

Groupes et anneaux

Le but de ce chapitre est de poursuivre l'approche d'unification entamée dans les chapitres 15 et 16. Cette fois nous allons étudier des opérations sur les ensembles et étudier leurs propriétés. Ce chapitre se veut avant tout un chapitre de présentation des notions de groupes, d'anneaux et de corps et de certains types d'applications entre ces ensembles. Nous allons en voir de nombreux exemples. C'est principalement en deuxième année que les résultats les plus délicats (et intéressants) seront étudiés... le temps de vous familiariser avec ces concepts très abstraits au premier abord.

Dans tout ce chapitre, E désigne un ensemble non vide.

I Lois de composition interne

1) Définition et premiers exemples

En clair, une LCI prend deux éléments de E et renvoie un élément de E .

On parle parfois simplement de loi pour parler de LCI.

Une loi est interne lorsqu'on ne peut pas « sortir de l'ensemble » !

\mathbb{K} désigne comme d'habitude \mathbb{R} ou \mathbb{C} .

Nous reparlerons de lois externes dans le chapitre 28.

Définition. Une loi de composition interne (LCI) sur E est une application φ de $E \times E$ dans E .

Notation : Une LCI sur E est ce qu'on a appelé jusqu'à présent une « opération » sur E . On la note donc en général de façon opérationnelle plutôt que fonctionnelle : pour tout $(x, y) \in E^2$, plutôt que de noter $\varphi(x, y)$ l'image de (x, y) , on note plutôt $x * y$, $x + y$, $x \times y$, $x \cdot y$, $x \top y$, $x \perp y$, $x \diamond y$, $x \circ y$, etc. selon les cas. On note la loi $*$, $+$, \times , \cdot , \top , \perp , \diamond , \circ etc. selon les cas au lieu de φ .

Exemples :

- L'addition (loi notée $+$) est une LCI sur \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} et \mathbb{C} ainsi que sur \mathbb{R}_+^* , sur \mathbb{Q}_+^* par exemple, mais pas sur \mathbb{R}^* car $-1 + 1 \notin \mathbb{R}^*$.
- La multiplication (loi notée \times ou \cdot) est une LCI sur \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} et \mathbb{C} .
- La soustraction (loi notée $-$) est une loi interne sur \mathbb{Z} , \mathbb{Q} , \mathbb{R} ou \mathbb{C} mais pas sur \mathbb{N} ni sur \mathbb{R}_+^* par exemple.
- Le quotient (loi notée $/$) est une LCI sur \mathbb{Q}^* , sur \mathbb{R}^* , sur \mathbb{C}^* mais pas sur \mathbb{Z}^* par exemple. Ce n'est pas une LCI sur \mathbb{Z} , \mathbb{Q} , \mathbb{R} ou \mathbb{C} car on ne peut pas diviser par 0 !
- La puissance, c'est-à-dire l'opération $(a, b) \mapsto a^b$ est une loi interne sur \mathbb{N} .
- L'addition de fonctions (loi notée $+$) et la multiplication de fonctions (loi notée \times ou \cdot) est une LCI sur $\mathbb{K}^{\mathbb{R}}$.
- L'addition de suites (loi notée $+$) et la multiplication de suites (loi notée \times ou \cdot) est une LCI sur $\mathbb{K}^{\mathbb{N}}$.
- L'intersection (loi notée \cap) et l'union (loi notée \cup) sont des LCI sur $\mathcal{P}(E)$.
- La composition (loi notée \circ) est une LCI sur E^E .
- Une relation d'ordre ou d'équivalence n'est pas une LCI car c'est une partie de $E \times E$ (et non pas une fonction de $E \times E$ dans E).

Remarque : Il existe aussi des lois qui ne sont pas des LCI.

- Il existe des lois de composition externe sur E . Il s'agit d'opérations d'un élément de E par un élément d'un autre ensemble K pour obtenir un élément de E .
Par exemple, la multiplication d'une fonction $f : \mathbb{R} \rightarrow \mathbb{R}$ par un réel λ (consistant à associer à (λ, f) la fonction λf) est une loi de composition dite externe sur $\mathbb{K}^{\mathbb{R}}$.
- On peut aussi imaginer des opérations qui sont des applications de $E \times E$ dans un autre ensemble.

Par exemple, le produit scalaire n'est pas une LCI sur \mathbb{R}^2 ou sur \mathbb{R}^3 puisque le produit scalaire de deux vecteurs du plan ou de l'espace est un réel (donc un élément d'un autre ensemble).

Le terme *magma* n'est pas officiellement au programme.

Munir un ensemble d'une LCI (ou de lois externes) est la base de ce qu'on appelle l'algèbre. Dans ce chapitre, nous nous concentrerons uniquement sur des LCI. Lorsque l'on munit un ensemble E d'une LCI $*$, on dit que le couple $(E, *)$ est un magma. Retenons que la particularité d'une LCI sur E est qu'elle laisse stable E :

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

Nous définirons la notion de stabilité dans le paragraphe 1.4.

Ci-dessus, nous avons vu des exemples déjà rencontrés cette année. Nous en verrons d'autres dans de futurs chapitres. On peut aussi en créer de toute pièce :

Exemples :

- On définit une opération \diamond par : $\forall (x, y) \in \mathbb{R}^2, x \diamond y = 0$. C'est une LCI sur \mathbb{R} appelée loi interne nulle... mais elle ne sert pas à grand-chose.
- Munissons l'ensemble {chou; navet; carotte} d'une LCI $+$ et d'une LCI \times définies par les tables suivantes :

$+$	chou	navet	carotte	\times	chou	navet	carotte
chou	chou	navet	carotte	chou	chou	chou	chou
navet	navet	carotte	chou	navet	chou	navet	carotte
carotte	carotte	chou	navet	carotte	chou	carotte	navet

Par exemple : navet + carotte = chou et navet \times carotte = carotte.

Dans tout le chapitre, quand on donnera la table d'une loi $*$, l'élément se trouvant à l'intersection de la ligne x et de la colonne y sera $x * y$. Ce sera surtout utile quand les lois ne seront pas commutatives.

Vous verrez que les lois définies sur {chou; navet; carotte} est intéressant dans la pratique.

Une question se pose : quand on munit un ensemble d'une loi, est-ce intéressant dans la pratique ? Ces lois possèdent-elles des propriétés qui les rendent maniables ?

Avant de passer en revue les propriétés intéressantes d'une loi, définissons, pour tout $n \in \mathbb{N} \setminus \{0; 1\}$ une addition et une multiplication sur $\mathbb{Z}/n\mathbb{Z}$, ensemble introduit dans le chapitre précédent.

Exemple : Soit $n \in \mathbb{N} \setminus \{0; 1\}$. Pour tout $a \in \mathbb{Z}$, on note \bar{a} la classe d'équivalence de a pour la relation $\equiv [n]$, autrement dit :

$$\bar{a} = \{a + kn \mid k \in \mathbb{Z}\} = a + n\mathbb{Z}.$$

On note $\mathbb{Z}/n\mathbb{Z} = \{\bar{a} \mid a \in \mathbb{Z}\} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$ l'ensemble des classes d'équivalence de $\equiv [n]$. On définit une addition $\bar{+}$ et une multiplication $\bar{\times}$ sur $\mathbb{Z}/n\mathbb{Z}$ par : pour tout $(\bar{a}, \bar{b}) \in (\mathbb{Z}/n\mathbb{Z})^2$,

$$\bar{a} \bar{+} \bar{b} = \overline{a + b} \quad \text{et} \quad \bar{a} \bar{\times} \bar{b} = \overline{ab}.$$

Ces deux opérations sont-elles bien définies ?

Mais on notera plus simplement $\bar{x} + \bar{y}$ et $\bar{x}\bar{y}$ au lieu de $\bar{x} \bar{+} \bar{y}$ et $\bar{x} \bar{\times} \bar{y}$ dans les paragraphes suivants.



Comme on l'a dit dans la chapitre précédent, les ensembles les $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N} \setminus \{0; 1\}$ sont au programme que de la deuxième année. Cela signifie que les résultats que nous allons voir sur eux dans ce chapitre ne sont pas exigibles pour le moment. Nous les voyons car ce sont des exemples particulièrement intéressants et cela permet de se familiariser avec eux.

Ci-dessous les tables de l'addition de $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}$:

+	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$\mathbb{Z}/2\mathbb{Z}$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$\mathbb{Z}/3\mathbb{Z}$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\mathbb{Z}/4\mathbb{Z}$

Ci-dessous les tables de la multiplication de $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}$:

\times	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

$\mathbb{Z}/2\mathbb{Z}$

\times	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

$\mathbb{Z}/3\mathbb{Z}$

\times	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$\mathbb{Z}/4\mathbb{Z}$



Notons tout de suite la forte similarité entre l'ensemble $\{\text{chou; navet; carotte}\}$ et l'ensemble $\mathbb{Z}/3\mathbb{Z}$. Ce ne sont pas les mêmes ensembles mais leurs lois $+$ et \times sont analogues. Nous y reviendrons dans la paragraphe II.4.d.



Lorsque $*$ est commutative (resp. associative) sur E , on dit aussi que $(E, *)$ est commutatif (resp. associatif).



La commutativité et l'associativité sur $\mathbb{K}^{\mathbb{R}}$ découlent de celles sur \mathbb{K} .

2) Propriétés des LCI

a) Commutativité et associativité

Définition. Une loi de composition interne $*$ sur E est dite :

- commutative si : $\forall (a, b) \in E^2, a * b = b * a$.
- associative si : $\forall (a, b, c) \in E^3, (a * b) * c = a * (b * c)$.

Exemples :

- L'addition et la multiplication sont des lois commutatives et associatives sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \dots$
- La soustraction sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \dots$ n'est ni associative ni commutative. En effet $(1 - 2) - 3 = -4 \neq 2 = 1 - (2 - 3)$ et $2 - 1 \neq 1 - 2$. De même le quotient sur $\mathbb{Q}^*, \mathbb{R}^*$ et \mathbb{C}^* n'est ni associatif ni commutatif. La puissance sur \mathbb{N} non plus.
- L'addition et la multiplication de fonctions est commutative et associative sur $\mathbb{K}^{\mathbb{R}}$. En effet :

On vérifie que l'addition et la multiplication sont des lois commutatives et associatives sur $\{\text{chou; navet; carotte}\}$. Pour la commutativité, il suffit de voir que les tableaux sont symétriques. Pour l'associativité, il faut le faire à la main un par un. Par exemple : $(\text{chou} \times \text{navet}) \times \text{carotte} = \text{chou} \times \text{carotte} = \text{chou}$, $\text{chou} \times (\text{navet} \times \text{carotte}) = \text{chou} \times \text{carotte} = \text{chou}$.

- L'addition et la multiplication de suites est commutative et associative sur $\mathbb{K}^{\mathbb{N}}$.
- L'intersection et l'union sont commutatives et associatives sur $\mathcal{P}(E)$.
- La composition est associative sur E^E , c'est-à-dire que pour toutes fonctions f, g, h de E dans E , $f \circ (g \circ h) = (f \circ g) \circ h$, mais n'est pas commutative en général comme on l'a vu dans le chapitre 15.
- Soit $n \in \mathbb{N} \setminus \{0; 1\}$. L'addition et la multiplication sont des lois associatives et commutatives sur $\mathbb{Z}/n\mathbb{Z}$. En effet :

On montre de même que $\overline{ab} = \overline{ba}$ et $(\overline{a}b)\overline{c} = \overline{a}(\overline{b}c)$.

Remarques :

- Dire qu'une loi est associative, c'est dire que les parenthèses sont inutiles, c'est-à-dire qu'on peut faire les opérations dans l'ordre que l'on veut. Pour tout a, b, c, d appartenant à E , alors :

- * On note simplement $a * b * c$ au lieu de $(a * b) * c$ puisque l'emplacement des parenthèses n'a aucune importance.
- * En posant $A = a * b$ et $C = c * d$ on a

$$(a * b * c) * d = (A * c) * d = A * (c * d) = (a * b) * (c * d) = a * (b * C) = a * (b * (c * d)),$$

ce que l'on peut encore écrire $a * (b * c * d)$. On voit bien encore que l'on peut mettre les parenthèses où l'on veut.

- * Par récurrence immédiate, pour tout $n \geq 3$, si a_1, \dots, a_n sont des éléments de E muni d'une LCI associative $*$, alors on pourra noter $a_1 * a_2 * a_3 * \dots * a_n$ sans s'embarasser de parenthèses.
- Dire qu'une loi est commutative, c'est dire qu'on peut changer la position respective des éléments (mais pas faire les opérations dans l'ordre qu'on veut si la loi n'est pas associative). Par exemple, si la loi est commutative sur E et si $(a, b, c, d) \in E^4$, alors $(a * b) * (c * d) = (b * a) * (d * c)$. De plus, si la loi est associative (ce qui sera le cas en pratique), cette quantité est égale à

$$a * b * c * d = a * c * b * d = c * a * b * d = \dots$$

La plupart des lois que l'on rencontrera seront associatives car les lois non associatives étant sont très peu maniables.

Convention de notation additive/multiplicative.

Sauf cas exceptionnels, les lois seront notées de deux façons dans la suite : additivement (c'est-à-dire notée $+$) ou multiplicativement (c'est-à-dire notée \times ou $*$ ou sans rien).

Par convention, les lois notées additivement sont toujours commutatives.

Remarques :

- Les lois notées multiplicativement seront parfois commutatives mais pas toujours.
- Par défaut, on notera une loi multiplicativement. On gardera la notation additive quand on voudra faire une analogie avec l'addition réelle.

« sans rien » signifie que l'on écrira ab le résultat de l'opération combinant a et b dans cet ordre.

- Soit $(a_i)_{i \in I}$ une famille d'éléments de E indexée par un ensemble fini I . Pour une loi associative notée additivement (donc commutative par convention), on définit les notations $\sum_{i \in I} x_i$ de la même façon que dans le chapitre 7. Pour une loi associative et **commutative**, on définit de même la notation $\prod_{i \in I} x_i$.



