliers d'un anneau (sous-entendu pour $\times$) ne sont pas des diviseurs de 0.

Définition 62 – Élément nilpotent d'un anneau, indice de nilpotence

Soit A un anneau. Un élément a de A est dit *nilpotent* lorsqu'il existe un entier $k \in \mathbb{N}^*$ tel que $a^k = 0_A$.
Le cas échéant, l'entier $\min\left\{k \in \mathbb{N}^* \;\middle|\; a^k = 0_A\right\}$ est appelé l'*indice de nilpotence de* a.

Remarque 63

- Dans un anneau intègre A, l'élément nul 0_A est l'unique élément nilpotent.
- Si x est un élément nilpotent d'un anneau A tel que $x^n = 0_A$, avec $n \in \mathbb{N}^*$, alors $x^k = 0_A$, pour tout $k \geqslant n$.
  En effet, pour tout $k \geqslant n$, $k - n \in \mathbb{N}$ et

$$x^k = x^n \times x^{k-n} = 0_A \times x^{k-n} = 0_A.$$

Éléments inversibles d'un anneau Par définition, tout anneau est en particulier un groupe (abélien) pour sa loi additive, ainsi lorsque l'on considère la notion d'éléments inversibles d'un anneau cela se réfère toujours aux éléments inversibles pour la multiplication (cette notion étant triviale pour la loi additive).

Définition-théorème 64 – Groupe des inversibles d'un anneau

Soit A un anneau. L'ensemble des éléments inversibles de A est un groupe pour la multiplication, souvent noté $A^\times$ ou $\mathrm{U}(A)$. ‡

Démonstration. Le théorème 32 s'applique au magma associatif unifère $(A, \times)$. ∎

†. Conformément au programme, tous les anneaux considérés dans le cadre du cours sont réputés *unitaires*, *i.e.* $1_A \neq 0_A$.
‡. $\mathrm{U}(A)$ pour *groupe des unités de* A.

Exemple 65

- $\mathrm{U}(\mathbb{Z}) = \{-1, 1\}$, $\mathrm{U}(\mathbb{Q}) = \mathbb{Q}^*$, $\mathrm{U}(\mathbb{R}) = \mathbb{R}^*$ et $\mathrm{U}(\mathbb{C}) = \mathbb{C}^*$.
- Le groupe des inversibles de A^X est l'ensemble des fonctions définies sur X et à valeurs dans $U(A)$, où X est un ensemble non vide et A un anneau (cf. les commentaires qui suivent la définition 24).

3.2 Sous-anneaux

Définition 66 – Sous-anneau

Soit A un anneau et B une partie de A stable par addition et multiplication. On dit que B est un sous-anneau de A lorsque

(i) $1_A \in B$; **(ii)** B est un anneau pour les lois induites par celles de A.

Exemple 67

- Tout anneau A est un sous-anneau de lui-même.
- $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$, qui est lui-même un sous-anneau de $\mathbb{R}$, qui est lui-même un sous-anneau de $\mathbb{C}$.

Remarque 68

- Si B est un sous-anneau de l'anneau A, alors 0_A est automatiquement un élément de B.

  En effet, B est alors un sous-groupe du groupe A (cf. théorème 35).
- À nouveau, la relation « être un sous-anneau » est une relation transitive sur tout ensemble d'anneaux.

Théorème 69 – Caractérisation des sous-anneaux

Soit A un anneau et B une partie de A. Les assertions suivantes sont équivalentes

(i) B est un sous-anneau de A.

(ii)
- $1_A \in B$;
- B est stable par différence : $\forall b, b' \in B, \quad b - b' \in B$;
- B est stable par produit : $\forall b, b' \in B, \quad bb' \in B$.

Démonstration. Exercice. ∎

✎ **En pratique** ✎ À l'instar de la structure de groupe, on privilégiera cette caractérisation pour établir qu'une partie d'un anneau en est un sous-anneau et on montrera en priorité qu'un ensemble est muni d'une structure d'anneau en le faisant apparaitre comme le sous-anneau d'un anneau de référence.

Exemple 70 Les ensembles $\mathscr{C}(I, \mathbb{K})$, $\mathscr{D}^k(I, \mathbb{K})$ (avec $k \in \mathbb{N}^*$) et $\mathscr{D}^\infty(I, \mathbb{K})$ sont des sous-anneaux de $\mathbb{R}^I$, où I est un intervalle et $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$.

En effet, on a bien sûr $\mathscr{C}(I, \mathbb{K}) \subset \mathbb{K}^I$. En outre, la fonction constante égale à 1 est continue sur I. Enfin, il est connu que la différence et le produit de deux fonctions continues le sont. On procède *mutatis mutandis* dans les autres cas.

Remarque 71 – Inversibles d'un sous-anneau Soit A un anneau et B un sous-anneau de A.
Quel lien y a-t-il entre $\mathrm{U}(A)$ et $\mathrm{U}(B)$?

