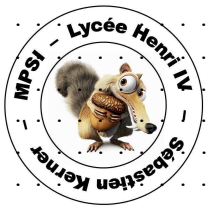
Lycée Henri IV
MPSI

**Cours**
Durée : 11 h

# STRUCTURES ALGÉBRIQUES

Les énoncés et parties suivis du symbole [✠] ne seront pas traités en cours.





# Prérequis

Revoir les chapitres sur :

- les nombres ;
- la théorie des applications ;
- les sommes et produits.

Dans ce cours, les lettres $E$, $F$, $G$, $H$, $A$, $B$, $I$, $K$, ... et $X$ désignent des ensembles (avec $X \neq \varnothing$). La lettre $J$ désigne un ensemble d'indices.

Les trois lettres AQT signifient « Âne Qui Trotte » et sont utilisées pour désigner une démonstration facile laissée au lecteur.

# A. Monoïdes

## A.1. Lois de composition interne

Une opération sur $E$ à valeurs dans $F$ est une application définie sur $E \times E$ dont l'ensemble d'arrivée est $F$. Nous connaissons déjà de nombreux exemples d'opérations comme l'addition et la multiplication dans les nombres réels ; le produit scalaire sur les vecteurs (du plan ou de l'espace) ou encore les relations (qui sont des opérations à valeurs booléennes).

Parmi ces opérations, certaines donnent un résultat dont la nature est différente de celle des objets opérés : ainsi le produit scalaire avale des vecteurs et renvoie un nombre réel. D'autres, au contraire, font opérer des éléments de $E$ pour donner un nouvel élément du même ensemble. On dit alors qu'elles sont internes. Ce sont ces dernières que nous nous proposons d'étudier.

**Définition 1**

Une loi de composition interne (en abrégé : l.c.i.) sur un ensemble $E$ est une application $*$ de $E \times E$ dans $E$, notée

$$\left\{ \begin{array}{ccc} E \times E & \longrightarrow & E \\ (a;b) & \longmapsto & a*b \end{array} \right.$$

Le couple $(E, *)$ est appelé un magma.

Une loi de composition sur $E$ est donc un mécanisme permettant, à partir de deux éléments quelconques $a$ et $b$ de $E$, de fabriquer un troisième élément de $E$, noté $a*b$. Au passage, on notera que la notation $*(a,b)$, habituellement utilisée pour signifier que l'application $*$ agit sur le couple $(a,b)$, est avantageusement remplacée par la notation opératoire $a*b$.

Il est important qu'une loi soit partout définie : le résultat $a*b$ doit avoir un sens quels que soient les éléments $a$ et $b$ de $E$.

Pour définir une loi, on peut se donner une formule ou une table de la loi (si $E$ est fini) :

$$\otimes \left\{ \begin{array}{ccc} ]0;1[\times]0;1[ & \longrightarrow & ]0;1[ \\ (x,y) & \longmapsto & \dfrac{x+y}{1+xy} \end{array} \right.$$

une formule donnant une loi sur $]0;1[$

(il faudrait vérifier qu'elle est interne)

| ↱ | ♣ | ♡ | ♠ |
|---|---|---|---|
| ♣ | ♣ | ♣ | ♡ |
| ♡ | ♡ | ♠ | ♠ |
| ♠ | ♠ | ♡ | ♣ |

une table de loi sur $\{\clubsuit, \heartsuit, \spadesuit\}$

**Exemples :**

- Sur $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, les opérations $+$, $-$ et $\times$ sont internes.
  Sur $\mathbb{Q}^*$, $\mathbb{R}^*$ et $\mathbb{C}^*$, la division $\div$ est une l.c.i.
  Sur $\mathbb{N}$, l'addition et la multiplication sont des l.c.i. mais pas la soustraction ni la division (puisque la différence ou le quotient d'entiers naturels n'est pas nécessairement un entier naturel). La soustraction devient une l.c.i. sur $\mathbb{Z}$ et la division devient une l.c.i. sur $\mathbb{Q}^*$.
- La composition $\circ$ des fonctions de $X$ dans $X$ est un autre exemple fondamental de loi de composition interne. Ainsi, $(X^X, \circ)$ est un magma.
- Les opérations de réunion $\cup$ et d'intersection $\cap$ sont des l.c.i. sur $\mathscr{P}(E)$.
- La concaténation est une l.c.i. sur l'ensemble des mots : "bon" + "jour" = "bonjour".

Deux opérations n'agissant pas sur le même ensemble devraient idéalement être notées de façons différentes. Cependant, dans la pratique, on utilise souvent un même symbole pour désigner des lois bien distinctes (penser aux différentes additions évoquées ci-dessus). Il faudra donc faire attention à manipuler ces opérations sans tout mélanger.

## A.2. Associativité et élément neutre

La structure magmatique (un simple ensemble muni d'une l.c.i.) est, en soi, assez pauvre. Nous allons voir dans ce paragraphe ce qu'il est bon de rajouter (au minimum) à cette structure pour attaquer les choses sérieuses.

Lorsqu'on effectue une opération avec plus de deux éléments d'un ensemble, il convient de préciser, au moyen de parenthèses, dans quel ordre on effectue les opérations. Ainsi, a priori, l'expression $a*b*c$ est ambiguë : on ne sait pas si elle désigne $(a*b)*c$ ou $a*(b*c)$. Pour échapper à ces problèmes de chronologie opératoire, on appréciera donc qu'une loi de composition possède la propriété suivante.

**Définition 2**

Soit $(E,*)$ un magma. On dit que la loi $*$ est associative lorsque

$$\forall a,b,c\in E,\qquad (a*b)*c=a*(b*c).$$

On peut retenir que, dans le cas d'une loi associative, la position des parenthèses n'a pas d'importance et donc aussi qu'il est inutile de mettre des parenthèses !!

**Exemples :**

- L'addition et la multiplication sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des lois associatives.
- La loi $\circ$ sur $X^X$ est associative.
- Sur $\mathscr{P}(E)$, la réunion $\cup$ et l'intersection $\cap$ sont associatives.
- La soustraction sur $\mathbb{Z}$ et la division sur $\mathbb{Q}^*$ ne sont pas associatives.

De nombreux magmas hébergent un élément inactif (c'est-à-dire qu'il laisse tous les autres éléments inchangés lorsqu'il opère sur eux). Cet élément se révèle bien utile par sa neutralité.

**Définition 3**

On dit que $e\in E$ est l'élément neutre du magma $(E,*)$ lorsque

$$\forall a\in E,\qquad a*e=a\quad\text{et}\quad e*a=a.$$

S'il existe, cet élément neutre est unique.

■ Soient $e_1$ et $e_2$ deux éléments neutres de $(E,*)$. Alors $e_1*e_2=e_1$ puisque $e_2$ est neutre et $e_1*e_2=e_2$ car $e_1$ est également neutre. Il s'ensuit que $e_1=e_2$ et donc qu'il y a bien au plus un élément neutre. ■

**Exemples :**

- Sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de l'addition, le nombre 0 est l'élément neutre.
  Sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de la multiplication, le nombre 1 est l'élément neutre. Pour la multiplication, le nombre 0 est absorbant (i.e. $\forall z\in\mathbb{C},\ 0\times z=0$).
- Le magma $(X^X,\circ)$ admet la fonction identité $\mathrm{Id}_X$ comme élément neutre.
- Le magma $\big(\mathscr{P}(E),\cup\big)$ admet $\varnothing$ comme élément neutre.
  Le magma $\big(\mathscr{P}(E),\cap\big)$ admet $E$ comme élément neutre.
- Le mot vide est l'élément neutre de l'ensemble des mots muni de la concaténation.
- La soustraction sur $\mathbb{Z}$ n'a pas d'élément neutre. Pour être précis, 0 est un élément neutre à droite puisque $\forall n\in\mathbb{Z},\ n-0=n$ mais il n'y a pas d'élément neutre à gauche puisqu'on ne peut pas trouver d'entiers $p$ tel que $\forall n\in\mathbb{Z},\ p-n=n$.
  De même, la division sur $\mathbb{Q}^*$ n'a pas d'élément neutre.

Le plus souvent, les l.c.i. sont associatives et possèdent un élément neutre.

**Définition 4**

Un magma dont la loi est associative et possède un élément neutre s'appelle un monoïde.

Dans la suite de ce cours, nous rencontrerons essentiellement des monoïdes. En effet, sans associativité et sans élément neutre, une l.c.i. est très difficile à manier et la structure qu'elle induit est pauvre.

**Exemples :**

- Les ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ munis de l'addition sont des monoïdes.
  Les ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ munis de la multiplication sont des monoïdes.
- $(X^X, \circ)$ est un monoïde.
- $\big(\mathscr{P}(E), \cup\big)$ et $\big(\mathscr{P}(E), \cap\big)$ sont des monoïdes.

## Monoïdes multiplicatifs et monoïdes additifs

Dans la pratique, les notations diffèrent quelque peu selon que l'on travaille avec une loi notée multiplicativement ou additivement.

▶ Le plus souvent, la loi d'un monoïde est notée multiplicativement, c'est-à-dire $a * b$, $a \times b$, $a \cdot b$ ou même (summum de l'abréviation) $ab$.

Dans ce cas, l'élément neutre est, en général, noté $e$ (pour $*$) ou $1_E$ (pour $\times$ ou $\cdot$).

Dans un tel monoïde, on peut sans souci introduire la notation $\prod$ de la façon suivante :

$$\prod_{k=1}^{0} a_k = 1_E \qquad \text{et} \qquad \forall n \in \mathbb{N}^*, \quad \prod_{k=1}^{n} a_k = a_1 * \cdots * a_n.$$

Plus particulièrement, on peut définir l'itération d'un élément $a \in E$ de la façon suivante :

$$a^0 = 1_E \qquad \text{et} \qquad \forall n \in \mathbb{N}^*, \quad a^n = \underbrace{a * \cdots * a}_{n \text{ facteurs } a}$$

▶ Dans certains cas particuliers (que l'on rencontre lorsque la loi est commutative, cf paragraphe A. 4.), la loi d'un monoïde est notée additivement, c'est-à-dire $a + b$.

Dans ce cas, l'élément neutre est, en général, noté $0_E$.

Dans un tel monoïde, on peut sans souci introduire la notation $\sum$ de la façon suivante :

$$\sum_{k=1}^{0} a_k = 0_E \qquad \text{et} \qquad \forall n \in \mathbb{N}^*, \quad \sum_{k=1}^{n} a_k = a_1 + \cdots + a_n.$$

Plus particulièrement, on peut définir l'itération d'un élément $a \in E$ de la façon suivante :

$$0a = 0_E \qquad \text{et} \qquad \forall n \in \mathbb{N}^*, \quad na = \underbrace{a + \cdots + a}_{n \text{ facteurs } a}$$

Attention ! Ces notations peuvent être trompeuses. Sur $E = \mathbb{R}^{\mathbb{R}}$ muni de la loi $\circ$, l'élément $1_E$ désigne la fonction identité alors que sur le même ensemble muni de la multiplication, $1_E$ désigne la fonction constante égale à 1.

## A.3. Symétrisabilité

**Définition 5**

Soit $(E,*)$ un monoïde d'élément neutre $e$. Un élément $a$ de $E$ est dit symétrisable dans $E$ s'il existe un élément de $E$ noté $a^{-1}$ tel que

$$a*a^{-1}=e \qquad \text{et} \qquad a^{-1}*a=e.$$

S'il existe, cet élément $a^{-1}$ est unique. On l'appelle le symétrique de $a$.

Dans le cas où la loi est notée multiplicativement, le symétrique de $a$ (s'il existe) s'appelle l'inverse de $a$. Il est caractérisé par les égalités $aa^{-1}=1_E$ et $a^{-1}a=1_E$.

Dans le cas où la loi est notée additivement, le symétrique de $a$ (s'il existe) est noté $-a$ est s'appelle l'opposé de $a$. Il est caractérisé par les égalités $a+(-a)=0_E$ et $(-a)+a=0_E$.

■ Soient $b$ et $c$ deux symétriques de $a$. Que vaut le bac ? Vaste question… Pour ce qui est de cette démonstration, on a $b*a*c=(b*a)*c=e*c=c$ d'une part et $b*a*c=b*(a*c)=b*e=b$ d'autre part. Donc $b=c$, ce qui démontre bien que $a$ possède au plus un symétrique. ■

La notation $1/x$, dangereuse, est à éviter (sauf dans $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$).

**Exemples :**

- Dans tout monoïde $(E,*)$, l'élément neutre $e$ est toujours symétrisable et son symétrique est lui-même (car $e*e=e$).
- Dans $(\mathbb{N},+)$, seul l'élément 0 possède un opposé.

  Dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ muni de l'addition, tout élément possède un opposé.
- Le seul élément inversible de $(\mathbb{N},\times)$ est 1.

  Dans $(\mathbb{Z},\times)$, les éléments inversibles sont 1 et $-1$.

  Dans $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ muni de la multiplication, tout élément non nul possède un inverse.
- Dans le monoïde $(X^X,\circ)$, les éléments symétrisables sont les bijections. Plus précisément, le symétrique d'une bijection $f$ est son application réciproque $f^{-1}$. La notation $f^{-1}$ pour la réciproque est donc compatible avec la notation du symétrique de $f$ pour la loi $\circ$.
- Dans $\big(\mathscr{P}(E),\cup\big)$, seul l'élément neutre $\varnothing$ est inversible (car si $A\cup B=\varnothing$ alors $A=B=\varnothing$).

  Dans $\big(\mathscr{P}(E),\cap\big)$, seul l'élément neutre $E$ est inversible (car si $A\cap B=E$ alors $A=B=E$).

Un élément symétrisable $a$ est un élément qui opère de manière réversible : on peut défaire une opération par $a$ en opérant par $a^{-1}$. Cela offre la possibilité de simplifier cet élément $a$, comme le justifie la proposition suivante.

**Proposition 1**

Soit $(E,*)$ un monoïde d'élément neutre $e$. Tout élément symétrisable $a$ de $E$ est simplifiable (ou régulier) c'est-à-dire que

$$\forall x,b\in E,\quad \begin{cases}(a*x=a*b) &\Longrightarrow &(x=b)\\ (x*a=b*a) &\Longrightarrow &(x=b)\end{cases}$$

■ La première (resp. seconde) implication se démontre en opérant par $a^{-1}$ à gauche (resp. à droite). ■

**Exemples :**

- Dans $(\mathbb{Z},\times)$, les éléments inversibles sont 1 et $-1$. Pour autant, 1 et $-1$ ne sont pas les seuls éléments simplifiables de $\mathbb{Z}$ ; en fait tout entier non nul est simplifiable ($nx=ny$ implique $x=y$ si $n\in\mathbb{Z}^*$). « Inversible » implique donc « simplifiable » mais la réciproque est fausse.

La proposition suivante rassemble les propriétés élémentaires de la symétrisabilité.

**Proposition 2**

Soient $(E,*)$ un monoïde d'élément neutre $e$ et $a,b$ deux éléments de $E$. Alors

(i) si $a$ est symétrisable, alors $a^{-1}$ l'est aussi et $(a^{-1})^{-1}=a$ ;

(ii) si $a$ et $b$ sont symétrisables, alors $a*b$ l'est aussi et l'on a $(a*b)^{-1}=b^{-1}*a^{-1}$.

■ (i) L'élément $a$ étant symétrisable, on a $a^{-1}*a=a*a^{-1}=e$. Pour savoir si $a^{-1}$ est lui aussi symétrisable, on cherche quel élément on doit faire opérer sur $a^{-1}$ pour obtenir $e$. Les égalités $a^{-1}*a=a*a^{-1}=e$ nous disent que c'est : « $a$ » ! Ainsi, $a^{-1}$ est symétrisable et $(a^{-1})^{-1}=a$.