Ne pas le confondre avec $n * x$ où $*$ serait une LCI notée multiplicativement puisque n n'est pas un élément de E en général !



Pour une loi notée différemment, la notation sera introduite par l'énoncé. On trouve par exemple parfois la notation f^n pour $\underbrace{f \circ \dots \circ f}_{n \text{ fois}}$ lorsque f est une application linéaire d'un espace vectoriel dans un autre (cf. chapitre 29).

- Soit $n \in \mathbb{N}^*$ et soit $x \in E$.
 - * Pour une loi associative notée additivement, on note nx l'élément $\underbrace{x + \dots + x}_{n \text{ fois}}$.
 - * Pour une loi associative notée multiplicativement, on note x^n l'élément $\underbrace{x * \dots * x}_{n \text{ fois}}$.



Prenez un temps pour réfléchir aux éventuelles formules concernant cette notation. On a l'habitude avec ces notations quand $E \subset \mathbb{C}$ mais sont-elles toutes vraies en général ? Il suffit de revenir à la définition pour s'en convaincre facilement.

Par exemple, si $(n, p) \in (\mathbb{N}^*)^2$ et $(x, y) \in E^2$,

$$- nx + px = \underbrace{(x + \dots + x)}_{n \text{ fois}} + \underbrace{(x + \dots + x)}_{p \text{ fois}} = \underbrace{x + \dots + x}_{n+p \text{ fois}} = (n+p)x$$

$$\text{et } x^n * x^p = \underbrace{(x * \dots * x)}_{n \text{ fois}} * \underbrace{(x * \dots * x)}_{p \text{ fois}} = \underbrace{x * \dots * x}_{n+p \text{ fois}} = (n+p)x.$$

$$- \text{De même } n(px) = (np)x \text{ et } (x^n)^p = x^{np}.$$

$$- nx + ny = \underbrace{(x + \dots + x)}_{n \text{ fois}} + \underbrace{(y + \dots + y)}_{m \text{ fois}} = \underbrace{(x + y) + \dots + (x + y)}_{n \text{ fois}} = n(x+y),$$

puisque $+$ est commutative par convention.



Mais, si $*$ n'est pas commutative, il est faux a priori que $x^n y^n = (xy)^n$.

Définition. Soient x et y dans E . On dit que x et y commutent (ou que x commute avec y ou le contraire) pour la loi $*$ lorsque $x * y = y * x$.

Remarques :

- Bien sûr, si $*$ est commutative, alors tout élément de E commute avec tout élément de E .
- Tout élément commute avec lui-même.

b) Distributivité

Lorsque l'ensemble est muni de deux lois, on peut se demander comment elles se comportent l'une par rapport à l'autre.

Définition. On suppose que E est muni de deux LCI $*$ et \top .

- On dit que $*$ est distributive à gauche par rapport à \top si :

$$\forall (a, b, c) \in E^3, \quad a * (b \top c) = (a * b) \top (a * c)$$

- On dit que $*$ est distributive à droite par rapport à \top si :

$$\forall (a, b, c) \in E^3, \quad (b \top c) * a = (b * a) \top (c * a)$$

- On dit que $*$ est distributive par rapport à \top si elle est distributive à gauche et à droite par rapport à \top .



Si les lois \top et $*$ sont commutatives, alors la loi \top est distributive par rapport à $*$ si et seulement si elle l'est à droite **ou** à gauche.

Exemples :

- Dans \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} et \mathbb{C} , la multiplication est distributive par rapport à l'addition.
- Dans $\mathbb{K}^{\mathbb{R}}$ et dans $\mathbb{K}^{\mathbb{N}}$, la multiplication est distributive par rapport à l'addition.

- Pour tout $n \in \mathbb{N} \setminus \{0; 1\}$, dans $\mathbb{Z}/n\mathbb{Z}$, la multiplication est distributive par rapport à l'addition. En effet :

Je vous laisse vérifier (à la main) que la multiplication est distributive sur l'addition sur $\{\text{chou}; \text{navet}; \text{carotte}\}$.

- Dans $\mathcal{P}(E)$, \cap est distributive sur \cup et \cup est distributive sur \cap . En effet, pour tout $(A, B, C) \in \mathcal{P}(E)^3$,

$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C) \quad \text{et} \quad (A \cup B) \cap C = (A \cap C) \cup (B \cap C)$$

et on conclut car \cap et \cup sont commutatives.

- La composition est distributive à droite sur l'addition dans $\mathbb{K}^{\mathbb{R}}$. En effet :

Mais elle n'est pas distributive à gauche. En effet, $\exp \circ (\sin + \cos)$ n'est pas égal à $\exp \circ \sin + \exp \circ \cos$ puisque, évaluée en 0, la première fonction vaut e et la deuxième $1 + e$.

3) Éléments particuliers pour une LCI

On suppose que E est muni d'une loi interne $*$.

La loi est donc notée multiplicativement, mais on aurait pu la noter additivement ou même de façon quelconque (T, \diamond etc.).

a) Élément neutre

Proposition/Définition. Soit $e \in E$. On dit que e est un élément neutre si, pour tout $x \in E$, $e * x = x * e = x$.

Si E admet un élément neutre, alors celui-ci est unique et on parle de l'élément neutre de E .

On pourrait aussi définir la notion d'élément neutre à gauche (lorsque $e * x = x$ pour tout $x \in E$) et à droite (lorsque $x * e = x$ pour tout $x \in E$). S'il y a un neutre à gauche et à neutre à droite, alors ils sont égaux (cf. démonstration ci-contre). Lorsque $*$ est commutative, un élément neutre à gauche est neutre à droite (et vice versa) donc neutre tout court. Lorsque $*$ n'est pas commutative, ce n'est pas forcément le cas. Par exemple la LCI puissance dans \mathbb{N} admet 1 pour neutre à droite (puisque $x^1 = x$ pour tout $x \in \mathbb{N}$) mais pas à gauche (puisque $1^x \neq x$ lorsque $x \in \mathbb{N}^*$). Il n'y a d'ailleurs pas d'élément neutre à gauche pour cet exemple. Nous n'étudierons (presque) jamais ce cas de figure.

DÉMONSTRATION.

□

Convention de notation additive/multiplicative.

Lorsque E possède un élément neutre pour une loi notée additivement, on le note 0_E ou simplement 0.

Lorsque E possède un élément neutre pour une loi notée multiplicativement, on le note 1_E ou simplement 1.

Remarque :

- Si E admet un élément neutre, celui-ci commute avec tout élément de E (par définition).
- Lorsque E est muni d'une loi $*$ associative et possède un élément neutre pour $*$, on dit que $(E, *)$ est un monoïde. Mais ce terme n'est pas officiellement au programme.

Exemples :

- 0 est l'élément neutre pour l'addition sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
- 1 est l'élément neutre de la multiplication sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

- La suite nulle est l'élément neutre pour l'addition sur $\mathbb{K}^{\mathbb{N}}$. La suite constante égale à 1 est l'élément neutre pour la multiplication sur $\mathbb{K}^{\mathbb{N}}$.
- La fonction nulle est l'élément neutre pour l'addition sur $\mathbb{K}^{\mathbb{R}}$. La fonction constante égale à 1 est l'élément neutre pour la multiplication sur $\mathbb{K}^{\mathbb{R}}$.
- La fonction Id_E est l'élément neutre pour la composition sur E^E .
- E est l'élément neutre de $\mathcal{P}(E)$ pour \cap (puisque $A \cap E = E \cap A = A$ pour tout $A \in \mathcal{P}(E)$) alors que \emptyset est l'élément neutre de $\mathcal{P}(E)$ pour \cup (puisque $A \cup \emptyset = \emptyset \cup A = A$ pour tout $A \in \mathcal{P}(E)$).
- Soit $n \in \mathbb{N} \setminus \{0; 1\}$. Alors $\bar{0}$ est l'élément neutre pour l'addition et $\bar{1}$ est l'élément neutre pour la multiplication sur $\mathbb{Z}/n\mathbb{Z}$. En effet :

- L'ensemble $2\mathbb{N}$, muni de la multiplication, n'admet pas d'élément neutre. En effet, il n'existe pas d'élément $e \in 2\mathbb{N}$ tel que $2e = 2$.

b) Élément symétrisable

Définition. On suppose que E admet un élément neutre e pour la LCI $*$. Soit $x \in E$. On dit que x admet un symétrique s'il existe $y \in E$ tel que $x * y = y * x = e$.

Proposition. Supposons que $*$ est **associative** sur E et que E admet un élément neutre pour $*$. Soit $x \in E$. Si x admet un symétrique, alors celui-ci est unique et est appelé le symétrique de x (pour la loi $*$). On le note x^{-1} par défaut.

DÉMONSTRATION.

□

Remarque : Si un élément x de E admet un symétrique, alors x commute avec son symétrique (par définition).

Convention de notation additive/multiplicative.

Lorsque $x \in E$ possède un unique symétrique pour une loi notée additivement, alors celui-ci est noté $-x$ et on parle de l'opposé de x (plutôt que de son symétrique).

Lorsque $x \in E$ possède un unique symétrique pour une loi notée multiplicativement, on dit que x est inversible. On note alors x^{-1} son symétrique et on l'appelle l'inverse de x .

Remarque : Si e est l'élément neutre sur E alors $e * e = e * e = e$ donc e admet un symétrique : lui-même. Par ailleurs un élément symétrisable qui n'est pas e peut tout à fait être égal à son symétrique, cf. exemple de (\mathbb{R}, \times) ci-dessous.

Exemples :

- Sur \mathbb{N} muni de l'addition, seul 0 admet un symétrique : lui-même. Sur \mathbb{N} muni de la multiplication, seul 1 admet un symétrique : lui-même.
- Sur \mathbb{Z} muni de l'addition, tout élément x admet un symétrique : $-x$. Sur \mathbb{Z} muni de la multiplication, seuls 1 et -1 admettent un symétrique (respectivement 1 et -1).

chou est l'élément neutre pour l'addition sur $\{\text{chou}; \text{navet}; \text{carotte}\}$ et navet est l'élément neutre pour la multiplication.

S'il n'y a pas d'élément neutre, cela n'a pas de sens de parler d'élément symétrisable. Ainsi, quand on parlera de symétrique, il sera sous-entendu qu'il existe un élément neutre.

Là encore, on pourrait définir les notions de symétrique à gauche de x (s'il existe $y \in E$ tel que $y * x = e$) et à droite (s'il existe $z \in E$ tel que $x * z = e$). Si x admet un neutre à gauche et à droite, alors ils sont égaux (cf. démonstration ci-contre). Lorsque $*$ est commutative, si x admet un symétrique à gauche, alors il en admet un droite (et vice versa) donc il en admet un tout court. Quand $*$ n'est pas commutatif, ce n'est pas forcément le cas (cf. exemple ci-contre dans E^E muni de la composition). Nous nous intéressons quasi exclusivement à l'existence de symétrique à gauche et à droite.



La notation $1/x$ est réservée à $x \in \mathbb{C}^*$ (et aux fonctions qui ne s'annulent pas, aux suites dont les termes sont non nuls). C'est tout !



On évite de noter f^{-1} l'inverse d'une fonction pour la multiplication. Cette notation est réservée à la réciproque de f quant elle est bijective, cf. point suivant).



On remarque que, pour l'addition sur l'ensemble $\{\text{chou; navet; carotte}\}$, chou admet lui-même pour symétrique (c'est l'élément neutre) et que navet et carotte sont symétriques l'un de l'autre (leurs produits est égal à chou). En revanche, chou n'admet pas de symétrique pour la loi \times .

• Sur \mathbb{Q}, \mathbb{R} ou \mathbb{C} munis de l'addition, tout élément x admet un symétrique : $-x$. Sur \mathbb{Q}, \mathbb{R} ou \mathbb{C} , tout élément non nul x admet un symétrique (un inverse) : $1/x$. Remarquons que -1 est son propre inverse.

• Sur $\mathbb{K}^{\mathbb{R}}$ muni de l'addition, tout élément f admet la fonction $-f$ pour symétrique. Sur $\mathbb{K}^{\mathbb{R}}$ muni de la multiplication, toute fonction f qui ne s'annule pas admet pour symétrique (la fonction $1/f$). Si f s'annule, elle n'admet pas de symétrique.

• Sur E^E , muni de la composition, une fonction admet un symétrique si et seulement si elle est bijective. Son symétrique est sa réciproque et est noté f^{-1} (on a bien $f \circ f^{-1} = f^{-1} \circ f = \text{Id}_E$).



On a vu dans le chapitre 15 que f est bijective si et seulement si il existe $g \in E^E$ telle que $f \circ g = g \circ f = \text{Id}_E$ et que $g = f^{-1}$ dans ce cas. Insistons une fois de plus sur l'importance d'avoir les deux égalités :

★ Déjà \circ n'est pas commutative !

★ On a vu dans l'exercice 32 du TD n° 15 que :

— il existe $g \in E^E$ tel que $g \circ f = \text{Id}_E$ (autrement f admet un inverse à gauche) si et seulement si f est injective.

— il existe $g \in E^E$ tel que $f \circ g = \text{Id}_E$ (autrement f admet un inverse à droite) si et seulement si f est surjective.

Or une injection non surjective admet plusieurs symétriques à gauche (on verra un exemple dans l'exercice __) et une surjection non injective admet plusieurs symétriques à droite.

• Pour la LCI \cap , aucun élément de $\mathcal{P}(E)$ n'admet de symétrique, à part le neutre E (en effet, l'intersection de deux parties différentes de E n'est jamais égale à E). Pour la LCI \cup , aucun élément de $\mathcal{P}(E)$ n'admet de symétrique, à part le neutre \emptyset (en effet, l'union de deux parties différentes de \emptyset n'est jamais égale à \emptyset).

• Soit $n \in \mathbb{N} \setminus \{0; 1\}$.

Proposition. Si x admet est inversible (ou symétrisable), alors x^{-1} l'est aussi, et $(x^{-1})^{-1} = x$.