- Tout élément de $\mathrm{U}(B)$ est inversible dans B, *i.e.* possède un inverse dans B, donc a fortiori dans A. Ainsi $\mathrm{U}(B) \subset \mathrm{U}(A) \cap B$.
- Mais l'inclusion réciproque est fausse. En effet, il ne suffit pas pour un élément de B d'être inversible dans A pour admettre un inverse dans B. Par exemple, pour $A = \mathbb{R}$ et $B = \mathbb{Z}$, on a $\mathrm{U}(\mathbb{Z}) = \{-1, 1\}$ et $\mathrm{U}(\mathbb{R}) \cap \mathbb{Z} = \mathbb{Z}^*$.

3.3 Structure de corps

Définition 72 – Corps

Un triplet $(\mathbb{K}, +, \times)$ est un *corps* lorsque $(\mathbb{K}, +, \times)$ est un anneau commutatif non réduit à $\{0\}$ et dont tous les éléments non nuls sont inversibles (pour la multiplication), *i.e.* dont le groupe des unités vérifie $\mathrm{U}(\mathbb{K}) = \mathbb{K}\backslash\{0\}$.

Dans un anneau, on ne peut pas diviser impunément par un élément non nul, qui n'a aucune raison d'être inversible a priori. En revanche, dans un corps, tout élément non nul étant inversible, on peut additionner, soustraire, multiplier et diviser par n'importe quel élément (sauf 0 pour la division). En particulier, tout corps est un anneau INTÈGRE (tous ses éléments non nuls sont inversibles et donc réguliers).

Exemple 73

- Les anneaux $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps. En revanche, l'anneau $\mathbb{Z}$ n'est pas un corps, puisque $\mathrm{U}(\mathbb{Z}) = \{-1, 1\} \neq \mathbb{Z}^*$.
- L'anneau $\mathbb{R}^X$ n'est pas un corps dès que X contient au moins deux éléments, dans la mesure où cet anneau n'est pas intègre (cf. exemple 61).

Notation 74 Si a et b sont deux éléments d'un corps $\mathbb{K}$, avec b non nul, on peut noter $\dfrac{a}{b}$ l'élément $ab^{-1} = b^{-1}a$ de $\mathbb{K}$. On dispose alors des règles de calcul suivantes (exercice)

$$\frac{a}{b} = \frac{a'}{b'} \iff ab' = a'b, \quad \frac{ax}{bx} = \frac{a}{b}, \quad \frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}, \quad \frac{a}{b} \times \frac{a'}{b'} = \frac{aa'}{bb'} \quad \text{et} \quad \left(\frac{a}{b}\right)^{-1} = \frac{b}{a} (\text{ si } a \neq 0),$$

pour tous $a, b, a', b', x \in \mathbb{K}$, avec $bb'x \neq 0$.

Définition 75 – Sous-corps

Soit $\mathbb{K}$ un corps. On appelle *sous-corps de* $\mathbb{K}$ un sous-anneau de $\mathbb{K}$ qui est un corps.

Exemple 76

- $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$, qui est lui-même un sous-corps de $\mathbb{C}$.
- Si $\mathbb{K}$ est un sous-corps de $\mathbb{C}$, il contient 1 et, par suite, tous les entiers naturels, puis tous les entiers relatifs. Enfin, étant stable par passage à l'inverse, il contient tous les rationnels, soit $\mathbb{Q} \subset \mathbb{K}$. Ainsi $\mathbb{Q}$ est le plus petit (au sens de l'inclusion) sous-corps de $\mathbb{C}$: on dit que $\mathbb{Q}$ est le *sous-corps premier* de $\mathbb{C}$.

Théorème 77 – Caractérisation des sous-corps

Soit $\mathbb{K}$ un coprs et $\mathbb{L}$ une partie de $\mathbb{K}$. Les assertions suivantes sont équivalentes

(i) $\mathbb{L}$ est un sous-corps de $\mathbb{K}$.

(ii)
- $1_{\mathbb{K}} \in \mathbb{L}$;
- $\mathbb{L}$ est stable par différence : $\forall x, x' \in \mathbb{L}, \quad x - x' \in \mathbb{L}$;
- $\mathbb{L}$ est stable par produit : $\forall x, x' \in \mathbb{L}, \quad xx' \in \mathbb{L}$;
- $\mathbb{L}$ est stable par inverse : $\forall x \in \mathbb{L}\backslash\{0_{\mathbb{K}}\}, \quad x^{-1} \in \mathbb{L}$.

Démonstration. Exercice. ∎

3.4 Morphismes d'anneaux

Définition 78 – Morphisme d'anneaux

Soit A et B deux anneaux. On appelle *morphisme (d'anneaux) de A dans B* toute application $f : A \longrightarrow B$ telle que

(i) $f(1_A) = 1_B$; **(ii)** $\forall x, y \in A, \quad f(x + y) = f(x) + f(y)$; **(iii)** $\forall x, y \in A, \quad f(x \times y) = f(x) \times f(y)$.

