Chapitre 18

Structures algébriques

Plan du chapitre

Hypothèse

Dans tout ce chapitre, E est un ensemble.

1 Vocabulaire introductif

1.1 Loi de composition interne

Définition 18.1 – Loi de composition interne

On appelle loi de composition interne sur E (en abrégé l.c.i.) toute application de $E \times E$ dans E.

Si on note $\top : E \times E \to E$ une l.c.i., alors on notera $x \top y$ au lieu de $\top(x,y)$.

Exemple 1. Mettre une croix dans le tableau suivant si l'opération donnée est une l.c.i. sur l'ensemble donné :

l.c.i. ?	$\mathbb{Z}$	$\mathbb{Z}^*$	$\mathbb{R}$	$\mathbb{R}_+^*$
$+$				
$-$				
$\times$				
$/$				

Exemple 2. Soit Ω un ensemble. Sur $E := \mathscr{P}(\Omega)$, on peut définir les l.c.i. suivantes :

1. La réunion : $(A,B) \mapsto A \cup B$
2. L'intersection : $(A,B) \mapsto A \cap B$
3. La différence : $(A,B) \mapsto A \setminus B$
4. Le passage au complémentaire $A \mapsto \Omega \setminus A$ n'est pas une l.c.i. car son ensemble de départ est $\mathscr{P}(\Omega)$, donc E et non $E \times E$.

Définition 18.2 – Commutativité, associativité

Une l.c.i. $\top$ sur un ensemble E est dite :

- commutative si $\quad \forall x,y \in E \quad x \top y = y \top x$,
- associative si $\quad \forall x,y,z \in E \quad (x \top y) \top z = x \top (y \top z)$.

Exemple 3. Les l.c.i. $+$ et $\times$ sont commutatives et associatives sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

La l.c.i. $-$ sur $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ est / n'est pas commutative et est / n'est pas associative.

Pour tout ensemble Ω, la réunion $\cup$ et l'intersection $\cap$ sont commutatives et associatives sur $\mathscr{P}(\Omega)$.

Remarque (Associativité et réécriture d'expressions)**.** Si $\top$ est une l.c.i. associative sur E, alors on peut écrire sans ambiguité $x \top y \top z$ sans préciser les parenthèses. On peut de même écrire, pour toute famille $(x_i)_{1 \leq i \leq n}$ d'éléments de E,

$$\top_{1 \leq i \leq n} x_i := x_1 \top x_2 \top \ldots \top x_n$$

Les lois $+, \times, \cup, \cap$ étant associatives, on peut donc écrire :

$$\sum_{i=1}^{n} x_i \qquad \prod_{i=1}^{n} x_i \qquad \bigcup_{i=1}^{n} A_i \qquad \bigcap_{i=1}^{n} A_i$$

et comme en plus ces lois sont commutatives, l'ordre des x_i ou des A_i importe peu. On peut donc réordonner et regrouper les termes comme on le souhaite, par exemple :

$$\begin{aligned} \sum_{i=0}^{9} x_i &= x_0 + x_1 + \cdots + x_9 \\ &= (x_0 + x_2 + \cdots + x_8) + (x_1 + x_3 + \cdots + x_9) \\ &= \sum_{i=0}^{4} x_{2i} \quad + \quad \sum_{i=0}^{4} x_{2i+1} \end{aligned}$$

Théorème 18.3

Soit X un ensemble. On considère X^X l'ensemble des applications de X dans X. Alors :

- la composition $\circ$ est une l.c.i. sur X^X.
- $\circ$ est associative.
- $\circ$ est non commutative (sauf si X est vide ou un singleton).

Ainsi, pour toutes applications $f,g,h \in X^X$, on peut écrire $f\circ g\circ h$ sans ambiguité [1].

Définition 18.4

Deux éléments $x,y \in E$ commutent (pour $\top$) si $x\top y = y\top x$.

Bien entendu, si $\top$ est commutative, alors tous les éléments de E commutent deux à deux.

Exemple 4. Soit $f,g \in \mathbb{C}^{\mathbb{C}}$ les fonctions définies par $f(z)=z^2$ et $g(z)=\bar{z}$. Montrer que f,g commutent.