(ii) On constate que d'une part $(a*b)*(b^{-1}*a^{-1})=a*(b*b^{-1})*a^{-1}=a*e*a^{-1}=a*a^{-1}=e$ et d'autre part $(b^{-1}*a^{-1})*(a*b)=b^{-1}*(a^{-1}*a)*b=b^{-1}*b=e$ donc $a*b$ est bien symétrisable avec $(a*b)^{-1}=b^{-1}*a^{-1}$. ■

Il faut bien noter l'inversion de l'ordre des lettres $a$ et $b$ lors du passage au symétrique (c'est le principe des chaussettes et des chaussures déjà évoqué pour les applications).

Soit $a$ un élément symétrisable d'un monoïde $(E,*)$. Alors, pour tout $n\in\mathbb{N}$, l'élément $a^n$ est symétrisable et $(a^n)^{-1}=(a^{-1})^n$ (on le démontre par récurrence à l'aide du (ii) de la proposition ci-dessus). Cet élément est naturellement noté $a^{-n}$, de sorte que $(a^n)^{-1}=(a^{-1})^n=a^{-n}$.

En cas de symétrisabilité, la notation $a^m$ possède donc un sens pour tout $m\in\mathbb{Z}$.

## A.4. Commutativité

**Définition 6**

Soient $(E, *)$ un monoïde.

On dit que deux éléments $a$ et $b$ commutent lorsque

$$a * b = b * a.$$

On dit que la loi $*$ est commutative lorsque tous les éléments du monoïde commutent deux à deux, c'est-à-dire

$$\forall a, b \in E, \qquad a * b = b * a.$$

La notation additive de la loi d'un monoïde est réservée à des cas particuliers bien spécifiques. Dans tous ces cas, la loi $+$ est commutative. On peut donc toujours écrire que $a+b = b+a$ comme on en a l'habitude.

Par contre, dans le cas multiplicatif, il faut prendre garde : en général, $ab$ n'est pas égal à $ba$.

**Exemples :**

- Dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, l'addition et la multiplication sont commutatives.
- Dans $X^X$, la loi $\circ$ n'est pas commutative (dès que $X$ possède au moins deux éléments).

  Même si cette loi n'est pas commutative, il existe des applications $f$ et $g$ qui commutent entre elles. En particulier, l'identité $\mathrm{Id}_X$ commute avec toute autre fonction.
- Dans $\mathscr{P}(E)$, les lois $\cup$ et $\cap$ sont commutatives.
- Dans tout monoïde $(E, *)$, si $a$ et $b$ sont deux éléments symétrisables qui commutent, alors $a^{-1}$ et $b^{-1}$ commutent également. En effet, l'égalité $a * b = b * a$ nous dit que $(a * b)^{-1} = (b * a)^{-1}$, c'est-à-dire $b^{-1} * a^{-1} = a^{-1} * b^{-1}$.

L'associativité de la loi $*$ (inhérente à la structure de monoïde) implique que, pour tout élément $a \in E$, deux puissances $a^n$ et $a^m$ commutent (avec $n, m \in \mathbb{N}$ voire $n, m \in \mathbb{Z}$ si $a$ est symétrisable). Plus précisément, on a $a^n * a^m = a^m * a^n = a^{n+m}$. Il s'ensuit que $(a^n)^m = (a^m)^n = a^{nm}$.

En notation additive, on a $na + ma = ma + na = (n + m)a$ et $m(na) = n(ma) = (nm)a$.

Sans hypothèse de commutation, il faut prendre garde aux autres règles habituelles sur les puissances. En particulier, la formule ci-dessous mérite d'être barrée puisqu'elle est généralement fausse :

$$(ab)^n \not= a^n b^n$$

Cela dit, ceux préférant voir le verre à moitié plein que le verre à moitié vide retiendront que cette formule est valide lorsque les éléments $a$ et $b$ commutent.

## A. 5. Distributivité

Nous envisageons dans ce paragraphe le cas où l'ensemble $E$ est pourvu de plusieurs lois.

**Définition 7**

Soit $E$ un ensemble muni de deux l.c.i. $*$ et $\top$ telles que $(E,*)$ et $(E,\top)$ sont des monoïdes. On dit que $*$ est distributive sur $\top$ lorsque

$$\forall a,b,c\in E,\quad \begin{cases} a*(b\top c)=(a*b)\top(a*c)\\ (b\top c)*a=(b*a)\top(c*a). \end{cases}$$

Dans le cas où $*$ est distributive sur $\top$ et $\top$ n'est pas distributive sur $*$, on décide par convention que $*$ est prioritaire sur $\top$, c'est-à-dire que l'expression $x*y\top x*z$ signifie $(x*y)\top(x*z)$ et non pas $x*(y\top x)*z$.

**Exemples :**

- Dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, la multiplication est distributive sur l'addition.
- Dans $\mathscr{P}(E)$, l'intersection est distributive sur la réunion et la réunion est distributive sur l'intersection.
- Dans $\mathbb{R}^{\mathbb{R}}$, la loi $\circ$ n'est distributive ni sur l'addition, ni sur la multiplication.

  En fait, il y a bien distributivité à droite : pour toutes fonctions $u,v,w\in\mathbb{R}^{\mathbb{R}}$, on a

  $$(u+v)\circ w=u\circ w+v\circ w\qquad\text{et}\qquad(u\times v)\circ w=(u\circ w)\times(v\circ w),$$

  mais il n'y a pas distributivité à gauche : autrement dit, en général, les fonctions $w\circ(u+v)$ et $w\circ u+w\circ v$ ne sont pas égales et il n'y a pas non plus égalité entre $w\circ(u\times v)$ et $(w\circ u)\times(w\circ v)$.

## A.6. Restrictions ou extensions de lois

Nous allons voir qu'il est possible de définir naturellement des lois sur une partie d'un monoïde, sur un produit cartésien de monoïdes, sur l'ensemble des fonctions à valeurs dans un monoïde ou encore sur l'ensemble des parties d'un monoïde.

### a) Loi induite

**Définition 8**

Soit $(E, *)$ un monoïde et $F$ une partie de $E$. On dit que $F$ est stable pour $*$ lorsque

$$\forall a, b \in F, \qquad a * b \in F,$$

c'est-à-dire lorsque $(F, *)$ est un magma.

On appelle alors loi induite par $*$ sur $F$ la restriction de $*$ à $F \times F$.

Lorsqu'une partie est stable, cela signifie en substance que les opérations entre les éléments de cette partie sont endémiques à cette partie.

Nous retrouverons ce vocabulaire biologique d'« endémisme » plus loin dans ce cours lorsque nous évoquerons les endomorphismes.

La loi induite ne diffère de la loi de départ que par son ensemble de définition. C'est pourquoi, dans la pratique, on note ces deux lois par le même symbole.

Attention ! Si certaines propriétés de la loi de départ se transmettent automatiquement à la loi induite (associativité, commutativité), d'autres propriétés, quant à elles, peuvent être modifiées quand on passe de $E$ à $F$. Par exemple :

- Si $e$ est l'élément neutre de $E$, rien ne dit a priori qu'il est dans $F$. Toutefois, si l'élément neutre $e$ de $E$ appartient à $F$ alors $e$ est également neutre dans $F$ et $(F, *)$ est alors un monoïde. Dans ce cas, on dit que $F$ est un sous-monoïde de $(E, *)$.
- Si $a$ est symétrisable dans $E$ et $a \in F$, rien ne dit que $a$ est symétrisable dans $F$ puisque $a^{-1}$ peut très bien ne pas appartenir à $F$. Toutefois, si $a^{-1}$ appartient à $F$ alors $a$ est symétrisable dans $F$ de symétrique $a^{-1}$.

**Exemples :**

- Dans $\mathbb{C}$, les parties $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$ sont stables pour l'addition et la multiplication.
  L'élément 2 est inversible pour $\times$ dans $\mathbb{C}$, $\mathbb{R}$ et $\mathbb{Q}$ mais ne l'est plus dans $\mathbb{Z}$ ou $\mathbb{N}$ (puisque $1/2$ n'est pas un entier).
- Si $X$ désigne un ensemble ordonné, le sous-ensemble de $X^X$ constitué des applications croissantes est stable pour la loi $\circ$.
- Dans $\mathbb{R}$, la partie $\mathbb{R}_+^*$ est stable pour $\times$ mais ce n'est pas le cas pour $\mathbb{R}_-^*$.
- Dans $(\mathbb{R}, \times)$, la partie $\{0\}$ est stable. Elle ne contient pas l'élément neutre 1 de $(\mathbb{R}, \times)$. Cela ne l'empêche pas d'avoir un élément neutre : 0 est neutre. On constate donc qu'une partie stable peut avoir son propre élément neutre (dans le cas où elle ne contient pas l'élément neutre du monoïde de départ).

### b) Loi produit

**Proposition 3**

Soient $(E,*)$ et $(F,\star)$ deux monoïdes. On peut définir sur $E\times F$ une loi produit, notée $\circledast$, telle que

$$\forall (x;y),(a;b)\in E\times F,\qquad (x;y)\circledast(a;b)=(x*a\,;\,y\star b).$$

On obtient ainsi un nouveau monoïde $(E\times F,\circledast)$ appelé monoïde produit.

De plus, si $*$ et $\star$ sont toutes les deux commutatives, alors $\circledast$ est également commutative.

■ Il est clair que le caractère interne des lois de $E$ et $F$ implique que la loi produit est interne sur $E\times F$. L'élément neutre de $(E\times F,\circledast)$ est $(e,f)$ où $e$ et $f$ sont respectivement les éléments neutres de $E$ et $F$. Enfin, si $(x;y)$, $(a;b)$ et $(\alpha;\beta)$ sont trois éléments de $E\times F$, on a

$$\begin{aligned}\big((x;y)\circledast(a;b)\big)\circledast(\alpha;\beta) &= (x*a;y\star b)\circledast(\alpha;\beta)\\ &= (x*a*\alpha;y\star b\star\beta)\\ &= (x;y)\circledast(a*\alpha;b\star\beta)\\ &= (x;y)\circledast\big((a;b)\circledast(\alpha;\beta)\big),\end{aligned}$$

ce qui établit l'associativité de la loi produit.

Donc $(E\times F,\circledast)$ est bien un monoïde.

Dans le cas où $*$ et $\star$ sont toutes les deux commutatives, on peut écrire, pour $(x;y)$ et $(a;b)$ dans $E\times F$, que

$$(x;y)\circledast(a;b)=(x*a;y\star b)=(a*x;b\star y)=(a;b)\circledast(x;y),$$

ce qui démontre que $\circledast$ est bien commutative dans ce cas. ■

Signalons que $(a;b)$ est symétrisable dans $E\times F$ pour la loi produit si, et seulement si, $a$ et $b$ sont symétrisables respectivement dans $(E,*)$ et $(F,\star)$. Dans ce cas, on a $(a;b)^{-1}=(a^{-1};b^{-1})$.

On peut généraliser la loi produit à un produit cartésien de trois, quatre, cinq, ... monoïdes.

Munir un produit cartésien de la loi produit revient à opérer sur plusieurs monoïdes de manière simultanée.

Le plus souvent, on effectue le produit cartésien d'un monoïde par lui-même. Cela permet de faire agir simultanément plusieurs fois la même opération sur les « coordonnées » d'un $n$-uplet d'éléments du monoïde.

**Exemples :**

- En effectuant le produit cartésien de $(\mathbb{R},+)$ avec lui-même, on obtient le monoïde $(\mathbb{R}^2,+)$, qui modélise (via les coordonnées dans un repère) l'addition sur l'ensemble des vecteurs du plan.
- Le produit cartésien de $(\mathbb{R},+)$ avec $([0;1],\times)$ est le monoïde produit $(\mathbb{R}\times[0;1],\circledast)$ tel que, pour tout $(x;t),(y;s)\in\mathbb{R}\times[0;1]$, on ait $(x;t)\circledast(y;s)=(x+y;ts)$.

### c) *Loi fonctionnelle*

**Proposition 4**

Soient $X$ un ensemble quelconque et $(E, *)$ un monoïde. On peut définir sur $E^X$ une loi fonctionnelle, notée également $*$, telle que, pour toutes applications $f$ et $g$ définies de $X$ dans $E$, l'application $f * g$ est définie par

$$\forall x \in X, \qquad (f * g)(x) = f(x) * g(x).$$

On obtient ainsi un nouveau monoïde $(E^X, *)$ appelé monoïde fonctionnel.

De plus, si $*$ est commutative, alors la loi fonctionnelle est également commutative.

■ Le caractère interne de la loi de $E$ implique que la loi fonctionnelle est interne sur $E^X$.

L'élément neutre de $(E^X, *)$ est la fonction $\mathbf{1} : X \longrightarrow E$ telle que $\forall x \in X,\ \mathbf{1}(x) = e$ où $e$ est l'élément neutre de $E$.

Enfin, si $f$, $g$ et $h$ sont trois éléments de $E^X$, on a, pour tout $x \in X$,

$$\big((f * g) * h\big)(x) = (f * g)(x) * h(x) = f(x) * g(x) * h(x) = f(x) * (g * h)(x) = \big(f * (g * h)\big)(x),$$

d'où $(f * g) * h = f * (g * h)$, ce qui établit l'associativité de la loi fonctionnelle.

Donc $(E^X, *)$ est bien un monoïde.

Dans le cas où $*$ est commutative, on peut écrire, pour $f, g \in E^X$, que, pour tout $x \in X$,

$$(f * g)(x) = f(x) * g(x) = g(x) * f(x) = (g * f)(x),$$

d'où $f * g = g * f$, ce qui démontre bien que la loi fonctionnelle est commutative dans ce cas. ■

Il est important de noter que l'extension de la loi d'un monoïde à l'ensemble des applications à valeurs dans ce monoïde ne nécessite aucune structure particulière sur l'ensemble de départ $X$.

Une fonction $f \in E^X$ est symétrisable pour la loi fonctionnelle si, et seulement si, pour tout $x \in X$, l'élément $f(x)$ est symétrisable dans $(E, *)$. Dans ce cas, le symétrique de $f$ est l'application de $E^X$, notée $1/f$ (ou $-f$ lorsque la loi est additive), définie par $1/f : x \longmapsto f(x)^{-1}$. Attention, on ne peut pas noter cette fonction $f^{-1}$ car cette notation désigne la réciproque de $f$ (c'est-à-dire le symétrique pour la loi $\circ$ lorsque $f$ est bijective).

**Exemples :**

- En considérant le monoïde $(\mathbb{R}, +)$ et un ensemble $X$, on obtient le monoïde $\mathbb{R}^X$ des fonctions réelles définies sur $X$, muni de l'addition des fonctions. La fonction nulle est l'élément neutre.

  En choisissant cette fois la multiplication, on munit $\mathbb{R}^X$ de la multiplication des fonctions. La fonction constante égale à 1 est l'élément neutre.

  En particulier, si $X = \mathbb{N}$, on voit que les suites réelles forment un monoïde à la fois pour la multiplication et pour l'addition.
- Le monoïde $(X^X, \circ)$ n'est pas un monoïde fonctionnel car $\circ$ n'est pas une loi étendue (il n'y a pas de loi $\circ$ sur $X$).

### *d) Loi ensembliste* [✠]

**Proposition 5**

Soit $(E,*)$ un monoïde. On peut définir sur $\mathscr{P}(E)$ une loi ensembliste, notée également $*$, telle que

$$\forall A,B\in\mathscr{P}(E),\qquad A*B=\{a*b : a\in A,\ b\in B\}.$$

On obtient ainsi un nouveau monoïde $\big(\mathscr{P}(E),*\big)$ appelé monoïde ensembliste.

De plus, si $*$ est commutative, alors la loi ensembliste est également commutative.