DÉMONSTRATION. Il suffit de voir que $x^{-1} * x = x * x^{-1} = e$. □



Lorsque $x \in E$ est tel que

$$\forall (y, z) \in E^2, \\ x * y = x * z \Rightarrow y = z,$$

on dit que x est régulier à gauche. Lorsque

$$\forall (y, z) \in E^2, \\ y * x = z * x \Rightarrow y = z \dots$$

Proposition (simplification par un élément symétrisable). On suppose que la loi $*$ est associative. Soient $(x, y, z) \in E^3$.

• Si $x * y = x * z$ et si x est symétrisable, alors $y = z$.



• Si $y * x = z * x$ et si x est symétrisable, alors $y = z$.

DÉMONSTRATION.

... on dit que x est régulier à droite. Ainsi tout élément symétrisable est régulier à gauche et à droite. Mais la réciproque est fautive. Par exemple tout élément de \mathbb{N} est régulier pour la loi $+$ mais aucun n'est symétrisable.


L'autre est analogue. □

Remarques :

-  Lorsque x n'est pas symétrisable, il est hors de question de conclure que, si $x * y = x * z$, alors $y = z$ (c'est peut-être le cas mais il faut alors procéder autrement). C'est l'une des difficultés de ce chapitre : ne pas croire que tout se passe exactement comme dans les ensembles classiques (\mathbb{C} typiquement), même si les notations et les concepts peuvent être analogues.
-  Si on a $x * y = z * x$ et que x est symétrisable, mais que $*$ n'est pas commutative, on ne peut a priori rien conclure.


Proposition. On suppose que la loi $*$ est associative. Si x et y sont deux éléments inversibles (ou symétrisables), alors $x * y$ est symétrisable et $(x * y)^{-1} = y^{-1} * x^{-1}$.

DÉMONSTRATION.

 On change l'ordre quand on inverse un produit, cf. l'analogie avec le trésor dans le chapitre 15.

Proposition. On suppose que la loi $*$ est associative. Soient $x \in E$ et $n \in \mathbb{N}$. Si x admet un symétrique, alors x^n aussi et on a $(x^n)^{-1} = (x^{-1})^n$.

DÉMONSTRATION.

 Ces notations n'ont de sens que lorsque E admet un élément neutre et que x admet un symétrique.

Par exemple, on pose $x^{-2} = (x^{-1})^2$.

Remarques :

- Si E est muni d'une loi associative notée additivement, cette proposition se reformule ainsi : lorsque $n \in \mathbb{N}^*$, si x admet un opposé, alors nx aussi et $-nx = n(-x)$.
- Lorsque $n \in \mathbb{Z} \setminus \mathbb{N}$, si $x \in E$ admet un symétrique, on note :
 - * $x^n = (x^{-1})^{-n} = \underbrace{x^{-1} * \dots * x^{-1}}_{-n \text{ fois}}$ lorsque la loi est notée multiplicativement.
 - * $nx = (-n)(-x) = \underbrace{(-x) + \dots + (-x)}_{-n \text{ fois}}$ lorsque la loi est notée additivement.
- Lorsque E admet e pour élément neutre, on convient que $x^0 = e$ pour tout $x \in E$ (ou $0x = e$ en notation additive).

4) Partie stable pour une LCI

Supposons que E soit muni d'une LCI $*$.

Définition. Soit F une partie non vide de E . On dit que F est stable par $*$ si, pour tout $(x, y) \in F^2$, $x * y \in F$.

On rencontrera dans ce chapitre ou en exercice ou l'an prochain d'autres types d'éléments remarquables comme les éléments idempotents (les $x \in E$ qui vérifient $x * x = x$), les diviseurs de zéro, les éléments nilpotents (cf. paragraphe III.2.c), les éléments absorbants (cf. deuxième année), etc.

Remarque : Rappelons que, au départ de ce chapitre, une LCI est une application de E^2 dans E . Une partie non vide F est donc stable par $*$ lorsque la restriction de cette application à F^2 est à valeurs dans F . Autrement dit, F est stable par $*$ quand cette restriction (que l'on note parfois $*_F$) est une LCI sur F .

Pour simplifier, on dira que $*$ est encore une LCI sur F ou que $*$ induit une LCI sur F .

Exemples :

- $2\mathbb{Z}$ est une partie de \mathbb{Z} stable par addition.
- \mathbb{R}_+^* est une partie de \mathbb{R} stable par multiplication.
- \mathbb{U} est une partie de \mathbb{C} stable par multiplication.

Le terme *induit* sera revu dans le chapitre 29 : on l'emploie pour désigner des applications qui sont restreintes au départ à l'arrivée à une partie stable.


Proposition. Soit F une partie non vide stable pour $*$.

- Si $*$ est associative sur E , alors $*$ est associative sur F .
- Si $*$ est commutative sur E , alors $*$ est commutative sur F .
- Si $*$ est distributive sur une LCI \top sur E et que F est aussi stable pour \top , alors $*$ est distributive sur \top sur F .

DÉMONSTRATION. Soient $(x, y, z) \in F^3$. Si $*$ est associative sur E , comme x, y et z appartient à E , on a $x * (y * z) = (x * y) * z$. Ainsi $*$ est associative sur F . Les deux autres sont analogues. \square

C'est le principe de « qui peut le plus, peut le moins. »

Le fait que F stable ne contienne pas le neutre de E ne l'empêche pas non plus systématiquement d'admettre un (autre) élément neutre. Par exemple : si $A \subset E$, alors $\mathcal{P}(A)$ est stable pour \cap , sans que E (le neutre de $\mathcal{P}(E)$ pour \cap) ne lui appartienne. C'est alors A qui est le neutre de $\mathcal{P}(A)$ pour \cap .

 On voit que les propriétés universelles (avec un \forall) restent valable sur une partie stable. Mais ce n'est pas le cas des propriétés existentielles (avec au moins un \exists) a priori :

- L'élément neutre de E peut ne pas appartenir à une partie F stable et donc F peut ne pas admettre d'élément neutre.

Par exemple, la partie $]0; 1[$ de \mathbb{R} est stable par multiplication. Mais elle n'admet pas d'élément neutre (seul 1 laisse inchangé un élément de $]0; 1[$ par multiplication).

- Si $x \in F$ admet un symétrique sur E pour $*$, et même lorsque F admet toujours un élément neutre pour $*$, rien ne dit que ce symétrique appartient encore à F lorsque F est stable.

Par exemple, la partie $]0; 1[$ de \mathbb{R} est stable par multiplication. Elle admet 1 pour élément neutre mais multiplier deux éléments différents de $]0; 1[$ ne donne jamais 1 donc 1 est le seul élément inversible de $]0; 1[$. Autre exemple : tout élément de \mathbb{Z} admet un symétrique pour l'addition, mais aucun élément de \mathbb{N}^ n'admet de symétrique pour l'addition dans \mathbb{N}^* , bien que \mathbb{N}^* soit stable par addition.*

5) Lois produits

Proposition/Définition (loi produit). Supposons que E soit muni d'une LCI $*$. Soit F un ensemble non vide muni d'une LCI \top . On définit alors une LCI \otimes sur $E \times F$ par :

$$\forall ((x, y), (x', y')) \in (E \times F)^2, \quad (x, y) \otimes (x', y') = (x * x', y \top y').$$

De plus :

- Si $*$ et \top sont associatives sur E et F respectivement, alors \otimes est associative sur $E \times F$.
- Si $*$ et \top sont commutatives sur E et F respectivement, alors \otimes est commutative sur $E \times F$.
- Si E admet e pour neutre pour $*$ et si F admet e' pour neutre pour \top , alors (e, e') est le neutre pour $(E \times F, \otimes)$.
- Pour tout $(x, y) \in E \times F$, si x admet x^{-1} pour symétrique dans E pour $*$ et si y admet y^{-1} pour symétrique dans F pour \top , alors (x, y) admet (x^{-1}, y^{-1}) pour symétrique dans $E \times F$ pour la loi \otimes .

Pour faire simple, la première coordonnée est dans E , la seconde dans F , et on définit la loi produit comme la première loi pour la première coordonnée, et la deuxième loi pour la deuxième coordonnée. On fait les opérations idoines coordonnée par coordonnée.

DÉMONSTRATION.

II Groupes

1) Notion de groupe

Définition (groupe). On dit qu'un ensemble G muni d'une LCI $*$ est un groupe si $*$ est associative, si G possède un élément neutre pour $*$, et si tout élément de G admet un symétrique pour $*$.

Si, de plus, $*$ est commutative, on dit que G est un groupe abélien (ou commutatif).

Remarques :

- Un groupe est avant tout la donnée d'un ensemble et d'une loi. S'il s'agit de G et $*$, on dit aussi que $(G, *)$ est un groupe.
- On parle de groupe additif quand il s'agit d'un groupe muni d'une loi notée additivement. Il est alors toujours abélien par convention.
- On parle de groupe multiplicatif quand il s'agit d'un groupe muni d'une loi notée multiplicativement. Quand on ne précisera pas la loi du groupe, c'est qu'il s'agit par défaut d'un groupe multiplicatif.

Exemples : On reprend tous les exemples du paragraphe I :

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes abéliens. Cependant, $(\mathbb{N}, +)$ n'est pas un groupe car les éléments non nuls n'ont pas de symétrie.
- (\mathbb{Q}, \times) , (\mathbb{R}, \times) et (\mathbb{C}, \times) ne sont pas des groupes car 0 n'a pas de symétrie pour la loi \times . De même, (\mathbb{Z}, \times) n'est pas un groupe car les entiers différents de ± 1 n'ont pas de symétrie pour la loi \times . En revanche (\mathbb{Q}^*, \times) , (\mathbb{R}^*, \times) et (\mathbb{C}^*, \times) sont des groupes abéliens (mais $(\mathbb{Q}^*, +)$, $(\mathbb{R}^*, +)$ et $(\mathbb{C}^*, +)$ ne sont pas des groupes puisqu'ils n'ont pas d'élément neutre). Les ensembles \mathbb{Q}_+^* et \mathbb{R}_+^* sont également des groupes abéliens pour la loi \times .

Le terme *abélien* vient du mathématicien norvégien Niels Henrik Abel.

Dans ce cours, on note $*$ les lois par défaut. Mais lorsque h et h' sont deux éléments d'un groupe, on écrira souvent hh' au lieu de $h * h'$.

Quand on parlera des groupes \mathbb{Z} , \mathbb{Q} , \mathbb{R} ou \mathbb{C} , il sera sous-entendu qu'on les munit de la loi $+$. Quand on parlera des groupes \mathbb{Q}^* , \mathbb{R}^* ou \mathbb{C}^* , il sera sous-entendu qu'on les munit de la loi \times .

Mais nous verrons dans l'exercice ___ que $\mathcal{P}(E)$, muni de la différence symétrique, est un groupe.

$\{\text{chou; navet; carotte}\}$ est un groupe abélien pour l'addition, mais ce n'est pas un groupe pour la multiplication puisque chou n'admet pas d'inverse.

- $(\mathbb{K}^{\mathbb{R}}, +)$ et $(\mathbb{K}^{\mathbb{N}}, +)$ sont des groupes abéliens. Mais $(\mathbb{K}^{\mathbb{R}}, \times)$ et $(\mathbb{K}^{\mathbb{N}}, \times)$ ne sont pas des groupes puisque tous les éléments n'admettent pas de symétrie.
- Si E est un ensemble non vide, alors $(\mathcal{P}(E), \cap)$ et $(\mathcal{P}(E), \cup)$ ne sont pas des groupes (car aucun élément sauf le neutre n'admet de symétrie).
- Soit $n \in \mathbb{N} \setminus \{0; 1\}$. Alors $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien. En revanche $(\mathbb{Z}/n\mathbb{Z}, \times)$ n'est pas un groupe en général puisque seules les classes d'équivalences des entiers premiers avec n sont inversibles (nous en reparlerons dans le paragraphe 1.3.b).
- Voyons un exemple inédit. Définissons sur $[0; 2\pi[$ la loi \oplus par : pour tout $(\theta, \theta') \in [0; 2\pi[$, $\theta \oplus \theta'$ est le réel de $[0; 2\pi[$ (celui-ci existe et est unique) qui est congru à $\theta + \theta'$ modulo 2π . Vérifions que $([0; 2\pi[, \oplus)$ est un groupe abélien.

- (E^E, \circ) n'est pas un groupe puisque toutes les fonctions de E dans E ne sont pas bijectives (on rappelle que cela signifie admettre un inverse pour la loi \circ). Pourtant \circ est associative et Id_E est l'élément neutre. Cela pousse à introduire les définitions suivantes :

Proposition/Définition (groupe symétrique).

- Soit E un ensemble non vide. On appelle permutation de E toute bijection de E sur E . On note S_E l'ensemble des permutations de E . Alors (S_E, \circ) est un groupe dont Id_E est l'élément neutre. On l'appelle le groupe symétrique sur E .
- Si $n \in \mathbb{N}^*$, l'ensemble $S_{\llbracket 1; n \rrbracket}$ des permutations de $\llbracket 1; n \rrbracket$ est noté plus simplement S_n : on l'appelle le groupe symétrique d'ordre n .

Remarque : En parcourant les propriétés du paragraphe I, on obtient (notamment) les propriétés suivantes dans un groupe :

- Un groupe n'est pas vide (il contient un élément neutre).
- L'élément neutre est unique (car la loi est associative).
- Tout élément d'un groupe $(G, *)$ est régulier (on dit aussi simplifiable) à gauche et à droite, c'est-à-dire, pour tout $(x, y, z) \in G^3$:
 - ★ si $x * y = x * z$, alors $y = z$.
 - ★ si $y * x = z * x$, alors $y = z$.

Le chapitre 35 tout entier sera consacré aux propriétés du groupe symétrique S_n . Nous verrons notamment qu'il n'est pas abélien dès que $n \geq 3$ (plus généralement E n'est pas abélien dès que son cardinal est supérieur à 3).

⚠ Si $x * y = z * x$, alors $y = x^{-1} * z * x$ mais on ne peut pas conclure que $y = z$ (à moins que z et x commutent).

- La loi d'un groupe G étant associative, pour tous $n \in \mathbb{Z}$ et $x \in G$, les notations x^n (dans un groupe multiplicatif) et nx (dans un groupe additif) ont un sens. Y compris lorsque $n < 0$ puisque x est symétrisable (comme tout élément d'un groupe).