1.2 Élément neutre

Définition 18.5 – Élément neutre

On suppose que $\top$ est une l.c.i. sur E. On dit que $e \in E$ est l'élément neutre (pour $\top$) si

$$\forall x \in E \qquad x\top e = e\top x = x$$

Lorsqu'un tel élément neutre existe, il est unique.

Démonstration. Démontrons l'unicité de l'élément neutre.

□

Exemple 5.

- 0 est l'élément neutre de $+$ sur $\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$. En effet, pour tout x appartenant à un de ces ensembles, on a

$$x+0=0+x=x$$

1. Avec $E \xrightarrow{f} F \xrightarrow{g} G \xrightarrow{h} H$, on a encore $(h\circ g)\circ f = h\circ(g\circ f)$, si bien qu'on peut écrire $h\circ g\circ f$ sans ambiguité. On dit encore dans ce cadre que $\circ$ est associative, mais c'est un abus car $\circ$ ne représente pas une l.c.i. : pour $g\circ f$, on dénote $\circ$ l'application de $G^F\times F^E$ dans G^E, tandis que pour $h\circ g$, on dénote $\circ$ l'application de $H^G\times G^F$ dans H^F.

- 1 est l'élément neutre de $\times$ sur $\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$. En effet, pour tout x appartenant à un de ces ensembles, on a

$$x\times 1 = 1\times x = x$$

- Sur $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$, la l.c.i. $-$ n'admet pas d'élément neutre.

- Soit X un ensemble. X^X muni de la loi $\circ$ admet pour élément neutre .....
- Soit Ω un ensemble. $\mathscr{P}(\Omega)$ muni de la loi $\cup$ admet pour élément neutre .....
- Soit Ω un ensemble. $\mathscr{P}(\Omega)$ muni de la loi $\cap$ admet pour élément neutre .....
- Soit Ω un ensemble. $\mathscr{P}(X)$ muni de la loi $\setminus$ n'admet pas d'élément neutre.

1.3 Élément symétrisable

Définition 18.6 – Élément symétrisable

On suppose que $\top$ est une l.c.i. sur E. Soit $e\in E$ un élément neutre (pour $\top$). On dit qu'un élément $x\in E$ est symétrisable (pour $\top$) si

$$\exists y\in E \qquad x\top y = y\top x = e$$

Tout élément $y\in E$ qui vérifie les deux égalités ci-dessus est appelé un symétrique de x (pour $\top$).

Remarque. Un même élément x peut avoir plusieurs symétriques. Néanmoins, lorsqu'il est unique, on note en général x', ou $-x$, ou encore x^{-1} ce symétrique (l'énoncé vous le précisera, ou bien cela dépendra de la notation de la loi, cf section 2.2).

Si x admet y pour symétrique, alors y admet x pour symétrique.

Exemple 6. Remplir le tableau suivant :

Soit E un ensemble		l.c.i. $+$	l.c.i. $\times$
élément neutre :			
$x\in E$ est symétrisable si... :			
ensemble des éléments symétrisables de E lorsque ...	$E=\mathbb{N}$		
	$E=\mathbb{Z}$		
	$E=\mathbb{Q}$		

2 Groupes

2.1 Définition et propriétés générales

Définition 18.7 – Groupe

Soit G un ensemble. On dit que $(G, \top)$ est un groupe si :

G1. $\top$ est une l.c.i. sur G, càd : .....

G2. $\top$ est associative, càd :

.....

G3. G possède un élément neutre (pour $\top$), càd :

.....

G4. Tout élément $a \in G$ est symétrisable (pour $\top$), càd :

.....

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

Attention à bien vérifier que l'élément neutre e, tout comme l'élément symétrique de a appartiennent bien à G ! Par abus de langage, on sous-entend parfois la loi $\top$ et on dit simplement que G est un groupe.

Exemple 7.