■ Le caractère interne de la loi de $E$ implique que la loi ensembliste est interne sur $\mathscr{P}(E)$.
L'élément neutre de $(\mathscr{P}(E),*)$ est le singleton $\{e\}$ où $e$ est l'élément neutre de $E$.
Enfin, si $A$, $B$ et $C$ sont trois parties de $E$, on a

$$\begin{aligned}(A*B)*C &= \{\gamma*c : \gamma\in A*B,\ c\in C\}\\ &= \{a*b*c : a\in A,\ b\in B,\ c\in C\}\\ &= \{a*\alpha : a\in A,\ \alpha\in B*C\}\\ &= A*(B*C),\end{aligned}$$

ce qui établit l'associativité de la loi ensembliste.
Donc $\big(\mathscr{P}(E),*\big)$ est bien un monoïde.

Dans le cas où $*$ est commutative, on peut écrire, pour $A,B\in\mathscr{P}(E)$, que

$$A*B=\{a*b : a\in A,\ b\in B\}=\{b*a : a\in A,\ b\in B\}=B*A,$$

ce qui démontre bien que la loi ensembliste est commutative dans ce cas. ■

On notera que si $e\in B$, alors $A\subset A*B$.

**Exemples :**

- Considérons le monoïde $(\mathbb{N},+)$. Le monoïde ensembliste associé est $\big(\mathscr{P}(\mathbb{N}),+\big)$. Dans ce monoïde, on a par exemple

$$\{1,2\}+\{2,3\}=\{1+2,1+3,2+2,2+3\}=\{3,4,4,5\}=\{3,4,5\}$$

et

$$\mathbb{N}+\mathbb{N}=\mathbb{N}.$$

- L'ensemble vide est un élément absorbant pour la loi ensembliste puisque, pour toute partie $A\in\mathscr{P}(E)$, on a $A*\varnothing=\varnothing*A=\varnothing$.
- Soit $(E,*)$ un monoïde, $x\in E$ et $A$ une partie de $E$. Dans le monoïde ensembliste $\big(\mathscr{P}(E),*\big)$, l'élément $\{x\}*A$ est noté $x*A$ et s'appelle le translaté de $A$ par $x$ à gauche. De même, $A*\{x\}$ est noté $A*x$ et s'appelle le translaté de $A$ par $x$ à droite.

  Avec une notation multiplicative, le translaté $xA$ de $A$ par $x$ à gauche et le translaté $Ax$ de $A$ par $x$ à droite sont donnés par

$$xA=\{xa : a\in A\}\qquad\text{et}\qquad Ax=\{ax : a\in A\}.$$

  Avec une notation additive (la loi $+$ étant évidemment commutative), le translaté de $A$ par $x$ (à gauche ou à droite, peu importe) est noté $A+x$ et vaut

$$A+x=\{a+x : a\in A\}.$$

  C'est dans ce dernier cas que la dénomination de « translaté » prend son sens : pour translater une partie d'une quantité $x$, il suffit d'ajouter $x$ à tous les éléments de cette partie.

2 h 15

# B. Groupes

Dans un groupe, on enrichit la structure de monoïde en présupposant la symétrisabilité de tous les éléments.

## B.1. Structure de groupe

**Définition 9**

Soit $(G, *)$ un magma. On dit que $(G, *)$ est un groupe lorsque c'est un monoïde dans lequel tout élément est symétrisable, autrement dit lorsque

(i) $*$ est associative ;

(ii) $G$ contient un élément neutre $e$ pour $*$ ;

(iii) tout élément $g$ de $G$ possède un symétrique $g^{-1}$ dans $G$.

Lorsque la loi est commutative, on dit que le groupe est commutatif ou abélien.

Pour vérifier qu'un ensemble muni d'une loi est un groupe, ce n'est pas trois propriétés qu'il faut démontrer (comme le laisse penser visuellement la définition ci-dessus) mais quatre ! Il faut d'abord vérifier que la loi est interne avant de regarder si elle est associative, unifère (c'est la façon prétentieuse de dire qu'elle possède un élément neutre) et symétrisable.

La loi d'un groupe est en général notée multiplicativement. Toutefois, lorsque la loi correspond à une addition, on opère additivement.

L'encadré ci-dessous rassemble des exemples essentiels de groupes.

**Exemples :**

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes abéliens.

  $(\mathbb{N}, +)$ n'est pas un groupe. Additivement, les ensembles de nombres sont donc des groupes à partir de $\mathbb{Z}$. En fait, c'est même pour cela que $\mathbb{Z}$ a été créé : pour remédier à l'absence d'opposé dans $\mathbb{N}$.

- $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$ sont des groupes abéliens.

  $(\mathbb{Z}^*, \times)$ n'est pas un groupe. Multiplicativement, les ensembles de nombres (privés de 0) sont donc des groupes à partir de $\mathbb{Q}^*$. En fait, c'est même pour cela que $\mathbb{Q}$ a été créé : pour remédier à l'absence d'inverse pour les éléments non nuls de $\mathbb{Z}$.

- On appelle permutation de $X$ toute bijection entre $X$ et $X$.

  L'ensemble des permutations de $X$ est un groupe pour la loi $\circ$. L'élément neutre est $\mathrm{Id}_X$ et, pour toute permutation $f$ de $X$, le symétrique de $f$ est la fonction réciproque $f^{-1}$ de $f$.

  Ce groupe des permutations de $X$ s'appelle le groupe symétrique de $X$ et il est noté $\mathfrak{S}_X$ (où la lettre $\mathfrak{S}$ est un « S majuscule gothique », ce que les moins doués du crayon pourront remplacer par un S curviligne $\mathscr{S}$ ou même un bête S classique $S$).

  Ce groupe symétrique n'est pas abélien dès que le cardinal de $X$ est supérieur ou égal à 3.

  Nous étudierons plus profondément le groupe symétrique d'un ensemble fini dans un prochain cours.

On notera que lorsqu'on parle du groupe $\mathbb{C}$, cela ne peut être que $(\mathbb{C}, +)$ puisque $(\mathbb{C}^*, +)$ n'est pas un groupe (pas de neutre). De même, lorsque l'on parle du groupe $\mathbb{C}^*$, on évoque nécessairement le groupe $(\mathbb{C}^*, \times)$ puisque $(\mathbb{C}, \times)$ n'est pas un groupe (0 n'est pas inversible).

Ainsi, parfois, on ne précise pas la loi d'un groupe parce que celle-ci est évidente. À vous de vous y retrouver !

La loi produit permet de fabriquer de nouveaux groupes en effectuant le produit cartésien de groupes connus.

**Proposition 6**

Soient $G_1$ et $G_2$ deux groupes. L'ensemble $G_1 \times G_2$, muni de la loi produit, est alors un groupe, appelé groupe produit de $G_1$ et $G_2$.

De plus, si $G_1$ et $G_2$ sont abéliens, alors $G_1 \times G_2$ l'est aussi.

■ Les groupes $G_1$ et $G_2$ étant des monoïdes, la proposition 3 dit que $G_1 \times G_2$ en est aussi un. De plus, si $(g_1, g_2) \in G_1 \times G_2$, l'élément $({g_1}^{-1}, {g_2}^{-1})$ de $G_1 \times G_2$ est clairement le symétrique de $(g_1, g_2)$. Enfin, si $G_1$ et $G_2$ sont abéliens, la proposition 3 que $G_1 \times G_2$ l'est aussi. ■

La propriété se généralise évidemment au produit cartésien de trois, quatre, cinq ... groupes.

Le plus souvent, on effectue le produit cartésien d'un groupe par lui-même.

La notion de groupe produit permet de donner de nouveaux exemples de groupes.

**Exemples :**

- $(\mathbb{Z}^2, +)$, $(\mathbb{Q}^2, +)$, $(\mathbb{R}^2, +)$ et $(\mathbb{C}^2, +)$ sont des groupes abéliens. On constate en particulier que l'addition confère au plan $\mathbb{R}^2$ une structure de groupe.

  Plus généralement, pour tout $n \in \mathbb{N}^*$, $(\mathbb{Z}^n, +)$, $(\mathbb{Q}^n, +)$, $(\mathbb{R}^n, +)$ et $(\mathbb{C}^n, +)$ sont des groupes abéliens.
- Pour tout $n \in \mathbb{N}^*$, $\big((\mathbb{Q}^*)^n, \times\big)$, $\big((\mathbb{R}^*)^n, \times\big)$ et $\big((\mathbb{C}^*)^n, \times\big)$ sont des groupes abéliens.

La loi fonctionnelle permet elle-aussi de fabriquer de nouveaux groupes à partir d'un groupe connu.

**Proposition 7**

Soient $G$ un groupe et $X$ un ensemble quelconque. L'ensemble $G^X$, muni de la loi fonctionnelle, est alors un groupe, appelé groupe fonctionnel de $X$ vers $G$.

De plus, si $G$ est abélien, $G^X$ l'est aussi.

■ Le groupe $G$ étant un monoïde, la proposition 4 dit que $G^X$ en est aussi un. De plus, si $f : X \longrightarrow G$, alors la fonction $1/f : X \longrightarrow G$ définie par $\forall x \in X,\ (1/f)(x) = f(x)^{-1}$ est clairement le symétrique de $f$ dans $G^X$. Enfin, si $G$ est abélien, la proposition 4 dit que $G^X$ l'est aussi. ■

Là encore, ce résultat permet de donner de nouveaux exemples de groupes.

**Exemples :**

- L'ensemble $\big(\mathbb{R}^X, +\big)$ des applications définies sur $X$ et à valeurs réelles est un groupe additif abélien.
- L'ensemble $\big((\mathbb{R}^*)^X, \times\big)$ des applications définies sur $X$, à valeurs réelles et ne s'annulant pas est un groupe multiplicatif abélien.
- L'ensemble $\big(\mathbb{R}^{\mathbb{N}}, +\big)$ des suites réelles est un groupe additif abélien.

Tous ces exemples marchent aussi bien avec des applications ou des suites à valeurs complexes.

L'encadré suivant rassemble les différentes règles de calcul valides (ou non) dans un groupe.

## Vade-mecum du calcul dans un groupe

En rassemblant tout ce que l'on sait déjà sur les monoïdes et la symétrisabilité, on peut dresser la liste de remarques suivantes concernant les groupes.

Dans toutes ces remarques, $(G,*)$ désigne un groupe d'élement neutre $e$ et $g, g_1, g_2, x$ sont quatre éléments de $G$.

- Un groupe n'est jamais vide puisqu'il possède (au moins) un unique élément neutre.
- Chaque élément de $G$ possède un unique symétrique et l'on a

$$e^{-1} = e, \qquad (g^{-1})^{-1} = g \qquad \text{et} \qquad (g_1 * g_2)^{-1} = {g_2}^{-1} * {g_1}^{-1}.$$

- Le symbole $\prod$ est utilisable (ou le symbole $\sum$ si la loi est notée $+$) ;
- Pour tout $n \in \mathbb{Z}$, le $n$-ème itéré de $g$, noté $g^n$ pour une loi multiplicative ou $ng$ pour une loi additive, est défini par

$$g^n = \begin{cases} \underbrace{g * \cdots * g}_{n \text{ fois}} & \text{si } n > 0 \\ e & \text{si } n = 0 \\ \underbrace{g^{-1} * \cdots * g^{-1}}_{|n| \text{ fois}} & \text{si } n < 0 \end{cases} \qquad ng = \begin{cases} \underbrace{g + \cdots + g}_{n \text{ fois}} & \text{si } n > 0 \\ 0 & \text{si } n = 0 \\ \underbrace{(-g) + \cdots + (-g)}_{|n| \text{ fois}} & \text{si } n < 0 \end{cases}$$

  et l'on a, pour tous $n, m \in \mathbb{Z}$, les propriétés multiplicatives

$$g^n * g^m = g^{n+m} \qquad \text{et} \qquad (g^n)^m = g^{nm}$$

  ou leurs homologues additives

$$(ng) + (mg) = (n+m)g \qquad \text{et} \qquad m(ng) = (mn)g.$$

- Tout élément est simplifiable à gauche comme à droite, ce qui signifie que l'équation $g * x = a$ admet pour unique solution $x = g^{-1} * a$ et l'équation $x * g = a$ admet pour unique solution $x = a * g^{-1}$.
- La quantité $(g_1 * g_2)^n$ n'est pas égale à ${g_1}^n * {g_2}^n$, sauf lorsque $g_1$ et $g_2$ commutent.

  Les lois additives étant commutatives, on a $n(g_1 + g_2) = ng_1 + ng_2$.
- La simplication $g * g^{-1} = e$ n'est envisageable que lorsque $g$ et $g^{-1}$ sont contiguës : ainsi, dans $g_1 * g_2 * {g_1}^{-1}$, on ne peut pas simplifier par $g_1$, sauf si $g_1$ et $g_2$ commutent.

**Exercice 1.**
Soit $G$ un groupe muni d'une loi multiplicative $\times$ et d'un élément neutre noté 1. Soient $a, b \in G$ tels que $a^2 b = ba$ et $b^2 a = ab$. Démontrer que $a = b = 1$.

◊ Les hypothèses s'écrivent $aab = ba$ et $bba = ab$. Dans le membre de gauche de la première égalité, on remplace $ab$ par la valeur donnée par la seconde égalité, ce qui donne $A\underline{BBA} = ba$. En simplifiant par $ba$ à droite, on obtient $ab = 1$. En reportant dans la première égalité, il vient $a = ba$, ce qui donne, après simplification par $a$ à droite, $b = 1$. Il s'ensuit que $a = 1$. ◊

## B. 2. Sous-groupes

**Définition 10**

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

Si $H_1$ est sous-groupe de $G$ et $H_2$ est un sous-groupe de $H_1$, alors $H_2$ est un sous-groupe de $G$.

Dans la pratique, on ne vérifie pas qu'un ensemble est un sous-groupe à l'aide de la définition mais avec la caractérisation des sous-groupes suivante.

**Proposition 8**

Soit $(G,*)$ un groupe d'élément neutre $e$. Une partie $H$ de $G$ est un sous-groupe de $G$ si, et seulement si,

(i) $e \in H$ ;

(ii) $H$ est stable pour $*$, c'est-à-dire $\forall h_1, h_2 \in H,\ h_1 * h_2 \in H$ ;

(iii) $H$ contient les symétriques de tous ses éléments, c'est-à-dire $\forall h \in H,\ h^{-1} \in H$.

On peut remplacer (ii) et (iii) par

(v) $\forall h_1, h_2 \in H,\ h_1 * {h_2}^{-1} \in H$.

■ $\Leftarrow$ Supposons d'abord qu'une partie $H$ de $G$ vérifie (i), (ii) et (iii).
La partie $H$ est alors stable pour $*$ d'après (ii).
La loi induite sur $H$ est associative et $H$ contient l'élément neutre $e$, donc $(H,*)$ est un monoïde.
Enfin, $H$ contient les symétriques de tous ses éléments.
La partie $H$ remplit donc bien toutes les conditions pour être un sous-groupe de $(G,*)$.

$\Rightarrow$ Réciproquement, supposons que $H$ est un sous-groupe de $(G,*)$.
Par définition, $H$ est stable pour $*$ donc (ii) est vérifiée.
Notons $e_G$ l'élément neutre de $G$ et $e_H$ celui de $H$. On a $e_G e_H = e_H = e_H e_H$, donc, par régularité de $e_H$, on a $e_H = e_G$, ce qui établit (i).
Soit $h \in H$. L'élément $h$ admet un inverse $h^{-1}$ au sens de $G$ et un inverse $h^-$ au sens de $H$. Alors $h^- h = e = h^{-1} h$, d'où, par régularité de $h$, on a $h^- = h^{-1}$, ce qui démontre que $h^{-1} \in H$. Ainsi $H$ contient bien les symétriques de tous ses éléments, c'est-à-dire que (iii) est vraie. ■

En notation additive, (i) devient $0 \in H$, (ii) devient $\forall h_1, h_2 \in H,\ h_1 + h_2 \in H$ et (iii) devient $\forall h \in H,\ -h \in H$. On peut remplacer (ii) et (iii) par (v) $\forall h_1, h_2 \in H,\ h_1 - h_2 \in H$.