Les morphismes d'anneaux de $(A, +, \times)$ dans $(B, +, \times)$ sont en particulier des morphismes de groupes de $(A, +)$ dans $(B, +)$. Ils en possèdent donc toutes les propriétés (cf. théorème 45), notamment :

$$f(0_A) = 0_B, \quad f(-x) = -f(x) \quad \text{et} \quad f(nx) = nf(x), \quad \text{pour tous } x \in A \text{ et } n \in \mathbb{Z}.$$

Par ailleurs, même si f n'est pas un morphisme de groupes pour les structures multiplicatives $((A,\times)$ et $(B,\times)$ n'étant même pas des groupes), on a quand même, pour tout $a \in \mathrm{U}(A)$,

$$f(a)f(a^{-1}) = f(aa^{-1}) = f(1_A) = 1_B \quad \text{et} \quad f(a^{-1})f(a) = 1_B,$$

de même, d'où $f(a) \in \mathrm{U}(B)$ et $f(a^{-1}) = f(a)^{-1}$. En résumé, $f|_{\mathrm{U}(A)}$ est un morphisme de groupes de $\mathrm{U}(A)$ dans $\mathrm{U}(B)$.

À l'instar des groupes, on dispose aussi de la terminologie : *endomorphisme d'anneau*, *isomorphisme d'anneaux*, *automorphisme d'anneau* et *anneaux isomorphes*. Enfin, la composée de deux morphismes (resp. isomorphismes) d'anneaux est un morphisme (resp. isomorphisme) d'anneaux, la réciproque d'un isomorphisme est un isomorphisme et l'image directe/réciproque d'un sous-anneau est encore un sous-anneau.

Exemple 79

- L'identité Id_A est un automorphisme de l'anneau A.
- La conjugaison $z \longmapsto \overline{z}$ est un automorphisme de l'anneau $\mathbb{C}$.

  En effet, la conjugaison est une involution, $\overline{1} = 1$ et, pour tous $z, z' \in \mathbb{C}$, $\overline{z+z'} = \overline{z} + \overline{z'}$ et $\overline{zz'} = \overline{z}\,\overline{z'}$.
- Si B est un sous-anneau de A, alors l'*injection canonique* $\left|\begin{array}{ccc} B & \longrightarrow & A \\ x & \longmapsto & x \end{array}\right.$ est un morphisme d'anneaux.
- La fonction nulle sur $\mathbb{R}$ est un morphisme pour les deux lois de l'anneau $\mathbb{R}$, mais n'est pas un morphisme d'anneaux, puisque l'image de 1 est 0 et non 1.

Remarque 80 – Noyau d'un morphisme d'anneaux Soit f un morphisme d'anneaux de A dans B. Dans la mesure où f est en particulier un morphisme de groupes pour les structures additives, on peut considérer son noyau $\mathrm{Ker}\, f = f^{-1}(\{0_B\})$. Ce dernier est un sous-groupe de A, mais n'en est pas un sous-anneau, puisqu'il ne contient pas 1_A. Toutefois, $\mathrm{Ker}\, f$ vérifie aussi la propriété

$$\forall a \in A, \quad \forall x \in \mathrm{Ker}\, f, \quad ax \in \mathrm{Ker}\, f.$$

On dit que $\mathrm{Ker}\, f$ est un *idéal de* A, notion essentielle de la théorie des anneaux qui est esquissée en filière MP.

Notons que l'on conserve l'équivalence : f est injectif si et seulement si son noyau est trivial.

Compétences à acquérir

- Établir qu'une loi est associative/commutative/distributive : exercices 1 à 3, 5, 13 et 14.
- Déterminer les éléments réguliers/inversibles pour une loi : exercices 1, 2, 29 et 32.
- Connaître les groupes/anneaux/corps usuels (exemples 28, 29, 40, 56, 70 et 73).
- Établir qu'un ensemble est un groupe/sous-groupe/anneau/sous-anneau : exercices 5, 7 à 12, 15, 16 et 32.
- Établir qu'une application est un morphisme de groupes/anneaux : exercices 21 et 22.
- Déterminer le noyau d'un morphisme : exercices 21 et 22

Quelques résultats classiques :

- Groupe des automorphismes d'un groupe (exemple 53).
- Intersection et union de sous-groupes (exercice 15).
- Classification des sous-groupes de $\mathbb{Z}$ (exemple 41).
- Sous-groupes de $\mathbb{U}_n$ (exercice 11).
- Classification des sous-groupes additifs de $\mathbb{R}$ (exercice 18).
- Un anneau intègre fini est un corps (exercice 30).
- Éléments nilpotents d'un anneau (exercice 35).
- Transport de structure (exemple 8).
- Sous-groupes des automorphismes intérieurs et centre d'un groupe (exercice 21).
- Théorème de Cayley (exercice 22).
- Différence symétrique de deux ensembles (exercice 31).
- Anneau des entiers de Gauss (exercice 32).