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes commutatifs. Mais $(\mathbb{N}, +)$ n'est pas un groupe car il y a des éléments de $\mathbb{N}$ qui ne sont pas symétrisables pour $+$ (cf plus haut).
- $(\mathbb{N}, \times)$, $(\mathbb{Z}, \times)$, $(\mathbb{Q}, \times)$, $(\mathbb{R}, \times)$ et $(\mathbb{C}, \times)$ ne sont pas des groupes car :
- $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$ sont des groupes commutatifs. Mais $(\mathbb{N}^*, \times)$ et $(\mathbb{Z}^*, \times)$ ne sont pas des groupe car (par exemple) 2 n'est pas symétrisable pour $\times$ car aucun élément b de $\mathbb{N}^*$ ou de $\mathbb{Z}^*$ ne vérifie $2b = 1$.

Notation (Lois $\times$ et $\cdot$, notation ab)**.** Soit a, b deux éléments d'un groupe $(G, \times)$. On préfèrera souvent noter ab plutôt que $a \times b$. De même, on emploie parfois une loi "point", qu'on note "$\cdot$" et à nouveau on préfère écrire ab plutôt que $a \cdot b$.

Exemple 8. Soit $n \in \mathbb{N}^*$. Montrer que $(\mathbb{R}_+^*, \times)$ est un groupe commutatif.

Théorème 18.8

Soit $(G, \top)$ un groupe. Alors l'élément neutre de G est unique.

De plus, tout élément x de G admet un **unique** symétrique : on l'appelera donc ***le*** symétrique de x.

Démonstration. On a déjà vu que l'élément neutre, s'il existe, est unique.

□

Remarque. Un groupe G est toujours non vide, car G possède un élément neutre.

G peut ne contenir que son élément neutre. Par exemple $\{0\}$ est un groupe pour $+$. Si un groupe est réduit à son élément neutre, on dira qu'il s'agit d'un groupe trivial.

2.2 Notations additive et multiplicative

Remarque. La notation additive $a+b$ n'est employée que pour une l.c.i. commutative.

$a,b,c \in E$	Notation additive : loi $+$	Notation multiplicative : loi $\cdot$ ou $\times$
Élément neutre	Noté 0 ou 0_E	Noté 1, 1_E ou e
Symétrique de a	Opposé : $-a$ $a+(-a)=(-a)+a=0$	Inverse : a^{-1} $aa^{-1}=a^{-1}a=e$
Itéré n-ième ($n \in \mathbb{N}^*$)	$na := \underbrace{a+\ldots+a}_{n \text{ fois}}$	$a^n := \underbrace{a\cdots a}_{n \text{ fois}}$
Itéré 0-ième	$0a := 0$	$a^0 := e$
Itéré $(-n)$-ième (si a est symétrisable)	$(-n)a := n(-a) = \underbrace{(-a)+\ldots+(-a)}_{n \text{ fois}}$	$a^{-n} := (a^{-1})^n = \underbrace{a^{-1}\cdots a^{-1}}_{n \text{ fois}}$
Opérations / itérations sur les itérés $(m,n \in \mathbb{Z})$	$na+ma=(n+m)a$	$a^n a^m = a^{n+m} = a^n a^m$
	$n(ma)=(nm)a$	$(a^n)^m = a^{nm} = (a^m)^n$

Remarque. Une fonction $f : E \to E$ est symétrisable pour $\circ$ si et seulement s'il existe $g : E \to E$ telle que

$$f \circ g = g \circ f = \mathrm{id}_E$$

c'est-à-dire si et seulement si f admet une application réciproque et dans ce cas $f^{-1} = g$. La notation f^{-1} pour une application réciproque est empruntée à la notation multiplicative ci-dessus.
Il arrive même que certains sujets notent "fg" pour la composée $f \circ g$ afin de mieux correspondre à la notation multiplicative ! Dans ce cas, on prendra garde au fait que f^n désigne la fonction $f \circ f \circ \cdots \circ f$ et non $x \mapsto f(x)^n$.

2.3 Calcul dans un groupe

Dans cette partie, sauf indication contraire on utilisera la notation a' pour noter le symétrique d'un élément a.

Théorème 18.9

Soit $(G,\top)$ un groupe et $a,b\in G$. On a :

$$(a')'=a \qquad \text{et} \qquad (a\top b)'=b'\top a'$$

En notation additive, cette propriété se réécrit :

En notation multiplicative, cette propriété se réécrit :

□

Définition 18.10 – Élément régulier

Soit $\top$ une l.c.i. sur E et $a\in E$.