Pour démontrer qu'un ensemble $G$ muni d'une loi $*$ est un groupe, on démontre en général que c'est un sous-groupe d'un groupe connu (on économise ainsi l'associativité, l'existence du neutre et l'existence du symétrique).

**Exemples :**

- Dans tout groupe $(G,*)$ d'élément neutre $e$, les ensembles $\{e\}$ et $G$ sont des sous-groupes de $G$. On les appelle les sous-groupes triviaux de $G$.
- Dans la liste $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, chacun est un sous-groupe (additif) de ceux qui le suivent.
- Dans la liste $\mathbb{Q}^*$, $\mathbb{R}^*$ et $\mathbb{C}^*$, chacun est un sous-groupe (multiplicatif) de ceux qui le suivent.
- L'ensemble $\mathbb{R}_+^*$ est un sous-groupe multiplicatif de $\mathbb{R}^*$. Par contre, $\mathbb{R}_-^*$ n'en est pas un.
- L'ensemble $\mathbb{U}$ des nombres complexes de module 1 est un sous groupe de $(\mathbb{C}^*, \times)$.
  Pour tout $n \in \mathbb{N}^*$, l'ensemble $\mathbb{U}_n$ des racines $n$-èmes de l'unité est un sous groupe de $(\mathbb{U}, \times)$.
- L'ensemble $\{s^+ \in \mathbb{C}^{\mathbb{C}} : \exists (a,b) \in \mathbb{C}^* \times \mathbb{C},\ \forall z \in \mathbb{C},\ s^+(z) = az + b\}$ contenant les similitudes directes du plan complexe est un sous-groupe de $(\mathfrak{S}(\mathbb{C}), \circ)$.

La proposition suivante énonce la stabilité de la structure de sous-groupe par intersection.

**Proposition 9**

Soit $(G,*)$ un groupe. Une intersection (finie ou infinie) de sous-groupes de $G$ est un sous-groupe de $G$.

■ Soit $(H_j)_{j\in J}$ une famille de sous-groupes de $(G,*)$. On pose $\widehat{H}=\bigcap_{j\in J} H_j$ et l'on désire démontrer que $\widehat{H}$ est un sous-groupe de $(G,*)$.

Pour cela, démontrons les propriétés (i), (ii) et (iii) de la caractérisation des sous-groupes.

On sait que $e\in H_j$ pour tout $j\in J$, donc $e\in\widehat{H}$ et (i) est vérifié.

Si $h_1$ et $h_2$ sont deux éléments de $\widehat{H}$, ce sont aussi deux éléments de $H_j$ pour tout $j\in J$. Il s'ensuit que $h_1*h_2\in H_j$ pour tout $j\in J$ et donc que $h_1*h_2\in\widehat{H}$. La propriété (ii) est donc bien vérifiée.

Enfin, si $h$ est un élément de $\widehat{H}$, il est aussi élément de chacun des $H_j$ et, par conséquent, son symétrique est aussi un élément de chaque $H_j$. D'où $h^{-1}\in\widehat{H}$ et (iii) est vérifiée. ■

Le résultat précédent devient faux si l'on remplace l'intersection par la réunion. Par exemple, $\mathbb{R}_+^*$ et $\{-1;1\}$ sont des sous-groupes multiplicatifs de $\mathbb{R}^*$ mais $\mathbb{R}_+^*\cup\{-1;1\}$ n'est pas un sous-groupe de $\mathbb{R}^*$ (puisque $-1\times 2=-2$ n'appartient pas à $\mathbb{R}_+^*\cup\{-1;1\}$ alors que $-1$ et $2$ y appartiennent).

On termine ce paragraphe en donnant la description des sous-groupes de $(\mathbb{Z},+)$. Rappelons que, pour tout $n\in\mathbb{N}$, on note $n\mathbb{Z}=\{kn : k\in\mathbb{Z}\}$ l'ensemble des multiples de $n$ dans $\mathbb{Z}$.

**Théorème 1**

Les sous-groupes de $(\mathbb{Z},+)$ sont exactement toutes les parties de la forme $n\mathbb{Z}$ avec $n$ parcourant $\mathbb{N}$.

■ $\Leftarrow$ Soit $n\in\mathbb{N}$. Démontrons que $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z},+)$.

On a $0=0\times n$ donc $0\in n\mathbb{Z}$.

Soient $a,b\in n\mathbb{Z}$. Il existe $k,\ell\in\mathbb{Z}$ tels que $a=kn$ et $b=\ell n$, ce qui donne $a+b=(k+\ell)n$ et donc $a+b\in n\mathbb{Z}$.

Soit $a\in n\mathbb{Z}$. Il existe $k\in\mathbb{Z}$ tel que $a=kn$. Alors $-a=(-k)n$ ce qui prouve que $-a\in n\mathbb{Z}$.

En conclusion, $n\mathbb{Z}$ est bien un sous-groupe de $\mathbb{Z}$.

$\Rightarrow$ Démontrons réciproquement qu'un sous-groupe $H$ de $(\mathbb{Z},+)$ est de la forme $n\mathbb{Z}$ avec $n\in\mathbb{N}$.

Si $H=\{0\}$, on a $H=0\mathbb{Z}$.

Au contraire, si $H\neq\{0\}$, on considère la partie $H_+^*=H\cap\mathbb{N}^*$ de $\mathbb{N}^*$. On sait qu'elle est non vide (comme $H\neq\{0\}$, il contient un entier non nul $k$ et son opposé $-k$ ; l'un des deux est dans $H_+^*$) et qu'elle admet, par conséquent, un plus petit élément $n$.

Comme $n\in H$, la stabilité de $H$ dans $\mathbb{Z}$ assure que les itérés de $n$ et les opposés de ces itérés sont dans $H$, d'où $n\mathbb{Z}\subset H$.

Inversement, si $m\in H$, on effectue la division euclidienne de $m$ par $n$, d'où $m=nq+r$ avec $0\leqslant r<n$. Alors $r=m-nq$ est un élément de $H$ (comme différence de deux éléments de $H$). La condition $0\leqslant r<n$ et la minimalité de $n$ dans $H_+^*$ implique donc forcément que $r=0$. Alors $m=nq$ ce qui démontre que $m\in n\mathbb{Z}$. Ainsi $H\subset n\mathbb{Z}$.

Finalement, $H=n\mathbb{Z}$. ■

**Exemples :**

- Soient $a,b\in\mathbb{N}$. L'ensemble $a\mathbb{Z}$ des multiples de $a$ et l'ensemble $b\mathbb{Z}$ des multiples de $b$ sont deux sous-groupes de $\mathbb{Z}$. Il s'ensuit que leur intersection $a\mathbb{Z}\cap b\mathbb{Z}$ est aussi un sous-groupe de $\mathbb{Z}$, ce qui permet d'affirmer l'existence de $\mu\in\mathbb{N}$ tel que $a\mathbb{Z}\cap b\mathbb{Z}=\mu\mathbb{Z}$. Ainsi, l'intersection de deux ensembles de multiples est un ensemble de multiples.

  Nous verrons, dans le chapitre d'arithmétique, que $\mu$ est le ppcm de $a$ et $b$.

4 h 00

## B.3. Morphismes de groupes

### a) Définitions

**Définition 11**

Soient $(G,*)$ et $(G',\star)$ deux groupes. On appelle (homo)morphisme de groupes de $G$ vers $G'$ toute application $\varphi : G \longrightarrow G'$ telle que

$$\forall g_1, g_2 \in G, \qquad \varphi(g_1 * g_2) = \varphi(g_1) \star \varphi(g_2).$$

Pour vérifier qu'une application $\varphi : G \longrightarrow G'$ est un morphisme de groupes, il faut contrôler que l'image d'un produit est le produit des images (c'est-à-dire $\forall g_1, g_2 \in G,\ \varphi(g_1 * g_2) = \varphi(g_1) \star \varphi(g_2)$) mais aussi que $G$ et $G'$ sont bel et bien des groupes.

La propriété des morphismes se généralise par récurrence à un plus grand nombre d'éléments ou à une puissance :

$$\forall g_1, \dots, g_n \in G, \quad \varphi\Big(\prod_{k=1}^{n} g_k\Big) = \prod_{k=1}^{n} \varphi(g_k) \qquad \text{et} \qquad \forall g \in G, \quad \forall n \in \mathbb{N}, \quad \varphi(g^n) = \big(\varphi(g)\big)^n.$$

**Exemples :**

- $\begin{cases} (\mathbb{Z},+) & \longrightarrow & (\mathbb{R}_+^*,\times) \\ n & \longmapsto & 2^n \end{cases}$ est un morphisme de groupes (d'après les règles des puissances).
- $\exp \begin{cases} (\mathbb{C},+) & \longrightarrow & (\mathbb{C}^*,\times) \\ z & \longmapsto & \mathrm{e}^z \end{cases}$ est un morphisme de groupes (d'après les propriétés de exp).
- Pour tout $n \in \mathbb{N}^*$, l'application $\begin{cases} (\mathbb{Z},+) & \longrightarrow & (\mathbb{U}_n,\times) \\ k & \longmapsto & \mathrm{e}^{2ik\pi/n} \end{cases}$ est un morphisme de groupes.
- Le module $|\cdot| \begin{cases} (\mathbb{C}^*,\times) & \longrightarrow & (\mathbb{R}^*,\times) \\ z & \longmapsto & |z| \end{cases}$ est un morphisme (pour la multiplication) car le module d'un produit est le produit des modules.
  Par contre, le module $|\cdot| : (\mathbb{C},+) \longrightarrow (\mathbb{R},+)$ n'est pas un morphisme additif car le module d'une somme n'est pas la somme des modules.

Les propriétés fondamentales des morphismes sont rassemblées dans la proposition suivante.

**Proposition 10**

Soient $(G,*)$ et $(G',\star)$ deux groupes d'éléments neutres respectifs $e$ et $e'$ et $\varphi : G \longrightarrow G'$ un morphisme de groupes de $G$ vers $G'$. Alors

(i) $\varphi(e) = e'$ (l'image du neutre est le neutre) ;

(ii) $\forall g \in G,\ \varphi(g^{-1}) = \big(\varphi(g)\big)^{-1}$ (l'image du symétrique est le symétrique de l'image).

■ (i) On a $\varphi(e) \star \varphi(e) = \varphi(e * e) = \varphi(e) = \varphi(e) \star e'$ d'où le résultat par régularité de $\varphi(e)$.

(ii) Soit $g \in G$. On a $\varphi(g) \star \varphi(g^{-1}) = \varphi(g * g^{-1}) = \varphi(e) = e' = \varphi(g) \star \varphi(g)^{-1}$, d'où $\varphi(g^{-1}) = \varphi(g)^{-1}$ par régularité de $\varphi(g)$. ■

Ces deux propriétés, associées à la définition d'un morphisme (l'image d'un produit est le produit des images), permettent de voir qu'un morphisme respecte la structure de groupe, c'est-à-dire qu'il transporte la loi d'un groupe à l'autre en lui conservant ses propriétés.

(ii) permet de généraliser le résultat sur l'image d'une puissance au cas des exposants négatifs :

$$\forall g \in G, \quad \forall n \in \mathbb{Z}, \quad \varphi(g^n) = \big(\varphi(g)\big)^n.$$

L'encadré suivant précise le vocabulaire lorsque le morphisme est particulier.

**Définition 12**

Un morphisme d'un groupe $G$ vers lui-même (avec la même l.c.i. au départ et à l'arrivée) est appelé un endomorphisme de $G$.

Un morphisme de groupes de $G$ vers $G'$ qui est bijectif est appelé un isomorphisme entre $G$ et $G'$. Les deux groupes $G$ et $G'$ sont alors dits isomorphes.

Un morphisme qui est à la fois un endomorphisme et un isomorphisme de $G$ (c'est-à-dire un morphisme bijectif d'un groupe $G$ vers lui-même) est appelé un automorphisme de $G$. On note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de $G$.

En linguistique, le préfixe « endo » signifie « à l'intérieur ». Il est très utilisé en dynamique des populations (endémisme) ou en médecine (glande endocrine). Pour le cas des endomorphismes, le préfixe signifie que l'on part d'un groupe et qu'on y reste !

Le mot « isomorphe » signifie « de même forme ». On constate effectivement que deux groupes finis qui sont isomorphes ont, au nom et à l'ordre des éléments près, les mêmes tables de lois.

Le préfixe « auto » signifie « soi-même » (l'élève idéal s'autoinstruit !). Un automorphisme est donc, en quelque sorte, une réécriture du groupe dans laquelle les éléments permutent leurs rôles.

**Exemples :**

- Si $(G,*)$ est un groupe d'élément neutre $e$, alors $\left\{\begin{array}{ccc} G & \longrightarrow & G \\ g & \longmapsto & e \end{array}\right.$ est un endomorphisme.
- Si $(G,*)$ est un groupe, alors $\mathrm{Id}_G$ est un automorphisme involutif de $G$ (c'est-à-dire qu'il est égal à sa réciproque).
- Si $(G,*)$ est abélien, la symétrisation $\left\{\begin{array}{ccc} G & \longrightarrow & G \\ g & \longmapsto & g^{-1} \end{array}\right.$ est un automorphisme involutif.
- Les applications $\exp : (\mathbb{R},+) \longrightarrow (\mathbb{R}_+^*,\times)$ et $\ln : (\mathbb{R}_+^*,\times) \longrightarrow (\mathbb{R},+)$ sont des isomorphismes réciproques l'un de l'autre.
- La conjugaison complexe $z \longmapsto \overline{z}$ est un automorphisme involutif de $(\mathbb{C},+)$ et aussi un automorphisme involutif de $(\mathbb{C}^*,\times)$.

### b) Opérations sur les morphismes de groupes

On commence par la composition.

**Proposition 11**

La composée de deux morphismes de groupes est un morphisme de groupes.
La composée de deux endomorphismes de groupe est un endomorphisme de groupe.
La composée de deux isomorphismes de groupes est un isomorphisme de groupes.
La composée de deux automorphismes de groupe est un automorphisme de groupe.

■ Soient $(G,*),(G',\star)$ et $(G'',\bullet)$ trois groupes et $\varphi : G \longrightarrow G'$ et $\psi : G' \longrightarrow G''$ deux morphismes de groupes composables. Pour tout $g_1, g_2 \in G$, on a

$$(\psi\circ\varphi)(g_1 * g_2) = \psi\big(\varphi(g_1 * g_2)\big) = \psi\big(\varphi(g_1)\star\varphi(g_2)\big) = \psi\big(\varphi(g_1)\big)\bullet\psi\big(\varphi(g_2)\big) = (\psi\circ\varphi)(g_1)\bullet(\psi\circ\varphi)(g_2),$$

donc $\psi\circ\varphi$ est bien un morphisme de groupes.

Les autres propriétés en découlent (parce qu'une composée de bijections est une bijection). ■

On poursuit avec le passage à l'application réciproque d'un isomorphisme.

**Proposition 12**

La bijection réciproque d'un isomorphisme de groupes est aussi un isomorphisme de groupes.