2) Groupes produits

La définition suivante découle immédiatement du paragraphe I.5 :

Définition (groupe produit). Soient $(G, *)$ et (H, \diamond) deux groupes. On définit une loi de composition interne \otimes sur $G \times H$ par :

$$\forall ((g, h), (g', h')) \in (G \times H)^2, \quad (g, h) \otimes (g', h') = (g * g', h \diamond h')$$

Alors $(G \times H, \otimes)$ est un groupe appelé groupe produit de $(G, *)$ et (H, \diamond) .

Plus précisément :

- Si e_G et e_H sont les neutres de $(G, *)$ et (H, \diamond) , alors (e_G, e_H) est le neutre de $(G \times H, \otimes)$.
- Le symétrique d'un élément $(g, h) \in G \times H$ pour \otimes est (g^{-1}, h^{-1}) où g^{-1} désigne le symétrique de g pour $*$ et h^{-1} le symétrique de h pour \diamond .

Enfin, si $(G, *)$ et (H, \diamond) sont abéliens, alors $(G \times H, \otimes)$ est abélien.

La notion de groupe produit permet de « dévisser » un gros groupe en deux groupes plus petits et plus simples, plus faciles à manier et qu'on connaît mieux.

On généralise aisément à un nombre fini quelconque de groupes, par récurrence :

Proposition/Définition. Soit $n \geq 2$. Soient $(G_1, *_1), \dots, (G_n, *_n)$ des groupes. On définit sur $G_1 \times \dots \times G_n$ une loi de composition interne \otimes par :

$$\forall ((g_1, \dots, g_n), (g'_1, \dots, g'_n)) \in (G_1 \times \dots \times G_n)^2, \\ (g_1, \dots, g_n) \otimes (g'_1, \dots, g'_n) = (g_1 *_1 g'_1, \dots, g_n *_n g'_n).$$

Alors $(G_1 \times \dots \times G_n, \otimes)$ est un groupe appelé groupe produit de $(G_1, *_1), \dots, (G_n, *_n)$.

En particulier, si $(G, *)$ est un groupe, alors, pour tout $n \geq 1$, (G^n, \otimes) est un groupe.

Exemples :

- Soit $n \geq 2$. Puisque $\mathbb{K} = \mathbb{R}$ ou \mathbb{C} est un groupe pour la loi $+$, \mathbb{K}^n est un groupe pour la loi produit que l'on note $+$ également, et qui consiste simplement à sommer coordonnée par coordonnée : pour tout $(x_1, \dots, x_n) \in \mathbb{K}^n$ et $(y_1, \dots, y_n) \in \mathbb{K}^n$,

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

- Puisque $\mathbb{Z}/2\mathbb{Z}$ est un groupe pour la loi $+$, $(\mathbb{Z}/2\mathbb{Z})^2$ est un groupe pour la loi produit que l'on note $+$ également. Ci-dessous la table du groupe :

+	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$

- Rappelons que (\mathbb{R}_+^*, \times) et $([0; 2\pi[, \otimes)$ sont des groupes (cf. paragraphe précédent). La loi produit sur $\mathbb{R}_+^* \times [0; 2\pi[$ (qui en fait un groupe) vérifie donc :

$$\forall ((r, \theta), (r', \theta')) \in \mathbb{R}_+^* \times [0; 2\pi[, \quad (r, \theta) \otimes (r', \theta') = (rr', \theta \oplus \theta').$$

Nous verrons dans le paragraphe II.4.d que ce groupe produit est isomorphe à \mathbb{C}^* .

3) Sous-groupes

On a vu plus haut dans des exemples de groupes inclus dans d'autres groupes. C'est une situation très habituelle : on parle de sous-groupe.

Un sous-groupe est tout simplement un groupe inclus dans un autre groupe pour la même loi.

Bien sûr, si K est un sous-groupe de H qui est un sous-groupe de G , alors K est un sous-groupe de G .

Cette proposition permet de ne se poser aucune question et de travailler avec le neutre sans préciser si c'est le neutre de G ou le neutre de H et de travailler avec le symétrique d'un élément sans préciser si c'est le symétrique dans G ou dans H .

Définition (sous-groupe). Soit $(G, *)$ un groupe. Soit H une partie non vide de G qui est stable pour $*$. On dit que H est un sous-groupe de G lorsque H est un groupe pour $*$.

Deux questions essentielles se posent :

- Le neutre sur G est-il le même que le neutre sur H ? On a vu dans le paragraphe 1.4 (dans la marge) qu'il pourrait avoir un neutre pour les éléments de H mais pas pour tous les éléments de G .
- Lorsque $h \in H$, le symétrique de h dans H coïncide-t-il avec son symétrique dans G ?

La réponse est oui :

Proposition. Soit $(G, *)$ un groupe. Soit H un sous-groupe de G .

- Si e est l'élément neutre de G pour $*$, alors $e \in H$ et e est le neutre sur H .
- Si $h \in H$, alors $h^{-1} \in H$ (où h^{-1} désigne le symétrique de h dans G pour $*$).

DÉMONSTRATION.

□

Remarque :

- Par contraposée, si une partie H de G ne contient pas le neutre de G , on sait directement que H n'est pas un groupe pour $*$. La réciproque est fautive : ce n'est pas parce que H contient le neutre que H est un sous-groupe.

Par exemple, $(\mathbb{R}_+, +)$ n'est pas un groupe bien qu'il contient le neutre du groupe $(\mathbb{R}, +)$.

- Si $*$ est commutative sur G , alors $*$ est commutative sur toute partie non vide stable pour $*$. Ainsi un sous-groupe d'un groupe abélien est encore un groupe abélien.

Dans la pratique, pour montrer qu'une partie d'un groupe est un sous-groupe, on utilise toujours l'une des caractérisations suivantes :

Théorème (caractérisation des sous-groupes). Soit $(G, *)$ un groupe. Soit H une partie de G . Les trois assertions suivantes sont équivalentes :

1. H est un sous-groupe de G ,
2. $\begin{cases} H \neq \emptyset \\ \forall (x, y) \in H^2, x * y \in H \text{ (stabilité par produit)} \\ \forall x \in H, x^{-1} \in H \text{ (stabilité par inverse)} \end{cases}$
3. $\begin{cases} H \neq \emptyset \\ \forall (x, y) \in H^2, x * y^{-1} \in H \text{ (stabilité par produit/inverse)} \end{cases}$

Ces caractérisations rendent rapide la vérification qu'une partie est un sous-groupe... bien plus que de vérifier que tous les axiomes sont vrais à un à un (ce qui est fastidieux, surtout pour l'associativité).

Le plus simple pour montrer que $H \neq \emptyset$ est de montrer que l'élément neutre de G appartient à H . Celui-ci doit appartenir à tout sous-groupe comme nous venons de le voir.

DÉMONSTRATION.

□

Remarque : En notation additive : si $(G, +)$ est un groupe et si H une partie de G , alors les trois assertions suivantes sont équivalentes :

1. H est un sous-groupe de G ,

2.

3.

Et pour montrer que $H \neq \emptyset$, le plus simple est de montrer que le neutre pour G (souvent noté 0 ou 0_G) appartient à H .

Exemples :

- Lorsque G est un groupe, $\{1_G\}$ et G sont des sous-groupes de G .
- \mathbb{Z} est un sous-groupe de \mathbb{Q} , qui est un sous-groupe de \mathbb{R} qui est un sous-groupe de \mathbb{C} pour l'addition.
- On a $\mathbb{U} \subset \mathbb{C}^*$, $1 \in \mathbb{U}$ et, pour tout $(z, z') \in \mathbb{U}^2$, $z(z')^{-1} = \frac{z}{z'} \in \mathbb{U}$. Ainsi \mathbb{U} est un sous-groupe de (\mathbb{C}^*, \times) et donc (\mathbb{U}, \times) est un groupe.
- Soit $n \in \mathbb{N}^*$. On a $\mathbb{U}_n \subset \mathbb{C}^*$, $1 \in \mathbb{U}_n$ et, pour tout $(z, z') \in \mathbb{U}_n^2$, $z(z')^{-1} = \frac{z}{z'} \in \mathbb{U}_n$. Ainsi \mathbb{U}_n est un sous-groupe de (\mathbb{C}^*, \times) et donc (\mathbb{U}_n, \times) est un groupe.
- Pour tout $\theta \in \mathbb{R}$, notons r_θ la rotation d'angle θ de centre O dans le plan \mathbb{R}^2 et notons $R = \{r_\theta \mid \theta \in \mathbb{R}\}$ l'ensemble des rotations de centre O . Montrons que R est un sous-groupe de $(S_{\mathbb{R}^2}, \circ)$:

On aurait aussi pu montrer que \mathbb{U}_n est un sous-groupe de \mathbb{U} .

Rappelons que $S_{\mathbb{R}^2}$ est l'ensemble des permutations de \mathbb{R}^2 (i.e. des bijections de \mathbb{R}^2 sur \mathbb{R}^2).

Ainsi un groupe non abélien (c'est le cas de $S_{\mathbb{R}^2}$) peut tout à fait admettre des sous-groupes abéliens.

Il est sous-entendu : pour la loi $+$. De plus, on rappelle que

$$n\mathbb{Z} = \{np \mid p \in \mathbb{Z}\}.$$

Si $p \in \mathbb{N}^*$, il s'agit de

$$\underbrace{n + \dots + n}_{p \text{ fois}}$$

Si $p \in \mathbb{Z} \setminus \mathbb{N}$, il s'agit de

$$\underbrace{(-n) + \dots + (-n)}_{-p \text{ fois}}$$

Si $p = 0$, il s'agit de 0 (cf. paragraphe 1.3.b et 1.3.a).

Remarquons que, contrairement à $S_{\mathbb{R}^2}$, R est abélien puisque, pour tout $\theta \in \mathbb{R}$, $r_\theta \circ r_{\theta'} = r_{\theta+\theta'} = r_{\theta'} \circ r_\theta$.

• Soit $n \in \mathbb{N}$. Montrons que $n\mathbb{Z}$ est un sous-groupe de \mathbb{Z} .

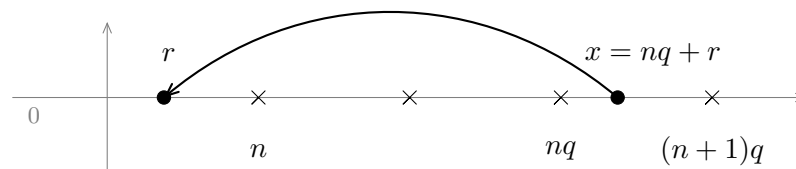
★ Tout d'abord, $0 \in n\mathbb{Z}$.

★ Soit $(x, y) \in (n\mathbb{Z})^2$. Il existe $(p, k) \in \mathbb{Z}^2$ tel que $x = np$ et $y = nk$ si bien que $x - y = n(p - k)$. Or, $p + k \in \mathbb{Z}$ donc $x - y \in n\mathbb{Z}$.

D'ailleurs ce sont les seuls sous-groupes de $(\mathbb{Z}, +)$ en vertu du théorème suivant (qui n'est au programme que de deuxième année...):

Proposition (sous-groupes de \mathbb{Z} – HP). Les sous-groupes de \mathbb{Z} sont exactement les $n\mathbb{Z}$, pour n appartenant à \mathbb{Z} .

DÉMONSTRATION.



□

D'autres résultats de deuxième année sont proposés en exercice dans la feuille de TD qui accompagne ce cours.

Terminons par un (autre) résultat sur les sous-groupes qui n'est au programme qu'en deuxième année mais déjà tout à fait accessible :

Proposition (intersection de sous-groupes – HP). Soit G un groupe. Toute intersection de sous-groupes de G est encore un sous-groupe de G .



L'union de deux sous-groupes n'est un sous-groupe que si l'un est inclus dans l'autre (cf. exercice __). L'union de plus de trois sous-groupes peut être ou ne pas être un groupe (cf. exercice __).

DÉMONSTRATION.

□

4) Morphismes de groupes

L'objectif de cette partie est d'étudier des fonctions allant d'un groupe dans un autre. Pour qu'elles soient intéressantes à étudier dans le cadre de ce chapitre, nous allons nous concentrer sur les fonctions qui préservent la structure de groupe, c'est-à-dire celles qui envoient la loi du groupe de départ sur la loi du groupe d'arrivée. On parle de morphisme de groupes.

Dans tout ce paragraphe $(G, *)$ et (G', \top) désignent des groupes. Notons e le neutre de G pour $*$ et e' le neutre de G' pour \top .

a) Définition et premiers exemples

Définition. On dit qu'une application $f : G \rightarrow G'$ est un morphisme de groupes de G dans G' si, pour tout $(x, y) \in G^2$, $f(x * y) = f(x) \top f(y)$.

Remarques :

- On parle parfois plus simplement de morphisme au lieu de morphisme de groupes. On retrouve aussi parfois le terme d'homomorphisme de groupes au lieu de morphisme de groupes (mais c'est plus rare).
- Lorsque $G = G'$ et que $* = \top$, on dit plutôt que f est un endomorphisme (de groupe) de G au lieu d'un morphisme de G dans G .

Exemples :

- La fonction exponentielle est un morphisme de $(\mathbb{R}, +)$ vers (\mathbb{R}_+^*, \times) . En effet, pour tout $(x, y) \in \mathbb{R}^2$, $\exp(x + y) = \exp(x) \exp(y)$.
- La fonction logarithme népérien est de même un morphisme de (\mathbb{R}_+^*, \times) vers $(\mathbb{R}, +)$.
- L'exponentielle complexe $z \mapsto e^z$ est un morphisme de groupes de $(\mathbb{C}, +)$ dans (\mathbb{C}^*, \times) .
- La fonction $x \mapsto e^{ix}$ est un morphisme de groupes de $(\mathbb{R}, +)$ dans (\mathbb{U}, \times) .
- $z \mapsto |z|$ est un endomorphisme de groupes de (\mathbb{C}^*, \times) . En effet, pour tous z et z' dans \mathbb{C}^* , $|z \times z'| = |z| \times |z'|$.
- Pour tout $z \in \mathbb{C}^*$, $k \mapsto z^k$ est un morphisme de groupes de $(\mathbb{Z}, +)$ dans (\mathbb{C}^*, \times) .
- Pour tout $\alpha \in \mathbb{R}^*$, $x \mapsto x^\alpha$ est un endomorphisme de groupes de (\mathbb{R}_+^*, \times) . En effet, pour tous x et y dans \mathbb{R}_+^* , $(xy)^\alpha = x^\alpha y^\alpha$.

b) Premières propriétés

Proposition. Soit f un morphisme de groupes de G dans G' . Alors $f(e) = e'$.