- On dit que a est régulier à gauche si : $\forall x,y\in E \quad (\ a\top x=a\top y \implies x=y\ )$
- On dit que a est régulier à droite si : $\forall x,y\in E \quad (\ x\top a=y\top a \implies x=y\ )$
- On dit que a est régulier si a est régulier à gauche et à droite.

Ainsi, a est un élément régulier à gauche (resp. à droite) si on peut "simplifier" par a à gauche (resp. à droite).

Théorème 18.11

Dans un groupe, tout élément est régulier.

Démonstration. Pour alléger la notation, on considère un groupe $(G,\cdot)$, i.e. une notation multiplicative. On note e son élément neutre. Soit $a\in G$. Montrons que a est régulier. Pour tous $x,y\in G$, on a :

$$\begin{aligned} ax=ay &\implies a^{-1}(ax)=a^{-1}(ay)\\ &\implies (a^{-1}a)x=(a^{-1}a)y \implies ex=ey \implies x=y \end{aligned}$$

donc a est régulier à gauche. On montre de même que a est régulier à droite. Donc a est régulier. □

Méthode – Opérations licites dans un groupe

Soit $(G,\cdot)$ un groupe (notation multiplicative). Soit $x,y \in G$.

1. On peut multiplier une égalité à gauche par tout élément $a \in G$ (ou par a^{-1}) : $\quad ax = ay \iff x = y$
2. On peut multiplier une égalité à droite par tout élément $a \in G$ (ou par a^{-1}) : $\quad xa = ya \iff x = y$
3. On peut passer au symétrique dans une égalité : $\quad x = y \iff x^{-1} = y^{-1}$

Exemple 9. Soit $(G,\cdot)$ un groupe et $a,b \in G$. Résoudre l'équation $x^{-1}a = ab$ d'inconnue $x \in G$.

Groupes usuels. On pourra utiliser sans justification que (avec $\mathbb{K}$ égal à $\mathbb{R}$ ou $\mathbb{C}$) :

- $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ sont des groupes pour $+$ (mais pas $\mathbb{N}$)
- $\mathbb{Q}^*,\mathbb{R}^*,\mathbb{C}^*$ sont des groupes pour $\times$ (mais pas $\mathbb{N}^*$ ou $\mathbb{Z}^*$)
- $\mathbb{K}^{\mathbb{N}}$ et $\mathbb{K}^{\mathbb{R}}$ sont des groupes pour $+$ (ou encore $\mathbb{K}^A$ et $\mathbb{K}^X$ avec $A \subset \mathbb{N}$ et $X \subset \mathbb{R}$)

On verra d'autres groupes usuels pour les matrices, les polynômes, les fractions rationnelles...

2.4 Sous-groupes

Définition 18.12

Soit $\top$ une l.c.i. sur E. Une partie $F \subset E$ est dite stable (par $\top$) si : $\quad \forall x,y \in F \qquad x \top y \in F$

Si F est stable par $\top$, alors on peut (co-)restreindre la l.c.i. $\top : E \times E \to E$ en une application notée :

$$\begin{aligned} \top_F : F \times F &\to F \\ (x,y) &\mapsto x \top y \end{aligned}$$

Dans ce cas, $\top_F$ est une l.c.i. sur $\boxed{F}$ et est appelée la loi induite (par $\top$) sur F.

Très souvent, on note encore $\top$ la l.c.i. $\top_F$ bien qu'il y ait ambiguité. Par ailleurs, la notation $\top_F$ n'est pas officielle.

Définition 18.13

Soit $(G,\top)$ un groupe. Une partie $H \subset G$ est dite un sous-groupe de G si H est une partie stable par $\top$ et si $(H,\top_H)$ est un groupe, où $\top_H$ est la loi induite sur H.