■ Soit $\varphi$ un isomorphisme de $(G,*)$ vers $(G',\star)$.
Nous savons déjà que $\varphi^{-1}$ est bijective (d'inverse $\varphi$).
Par ailleurs, pour tous $g'_1, g'_2 \in G'$, on a

$$\varphi^{-1}(g'_1\star g'_2) = \varphi^{-1}\Big(\varphi\big(\varphi^{-1}(g'_1)\big)\star\varphi\big(\varphi^{-1}(g'_2)\big)\Big) = \varphi^{-1}\Big(\varphi\big(\varphi^{-1}(g'_1) * \varphi^{-1}(g'_2)\big)\Big) = \varphi^{-1}(g'_1) * \varphi^{-1}(g'_2),$$

ce qui démontre que $\varphi^{-1}$ est bien un morphisme de groupes de $G'$ vers $G$.
Donc $\varphi^{-1}$ un isomorphisme de $(G',\star)$ vers $(G,*)$. ■

On peut traduire structurellement cette proposition de la façon suivante.

**Corollaire 1**

Soit $(G,*)$ un groupe. Alors $\mathrm{Aut}(G)$ est un groupe pour la loi $\circ$.

■ On sait déjà que la loi $\circ$ est associative. $\mathrm{Id}_G$ est un automorphisme. Si $\varphi_1$ et $\varphi_2$ sont deux automorphismes de $G$, leur composée est bien sûr bijective et c'est aussi un morphisme d'après la proposition 11, donc $\varphi_1\circ\varphi_2 \in \mathrm{Aut}(G)$. Enfin, si $\varphi \in \mathrm{Aut}(G)$, la proposition précédente nous dit que $\varphi^{-1} \in \mathrm{Aut}(G)$. Donc $\big(\mathrm{Aut}(G),\circ\big)$ est bien un groupe. ■

On termine ce paragraphe par une dernière opération sur les morphismes : la restriction.

**Proposition 13**

Soit $\varphi : G \longrightarrow G'$ un morphisme de groupes de $(G,*)$ vers $(G',\star)$. Si $H$ est un sous-groupe de $G$ et $H'$ est un sous-groupe de $G'$ tels que $\varphi(H) \subset H'$, alors la restriction de $\varphi$ de $H$ vers $H'$, définie par

$$\varphi\big|_H^{H'} \left\{ \begin{array}{ccc} H & \longrightarrow & H' \\ h & \longmapsto & \varphi(h) \end{array} \right.$$

est un morphisme de groupe de $(H,*)$ vers $(H',\star)$.

■ AQT ■

On retiendra que le caractère morphique est une propriété intrinsèque de la relation fonctionnelle, c'est-à-dire qu'il ne dépend pas des groupes de départ et d'arrivée du morphisme.

### c) Image morphique (directe ou indirecte) d'un sous-groupe

**Proposition 14**

Soit $\varphi : G \longrightarrow G'$ un morphisme de groupes de $(G, *)$ vers $(G', \star)$.

(i) Si $H$ est un sous-groupe de $G$, alors $\varphi(H)$ est un sous-groupe de $G'$.

(ii) Si $H'$ est un sous-groupe de $G'$, alors $\varphi^{-1}(H')$ est un sous-groupe de $G$.

■ On note $e$ et $e'$ les éléments neutres respectifs de $G$ et $G'$.

(i) Soit $H$ un sous-groupe de $G$.
On a $e' = \varphi(e) \in \varphi(H)$ car $e \in H$.
Soient $g'_1, g'_2 \in \varphi(H)$ de sorte qu'il existe alors $g_1, g_2 \in H$ tel que $g'_1 = \varphi(g_1)$ et $g'_2 = \varphi(g_2)$. Alors $g'_1 \star g'_2 = \varphi(g_1) \star \varphi(g_2) = \varphi(g_1 * g_2) \in \varphi(H)$ puisque $g_1 * g_2 \in H$.
Soit $g' \in \varphi(H)$. Il existe $g \in H$ tel que $g' = \varphi(g)$. Alors $(g')^{-1} = \varphi(g)^{-1} = \varphi(g^{-1}) \in \varphi(H)$ puisque $g^{-1} \in H$.
Donc $\varphi(H)$ est un sous-groupe de $G'$.

(ii) Soit $H'$ un sous-groupe de $G'$.
Comme $\varphi(e) = e' \in H'$, on a $e \in \varphi^{-1}(H')$.
Soient $g_1, g_2 \in \varphi^{-1}(H')$ de sorte que $\varphi(g_1) \in H'$ et $\varphi(g_2) \in H'$. Alors $\varphi(g_1 * g_2) = \varphi(g_1) \star \varphi(g_2) \in H'$ puisque $H'$ est un sous-groupe. Par suite, $g_1 * g_2 \in \varphi^{-1}(H')$.
Soient $g \in \varphi^{-1}(H')$. On a alors $\varphi(g) \in H'$, ce qui implique que $\varphi(g^{-1}) = \varphi(g)^{-1} \in H'$ puisque $H'$ est un sous-groupe. Par suite, $g^{-1} \in \varphi^{-1}(H')$.
Donc $\varphi^{-1}(H')$ est un sous-groupe de $G$. ■

Cet énoncé est une preuve supplémentaire du fait qu'un morphisme de groupes respecte la structure de groupe.

**Exemples :**

- Soit $\varphi$ un morphisme de groupes de $(G, *)$ vers $(\mathbb{U}_3, \times)$, qui n'est pas constant.
Démontrons que $\varphi$ est surjectif.
On sait que $\varphi(G)$ est un sous-groupe de $(\mathbb{U}_3, \times)$ où, rappelons-le, $\mathbb{U}_3 = \{1, j, j^2\}$.
Or $(\mathbb{U}_3, \times)$ n'admet que deux sous-groupes (les triviaux) : $\{1\}$ et $\mathbb{U}_3$. En effet, si un sous-groupe de $\mathbb{U}_3$ contient $j$ (respectivement $j^2$), il doit aussi contenir $j \times j = j^2$ (respectivement $j^2 \times j^2 = j^4 = j$) et ce sous-groupe est donc $\mathbb{U}_3$ tout entier.
On a donc $\varphi(G) = \{1\}$ ou $\varphi(G) = \mathbb{U}_3$. Comme $\varphi$ n'est pas constant, il est impossible que $\varphi(G) = \{1\}$, donc on a $\varphi(G) = \mathbb{U}_3$. Cela prouve que $\varphi$ est surjectif.

### d) Noyau et image d'un morphisme de groupes

**Définition 13**

Soient $(G,*)$ et $(G',\star)$ deux groupes d'éléments neutres respectifs $e$ et $e'$ et $\varphi : G \longrightarrow G'$ un morphisme de groupes de $G$ vers $G'$. On appelle

▷ noyau de $\varphi$ le sous-groupe de $G$ défini par

$$\operatorname{Ker}\varphi = \varphi^{-1}(\{e'\}) = \{g \in G : \varphi(g) = e'\}\,;$$

▷ image de $\varphi$ le sous-groupe de $G'$ défini par

$$\operatorname{Im}\varphi = \varphi(G) = \{g' \in G' : \exists g \in G,\ g' = \varphi(g)\} = \{\varphi(g) : g \in G\}.$$

■ On peut utiliser la proposition 14 ou faire une démonstration à la main :

(i) Comme $\varphi(e) = e'$, on a bien $e \in \operatorname{Ker}\varphi$.
Soient $g_1, g_2 \in \operatorname{Ker}\varphi$. On a $\varphi(g_1) = e'$ et $\varphi(g_2) = e'$, d'où $\varphi(g_1 * g_2) = \varphi(g_1) \star \varphi(g_2) = e' \star e' = e'$ et donc $g_1 * g_2 \in \operatorname{Ker}\varphi$.
Soient $g \in \operatorname{Ker}\varphi$. On a $\varphi(g) = e'$, d'où $\varphi(g^{-1}) = \varphi(g)^{-1} = (e')^{-1} = e'$ et donc $g^{-1} \in \operatorname{Ker}\varphi$.
Donc $\operatorname{Ker}\varphi$ est un sous-groupe de $G$.

(ii) Comme $e' = \varphi(e)$, on a $e' \in \operatorname{Im}\varphi$.
Soient $g'_1, g'_2 \in \operatorname{Im}\varphi$ de sorte qu'il existe $g_1, g_2 \in G$ tels que $g'_1 = \varphi(g_1)$ et $g'_2 = \varphi(g_2)$. On a alors $g'_1 \star g'_2 = \varphi(g_1) \star \varphi(g_2) = \varphi(g_1 * g_2) \in \operatorname{Im}\varphi$.
Soit $g' \in \operatorname{Im}\varphi$. Il existe alors $g \in G$ tel que $g' = \varphi(g)$. Donc $(g')^{-1} = \varphi(g)^{-1} = \varphi(g^{-1}) \in \operatorname{Im}\varphi$.
Donc $\operatorname{Im}\varphi$ est un sous-groupe de $G'$ ■

Pour démontrer qu'une partie d'un groupe est un sous-groupe, il suffit donc de réaliser cette partie comme le noyau ou l'image d'un morphisme de groupes.

**Exemples :**

- Pour le morphisme $\varphi \left\{ \begin{array}{ccc} (\mathbb{R},+) & \longrightarrow & (\mathbb{C}^*,\times) \\ x & \longmapsto & \mathrm{e}^{ix} \end{array} \right.$, on a $\operatorname{Ker}\varphi = 2\pi\mathbb{Z}$ et $\operatorname{Im}\varphi = \mathbb{U}$.
- Pour le module $|\cdot| \left\{ \begin{array}{ccc} (\mathbb{C}^*,\times) & \longrightarrow & (\mathbb{R}^*,\times) \\ z & \longmapsto & |z| \end{array} \right.$, on a $\operatorname{Ker}(|\cdot|) = \mathbb{U}$ et $\operatorname{Im}(|\cdot|) = \mathbb{R}_+^*$.
- Pour exp $\left\{ \begin{array}{ccc} (\mathbb{R},+) & \longrightarrow & (\mathbb{R}_+^*,\times) \\ x & \longmapsto & \mathrm{e}^{x} \end{array} \right.$, on a $\operatorname{Ker}(\exp) = \{0\}$ et $\operatorname{Im}(\exp) = \mathbb{R}_+^*$.
- Pour ln $\left\{ \begin{array}{ccc} (\mathbb{R}_+^*,\times) & \longrightarrow & (\mathbb{R},+) \\ x & \longmapsto & \ln x \end{array} \right.$, on a $\operatorname{Ker}(\ln) = \{1\}$ et $\operatorname{Im}(\ln) = \mathbb{R}$.

Le noyau et l'image permettent de caractériser l'injectivité et la surjectivité.

**Proposition 15**

Soient $(G,*)$ et $(G',\star)$ deux groupes d'éléments neutres respectifs $e$ et $e'$ et $\varphi : G \longrightarrow G'$ un morphisme de groupes de $G$ vers $G'$. Alors

(i) $\varphi$ est injectif si, et seulement si, $\operatorname{Ker}\varphi = \{e\}$ ;

(ii) $\varphi$ est surjectif si, et seulement si, $\operatorname{Im}\varphi = G'$.

■ (i) Si $\varphi$ est injectif, $\operatorname{Ker}\varphi = \varphi^{-1}(\{e'\})$ est ou bien $\varnothing$ ou bien un singleton. Cela ne peut être que $\{e\}$ puisque l'élément $e$ appartient toujours au sous-groupe $\operatorname{Ker}\varphi$. Donc $\operatorname{Ker}\varphi = \{e\}$.

Réciproquement, supposons que $\operatorname{Ker}\varphi = \{e\}$. Soient $g_1, g_2 \in G$ tels que $\varphi(g_1) = \varphi(g_2)$. On a alors $\varphi(g_1) \star \varphi(g_2)^{-1} = e'$ ce qui s'écrit $\varphi(g_1 * {g_2}^{-1}) = e'$ ou encore $g_1 * {g_2}^{-1} \in \operatorname{Ker}\varphi$. On a donc $g_1 * {g_2}^{-1} = e$ c'est-à-dire $g_1 = g_2$. Cela démontre bien l'injectivité de $\varphi$.

(ii) La surjectivité de $\varphi$ équivaut, par définition, à $\operatorname{Im}\varphi = G'$. ■

Pour étudier l'injectivité d'un morphisme de groupe, on utilise systématiquement (i).

# C. Anneaux

Dans un anneau, on enrichit la structure de groupe en introduisant une seconde loi.

L'appelation « anneau » n'a rien à voir avec la breloque que l'on porte au doigt. C'est une traduction du vocable allemand « ring » qui désigne, en jargon teuton, un « réseau d'individus ». Dans un anneau, les liens entre les différents éléments sont donc plus forts que dans un groupe.

## C.1. Structure d'anneau

**Définition 14**

On appelle anneau un ensemble $A$ muni de deux l.c.i. : une loi d'addition notée $+$ et une loi de multiplication notée $\times$, telles que

(i) $(A, +)$ est un groupe abélien d'élément neutre $0$ ;

(ii) $(A, \times)$ est un monoïde d'élément neutre $1$ ;

(iii) $\times$ est distributive par rapport à $+$.

Si $\times$ est de plus commutative, on dit que $(A, +, \times)$ est un anneau commutatif.

On pose $A^* = A \setminus \{0\}$.

On adopte les notations classiques pour la loi additive et pour la loi multiplicative. Ainsi, si $a \in A$, on note $-a$ l'opposé de $a$ et $a^{-1}$ l'inverse de $a$ lorsque $a$ est inversible. Pour tout $n \in \mathbb{Z}$, le $n$-ème itéré additif de $a \in A$ est noté $na$ et le $n$-ème itéré additif multiplicatif de $a$ est noté $a^n$ (où $n$ n'a le droit d'être strictement négatif que lorsque $a$ est inversible).

Pour vérifier que $(A, +, \times)$ est un anneau, on doit contrôler que $+$ est interne, que $+$ est associative, que $+$ admet un élément neutre, que tout élément admet un opposé, que $+$ est commutative, que $\times$ est interne, que $\times$ est associative, que $\times$ admet un élément neutre et enfin que $\times$ est distributive sur $+$. Ouf !

Dans la pratique, nous verrons qu'il est souvent plus simple de démontrer qu'un ensemble est un sous-anneau d'un anneau connu, plutôt que de vérifier cette longue liste de propriétés.

Nous donnons ci-dessous des exemples fondamentaux d'anneaux.

**Exemples :**

- Il est possible que les deux éléments neutres $0$ et $1$ soient égaux ! Mézalors, on a $1 = 1 + 1$, ce qui implique, pour tout élément $a$ de l'anneau, que $a = a + a$ c'est-à-dire $a = 0$. Donc, dans ce cas, l'anneau se réduit à l'anneau nul $\{0\}$ (« nul » dans tous les sens du terme : parce qu'il ne contient que $0$ mais aussi parce qu'il est sans intérêt !).
- $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ sont des anneaux commutatifs.
- L'ensemble des suites réelles $(\mathbb{R}^{\mathbb{N}}, +, \times)$ et l'ensemble des suites complexes $(\mathbb{C}^{\mathbb{N}}, +, \times)$ sont des anneaux commutatifs.

  Plus généralement, $(\mathbb{R}^X, +, \times)$ et $(\mathbb{C}^X, +, \times)$ sont des anneaux commutatifs.

  De manière encore plus générale, si $(A, +, \times)$ désigne un anneau, l'ensemble fonctionnel $(A^X, +, \times)$ est également un anneau. Il est commutatif dès que $A$ l'est.
- $(\mathbb{R}^{\mathbb{R}}, +, \circ)$ n'est pas un anneau puisque $\circ$ n'est pas distributive sur $+$.

Nous verrons d'autres anneaux fondamentaux au cours de cette année ; en particulier l'anneau des matrices carrées $n \times n$ et celui des polynômes.

N'aller pas croire naïvement, à partir de cette courte liste d'exemples, que tous les anneaux sont commutatifs. Nous verrons, par exemple, que l'anneau des matrices carrées $n \times n$ ne l'est pas.