En d'autres termes, une fonction est un morphisme de groupes de G dans G' lorsqu'elle « transforme la loi de G en la loi de G' ».



On parlera plus bas d'isomorphisme quand un morphisme est bijectif.

DÉMONSTRATION.

□

Proposition. Soit f un morphisme de groupes de G dans G' . Alors, pour tout $x \in G$, $(f(x))^{-1} = f(x^{-1})$.

DÉMONSTRATION.


□

Proposition. Soit f un morphisme de groupes de G dans G' . Alors, pour tout $n \in \mathbb{N}^*$ et $(x_1, \dots, x_n) \in G^n$, $f(x_1 * x_2 * \dots * x_n) = f(x_1) \top f(x_2) \top \dots \top f(x_n)$.

~> DÉMONSTRATION LAISSÉE EN EXERCICE.

Se montre aisément par récurrence sur n .

Corollaire. Soit f un morphisme de groupes de G dans G' . Alors, pour tous $x \in G$ et $n \in \mathbb{Z}$, $f(x^n) = f(x)^n$.

 Ne pas perdre de vue que $f(x^n)$ est

$$f(x^n) = f(\underbrace{x * \dots * x}_{n \text{ fois}}) \quad \text{et} \quad f(x)^n = \underbrace{f(x) \top \dots \top f(x)}_{n \text{ fois}}$$

Si la loi de G est notée $+$, on a plutôt

$$f(nx) = f(x)^n.$$

Si la loi de G' est notée $+$, on a plutôt

$$f(x^n) = nf(x).$$

Si les deux lois sont notées $+$, on a plutôt

$$f(nx) = nf(x).$$

DÉMONSTRATION.

□

Proposition. Soit (G'', \diamond) un groupe. Soient f un morphisme de groupes de G dans G' et g un morphisme de groupes de G' dans G'' . Alors $g \circ f$ est un morphisme de groupes de G dans G'' .

DÉMONSTRATION.

□

c) Image directe, image réciproque, image et noyau

Proposition. Soit f un morphisme de groupes de G dans G' .

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

Un morphisme transporte donc la structure de groupe à l'arrivée ou au départ.

DÉMONSTRATION.

Rappelons que la notation $f^{-1}(K)$ désigne l'ensemble des éléments de G dont l'image par f appartient à K . Cela ne sous-entend pas que f est une bijection.

□

De la proposition précédente, on retiendra principalement deux cas particuliers très utiles en pratique :

La notation $\text{Im}(f)$ au lieu de $f(G)$ n'est autorisée que pour un morphisme de groupes! Idem ci-dessous pour $\text{Ker}(f)$.

Définition (image). Soit f est un morphisme de groupes de G dans G' . L'ensemble $f(G) = \{f(x) \mid x \in G\}$ est appelé l'image de f et noté $\text{Im}(f)$.

Remarques :

- On a $\text{Im}(f) \subset G'$: l'image est incluse dans le groupe d'arrivée! Soit $y \in G'$. Par définition :

$$x \in \text{Im}(f) \iff \exists x \in G, y = f(x).$$

- Rappelons (cf. chapitre 15) que f est surjective si et seulement si $\text{Im}(f) = G'$

Proposition. Soit f un morphisme de groupes de G dans G' . Alors $\text{Im}(f)$ est un sous-groupe de G' .

DÉMONSTRATION. Découle de la proposition ci-dessus car G est un sous-groupe de G . □

Le noyau doit son nom à *Kern* qui veut dire noyau en allemand (et non pas à *kernel* qui veut dire noyau en anglais).

Définition (noyau). Soit f un morphisme de groupes de G dans G' . L'ensemble $f^{-1}(\{e'\}) = \{x \in G \mid f(x) = e'\}$ est appelé le noyau de f et noté $\text{Ker}(f)$.

Remarque : On a $\text{Ker}(f) \subset G$: le noyau est inclus dans le groupe de départ! Soit $x \in G$. Par définition :

$$x \in \text{Ker}(f) \iff f(x) = e'.$$

Proposition. Soit f un morphisme de groupes de G dans G' . Alors $\text{Ker}(f)$ est un sous-groupe de G .

DÉMONSTRATION. Découle de la proposition ci-dessus car $\{e'\}$ est un sous-groupe de G' . \square

Exemples :

- Si $f = \exp$ désigne l'exponentielle de \mathbb{R} dans \mathbb{R}_+^* , alors
- Si $f : z \mapsto e^z$ désigne l'exponentielle complexe, alors :
- Si $f : x \in \mathbb{R} \mapsto e^{ix}$, alors
- Si $f : z \mapsto |z|$, alors
- Soit $n \in \mathbb{N}^*$. L'application $f : k \mapsto e^{\frac{2ik\pi}{n}}$ est un morphisme de groupes de $(\mathbb{Z}, +)$ dans (\mathbb{C}^*, \times) . On a

Autrement dit, f est injective si et seulement si seul e a pour image e' . Il suffit donc de tester qu'un élément a un seul antécédent (e' en l'occurrence) au lieu de tous! C'est une propriété très remarquable des morphismes.

Proposition. Soit f est un morphisme de groupes de G dans G' . Alors f est injective si et seulement si $\text{Ker}(f) = \{e\}$.

DÉMONSTRATION.

Remarques :

- Puisque $\text{Ker}(f)$ est un sous-groupe de G , il est automatique que $e \in \text{Ker}(f)$ et donc $\{e\} \subset \text{Ker}(f)$. Ainsi, quand on veut montrer que $\text{Ker}(f) = \{e\}$, on se passera de montrer $\{e\} \subset \text{Ker}(f)$ et on se contentera de montrer que $\text{Ker}(f) \subset \{e\}$. Pour cela, on écrit « Soit $x \in \text{Ker}(f)$. On a $f(x) = e'$ » et on résout pour trouver que $x = e$ et conclure.
- Et si $\text{Ker}(f) \neq \{e\}$, quel est l'intérêt du noyau ? Et bien pour résoudre des équations : donnons-nous $y \in G'$ et f un morphisme de groupes de G dans G' . On souhaite résoudre l'équation $y = f(x)$ d'inconnue $x \in G$.
 - ★ Si $y \notin \text{Im}(f)$, alors $y = f(x)$ n'admet pas de solution.



En notation addition, l'ensemble des solutions est

$$\{x_0 + z \mid z \in \text{Ker}(f)\},$$

on retrouve bien l'allure des solutions générales équations différentielles linéaires.

On en reparlera plus spécifiquement dans les chapitres 28, 29 et 37.

* Si $y \in \text{Im}(f)$, alors



d) Isomorphismes de groupe

Définition. Soit f un morphisme de groupes de G dans G' . Si f est une bijection de G sur G' , alors on dit que f est un isomorphisme de groupes.

Remarque : Lorsque $G = G'$ et $*$ = \top , on parle plutôt d'automorphisme (de groupe) de G au lieu d'isomorphisme de G dans G .

Proposition. Soit f un isomorphisme de groupes de G dans G' . Alors f^{-1} est un isomorphisme de groupes de G' dans G .

DÉMONSTRATION.



□

Définition. S'il existe un isomorphisme de groupes de G sur G' , on dit que G' est isomorphe à G ou que G et G' sont isomorphes.

Proposition. La relation « être isomorphe à » est une relation d'équivalence.

DÉMONSTRATION.

- Soit G un groupe. Alors Id_G est un isomorphisme de groupes de G dans G . Ainsi G est isomorphe à G : c'est une relation réflexive.
- Soient G et G' deux groupes. Si G est isomorphe à G' , il existe un isomorphisme de groupes de G' dans G . Puisque f^{-1} est un isomorphisme de groupes de G dans G' , il vient que G' est isomorphe à G . Ainsi c'est une relation symétrique.
- Soient G, G' et G'' deux groupes tels que G est isomorphe à G' et G' est isomorphe à G'' . Il existe alors un isomorphisme f de G' dans G et un isomorphisme g de G'' dans G' . L'application est $f \circ g$ est alors un isomorphisme (car la composée de deux morphismes est un morphisme et la composée de deux bijections est une bijection) de G'' dans G . Ainsi G est isomorphe à G'' . □

Remarques :

- Pour montrer qu'un morphisme de G dans G' est un isomorphisme, il (faut et il) suffit de montrer que $\text{Im}(f) = G'$ et que $\text{Ker}(f) = \{e\}$... mais ne pas oublier de montrer que c'est un morphisme dans un premier temps.

- S'il existe un morphisme f de groupe injective de G dans G' , alors f réalise une bijection de G dans $f(G)$. On vérifie aisément que restreindre f à $f(G)$ à l'arrivée ne change pas le fait que c'est un morphisme de groupes et donc G et $f(G)$ sont isomorphe.
- Lorsque deux groupes G et G' sont isomorphes, il y a deux aspects à prendre en compte :
 - ★ Le fait qu'il existe une bijection entre les deux signifie que l'on peut « renuméroter » les éléments de G' avec ceux de G .
 - ★ Le fait qu'il s'agisse d'un morphisme signifie que la structure de groupe est préservée par la bijection.


On peut dire en quelque sorte que les groupes G et G' sont « les mêmes ». Pour comprendre cela encore mieux, remarquons que deux groupes isomorphes ont la même table de loi (même si on ne représente effectivement cette table que lorsque le groupe est fini et de « petit » cardinal). En effet, si f est un isomorphisme de $(G, *)$ dans (G', \top) , alors, pour tout $(x, y, z) \in G^3$,

$$f(x) \top f(y) = f(z) \iff f(x * y) = f(z) \iff x * y = z$$

(car f est injective). Ainsi z se trouve à l'intersection de la ligne x et de la colonne y si et seulement si $f(z)$ se trouve à l'intersection de la ligne $f(x)$ et de la colonne $f(y)$.

Exemples :

- $(\mathbb{R}, +)$ et (\mathbb{R}_+^*, \times) sont isomorphes via la bijection \exp qui est un morphisme de groupes (cf. plus haut).

 On a vu que $f : x \mapsto e^{ix}$ est un morphisme de groupes de $(\mathbb{R}, +)$ dans (\mathbb{U}, \times) mais n'est pas bijectif car il n'est pas injectif (0 et 2π ont la même image par exemple).

Cependant f est un isomorphisme de groupes entre $([0; 2\pi[, \oplus)$ (LCI définie au paragraphe II.1) dans (\mathbb{U}, \times) . En effet :

- L'application qui à toute rotation d'angle θ et de centre O associe $e^{i\theta}$ est un isomorphisme de (R, \circ) dans (\mathbb{U}, \times) .

↪ DÉMONSTRATION LAISSÉE EN EXERCICE.


- Montrons que (\mathbb{C}^*, \times) et le groupe produit $(\mathbb{R}_+^* \times [0; 2\pi[, \otimes)$ (le groupe produit de (\mathbb{R}_+^*, \times) et de $([0; 2\pi[, \oplus)$) sont isomorphes. Pour cela, considérons la fonction $\varphi : (r, \theta) \in \mathbb{R}_+^* \times [0; 2\pi[\mapsto re^{i\theta}$ et montrons que c'est un isomorphisme.


Et réciproquement, deux groupes ayant la même table sont isomorphes : il suffit de prendre la fonction qui envoie chaque élément de la première table sur l'élément correspondant de la deuxième table.

Pour les mêmes raisons l'exponentielle complexe est un morphisme de groupes de $(\mathbb{C}, +)$ dans (\mathbb{C}^*, \times) qui n'est pas un isomorphisme.

Remarquons que l'application f qui va de $\{\text{chou; navet; carotte}\}$ dans $\mathbb{Z}/3\mathbb{Z}$ telle que $f(\text{chou}) = \bar{0}$, $f(\text{navet}) = \bar{1}$ et $f(\text{carotte}) = \bar{2}$ est un isomorphisme de groupes pour les lois additives.

- Soit $n \in \mathbb{N} \setminus \{0; 1\}$. Les groupes $(\mathbb{Z}/n\mathbb{Z}, +)$ et (\mathbb{U}_n, \times) sont isomorphes. En effet, notons $\psi : \bar{k} \in \mathbb{Z}/n\mathbb{Z} \mapsto e^{\frac{2ik\pi}{n}}$.


 On verra dans le chapitre 30 (et on en a parlé dans la paragraphe hors-programme du chapitre 15) que deux ensembles finis ayant le même nombre d'éléments sont en bijection. Une question se pose alors : deux groupes finis de même cardinal (on parle d'ordre) sont-ils isomorphes ? Et bien pas forcément !


 Il s'agit du groupe (\mathbb{U}_4, \times) et du groupe produit (\mathbb{U}_2, \times) avec lui-même.

Par exemple les groupes $\mathbb{U}_4 = \{-1; -i; 1; i\}$ et $\mathbb{U}_2^2 = \{(-1, -1); (-1, 1); (1, -1); (1, 1)\}$ ne sont pas isomorphes. En effet :

III Anneaux

1) Notion d'anneau

 On note A^* l'ensemble $A \setminus \{0_A\}$.

 On réserve l'adjectif abélien pour les groupes, cela n'a pas de sens de dire qu'un anneau est abélien.

Définition. Soit A un ensemble muni de deux lois internes $+$ et \times . On dit que $(A, +, \times)$ est un anneau si :



- $(A, +)$ est un groupe **abélien** dont l'élément neutre est noté 0_A ou 0 .
- \times est associative
- A admet un élément neutre pour \times , noté 1_A ou 1 .
- \times est distributive par rapport à $+$.