L'encadré suivant rassemble les différentes règles de calcul valides (ou non) dans un anneau.

## Vade-mecum du calcul dans un anneau

La liste de remarques suivantes concerne plus particulièrement les anneaux. Elle complète les règles de calcul que nous avions déjà vues dans le cas des groupes (qui restent évidemment valables dans un anneau, sous réserve d'existence des inverses).

Dans toutes ces remarques, $(A,+,\times)$ est un anneau et $a,b,c$ sont trois éléments de $A$.

- ▶ L'élément 0 est absorbant pour la loi $\times$, c'est-à-dire
$$0_A \times a = a \times 0_A = 0_A.$$
- ▶ On a
$$(-1_A) \times a = a \times (-1_A) = -a.$$
- ▶ Pour tout $n \in \mathbb{Z}$, on a
$$(na)b = a(nb) = n(ab),$$
ce qui nous permet de ne pas mettre de parenthèse en écrivant $nab$.
- ▶ La soustraction, notée $-$, est la loi définie par
$$a - b = a + (-b).$$
C'est une loi qui n'est ni associative, ni commutative. Par contre, la multiplication $\times$ est distributive sur $-$, c'est-à-dire
$$a(b-c) = ab - ac \quad \text{et} \quad (b-c)a = ba - ca.$$
- ♡ On peut utiliser l'astuce de Binet additive : $a = a + b - b$.
Si $b$ est inversible, on peut utiliser l'astuce de Binet multiplicative : $a = abb^{-1} = b^{-1}ba$.
- ▶ Si $a$ et $b$ commutent pour $\times$, alors, pour tout $n \in \mathbb{N}$, la formule du binôme s'applique :
$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$
- ▶ Si $a$ et $b$ commutent pour $\times$, alors, pour tout $n \in \mathbb{N}$, la formule de Bernoulli s'applique :
$$a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^{n-1-k} b^k.$$
- ▶ Sans hypothèse adéquate, on ne peut pas simplifier un facteur. Ainsi, l'égalité $ab = ac$ (ou $ba = ca$) n'implique pas que $b = c$ même si l'on sait que $a \neq 0$.

■
- ▶ On a $0a + a = (0+1)a = 1a = a$, ce qui donne $0a = 0$ en simplifiant $a$.
- ▶ On a $a + (-1_A)a = 1_A a + (-1_A)a = (1 + (-1_A))a = 0_A a = 0_A$ donc $(-1_A)a = -a$.
- ▶ Soit $n \in \mathbb{Z}$. On démontre $(na)b = n(ab)$. L'autre égalité se démontre de même.
Si $n = 0$, le résultat découle de la définition et de l'absorbance de 0.
Si $n \in \mathbb{N}^*$, on peut écrire que $(na)b = \big(\sum_{k=1}^{n} a\big)b = \sum_{k=1}^{n} ab = n(ab)$.
Pour $n = -1$, on a $ab + (-a)b = \big(a + (-a)\big)b = 0b = 0$ donc $(-a)b = -(ab)$.
Pour $n \in \mathbb{Z} \setminus \mathbb{N}$, on a alors $(na)b = \big(\sum_{k=1}^{-n} (-a)\big)b = \sum_{k=1}^{-n} (-a)b = \sum_{k=1}^{-n} -(ab) = n(ab)$.
- ▶ On a $a(b-c) = a\big(b + (-c)\big) = ab + a(-c) = ab - ac$. Idem pour l'autre égalité.
- ▶ Pour le binôme et Bernoulli, les démonstrations habituelles fonctionnent. ■

On peut retenir de ce vade-mecum qu'à l'exception des problèmes de commutation et d'inversibilité (dûment indiqués ci-avant), presque tous les réflexes de calcul acquis dans les ensembles de nombres restent valables pour les calculs dans un anneau.

**Exemples :**

- La formule $\forall n \in \mathbb{Z},\ (na)b = a(nb) = n(ab)$ implique que, pour tous $n, m \in \mathbb{Z}$, on a

$$(na)(mb) = (nm)(ab).$$

  En particulier, pour $n$ et $m$ choisis dans $\{-1; 1\}$, on obtient les trois égalités

$$a(-b) = -(ab), \qquad (-a)b = -(ab) \qquad \text{et} \qquad (-a)(-b) = ab$$

  qui justifient que la règle des signes (bien connue dans $\mathbb{R}$) se généralise dans un anneau.

- Si $a$ et $b$ commutent, la formule du binôme pour $n = 2$ nous dit que

$$(a+b)^2 = a^2 + 2ab + b^2.$$

  Par contre, si l'on ne sait pas que $a$ et $b$ commutent (a fortiori si l'on sait qu'ils ne commutent pas), alors on peut seulement écrire que

$$(a+b)^2 = a^2 + ab + ba + b^2.$$

- Si $a$ et $b$ commutent, la formule de Bernoulli pour $n = 2$ nous dit que

$$a^2 - b^2 = (a-b)(a+b).$$

  Par contre, si l'on ne sait pas que $a$ et $b$ commutent, l'égalité ci-dessus est fausse puisque le membre de droite est donné par

$$(a-b)(a+b) = a^2 + ab - ba - b^2.$$

- Si $a$ et $b$ commutent, la formule de Bernoulli pour $n = 3$ nous dit que

$$a^3 - b^3 = (a-b)(a^2 + ab + b^2).$$

- Soit $(A, +, \times)$ un anneau. Pour tout $q \in A$ et tout $n \in \mathbb{N}$, la formule de Bernoulli nous dit que $1 - q^{n+1} = (1-q)\sum_{k=0}^{n} q^k$, donc, lorsque l'élément $1-q$ est inversible, on obtient la formule de sommation d'une suite géométrique :

$$\sum_{k=0}^{n} q^k = (1-q)^{-1}(1-q^{n+1}).$$

## C. 2. Diviseurs de zéro et anneaux intègres

On a déjà signalé que 0 est un élément absorbant pour la loi $\times$, c'est-à-dire que, pour tout $a \in A$, on a $a \times 0 = 0 \times a = 0$. La réciproque n'est par contre par nécessairement vraie : il se peut qu'un produit $ab$ d'éléments de $A$ soit nul sans qu'aucun des éléments $a$ ou $b$ ne soit nul.

**Définition 15**

Soit $(A, +, \times)$ un anneau.

On dit qu'un élément $a$ de $A$ est un diviseur de zéro si $a \neq 0$ et s'il existe un élément non nul $b$ de $A$ tel que $ab = 0$ ou $ba = 0$.

On dit que l'anneau $A$ est intègre si $A \neq \{0\}$ et s'il ne possède pas de diviseurs de zéro, autrement dit lorsque

$$\forall a, b \in A, \qquad (ab = 0) \Longrightarrow (a = 0 \text{ ou } b = 0).$$

Dans un anneau intègre, on peut donc utiliser la règle que nous avons tous apprise quand nous étions petits : « un produit de facteurs est nul si, et seulement si, au moins l'un des facteurs est nul ». C'est très pratique pour résoudre des équations :-)

A contrario, dans un anneau qui n'est pas intègre, l'information $ab = 0$ ne permet pas d'en déduire quoi que soit à propos de la nullité de $a$ ou $b$. Dans un anneau qui n'est pas intègre, il n'est pas donc pas toujours facile de résoudre des équations :-(

Lorsqu'un élément $a$ n'est pas un diviseur de 0, cet élément est simplifiable. En effet, si l'on a $ab = ac$, on a $a(b - c) = 0$ ce qui implique, puisque $a$ n'est pas un diviseur de 0, que $b - c = 0$ c'est-à-dire $b = c$ (on procède de même en partant de $ba = ca$).

Ainsi, un anneau intègre est un anneau où tout élément non nul est simplifiable.

Côté bizarrerie, dans un anneau non-intègre, il est tout à fait possible de rencontrer un élément $a$ non nul tel que $a^n = 0$ avec $n \geqslant 2$. Un tel élément est alors dit nilpotent.

**Exemples :**

- Les anneaux de nombres $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ sont intègres.

  En particulier, le fait que $\mathbb{Z}$ soit intègre implique que tous les entiers non nuls sont simplifiables (c'est-à-dire que $nk = n\ell$ implique $k = \ell$ lorsque $n \in \mathbb{Z}^*$) alors même que dans $\mathbb{Z}$, seuls $-1$ et 1 sont inversibles !
- L'anneau des suites réelles $(\mathbb{R}^{\mathbb{N}}, +, \times)$ et l'anneau des suites complexes $(\mathbb{C}^{\mathbb{N}}, +, \times)$ ne sont pas intègres. En effet, si l'on considère les deux suites $(u_n)_{n\geqslant 0}$ et $(v_n)_{n\geqslant 0}$ définie par $\forall n \in \mathbb{N},\ u_n = 1 + (-1)^n$ et $\forall n \in \mathbb{N},\ v_n = 1 - (-1)^n$ alors la suite produit $(u_n v_n)_{n\geqslant 0}$ est nulle (car $u_n$ est nulle quand $v_n$ ne l'est pas et vice-versa) sans qu'aucune des deux suites $(u_n)_{n\geqslant 0}$ et $(v_n)_{n\geqslant 0}$ ne soit la suite nulle.
- De même, les anneaux fonctionnels $(\mathbb{R}^X, +, \times)$ et $(\mathbb{C}^X, +, \times)$ ne sont pas intègres (dès que $X$ possède au moins deux éléments).

Nous rencontrerons plus tard l'anneau des polynômes qui est intègre et l'anneau des matrices carrées $n \times n$ qui ne l'est pas.

7 h 00

## C. 3. Groupe des éléments inversibles

Rappelons que dans un anneau $(A, +, \times)$, les éléments n'ont pas tous un inverse pour la multiplication puisque $(A, \times)$ est seulement un monoïde, pas un groupe.

**Définition 16**

Soient $(A, +, \times)$ un anneau. L'ensemble $\mathrm{U}(A)$ des éléments inversibles de $A$ est un groupe pour la loi $\times$, que l'on appelle le groupe des unités de $A$.

■ Le produit de deux inversibles étant lui-même un inversible, on sait que $\times$ est interne sur $\mathrm{U}(A)$.
La multiplication est associative sur $\mathrm{U}(A)$ puisqu'elle l'est sur $A$ tout entier.
L'élément neutre 1 de la multiplication est inversible (puisque $1 \times 1 = 1$) donc 1 est dans $\mathrm{U}(A)$, ce qui signifie que $\mathrm{U}(A)$ possède bien un élément neutre.
Si $a$ est un élément de $\mathrm{U}(A)$ c'est-à-dire un élément inversible, alors $a^{-1}$ est lui aussi un élément inversible (d'inverse $a$), c'est-à-dire $a^{-1} \in \mathrm{U}(A)$. Ainsi $a$ est bien inversible dans $\mathrm{U}(A)$.
Donc $\big(\mathrm{U}(A), \times\big)$ est bien un groupe. ■

Le groupe des unités de $A$ est aussi parfois noté $A^\times$ (lire « $A$ croix »). La notation est dangereuse car on la confond souvent avec $A^*$.

**Exemples :**

- $\mathrm{U}(\mathbb{Z}) = \{-1; 1\}$, $\mathrm{U}(\mathbb{Q}) = \mathbb{Q}^*$, $\mathrm{U}(\mathbb{R}) = \mathbb{R}^*$ et $\mathrm{U}(\mathbb{C}) = \mathbb{C}^*$
- Le groupe des éléments inversibles de l'anneau $(\mathbb{R}^{\mathbb{N}}, +, \times)$ des suites réelles est l'ensemble des suites qui ne s'annulent jamais.

## C.4. Sous-anneaux

**Définition 17**

Soit $(A,+,\times)$ un anneau. On appelle sous-anneau de $A$ toute partie $B$ de $A$ telle que

(i) $B$ est stable pour $+$ et $\times$ ;

(ii) $B$, muni des lois induites, est encore un anneau ;

(iii) $1_B = 1_A$.

Si $B_1$ est sous-anneau de $A$ et $B_2$ est un sous-anneau de $B_1$, alors $B_2$ est un sous-anneau de $A$.

Comme dans le cas des groupes, on ne vérifie pas qu'un ensemble est un sous-anneau à l'aide de la définition mais avec la caractérisation des sous-anneaux suivante.

**Proposition 16**

Une partie $B$ d'un anneau $(A,+,\times)$ est un sous anneau si, et seulement si,

(i) $1_A \in B$ ;

(ii) $\forall b_1, b_2 \in B,\ b_1 - b_2 \in B$ ;

(iii) $\forall b_1, b_2 \in B,\ b_1 b_2 \in B$.

■ $\Leftarrow$ Soit $B$ une partie de $A$ vérifiant (i), (ii) et (iii). D'après (i) et (ii), on a $1_A - 1_A \in B$, c'est-à-dire $0_A \in B$. Combiné avec (ii), cette propriété nous dit que $(B,+)$ est un sous-groupe de $(A,+)$. De plus, $B$ est stable par $\times$ et la loi induite est évidemment associative et distributive par rapport à $+$ (elle l'était déjà dans $A$). Enfin, d'après (i), $B$ possède un élément neutre pour $\times$ qui est le même que celui de $A$. Donc $B$ est un sous-anneau de $A$.

$\Rightarrow$ Soit $B$ un sous-anneau de $A$. Il contient $1_A$ par définition donc (i) est vraie. On sait que $B$ est stable par $+$ et qu'il contient les opposés de ses éléments (puisque $(B,+)$ est un groupe), donc il est stable par $-$, ce qui démontre que (ii) est vraie. Enfin, $B$ est stable par $\times$ par définition donc (iii) est vraie. ■

Pour démontrer qu'un ensemble $B$ muni de deux lois $+$ et $\times$ est un anneau, on démontre en général que c'est un sous-anneau d'un anneau connu (on économise ainsi l'associativité, l'existence de l'opposé, la distributivité de $\times$ sur $+$ et la présence de $0_A$ dans $B$).

**Exemples :**

- Tout anneau est un sous-anneau de lui-même. Par contre (et cela peut surprendre), $\{0\}$ n'est pas un sous-anneau de $A$ (sauf si $A$ est l'anneau nul lui-même) car $1 \notin \{0\}$.
- Dans la liste $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$, chacun est un sous-anneau de ceux qui le suivent.
- L'ensemble des suites convergentes et l'ensemble des suites périodiques sont des sous-anneaux de $(\mathbb{R}^{\mathbb{N}},+,\times)$.
- L'ensemble des fonctions polynomiales, l'ensemble des fonctions continues, l'ensemble des fonctions bornées sont des sous-anneaux de $(\mathbb{R}^{\mathbb{R}},+,\times)$.
- Dans tout anneau $(A,+,\times)$, l'ensemble $\mathbb{Z}1_A = \{n1_A : n \in \mathbb{Z}\}$ est un sous-anneau de $A$ (y réfléchir).

  En particulier, le seul sous-anneau de $\mathbb{Z}$ est $\mathbb{Z}$ lui-même.

  Les sous-groupes de $\mathbb{Z}$, qui sont (rappelons-le) de la forme $n\mathbb{Z}$ où $n \in \mathbb{N}$, ne sont donc pas des sous-anneaux de $\mathbb{Z}$ (sauf pour $n = 1$). Il s'en faut de peu puisque les $n\mathbb{Z}$ vérifient bien les propriétés (ii) et (iii) de la caractérisation des sous-anneaux. Seule la propriété (i) fait défaut (sauf si $n = 1$) puisque 1 n'est pas un multiple de $n$ lorsque $n \geqslant 2$.

  On constate sur cet exemple que la structure de sous-anneau est parfois trop restrictive. Nous allons voir qu'il est bénéfique de la remplacer par la notion d'idéal (plus souple).

La proposition suivante énonce la stabilité de la structure de sous-anneau par intersection.