Si la loi \times est de plus commutative, l'anneau est dit commutatif.


Remarques :

- Puisque $(A, +)$ est un groupe, on retrouve toutes les propriétés des groupes vus dans le paragraphe précédent :
 - * A n'est pas vide (il contient un élément neutre qui est unique).
 - * Tout élément de $(A, +)$ est régulier, c'est-à-dire, pour tout $(a, b, c) \in A^3$, si $a + b = a + c$ ou $b + a = c + a$, alors $b = c$.

Pour tout $a \in A$, on note $-a$ le symétrique de a pour la loi $+$.


- On parle parfois d'anneau sans préciser les lois. Par défaut, la première loi est notée additivement (elle est toujours commutative) et la seconde est notée multiplicativement (elle n'est pas forcément commutative). On pourrait noter les lois autrement mais c'est rare : tout l'intérêt d'un anneau est de se rapprocher les deux lois de celles de \mathbb{Z} (même si nous verrons qu'un anneau ne partage pas toutes les propriétés de \mathbb{Z} non plus a priori).
- Lorsque a et b sont des éléments d'un anneau A , on notera ab le produit $a \times b$.
 Mais le produit n'est pas commutatif en général (contrairement à l'addition). Rappelons qu'on dit que deux éléments a et b commutent (pour le produit) lorsque $ab = ba$.
-  Nous allons voir que, sauf si A est réduit à $\{0_A\}$, 0_A n'est jamais inversible pour \times si bien que, dans un anneau non réduit à 0_A , (A, \times) n'est jamais un groupe. Nous verrons aussi que (A^*, \times) n'est pas non plus un groupe en général puisque tout élément non nul n'est pas inversible a priori. C'est d'ailleurs l'un des points centraux de ce paragraphe.

 Mais on ne note jamais \times la première loi et $+$ la deuxième.

 Puisque la loi $+$ est commutative, quand on dira que deux éléments commutent, cela concernera toujours la loi \times .

Exemples :

- $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des anneaux commutatifs.
- $(\mathbb{K}^{\mathbb{R}}, +, \times)$ et $(\mathbb{K}^{\mathbb{N}}, +, \times)$ sont des anneaux commutatifs.
- $(\mathbb{K}^{\mathbb{R}}, +, \circ)$ n'est pas un anneau car la composition n'est distributive par rapport à l'addition qu'à gauche.
- En ressemblant tout ce que nous avons montré dans les paragraphes précédents, pour tout $n \in \mathbb{N} \setminus \{0; 1\}$, $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.


 $\{\text{chou; navet; carotte}\}$ est un anneau commutatif.

Remarque : Nous n'avons pas vraiment vu d'anneaux non commutatifs pour le moment. L'exemple classique est celui des matrices carrées d'une taille donnée (cf. chapitre 23).

Proposition/Définition (anneau produit). Soient $(A, +, \times)$ et $(A', +, \times)$ deux anneaux. On définit deux LCI \oplus et \otimes sur $A \times A'$ par : pour tous (a, b) et (x, y) dans $A \times A'$,

$$(a, b) \oplus (x, y) = (a + x, b + y) \quad \text{et} \quad (a, b) \otimes (x, y) = (a \times x, b \times y).$$

Alors $(A \times A', \oplus, \otimes)$ est un anneau appelé anneau produit de A et A' . De plus, si A et A' sont commutatifs, alors $A \times A'$ est commutatif.

 On note différemment les lois de A et de A' pour bien comprendre la preuve mais souvent on les note de la même façon. De plus \oplus et \otimes sont en général encore notées $+$ et \times .

DÉMONSTRATION. Tout découle immédiatement du paragraphe 1.5 sauf la distributivité de \otimes sur \oplus . Soit (a, b) , (x, y) et (s, t) dans $A \times A'$. On a :

$$(a, b) \otimes ((x, y) \oplus (s, t)) = (a, b) \otimes (x + s, y + t) = (a \times (x + s), b \times (y + t)).$$

Puisque \times est distributive sur $+$ et \times est distributive sur $+$, il vient que :

$$(a, b) \otimes ((x, y) \oplus (s, t)) = (a \times x + a \times s, b \times y + b \times t) = (a \times x, b \times y) \oplus (a \times s, b \times t)$$

donc $(a, b) \otimes ((x, y) \oplus (s, t)) = (a, b) \otimes (x, y) \oplus (a, b) \otimes (s, t)$. On montre la distributivité à droite de même. \square

2) Propriétés des anneaux

a) 0 est absorbant

Proposition. Soit A un anneau. L'élément neutre de 0_A pour la somme est absorbant, c'est-à-dire :

$$\forall a \in A, \quad a \times 0_A = 0_A \times a = 0_A.$$

DÉMONSTRATION.

L'égalité $a \times 0_A = 0_A$ s'obtient de façon analogue (en exploitant la distributivité à droite). \square

Corollaire. Soit A un anneau. On a $0_A = 1_A$ si et seulement si A est un singleton.

DÉMONSTRATION.

Le cas où A est réduit à singleton n'est pas très intéressant. Nous supposons dans la suite que ce n'est pas le cas et, alors $1_A \neq 0_A$.

b) Calcul dans un anneau


Dans ce paragraphe, on se donne A un anneau.

Commençons par quelques rappels de notation. Soit $a \in A$.

- Si $n \in \mathbb{N}^*$, on note $na = \underbrace{a + \dots + a}_{n \text{ termes}}$. Si $n \in \mathbb{Z} \setminus \mathbb{N}$, on note $na = \underbrace{(-a) + \dots + (-a)}_{-n \text{ termes}}$.

Enfin, on convient $0a = 0_A$. Toutes les propriétés déjà vues dans les paragraphes précédents sont vraies.

- Si $n \in \mathbb{N}$, on note $a^n = \underbrace{a \times \dots \times a}_{n \text{ termes}}$. On convient que $a^0 = 1_A$.

 Toutefois, lorsque a n'est pas inversible, la notation a^n n'a pas de sens lorsque $n \in \mathbb{Z} \setminus \mathbb{N}$.

Les propriétés suivantes ont déjà été évoquées plus haut : pour tout $(a, b) \in A^2$,

- pour tout $(n, p) \in \mathbb{Z}^2$,
 - ★ $(n + p)a = na + pa$,
 - ★ $(np)a = n(pa) = p(na)$,
 - ★ $n(-a) = (-n)a = -(na)$ (et on note $-na$ tout simplement).
 - ★ $n(a + b) = na + nb$ et $n(a - b) = na - nb$,
- pour tout $(n, p) \in \mathbb{N}^2$,
 - ★ $a^{n+p} = a^n a^p$,
 - ★ $a^{np} = (a^n)^p = (a^p)^n$,

Si, de plus, a est inversible, alors ces deux dernières propriétés restent valables pour tout $(n, p) \in \mathbb{Z}^2$.

Ne pas confondre $0a$ avec $0_A \times a \dots$ même si, en l'occurrence, cela fait la même chose.

La plupart ont déjà été montrées mais elles se retrouvent facilement.

Rappelons enfin que, dans un anneau, \times est distributive sur $+$, c'est-à-dire

$$\forall (a, b, c) \in A^3, \quad a(b + c) = ab + ac \quad \text{et} \quad (b + c)a = ba + ca.$$

Cela permet de montrer de nombreuses autres propriétés très familières :

Proposition. Soit $(a, b, c) \in A^3$. On a :

- $(-a)b = a(-b) = -ab$ et $(-a)(-b) = ab$.
En particulier $(-1_A)a = a(-1_A) = -a$ et $(-1_A)^2 = 1_A$.
- Pour tout $n \in \mathbb{Z}$, $(na)b = a(nb) = nab$.
- $a(b - c) = ab - ac$ et $(b - c)a = ba - ca$,



On ne peut pas juste écrire que $ab = ba$. On ne sait pas ici si a et b commutent !



Avec des pointillés, cela semble immédiat par distributivité lorsque $n \in \mathbb{N}^*$:

$$\begin{aligned} (na)b &= \underbrace{(a + \dots + a)}_{n \text{ fois}} b \\ &= \underbrace{ab + \dots + ab}_{n \text{ fois}} \\ &= nab. \end{aligned}$$

Idem pour l'autre.

DÉMONSTRATION.

□

De nombreuses propriétés s'étendent par récurrence :

- Pour tout $n \geq 2$, pour tout $(a_1, \dots, a_n) \in A^n$ et $b \in A$,

$$b \left(\sum_{k=1}^n a_k \right) = \sum_{k=1}^n ba_k \quad \text{et} \quad \left(\sum_{k=1}^n a_k \right) b = \sum_{k=1}^n a_k b.$$

- Pour tout $n \geq 2$, pour tout $(a_1, \dots, a_n) \in A^n$ et $(b_1, \dots, b_n) \in A^n$,

$$\left(\sum_{i=1}^n a_i \right) \left(\sum_{j=1}^n b_j \right) = \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} a_i b_j.$$



Il faut impérativement garder l'ordre des termes en développant/factorisant car le produit n'est pas commutatif a priori. Par exemple, lorsque a et b sont dans A , on a :

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

mais hors de question de simplifier en $a^2 + 2ab + b^2 \dots$ à moins que a et b ne commutent. Explorons cette hypothèse supplémentaire.



C'est un cas particulier de la formule ci-dessus

Lemme. Soient a et b deux éléments de A qui commutent. Alors, pour tout $k \in \mathbb{N}$, a et b^k commutent.

DÉMONSTRATION. Raisonnons par récurrence sur k .

- Pour tout $k \in \mathbb{N}$, notons H_k : « $ab^k = b^ka$ ».
- $b^0 = 1_A$ et tout élément de A commute avec le neutre donc H_0 est vraie.
- Soit $k \in \mathbb{N}$. Supposons H_k vraie. On a $ab^{k+1} = ab^kb$ donc (par hypothèse de récurrence), $ab^{k+1} = b^kab$. Puisque a et b commutent, il vient $ab^{k+1} = b^kba = b^{k+1}a$ donc H_{k+1} est vraie.
- D'après le principe de récurrence, H_k est vraie pour tout $k \in \mathbb{N}$. □

Proposition. Soient a et b deux éléments de A qui commutent. Soit $(k, \ell) \in \mathbb{N}^2$. Alors $a^k b^\ell = b^\ell a^k$.

DÉMONSTRATION. On applique le lemme avec a, b et ℓ : $ab^\ell = b^\ell a$. Puis on applique encore le lemme avec b, a^ℓ et k : $a^k b^\ell = b^\ell a^k$. □

Proposition. Soient a et b deux éléments de A qui commutent. Alors, pour tout $k \in \mathbb{N}$, $(ab)^k = a^k b^k$.

DÉMONSTRATION. Raisonnons par récurrence sur k .

- Pour tout $k \in \mathbb{N}$, notons H_k : « $(ab)^k = a^k b^k$ ».
- $(ab)^0 = 1_A = 1_A 1_A = a^0 b^0$ donc H_0 est vraie.
- Soit $k \in \mathbb{N}$. Supposons H_k vraie. On a alors $(ab)^{k+1} = (ab)^k ab = a^k b^k ab$. Puisque a et b commutent, a et b^k aussi (d'après le lemme) et donc $(ab)^{k+1} = a^k ab^k b = a^{k+1} b^{k+1}$. Ainsi $H(k+1)$ est vraie.
- D'après le principe de récurrence, H_k est vraie pour tout $k \in \mathbb{N}$. □



L'hypothèse que a et b commutent est indispensable.

Théorème (formule du binôme de Newton). Soient a et b deux éléments de A qui commutent. Alors, pour tout $n \in \mathbb{N}$,

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

DÉMONSTRATION. On raisonne par récurrence sur $n \in \mathbb{N}$.

- **Initialisation** : Nous avons

$$\sum_{k=0}^0 \binom{0}{k} a^k b^{0-k} = 1_A = (a + b)^0.$$

donc la formule est vraie au rang 0.

- **Hérédité** : Soit $n \in \mathbb{N}$. Supposons que la formule soit vraie au rang n . Alors, $(a + b)^{n+1} = (a + b)^n \times (a + b)$ et, par hypothèse de récurrence,

$$\begin{aligned} (a + b)^{n+1} &= \left(\sum_{k=0}^n \binom{n}{k} a^k b^{n-k} \right) \times (a + b) \\ &= \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} a + \sum_{k=0}^n \binom{n}{k} a^k b^{n-k+1}, \end{aligned}$$

par distributivité (à droite) du produit sur la somme. Or, a et b commutent donc, d'après le lemme ci-dessus,

$$\begin{aligned}(a+b)^{n+1} &= \sum_{k=0}^n \binom{n}{k} a^k a b^{n-k} + \sum_{k=0}^n \binom{n}{k} a^k b^{n-k+1} \\ &= \sum_{k=0}^n \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^n \binom{n}{k} a^k b^{n-k+1}.\end{aligned}$$



A partir de cette ligne, la démonstration est totalement identique au cas complexe.

Faisons le changement d'indice $p = k + 1$ dans la première somme :

$$\begin{aligned}(a+b)^{n+1} &= \sum_{p=1}^{n+1} \binom{n}{p-1} a^p b^{n-p+1} + \sum_{k=0}^n \binom{n}{k} a^k b^{n+1-k} \\ &= a^0 b^{n+1} + \sum_{k=1}^n \left(\binom{n}{k-1} + \binom{n}{k} \right) a^k b^{n+1-k} + a^{n+1} b^0 \\ &= b^{n+1} + \sum_{k=1}^n \binom{n+1}{k} a^k b^{n+1-k} + a^{n+1},\end{aligned}$$

d'après la formule de Pascal. Finalement, puisque $\binom{n+1}{n+1} = \binom{n+1}{0} = 1$, nous obtenons que la formule est vraie au rang $n+1$.

- **Conclusion.** Par récurrence, pour tout $n \in \mathbb{N}$, la formule est vraie au rang n . \square

Théorème. Soient $n \in \mathbb{N}^*$ et $(a, b) \in A^2$ qui commutent. Alors :

$$a^n - b^n = (a - b) \times \left(\sum_{k=0}^{n-1} a^k b^{n-1-k} \right)$$

\rightsquigarrow DÉMONSTRATION LAISSÉE EN EXERCICE.