**Proposition 17**

Soit $(A, +, \times)$ un anneau. Une intersection (finie ou infinie) de sous-anneaux de $A$ est un sous-anneau de $A$.

■ Soit $(B_j)_{j\in J}$ une famille de sous-anneaux de $(A, +, \times)$. Démontrons que $\widehat{B} = \bigcap_{j\in J} B_j$ est un sous-anneau de $(A, +, \times)$.

Pour cela, démontrons les propriétés (i), (ii) et (iii) de la caractérisation des sous-anneaux.

On sait que $1_A \in B_j$ pour tout $j \in J$, donc $1_A \in \widehat{B}$ et (i) est vérifiée.

Si $b_1$ et $b_2$ sont deux éléments de $\widehat{B}$, ce sont aussi deux éléments de $B_j$ pour tout $j \in J$. Il s'ensuit que $b_1 - b_2 \in B_j$ et $b_1 b_2 \in B$ pour tout $j \in J$ et donc que $b_1 - b_2 \in \widehat{B}$ et $b_1 b_2 \in \widehat{B}$. Les propriétés (ii) et (iii) sont donc bien vérifiées. ■

Comme pour les groupes, le résultat précédent devient faux si l'on remplace l'intersection par la réunion.

## C. 5. Idéaux

Dans ce paragraphe, tous les anneaux considérés sont commutatifs.

Comme on l'a déjà souligné à propos de $\mathbb{Z}$, la notion de sous-anneau est souvent trop restrictive. On lui substitue par conséquent une structure moins riche mais aussi plus souple : la notion d'idéal.

**Définition 18**

Soit $(A, +, \times)$ un anneau commutatif. On appelle idéal de $A$ toute partie $I$ de $A$ telle que

(i) $(I, +)$ est un sous-groupe de $(A, +)$ ;

(ii) $\forall i \in I,\ \forall a \in A,\ ia \in I$ (absorption ou hyperstabilité).

Un idéal est donc un sous-groupe additif de l'anneau qui est hyperstable pour $\times$, c'est-à-dire stable pour la multiplication par tout élément de $A$, même ceux qui ne sont pas dans $I$.

Cette fois-ci, pas de caractérisation des idéaux ! Pour démontrer qu'une partie d'un anneau est un idéal, on démontre que c'est un sous-groupe additif de l'anneau puis on prouve l'hyperstabilité.

**Exemples :**

- Dans tout anneau commutatif $(A, +, \times)$, les ensembles $\{0\}$ et $A$ sont des idéaux. On les appelle les idéaux triviaux de $A$.

  Plus généralement, si $x \in A$, l'ensemble $xA = \{xa : a \in A\}$ des « multiples » de $a$ est un idéal de $A$, appelé idéal engendré par $a$. C'est un sous-groupe de $(A, +)$ de manière évidente. Par ailleurs, il est clairement hyperstable dans $A$ puisque le produit d'un multiple de $a$ par n'importe quel élément de $A$ est encore un multiple de $a$.

- Les idéaux de $(\mathbb{Z}, +, \times)$ sont exactement les $n\mathbb{Z}$ avec $n \in \mathbb{N}$.

  Ce sont des idéaux (on vient de le dire) et ce sont les seuls candidats puisque l'on sait qu'ils sont exactement les sous-groupes de $(\mathbb{Z}, +)$.

- Les seuls idéaux de $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont les idéaux triviaux.

  En effet, si $I$ désigne un idéal de $\mathbb{K}$ (où $\mathbb{K}$ désigne $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$) alors ou bien $I = \{0\}$, ou bien $I$ contient un élement non nul $x_0$. Mézalors, pour tout $x \in \mathbb{K}$, l'hyperstabilité de $I$ nous dit que l'élément $x = (xx_0^{-1})x_0$ appartient à $I$ et donc que $I = \mathbb{K}$. Vive Binet !

- Soit $I$ un idéal d'un anneau $A$. Si $1 \in I$, alors l'hyperstabilité de $I$ implique que $I = A$.

  Plus généralement, si $I \cap \mathrm{U}(A) \neq \varnothing$ (où $\mathrm{U}(A)$ est, rappelons-le, le groupe des unités de $A$), alors $I = A$. Pour le démontrer, il suffit d'adapter la démonstration ci-dessus justifiant que les seuls idéaux de $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont les triviaux.

La notion d'idéal est centrale en arithmétique. Elle permet, entre autres choses, de caractériser la divisibilité dans un anneau intègre.

La proposition suivante énonce la stabilité de la structure d'idéal par intersection.

**Proposition 18**

Soit $(A, +, \times)$ un anneau commutatif. Une intersection (finie ou infinie) d'idéaux de $A$ est un idéal de $A$.

■ Soit $(I_j)_{j\in J}$ une famille d'idéaux de $(A, +, \times)$. Démontrons que $\widehat{I} = \bigcap_{j\in J} I_j$ est un idéal de $(A, +\times)$.
La proposition 9 nous dit que $(\widehat{I}, +)$ est un sous-groupe de $(A, +)$.
Soient $i \in \widehat{I}$ et $a \in A$. Comme $i \in \widehat{I}$, on a $i \in I_j$ pour tout $j \in J$. Il s'ensuit, par hyperstabilité de $I_j$, que $ia \in I_j$ pour tout $j \in J$ et donc que $ia \in \widehat{I}$.
La partie $\widehat{I}$ est donc bien un idéal de $A$. ■

Le résultat précédent devient évidemment faux si l'on remplace l'intersection par la réunion.

On termine ce paragraphe avec la notion de somme d'idéaux.

Rappelons que si $A$ et $B$ désignent deux parties d'un monoïde additif $(E,+)$, la partie $A+B$ est définie, dans le monoïde ensembliste $\big(\mathscr{P}(E),+\big)$, par

$$A+B=\{a+b : a\in A,\ b\in B\}.$$

**Proposition 19**

Soient $(A,+,\times)$ un anneau commutatif et $I,I'$ deux idéaux de $A$. La partie $I+I'$ est un idéal de $A$. C'est même le plus petit idéal de $A$ qui contient $I$ et $I'$. On l'appelle l'idéal engendré par $I$ et $I'$.

■ On a $0=0+0$ avec $0\in I$ et $0\in I'$ donc $0\in I+I'$. Par ailleurs, si $s,s'\in I+I'$, on a $s=i_1+i'_1$ et $s'=i_2+i'_2$ où $i_1,i_2\in I$ et $i'_1,i'_2\in I'$, donc $s-s'=(i_1-i_2)+(i'_1-i'_2)$ avec $i_1-i_2\in I$ et $i'_1-i'_2\in I'$ puisque $I$ et $I'$ sont des groupes additifs, ce qui prouve que $s-s'\in I+I'$. On en déduit que $I+I'$ est un sous-groupe additif de $(A,+)$.

Soit $s\in I+I'$ et $a\in A$. On a $s=i+i'$ avec $i\in I$ et $i'\in I'$, donc $sa=ia+i'a$. L'hyperstabilité de $I$ nous dit que $ia\in I$ et l'hyperstabilité de $I'$ nous dit que $i'a\in I'$. Donc $sa\in I+I'$. Ainsi, $I+I'$ est hyperstable.

En conclusion, $I+I'$ est bien un idéal de $A$.

Il est clair que $I\subset I+I'$ puisque tout élément $i$ de $I$ s'écrit $i=i+0$ avec $i\in I$ et $0\in I'$. De même, on démontre que $I'\subset I+I'$.

Enfin, si un idéal contient $I$ et $I'$, alors cet idéal contient $I+I'$ (stabilité additive). Cela prouve bien que $I+I'$ est le plus petit idéal de $A$ qui contient $I$ et $I'$. ■

**Exemples :**

- Soient $a,b\in\mathbb{N}$. L'ensemble $a\mathbb{Z}$ des multiples de $a$ et l'ensemble $b\mathbb{Z}$ des multiples de $b$ sont deux idéaux de $\mathbb{Z}$. Il s'ensuit que leur somme $a\mathbb{Z}+b\mathbb{Z}$ est aussi un idéal de $\mathbb{Z}$, ce qui permet d'affirmer l'existence de $\delta\in\mathbb{N}$ tel que $a\mathbb{Z}+b\mathbb{Z}=\delta\mathbb{Z}$.

  Nous verrons, dans le chapitre d'arithmétique, que $\delta$ est le pgcd de $a$ et $b$.

## C. 6. Morphismes d'anneaux

### a) Définitions

**Définition 19**

Soient $A$ et $A'$ deux anneaux. On appelle morphisme d'anneaux de $A$ dans $A'$ toute application $\varphi : A \longrightarrow A'$ telle que

(i) $\forall a, b \in A,\ \varphi(a+b) = \varphi(a) + \varphi(b)$ ;

(ii) $\forall a, b \in A,\ \varphi(ab) = \varphi(a)\varphi(b)$ ;

(iii) $\varphi(1_A) = 1_{A'}$.

**Exemples :**

- $(u_n) \longmapsto \lim u_n$ est un morphisme de l'anneau des suites réelles convergentes vers $\mathbb{R}$.
  Cela découle du fait la limite d'une somme est la somme des limites et que la limite d'un produit est le produit des limites.
- $f \longmapsto f(0)$ est un morphisme d'anneaux de $\mathbb{R}^{\mathbb{R}}$ vers $\mathbb{R}$.
- L'application nulle n'est jamais un morphisme d'anneaux (sauf si $A'$ est l'anneau nul).

Les premières propriétés des morphismes d'anneaux sont rassemblées ci-dessous.

**Proposition 20**

Soient $A$ et $A'$ deux anneaux et $\varphi : A \longrightarrow A'$ un morphisme d'anneaux de $A$ vers $A'$. Alors

(i) $\varphi(0) = 0$ ;

(ii) $\forall a \in A,\ \varphi(-a) = -\varphi(a)$ ;

(iii) $\varphi(1) = 1$ (c'est dans la définition !) ;

(iv) pour tout inversible $a$ dans $A$, $\varphi(a)$ est inversible dans $A'$ et $\varphi(a^{-1}) = \big(\varphi(a)\big)^{-1}$.

■ Cela découle du fait qu'un morphisme d'anneaux de $A$ dans $A'$ est un morphisme du groupe $(A, +)$ vers le groupe $(A', +)$ ainsi qu'un morphisme du groupe $\big(\mathrm{U}(A), \times\big)$ vers le groupe $\big(\mathrm{U}(A'), \times\big)$ ■

On retient que, pour un morphisme d'anneaux, l'image de l'élément neutre pour $+$ (respectivement pour $\times$) est l'élément neutre pour $+$ (respectivement pour $\times$), que l'image de l'opposé est l'opposé de l'image et que l'image du symétrique (s'il existe) est le symétrique de l'image.

Comme pour les groupes, on utilise un vocabulaire adapté lorsque le morphisme est particulier.

**Définition 20**

Un morphisme d'un anneau $A$ vers lui-même (avec les mêmes l.c.i. au départ et à l'arrivée) est appelé un endomorphisme de $A$.

Un morphisme d'anneaux de $A$ vers $A'$ qui est bijectif est appelé un isomorphisme entre $A$ et $A'$. Les deux anneaux $A$ et $A'$ sont alors dits isomorphes.

Un morphisme qui est à la fois un endomorphisme et un isomorphisme de $A$ (c'est-à-dire un morphisme bijectif d'un anneau $A$ vers lui-même) est appelé un automorphisme de $A$.

**Exemples :**

- $\mathrm{Id}_A$ est un automorphisme de l'anneau $A$. Sa réciproque est elle-même.
- $z \longmapsto \overline{z}$ est un automorphisme de l'anneau $(\mathbb{C}, +, \times)$. Sa réciproque est elle-même.

### b) Opérations sur les morphismes d'anneaux

Tout marche ici comme dans les groupes.

On commence par la composition.

**Proposition 21**

La composée de deux morphismes d'anneaux est un morphisme d'anneaux.
La composée de deux endomorphismes d'anneau est un endomorphisme d'anneau.
La composée de deux isomorphismes d'anneaux est un isomorphisme d'anneaux.
La composée de deux automorphismes d'anneau est un automorphisme d'anneau.

■ Soient $A$, $A'$ et $A''$ trois anneaux et $\varphi : A \longrightarrow A'$ et $\psi : A' \longrightarrow A''$ deux morphismes d'anneaux composables. Pour tout $a, b \in A$, on a

$$(\psi \circ \varphi)(a+b) = \psi\big(\varphi(a+b)\big) = \psi\big(\varphi(a)+\varphi(b)\big) = \psi\big(\varphi(a)\big) + \psi\big(\varphi(b)\big) = (\psi \circ \varphi)(a) + (\psi \circ \varphi)(b),$$

$$(\psi \circ \varphi)(ab) = \psi\big(\varphi(ab)\big) = \psi\big(\varphi(a)\varphi(b)\big) = \psi\big(\varphi(a)\big)\psi\big(\varphi(b)\big) = (\psi \circ \varphi)(a)(\psi \circ \varphi)(b)$$

et

$$(\psi \circ \varphi)(1_A) = \psi\big(\varphi(1_A)\big) = \psi(1_{A'}) = 1_{A''},$$

donc $\psi \circ \varphi$ est bien un morphisme d'anneaux.

Les autres propriétés en découlent (parce qu'une composée de bijections est une bijection). ■

On poursuit avec le passage à l'application réciproque d'un isomorphisme.

**Proposition 22**

La bijection réciproque d'un isomorphisme d'anneaux est aussi un isomorphisme d'anneaux.

■ Soit $\varphi$ un isomorphisme de $A$ vers $A'$.
Nous savons déjà que $\varphi^{-1}$ est bijective (d'inverse $\varphi$).
Par ailleurs, pour tous $a', b' \in G'$, on a

$$\varphi^{-1}(a'+b') = \varphi^{-1}\Big(\varphi\big(\varphi^{-1}(a')\big) + \varphi\big(\varphi^{-1}(b')\big)\Big) = \varphi^{-1}\Big(\varphi\big(\varphi^{-1}(a') + \varphi^{-1}(b')\big)\Big) = \varphi^{-1}(a') + \varphi^{-1}(b'),$$

$$\varphi^{-1}(a'b') = \varphi^{-1}\Big(\varphi\big(\varphi^{-1}(a')\big)\varphi\big(\varphi^{-1}(b')\big)\Big) = \varphi^{-1}\Big(\varphi\big(\varphi^{-1}(a')\varphi^{-1}(b')\big)\Big) = \varphi^{-1}(a')\varphi^{-1}(b')$$

et

$$\varphi^{-1}(1_{A'}) = \varphi^{-1}\big(\varphi(1_A)\big) = 1_A,$$

ce qui démontre que $\varphi^{-1}$ est bien un morphisme de groupes de $A'$ vers $A$.
Donc $\varphi^{-1}$ un isomorphisme de $A'$ vers $A$. ■

On termine ce paragraphe par une dernière opération sur les morphismes : la restriction.

**Proposition 23**

Soit $\varphi : A \longrightarrow A'$ un morphisme d'anneaux de $A$ vers $A'$. Si $B$ est un sous-anneau de $A$ et $B'$ est un sous-anneau de $B'$ tels que $\varphi(B) \subset B'$, alors la restriction de $\varphi$ de $B$ vers $B'$, définie par

$$\varphi\big|_B^{B'} \left\{ \begin{array}{ccc} B & \longrightarrow & B' \\ b & \longmapsto & \varphi(b) \end{array} \right.$$

est un morphisme d'anneaux de $B$ vers $B'$.

■ AQT ■

9 h 00

### c) Image morphique (directe ou indirecte) d'un sous-anneau ou d'un idéal

Les morphismes d'anneaux se comportent avec les sous-anneaux comme les morphismes de groupes avec les sous-groupes.

**Proposition 24**

Soit $\varphi : A \longrightarrow A'$ un morphisme d'anneaux.

(i) Si $B$ est un sous-anneau de $A$, alors $\varphi(B)$ est un sous-anneau de $A'$.

(ii) Si $B'$ est un sous-anneau de $A'$, alors $\varphi^{-1}(B')$ est un sous-anneau de $A$.

■ (i) Soit $B$ un sous-anneau de $A$.
On a $1_{A'} = \varphi(1_A) \in \varphi(B)$ car $1_A \in B$.
Soient $a', b' \in \varphi(B)$ de sorte qu'il existe alors $a, b \in B$ tel que $a' = \varphi(a)$ et $b' = \varphi(b)$. Alors $a'-b' = \varphi(a)-\varphi(b) = \varphi(a-b) \in \varphi(B)$ puisque $a-b \in B$. On a aussi $a'b' = \varphi(a)\varphi(b) = \varphi(ab) \in \varphi(B)$ puisque $ab \in B$.
Donc $\varphi(B)$ est un sous-anneau de $A'$.

(ii) Soit $B'$ un sous-anneau de $A'$.
Comme $\varphi(1_A) = 1_{A'} \in B'$, on a $1_A \in \varphi^{-1}(B')$.
Soient $a, b \in \varphi^{-1}(B')$ de sorte que $\varphi(a) \in B'$ et $\varphi(b) \in B'$. Alors $\varphi(a-b) = \varphi(a) - \varphi(b) \in B'$ et $\varphi(ab) = \varphi(a)\varphi(b) \in B'$ puisque $B'$ est un sous-anneau. Par suite, $a - b \in \varphi^{-1}(B')$ et $ab \in \varphi^{-1}(B')$.
Donc $\varphi^{-1}(B')$ est un sous-anneau de $A$. ■

Avec les idéaux, on a un énoncé similaire (bien qu'un poil plus subtil pour l'image directe).

**Proposition 25**

Soit $\varphi : A \longrightarrow A'$ un morphisme d'anneaux commutatifs.

(i) Si $I$ est un idéal de $A$, alors $\varphi(I)$ est un idéal de l'anneau $\varphi(A)$ (mais pas de $A'$).

(ii) Si $I'$ est un idéal de $A'$, alors $\varphi^{-1}(I')$ est un idéal de $A$.

■ (i) Soit $I$ un idéal de $A$.
Notons que la proposition précédente nous dit que $\varphi(A)$ est un sous-anneau de $(A', +, \times)$
Comme $I$ est un sous-groupe de $(A, +)$ et que $\varphi$ est un morphisme de groupe de $(A, +)$ vers $\big(\varphi(A), +\big)$, la proposition 14 nous dit que $\varphi(I)$ est un sous-groupe de $\big(\varphi(A), +\big)$.
Soit $i' \in \varphi(I)$ et $a' \in \varphi(A)$ de sorte qu'il existe $i \in I$ et $a \in A$ tels que $i' = \varphi(i)$ et $a' = \varphi(a)$. Alors $i'a' = \varphi(i)\varphi(a) = \varphi(ia) \in \varphi(I)$ car $ia \in I$ puisque $I$ est un idéal. Donc $\varphi(I)$ est hyperstable dans $\varphi(A)$.
Ainsi $\varphi(I)$ est un idéal de $\varphi(A)$.

(ii) Soit $I'$ un idéal de $A'$.
Comme $I'$ est un sous-groupe de $(A', +)$ et que $\varphi$ est un morphisme de groupe de $(A, +)$ vers $(A', +)$, la proposition 14 nous dit que $\varphi^{-1}(I')$ est un sous-groupe de $(A, +)$.
Soit $i \in \varphi^{-1}(I')$ et $a \in A$. Alors $\varphi(ia) = \varphi(i)\varphi(a) \in I'$ car $\varphi(i) \in I'$ et $I'$ est un idéal, ce qui démontre que $ia \in \varphi^{-1}(I')$. Ainsi, $\varphi^{-1}(I')$ est hyperstable dans $A$.
Donc $\varphi^{-1}(I')$ est un idéal de $A$. ■

### d) Noyau et image d'un morphisme d'anneaux

Un morphisme d'anneaux $\varphi : A \longrightarrow A'$ étant a fortiori un morphisme de groupes additifs, on peut utiliser son noyau et son image définis par

$$\operatorname{Ker}\varphi = \{a \in A : \varphi(a) = 0_{A'}\} \qquad \text{et} \qquad \operatorname{Im}\varphi = \{a' \in A : \exists a \in A,\ a' = \varphi(a)\}.$$

Dans le cadre des morphismes d'anneaux, le noyau et l'image héritent des structures décrites dans l'énoncé suivant.

**Proposition 26**

Soit $\varphi : A \longrightarrow A'$ un morphisme d'anneaux commutatifs. Alors

(i) $\operatorname{Ker}\varphi$ est un idéal de $A$.

(ii) $\operatorname{Im}\varphi$ est un sous-anneau de $A'$.

■ (i) On peut utiliser la proposition 25 car $\operatorname{Ker}\varphi = \varphi^{-1}(\{0\})$ et $\{0\}$ est un idéal de $A'$.

On peut aussi faire une démonstration à la main.
Comme $\{0_{A'}\}$ est un sous-groupe de $(A', +)$ et que $\varphi$ est un morphisme de groupe de $(A, +)$ vers $(A', +)$, la proposition 14 nous dit que $\varphi^{-1}(\{0_{A'}\}) = \operatorname{Ker}\varphi$ est un sous-groupe de $(A, +)$.
Soit $i \in \operatorname{Ker}\varphi$ et $a \in A$. Alors $\varphi(ia) = \varphi(i)\varphi(a) = 0_{A'}\varphi(a) = 0_{A'}$, ce qui démontre que $ia \in \operatorname{Ker}\varphi$.
Ainsi, $\operatorname{Ker}\varphi$ est hyperstable dans $A$.
Donc $\operatorname{Ker}\varphi$ est un idéal de $A$.

(ii) On peut utiliser la proposition 24 car $\operatorname{Im}\varphi = \varphi(A)$ et $A$ est un sous-anneau de $A$ (pardi !).

On peut aussi faire une démonstration à la main.
On a $1_{A'} = \varphi(1_A) \in \operatorname{Im}\varphi$.
Soient $a', b' \in \operatorname{Im}\varphi$ de sorte qu'il existe alors $a, b \in A$ tel que $a' = \varphi(a)$ et $b' = \varphi(b)$. Alors $a' - b' = \varphi(a) - \varphi(b) = \varphi(a - b) \in \operatorname{Im}\varphi$ et $a'b' = \varphi(a)\varphi(b) = \varphi(ab) \in \operatorname{Im}\varphi$.
Donc $\operatorname{Im}\varphi$ est un sous-anneau de $A'$. ■

Terminons ce paragraphe en insistant sur le fait que les résultats de la proposition 15 sont toujours valables (parce qu'un morphisme d'anneaux est un morphisme de groupes additifs). Autrement dit, le noyau et l'image permettent de caractériser l'injectivité et la surjectivité d'un morphisme d'anneaux $\varphi : A \longrightarrow A'$ grâce aux équivalences :

$$(\varphi \text{ injectif}) \Longleftrightarrow (\operatorname{Ker}\varphi = \{0_A\}) \qquad \text{et} \qquad (\varphi \text{ surjectif}) \Longleftrightarrow (\operatorname{Im}\varphi = A').$$

9 h 45

# D. Corps

La présentation du concept de corps relève d'une démarche similaire à l'introduction des groupes à partir des monoïdes : on ajoute une condition d'inversibilité à tous les éléments (non nuls).

Le mot « corps » ne doit pas être pris dans son sens biologique mais dans son acception de groupe, de réseau… bref de corporation. Ainsi, en allant des « groupes » aux « anneaux » puis aux « corps », on rencontre des réunions d'éléments liés par des concepts de plus en plus forts.

## D.1. Structure de corps

**Définition 21**

On appelle corps un anneau $K$, non réduit à $\{0\}$, dont tous les éléments non nuls sont inversibles, c'est-à-dire tel que $\mathrm{U}(K) = K^*$ où, rappelons-le, $K^* = K \setminus \{0\}$.

On peut reformuler cette définition en disant que $(K, +, \times)$ est un corps lorsque $(K, +, \times)$ est un anneau et $(K^*, \times)$ est un groupe.

La plupart des corps sont commutatifs mais pas tous… Le programme demande cependant de ne s'intéresser qu'aux corps commutatifs.

**Exemples :**

- $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont les trois principaux corps que nous rencontrerons cette année.
- Nous rencontrerons plus tard un corps non commutatif plus gros que $\mathbb{C}$ : le corps des quaternions d'Hamilton.
- En arithmétique modulaire, nous verrons que l'ensemble $\{0; 1\}$ muni de l'addition et de la multiplication modulo 2 est un corps fini à 2 éléments.

  Plus généralement, pour tout nombre premier $p$, nous croiserons des corps de cardinal $p$.

  De façon encore plus générale, on peut démontrer que le cardinal $q$ d'un corps fini ne peut être que la forme $q = p^n$ où $p$ est un nombre premier et $n \in \mathbb{N}^*$ et que, pour tout nombre $q$ de cette forme, il existe un « unique » corps à $q$ élements, traditionnellement noté $\mathbb{F}_q$.

  Pour tous ces corps finis, la question de leur commutativité ne se pose pas puisqu'un très joli (et difficile) théorème, dû à Wedderburn, affirme que tout corps fini est commutatif.

Dans un corps, les problèmes d'intégrité n'existent pas, comme l'énonce la proposition suivante.

**Proposition 27**

Un corps est un anneau intègre.

■ Soient $K$ un corps et $x, y \in K$ tels que $xy = 0$. Dans le corps, l'élément $x$ est ou bien nul ou bien inversible. Dans ce dernier cas, on a $x^{-1}xy = x^{-1}0$, d'où $y = 0$. ■

Un corps étant toujours intègre et souvent commutatif, on peut donc retenir que, dans un corps, les calculs se déroulent comme on a l'habitude de les mener dans $\mathbb{R}$ ou $\mathbb{C}$.

La réciproque de la proposition 27 est fausse : $\mathbb{Z}$ est un anneau intègre mais n'est pas un corps.

On voit donc que tout sous-anneau d'un corps est un anneau intègre. Il est à noter que la réciproque est vraie dans le cas commutatif : on sait construire le corps des fractions d'un anneau commutatif intègre $A$, c'est-à-dire le plus petit corps commutatif dont $A$ est un sous-anneau (cf annexe). Par exemple, le corps des fractions de $\mathbb{Z}$ est $\mathbb{Q}$. Pour tout dire, c'est même ainsi que l'on construit $\mathbb{Q}$ à partir de $\mathbb{Z}$.

## D. 2. Sous-corps et idéaux d'un corps

**Définition 22**

On appelle sous-corps d'un corps $K$ une partie $L$ de $K$ qui est stable par $+$ et $\times$ et qui, munie des lois induites, est encore un corps.

$L$ a nécessairement le même élément neutre multiplicatif que $K$, c'est-à-dire $1_L = 1_K$. En effet, on a $1_L.1_L = 1_L = 1_K.1_L$ ce qui donne $1_K = 1_L$ après simplification par $1_L$ dans $K$ (on sait que tous les éléments non nuls de $K$ sont simplifiables puisqu'ils sont inversibles).

Si $L_1$ est sous-corps de $K$ et $L_2$ est un sous-corps de $L_1$, alors $L_2$ est un sous-corps de $K$.

Comme dans le cas des groupes ou des anneaux, on ne vérifie pas qu'un ensemble est un sous-corps à l'aide de la définition mais avec la caractérisation des sous-corps suivante.

**Proposition 28**

Une partie $L$ d'un corps $K$ est un sous-corps de $K$ si, et seulement si,

(i) $1_K \in L$ ;

(ii) $\forall x, y \in L,\ x - y \in L$ ;

(iii) $\forall x \in L,\ \forall y \in L^*,\ xy^{-1} \in L$.

■ En exercice. ■

**Exemples :**

- $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$ et $\mathbb{R}$ est un sous-corps de $\mathbb{C}$.
- Il existe toute une ribambelle de corps entre $\mathbb{Q}$ et $\mathbb{C}$. Ils sont généralement très utiles en arithmétique. Nous rencontrerons en exercice le corps $\mathbb{Q}(i)$ des nombres de Gauss.
- En utilisant l'axiome du choix, on peut montrer qu'il existe aussi des corps entre $\mathbb{R}$ et $\mathbb{C}$ mais ceux-ci sont très compliqués et peu utiles en pratique.

La proposition suivante donne les idéaux d'un corps.

**Proposition 29**

Les seuls idéaux d'un corps commutatifs $K$ sont les idéaux triviaux $\{0\}$ et $K$.

■ Nous avons déjà fait la démontration dans le cas de $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$. Répétons la.
Soit $I$ un idéal de $K$.
Si $I = \{0\}$, c'est terminé.
Sinon $I$ contient un élement non nul $x_0$. Mézalors, pour tout $x \in K$, l'hyperstabilité de $I$ nous dit que l'élément $x = (x{x_0}^{-1})x_0$ appartient à $I$ et donc que $I = K$. ■

## D.3. Morphismes de corps

**Définition 23**

Un morphisme de corps n'est rien d'autre qu'un morphisme d'anneaux entre deux anneaux qui sont des corps.

Le vocabulaire et les notations des morphismes d'anneaux sont utilisables pour les morphismes de corps.

**Exemples :**

- L'application nulle n'est jamais un morphisme de corps. Elle n'envoit pas 1 sur 1.
- Nous verrons en exercice que le seul endomorphisme de corps de $\mathbb{R}$ est l'identité.
- On peut démontrer que les seuls endomorphismes de corps de $\mathbb{C}$ qui conservent $\mathbb{R}$ (c'est-à-dire tels que l'image d'un nombre réel est un nombre réel) sont l'identité et la conjugaison.

  Si l'on retire la condition « qui conservent $\mathbb{R}$ », on peut démontrer (avec l'axiome du choix) qu'il existe une infinité d'endomorphismes de corps de $\mathbb{C}$. Ils sont très moches puisqu'ils ne sont continus en aucun point de $\mathbb{C}$.

Tous les résultats vus à propos des morphismes d'anneaux s'appliquent aux morphismes de corps.

En bonus, on a le résultat suivant, spécifique aux morphismes de corps.

**Proposition 30**

Un morphisme de corps est toujours injectif.

■ Soit $\varphi : K \longmapsto K'$ un morphisme de corps. Démontrons que $\varphi$ est injectif en prouvant que $\operatorname{Ker}\varphi = \{0_K\}$.

On propose deux démonstrations pour le prix d'une ! La première est plus élémentaire que la seconde et la seconde nécessite en plus de supposer que le corps des commutatif.

▷ On raisonne par l'absurde en supposant l'existence de $x_0 \in \operatorname{Ker}\varphi$ et $x_0 \neq 0$. Alors $x_0$ est inversible, ce qui permet d'écrire que

$$1_{K'} = \varphi(1_K) = \varphi(x_0.{x_0}^{-1}) = \varphi(x_0).\varphi({x_0}^{-1}) = 0_{K'}.\varphi({x_0}^{-1}) = 0_{K'},$$

ce qui est absurde !

▷ D'après la proposition 26, $\operatorname{Ker}\varphi$ est un idéal de $K$. Donc, par la proposition 11, on a $\operatorname{Ker}\varphi = \{0_K\}$ ou $\operatorname{Ker}\varphi = K$. Comme $\varphi \neq 0$ (puisque l'application nulle n'est pas un morphisme de corps), on ne peut pas avoir $\operatorname{Ker}\varphi = K$ et l'on a bien $\operatorname{Ker}\varphi = \{0_K\}$. ■

11 h 00