Puisque 1_A commute avec tout élément de A , on a :

Corollaire. Pour tous $n \in \mathbb{N}^*$ et $a \in A$,

$$1_A - a^n = (1_A - a) \times \sum_{k=0}^{n-1} a^k.$$

c) Diviseurs de zéro et intégrité

En dehors de la non commutativité potentielle de la loi \times , explorons une autre propriété des anneaux qui n'a pas lieu dans \mathbb{Z} : l'existence possible de diviseurs de zéro.



Ainsi, dans un anneau quelconque, il est faux de dire que, si un produit de deux éléments nuls, alors l'un des deux est nul !!

Définition. Soit A un anneau. Soit $a \in A$. On dit que :

- a est un diviseur de zéro à gauche si $a \neq 0$ et s'il existe $b \in A^*$ tel que $a \times b = 0$.
- a est un diviseur de zéro à droite si $a \neq 0$ et s'il existe $b \in A^*$ tel que $b \times a = 0$.
- a est un diviseur de zéro si a est un diviseur de zéro à gauche ou à droite.

Nous rencontrerons principalement des diviseurs de zéro dans les ensembles de matrices (cf. chapitre 23) mais il existe d'autres situations simples où on en rencontre :

Exemples :

- Sur $(\mathbb{K}^{\mathbb{R}}, +, \times)$, les diviseurs de zéro sont exactement les fonctions non nulles qui s'annulent. En effet :

- Pour les mêmes raisons, sur l'anneau $(\mathbb{K}^{\mathbb{N}}, +, \times)$, les diviseurs de zéro sont exactement les suites dont un terme est nul et n'étant pas la suite nulle.
- Dans $\mathbb{Z}/6\mathbb{Z}$, $\bar{2}$ et $\bar{3}$ sont des diviseurs de zéro car $\bar{2} \times \bar{3} = \bar{0}$.

Définition (anneau intègre). Un anneau est dit intègre s'il n'admet pas de diviseur de zéro.

Remarque : Autrement dit, un anneau A est intègre si le produit de deux éléments non nuls est non nul, c'est-à-dire

$$\forall (a, b) \in A^2, \quad (a \neq 0 \text{ et } b \neq 0) \implies ab \neq 0.$$

Par contraposée, cela revient au même que :

$$\forall (a, b) \in A^2, \quad ab = 0 \implies (a = 0 \text{ ou } b = 0).$$

Exemples :

- \mathbb{Z} , \mathbb{Q} , \mathbb{R} et \mathbb{C} sont des anneaux intègres.
- $\mathbb{K}^{\mathbb{R}}$ et $\mathbb{K}^{\mathbb{N}}$ ne sont pas intègres comme on l'a vu plus haut.
- Soit $n \in \mathbb{N} \setminus \{0; 1\}$. Montrons que $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier.

- Si A et A' sont deux anneaux non réduits à un singleton, alors l'anneau produit $A \times A'$ (dont l'élément neutre pour l'addition est $(0_A, 0_{A'})$) n'est pas intègre. En effet : $(1_A, 0_{A'}) \times (0_A, 1_{A'}) = (0_A, 0_{A'})$ alors que $(1_A, 0_{A'})$ et $(0_A, 1_{A'})$ ne sont pas $(0_A, 0_{A'})$.



Mais si $ab = ca$, on ne peut toujours pas simplifier puisque A n'est pas commutatif a priori.

Proposition. Si A est un anneau intègre, alors tout élément différent de 0 est régulier pour \times , c'est-à-dire, pour tout $(a, b, c) \in A^3$,

- Si $ab = ac$ et $a \neq 0$, alors $b = c$.
- Si $ba = ca$ et $a \neq 0$, alors $b = c$.

DÉMONSTRATION.



La preuve de la régularité ne découle par cette fois de l'existence d'un symétrique!!!

□

Remarque : Si A n'est pas un anneau intègre, il se peut qu'il existe des éléments a tels que $a^2 = 0$.

Par exemple, dans $\mathbb{Z}/4\mathbb{Z}$, $\bar{2}^2 = \bar{0}$.

Plus généralement, on dit qu'un élément a de A est nilpotent s'il existe $n \in \mathbb{N}^*$ tel que $a^n = 0$. Nous étudierons plus longuement ce type d'éléments dans le cas particulier où A est l'ensemble des matrices carrées d'une taille donnée dans le chapitre 23.



Et aussi dans l'exercice ...

3) Éléments inversibles d'un anneau et corps

On se donne dans ce paragraphe un anneau $(A, +, \times)$ qui n'est pas un singleton (donc on a $0_A \neq 1_A$).

Proposition. 0_A n'est pas inversible.

DÉMONSTRATION. Puisque 0_A est absorbant, pour tout $a \in A$, $a \times 0_A = 0_A \neq 1_A$: il n'existe donc pas d'élément $a \in A$ tel que $a \times 0_A = 0_A \times a = 1_A$, 0_A n'est pas inversible. □

Proposition. Un diviseur de zéro n'est pas inversible.



Attention, la réciproque est fautive : un élément non inversible n'est pas forcément un diviseur de zéro (par exemple, dans \mathbb{Z} , 2 n'est pas inversible alors que ce n'est pas un diviseur de zéro).

DÉMONSTRATION.

□

Définition. On note $U(A)$ ou A^\times l'ensemble des éléments inversibles de A .

Ne pas confondre A^\times avec $A^* = A \setminus \{0\}$. On a $A^\times \subset A^*$ puisque 0 n'est pas inversible mais ces deux ensembles ne sont pas égaux en général (voir ci-dessous). On préférera donc utiliser la notation $U(A)$ (un inversible est parfois appelé une unité, d'où cette notation)... le programme nous laisse libre à ce sujet.

Proposition. $(U(A), \times)$ est un groupe.



On ne connaît pas de groupe plus gros duquel $U(A)$ serait un sous-groupe. On doit tout vérifier à la main.

DÉMONSTRATION.

□

Exemples :

- Un produit de deux entiers est égal à 1 si et seulement si ces deux entiers sont 1 et 1 ou bien -1 et -1 . Ainsi $U(\mathbb{Z}) = \{\pm 1\}$.
- $U(\mathbb{Q}) = \mathbb{Q}^*$, $U(\mathbb{R}) = \mathbb{R}^*$ et $U(\mathbb{C}) = \mathbb{C}^*$.
- Soit $n \in \mathbb{N} \setminus \{0; 1\}$. On a vu dans le paragraphe 1.3.b que, pour tout $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$, \bar{a} est inversible pour \times si et seulement si $a \wedge n = 1$. Ainsi $U(\mathbb{Z}/n\mathbb{Z}) = \{\bar{a} \mid a \wedge n = 1\}$.

Définition (corps). Soit $(K, +, \times)$ un anneau. On dit que K est un corps si K est commutatif et si tout élément de K distinct de 0_K est inversible.

C'est-à-dire si tout élément distinct de 0_K est inversible.

Exemples :

- \mathbb{Q} , \mathbb{R} et \mathbb{C} sont des corps mais \mathbb{Z} n'est pas un corps.
- Soit $n \in \mathbb{N} \setminus \{0; 1\}$. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier. En effet

Remarques :


- Soit K un anneau. Soit $(a, b, c) \in K^3$ tel que $ab = ca$ et $a \neq 0$. On a vu qu'on ne peut pas conclure que $b = c$ en général, y compris si l'anneau K est intègre. Mais si, on sait que K est un corps, puisque celui-ci est commutatif, on a d'abord $ab = ac$ et donc $b = c$ (en multipliant à gauche. par a^{-1} de chaque côté).
- Si K est un anneau commutatif, alors K est un corps si et seulement si $U(K) = K^*$.

Proposition. Un corps est un anneau intègre.

DÉMONSTRATION.

□

Remarques :

- Il en découle qu'un corps ne contient aucun diviseur de zéro ni aucun élément nilpotent non nul (cf. paragraphe précédent).
- On a vu ci-dessus qu'un anneau produit de deux anneaux non réduits à un singleton n'est pas intègre et donc n'est pas un corps.
-  La réciproque est fautive : un anneau intègre n'est pas un corps en général.
Par exemple, \mathbb{Z} est un anneau intègre mais n'est pas un corps.

Il existe tout de même une réciproque partielle : un anneau commutatif intègre **fini** est un corps (cf. exercice __).

4) Sous-anneaux

Dans le paragraphe II.3, nous avons vu qu'un sous-groupe d'un groupe G admet automatiquement le même élément neutre que G . Un anneau B inclus dans un anneau A possède-t-il à son tour le même élément neutre que A pour la multiplication ? Et bien pas forcément !

Considérons B l'ensemble des fonctions de \mathbb{R} dans \mathbb{R} qui sont nulles sur \mathbb{R}_+^* . Alors $(B, +, \times)$ est un anneau dont l'élément neutre pour la multiplication est $1_{\mathbb{R}_+^*}$.

↪ DÉMONSTRATION LAISSÉE EN EXERCICE.

C'est donc un anneau inclus dans l'anneau $(\mathbb{R}^{\mathbb{R}}, +, \times)$ mais il ne possède pas le même élément neutre que ce dernier qui est la fonction constante égale à 1.

Pour cette raison, nous allons contraindre la définition d'un sous-anneau à ce que les neutres soient les mêmes.



En d'autres termes, un sous-anneau de A est un anneau inclus dans A pour les mêmes lois et les mêmes éléments neutres que A (même si le neutre pour l'addition appartient automatiquement à B puisque $(B, +)$ est un sous-groupe de $(A, +)$).

Définition. Soit $(A, +, \times)$ un anneau. Soit B une partie de A . On dit que B est un sous-anneau de A si :

- B est stable pour les lois $+$ et \times ,
- $1_A \in B$,
- $(B, +, \times)$ est un anneau.

Si A et B sont des corps, on dit que B est un sous-corps de A .

Exemples :

- \mathbb{Z} est un sous-anneau de \mathbb{Q} , qui est un sous-anneau de \mathbb{R} qui est lui-même un sous-anneau de \mathbb{C} .
- Si A est un anneau non réduit à un singleton, alors $0_A \neq 1_A$ et donc $\{0_A\}$ n'est pas un sous-anneau de A puisqu'il ne contient pas 1_A (mais c'est tout de même un anneau).
- Pour tout $n \in \mathbb{N}^*$, $(n\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Z}, +)$ (ce sont d'ailleurs les seuls sous-groupes de \mathbb{Z} , comme nous l'avons vu) mais 1 n'appartient à $n\mathbb{Z}$ que lorsque $n = 1$. Par conséquent \mathbb{Z} est le seul sous-anneau de \mathbb{Z} .



Pour une caractérisation des sous-corps, il suffit d'ajouter la stabilité par inverse aux points 2 et 3 : une partie L d'un corps K est un sous-corps de K si et seulement si :

- $1_K \in L$,
- $\forall (x, y) \in L^2, x - y \in L$
- $\forall (x, y) \in L^2, xy \in L$
- $\forall x \in L^*, x^{-1} \in L$.

Mais les notions de sous-corps et de morphismes de corps (cf. prochain paragraphe) ne sont pas explicitement au programme.

Proposition (caractérisation des sous-anneaux). Soit A un anneau. Soit B une partie de A . Les trois assertions suivantes sont équivalentes :

1. B est un sous-anneau de A ,
2. $\left\{ \begin{array}{l} (B, +) \text{ est un sous-groupe de } (A, +) \\ 1_A \in B \\ \forall (a, b) \in B^2, ab \in B \text{ (stabilité par produit)} \end{array} \right.$
3. $\left\{ \begin{array}{l} 1_A \in B \\ \forall (a, b) \in B^2, a - b \in B \text{ (stabilité par soustraction)} \\ \forall (a, b) \in B^2, ab \in B \text{ (stabilité par produit)} \end{array} \right.$

DÉMONSTRATION. Notons que les points 2 et 3 sont équivalents en vertu de la caractérisation des sous-groupes vue dans le paragraphe II.3 (le fait que $1_A \in B$ garantissant que $B \neq \emptyset$ et permettant de montrer que 3 implique 2). Le fait que 1 entraîne 2 est immédiat. Reste à montrer que 2 implique 1. Supposons donc que les hypothèses du point 2 sont vérifiées.

- $(B, +)$ est bien un groupe (abélien forcément vu la notation additive) de A ,
- \times est stable sur B donc \times est associative sur B (car elle l'est sur A) et distributive sur $+$ sur B (car elle l'est sur A).
- Enfin, $1_A \in B$ donc B admet un élément neutre pour \times .

Ainsi B est bien un sous-anneau de A . □

Exemples :

- Notons $\mathbb{Z}[i] = \{a + ib \mid (a, b) \in \mathbb{Z}^2\}$. Montrons qu'il s'agit d'un sous-anneau de \mathbb{C} .

Maintenant déterminons $U(\mathbb{Z}[i])$.

- On montre de même que $\mathbb{Q}[i] = \{a + ib \mid (a, b) \in \mathbb{Q}^2\}$ est un sous-anneau de \mathbb{C} . Par ailleurs, pour tout $z = a + ib \in \mathbb{Q}[i]$ non nul, $a^2 + b^2 \neq 0$ et $z' = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}i \in \mathbb{Q}[i]$ vérifie $zz' = 1$ si bien que $U(\mathbb{Q}[i]) = \mathbb{Q}[i]^*$ et donc $\mathbb{Q}[i]$ est un corps.

C'est même un sous-corps de \mathbb{C} .

5) Morphismes d'anneaux

On pourrait noter les lois de A et A' différemment : si les anneaux sont $(A, +, \times)$ et $(A', +, \times)$, alors pour tout $(a, b) \in A^2$,

$$f(a + b) = f(a) + f(b)$$

$$f(a \times b) = f(a) \times f(b).$$

Définition. Soient A et A' deux anneaux. On dit qu'une application $f : A \rightarrow A'$ est un morphisme d'anneaux si :

- pour tout $(a, b) \in A^2$, $f(a + b) = f(a) + f(b)$,
- pour tout $(a, b) \in A^2$, $f(ab) = f(a)f(b)$,
- $f(1_A) = 1_{A'}$.

Si A et A' sont deux corps, on parle de morphisme de corps.

Remarques :

- En d'autres termes, un morphisme d'anneau est une fonction qui est compatible avec les deux lois qui envoient le neutre pour la multiplication du premier anneau sur le neutre pour la multiplication du deuxième anneau.
- Contrairement à un morphisme de groupes, qui envoie le neutre pour l'addition du premier groupe sur le neutre pour l'addition du deuxième groupe, ce n'est pas automatique pour les neutres pour la multiplication. En effet, par exemple, $x \mapsto 0_{A'}$ vérifie les deux premiers points mais pas le troisième.
- Si $A = A'$ et les lois sont les mêmes, on parle d'endomorphisme d'anneaux.

Proposition. Soient A et A' deux anneaux. Soit f un morphisme d'anneaux de A dans A' . Alors f est un morphisme de groupes de $(A, +)$ dans $(A', +)$ et donc :

- $f(0_A) = 0_{A'}$,
 - Pour tout $a \in A$, $f(-a) = -f(a)$.
 - Pour tout $a \in A$ et $n \in \mathbb{Z}$, $f(na) = nf(a)$.
 - $\text{Ker}(f) = \{x \in A \mid f(x) = 0_{A'}\}$ est un sous-groupe de $(A, +)$.
- De plus $\text{Ker}(f) = \{0_A\}$ si et seulement si f est injective.



Les propriétés suivantes sont, elles, relatives à la structure d'anneau de A et de A' :

Proposition. Soient A et A' deux anneaux. Soit f un morphisme d'anneaux de A dans A' .

- Pour tout $a \in A$, pour tout $n \in \mathbb{N}$, $f(a^n) = f(a)^n$.
- Pour tout $a \in U(A)$, $f(a) \in U(A')$ et $f(a^{-1}) = f(a)^{-1}$.
- Si f est bijective, alors f^{-1} est un morphisme d'anneaux.
- Soit A'' un anneau. Si g est un morphisme d'anneaux de A' dans A'' , alors $g \circ f$ est un morphisme d'anneaux de A dans A'' .
- L'image directe d'un sous-anneau de A par f est un sous-anneau de A' . En particulier $\text{Im}(f) = f(A)$ est un sous-anneau de A' .
- L'image réciproque d'un sous-anneau de A' par f est un sous-anneau de A .

↪ DÉMONSTRATION LAISSÉE EN EXERCICE.

Remarques :

-  Les éléments de A ne sont pas forcément inversibles pour la loi \times , cela n'a donc pas de sens d'écrire a^n lorsque $n \in \mathbb{Z} \setminus \mathbb{N}$. Cependant, lorsque a est inversible, $f(a)$ est inversible et $f(a)^{-1} = f(a^{-1})$. Dans ce cas, pour tout $n \in \mathbb{Z}$, $f(a^n) = f(a)^n$.
-  On a $\text{Ker}(f) = f^{-1}(\{0_{A'}\})$ mais $\{0_{A'}\}$ n'est pas un sous-anneau de A' donc, $\text{Ker}(f)$ n'est pas forcément un sous-anneau de A ! En fait $\text{Ker}(f)$ n'est jamais un sous-anneau dès que A' possède au moins deux éléments. En effet, si $\text{Ker}(f)$ est un sous-anneau de A , alors $1_A \in \text{Ker}(f)$ donc $f(1_A) = 0_{A'}$ donc $1_{A'} = 0_{A'}$ (puisque $f(1_A) = 1_{A'}$) et donc A' est un singleton.

Définition. Un morphisme d'anneaux qui est bijectif est appelé un isomorphisme d'anneaux.

Remarque : Un morphisme bijectif d'anneaux entre un anneau et lui même (pour les mêmes lois) est appelé un automorphisme d'anneaux.

Définition. Lorsqu'il existe un isomorphisme d'anneaux de A dans A' , on dit que A' est isomorphe à A ou que A et A' sont isomorphes.

Proposition. La relation « être isomorphe à » est une relation d'équivalence.


↪ DÉMONSTRATION LAISSÉE EN EXERCICE.

Exemples :

- Si A est un anneau, alors Id_A est un isomorphisme d'anneaux.
- Si A est un anneau et B un sous-anneau de A , alors l'injection canonique

$$i : \begin{cases} B & \longrightarrow A \\ x & \longmapsto x \end{cases}$$

est un morphisme d'anneau injectif de B dans A .

 L'ajout des deux points supplémentaire dans la définition d'un morphisme d'anneaux (par rapport à la définition d'un morphisme de groupes) fait qu'il se peut tout à fait que deux anneaux soient isomorphes en tant que groupes mais pas en tant qu'anneaux mais ce cas de figure est rare en pratique.

- La conjugaison complexe ($z \mapsto \bar{z}$) est un isomorphisme d'anneaux (et même de corps) de \mathbb{C} dans lui-même.
- Soit $a \in \mathbb{R}$. La fonction (appelée évaluation en a)

$$\varphi : \begin{cases} \mathbb{K}^{\mathbb{R}} & \longrightarrow & \mathbb{R} \\ f & \longmapsto & f(a) \end{cases}$$

est un morphisme d'anneaux. En effet : $\varphi(x \mapsto 1) = 1$ et, pour tout $(f, g) \in (\mathbb{K}^{\mathbb{R}})^2$,

$$\varphi(f + g) = (f + g)(a) = f(a) + g(a) = \varphi(f) + \varphi(g)$$

et

$$\varphi(fg) = (fg)(a) = f(a)g(a) = \varphi(f)\varphi(g).$$

Il est surjectif (car, pour tout $a \in \mathbb{R}$, $a = \varphi(x \mapsto a)$) mais non injectif car $\text{Ker}(\varphi)$ est l'ensemble des fonctions nulles en a , qui n'est pas réduit à la fonction nulle.

- Soit $n \in \mathbb{Z} \setminus \{0; 1\}$. La fonction

$$\varphi : \begin{cases} \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ k & \longmapsto & \bar{k} \end{cases}$$

est un morphisme d'anneaux. En effet, $\varphi(1) = \bar{1}$ et, pour tout $(k, k') \in \mathbb{Z}^2$,

$$\varphi(k + k') = \overline{k + k'} = \bar{k} + \bar{k}' = \varphi(k) + \varphi(k')$$

et

$$\varphi(kk') = \overline{kk'} = \bar{k}\bar{k}' = \varphi(k)\varphi(k').$$

Il est surjectif et de noyau $n\mathbb{Z}$.

- Soit p un nombre premier. Montrons que la fonction

$$f : \begin{cases} \mathbb{Z}/p\mathbb{Z} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \\ \bar{a} & \longmapsto & \bar{a}^p \end{cases}$$

est un isomorphisme d'anneaux.

Remarquons que l'application f qui va de $\{\text{chou; navet; carotte}\}$ dans $\mathbb{Z}/3\mathbb{Z}$ telle que $f(\text{chou}) = \bar{0}$, $f(\text{navet}) = \bar{1}$ et $f(\text{carotte}) = \bar{2}$ est un isomorphisme d'anneaux

En fait c'est l'identité de $\mathbb{Z}/p\mathbb{Z}$ mais faisons comme si on n'avait rien vu...

On l'appelle l'isomorphisme de Frobenius.

6) Construction de \mathbb{C} (HP)

Nous la prouverons une nouvelle fois l'existence de \mathbb{C} dans l'exercice 26 du chapitre 23.

La construction de \mathbb{C} (à partir de \mathbb{R}) est officiellement hors-programme. Pourtant nous avons désormais tout en main pour le faire correctement. Ce paragraphe est donc hors-programme mais très instructif pour la manipulation des objets étudiés dans ce chapitre.

On munit \mathbb{R}^2 des deux lois internes $+$ et \times définies par : pour tous (a, b) et (x, y) dans \mathbb{R}^2 ,

$$(a, b) + (x, y) = (a + x, b + y) \quad \text{et} \quad (a, b) \times (x, y) = (ax - by, ay + bx).$$

Ces deux lois sont bien internes par construction. Montrons que $(\mathbb{R}^2, +, \times)$ est un corps.

- $(\mathbb{R}^2, +)$ est le groupe produit de $(\mathbb{R}, +)$ avec lui-même. C'est donc un groupe abélien (cf. paragraphe II.2).
- Montrons que la loi \times est associative, commutative et distributive par rapport à la loi $+$. Soient (a, b) , (x, y) et (u, v) trois éléments de \mathbb{R}^2 .

★ D'une part :

$$\begin{aligned}(a, b) \times ((x, y) \times (u, v)) &= (a, b) \times (xu - yv, xv + uy) \\ &= (axu - ayv - bxv - buy, axv + auy + bxu - byv)\end{aligned}$$

et d'autre part :

$$\begin{aligned}((a, b) \times (x, y)) \times (u, v) &= (ax - by, ay + bx) \times (u, v) \\ &= (axu - uby - vay - vxb, axv - byv + uay + uxb)\end{aligned}$$

La loi \times est donc bien associative.

- ★ Les réels a et x , b et y jouant le même rôle dans l'expression de $(a, b) \times (x, y)$, la loi est commutative.
- ★ On montre de façon analogue qu'elle est distributive à gauche par rapport à l'addition, c'est-à-dire

$$\begin{aligned}(a, b) \times ((x, y) + (u, v)) &= (a, b) \times (x + u, y + v) \\ &= (a(x + u) - b(y + v), a(y + v) + b(x + u)) \\ &= (ax - by + au - bv, ay + bx + av + bu) \\ &= (ax - by, ay + bx) + (au - bv, av + bu) \\ &= (a, b) \times (x, y) + (a, b) \times (u, v).\end{aligned}$$

Un sens suffit puisque \times est commutative.

Ainsi \times est distributive par rapport à $+$.

Un sens suffit puisque \times est commutative.

- Pour tout $(a, b) \in \mathbb{R}^2$, $(1, 0) \times (a, b) = (a, b)$ donc le neutre de la loi \times est $(1, 0)$.

Finalement, $(\mathbb{R}^2, +, \times)$ est bien un anneau commutatif. Montrons que c'est un corps : pour cela il (faut et il) suffit de prouver tout tout élément non nul est inversible. Considérons

$(x, y) \in \mathbb{R}^2 \setminus \{(0, 0)\}$. On a alors $x^2 + y^2 \neq 0$ et on peut donc poser $x' = \frac{x}{x^2 + y^2}$ et $y' = \frac{-y}{x^2 + y^2}$. On a

$$(x, y) \times (x', y') = (xx' - yy', xy' + x'y) = \left(\frac{x^2 + y^2}{x^2 + y^2}, \frac{-xy + xy}{x^2 + y^2} \right) = (1, 0).$$

Puisque \times est commutative, il s'ensuit que (x, y) est inversible et que (x', y') est l'inverse de (x, y) . Finalement $(\mathbb{R}^2, +, \times)$ est bien un corps.

Notons alors \mathbb{C} l'ensemble \mathbb{R}^2 , muni de ces deux lois. Montrons que \mathbb{C} vérifie les propriétés admises dans le chapitre 6 :

- Considérons l'application

$$f : \begin{cases} \mathbb{R} & \longrightarrow & \mathbb{R}^2 \\ x & \longmapsto & (x, 0) \end{cases}$$

Il s'agit d'un morphisme de corps. En effet $f(1) = (1, 0)$ et, pour tout $(x, y) \in \mathbb{R}^2$, $f(x + y) = (x + y, 0) = (x, 0) + (y, 0) = f(x) + f(y)$ et

$$f(x) \times f(y) = (x, 0) \times (y, 0) = (xy - 0, x0 + y0) = (xy, 0) = f(xy).$$

Soit $x \in \text{Ker}(f)$. Alors $f(x) = (0, 0)$ donc $(x, 0) = (0, 0)$ et donc $x = 0$. Ainsi $\text{Ker}(f) = \{0\}$: f est injective. Par conséquent, \mathbb{R} est isomorphe à $\text{Im}(f)$: on peut donc « identifier » \mathbb{R} à $\text{Im}(f)$. Autrement dit, \mathbb{C} contient une copie conforme de \mathbb{R} que l'on « identifie » à \mathbb{R} : on peut donc dire (par abus de langage) que \mathbb{C} contient \mathbb{R} , et, si $x \in \mathbb{R}$, on identifie le réel x à l'élément $(x, 0)$ de \mathbb{C} .

- Posons $i = (0, 1)$. Alors $i \times i = (0 - 1, 0 + 0) = (-1, 0)$. Or, on identifie $(-1, 0)$ et le réel -1 : il existe bien un élément $i \in \mathbb{C}$ vérifiant $i^2 = -1$.
- Les lois $+$ et \times prolongent celles de \mathbb{R} . En effet, donnons-nous a et x des réels. On a vu qu'on les identifie à $(a, 0)$ et $(x, 0)$. On a $(a, 0) + (x, 0) = (a + x, 0)$ et $(a, 0) \times (x, 0) = (ax, 0)$ (ce que l'on a montré en prouvant que f étant un morphisme de corps). En d'autres termes, les opérations $+$ et \times donnent les mêmes résultats que la somme et le produit lorsqu'on les applique à des réels : ces nouvelles opérations prolongent donc celles de \mathbb{R} .
- Enfin, pour tout $z = (x, y) \in \mathbb{R}^2$, on a $z = (x, 0) + (y, 0) \times (0, 1) = x + iy$. De plus, si $z = a + ib$ (avec a et b des réels), alors $z = (a, 0) + (0, b) \times (0, 1) = (a, b)$ d'où $x = a$ et $y = b$. Tout complexe z s'écrit de façon unique sous la forme $x + iy$.

Nous avons donc enfin prouvé l'existence de \mathbb{C} et qu'il vérifie bien les propriétés admises dans le chapitre 6.



On montre facilement que l'image d'un morphisme de corps est un corps. Ainsi, \mathbb{R} et $\text{Im}(f)$ sont deux corps isomorphes. Puisque ces deux corps sont isomorphes, comme pour les groupes, ils représentent « le même corps ».