Autrement dit, pour que H soit un sous-groupe de G, il faut que $(H,\top_H)$ vérifie les propriétés **G1.** à **G4.** Cela fait beaucoup à vérifier. En pratique, on utilise systématiquement les caractérisations qui suivent :

Théorème 18.14 – Caractérisation d'un sous-groupe (en 3 assertions)

Soit $(G,\cdot)$ un groupe d'élément neutre e. Une partie $H \subset G$ est un sous-groupe si et seulement si :

2. H est stable par la l.c.i. $\cdot$:
3. H est stable par passage au symétrique :

Si on utilise pour la loi de G la notation additive (loi $+$), les assertions 2 et 3 se réécrivent :

2 .....

3 .....

Remarque. On notera que le groupe G n'intervient pas dans les assertions 1–2–3 : il faut juste vérifier que $H \subset G$, qui est une "condition zéro".

Exemple 10.

- $\mathbb{Z}$ et $\mathbb{Q}$ sont des sous-groupes de $(\mathbb{R},+)$.
- $\mathbb{N}$ n'est pas un sous-groupe de $(\mathbb{Z},+)$ car $1 \in \mathbb{N}$ mais $-1 \notin \mathbb{N}$ (assertion 3 non vérifiée).
- $A := \{-2,2\}$ n'est pas un sous-groupe de $(\mathbb{R}^*,\times)$ car $2\times 2 \notin A$ (assertion 2 non vérifiée).
- $\mathbb{R}_+^*$ est un sous-groupe de $(\mathbb{R}^*,\times)$.
- $\mathbb{Q}^*$ est un sous-groupe de $(\mathbb{R}^*,\times)$, même preuve que ci-dessus.

On peut condenser les assertions 2 et 3 de la propriété 18.14 ci-dessus en une seule :

Théorème 18.15 – Caractérisation d'un sous-groupe (en 2 assertions)

Soit $(G,\cdot)$ un groupe (notation multiplicative) d'élément neutre e. Une partie $H \subset G$ est un sous-groupe si et seulement si :

Exemple 11. Soit G un groupe d'élément neutre e. Alors $\{e\}$ et G sont des sous-groupes de G. $\{e\}$ est appelé le sous-groupe trivial de G.

Remarque. Pour les propriétés 18.14 et 18.15, la majorité des auteurs prennent une condition 1 différente, à savoir l'assertion "$H \neq \varnothing$". En fait, les deux versions sont équivalentes, car on peut montrer que :

$$\begin{cases} 1a & e \in H \\ 2a & \forall x,y \in H \qquad xy^{-1} \in H \end{cases} \iff \begin{cases} 1b & H \neq \varnothing \\ 2b & \forall x,y \in H \qquad xy^{-1} \in H \end{cases}$$

(et idem pour la propriété 18.14). Le sens direct est évident. Pour le sens réciproque, supposons 1b et 2b. Montrons 1a et 2a. Tout d'abord, on a 2b $\implies$ 2a donc il suffit de montrer 1a. Par 1b, on a $H \neq \varnothing$, donc il existe un élément x_0 dans H. Alors, en prenant $(x,y) = (x_0,x_0)$, l'assertion 2b entraine $x_0x_0^{-1} \in H$, ou encore $e \in H$. D'où 1a. Finalement, l'équivalence ci-dessus est vérifiée.

Méthode

- Pour montrer que $(G,\top)$ est un groupe, il suffit souvent de montrer que G est un sous-groupe d'un groupe "usuel" $(G',\top)$, avec la même loi $\top$.
- Pour montrer que H n'est pas un sous-groupe d'un groupe G, il suffit de montrer que H ne vérifie pas une des trois assertions de la propriété 18.14.

Exemple 12. $\mathbb{Z}^*$ n'est pas un sous-groupe de $(\mathbb{Z},+)$ car $0 \notin \mathbb{Z}^*$ alors que 0 est l'élément neutre pour la loi $+$.

Exemple 13. Montrer que $(\mathbb{U},\times)$ est un groupe.

2.5 Morphismes de groupes

Définition 18.16 – Morphisme de groupes

Soit $(G,\top)$ et $(G',\perp)$ deux groupes. On dit que $f : G \to G'$ est un morphisme (de groupes) si

$$\forall x,y \in G \qquad f(x\top y) = f(x)\perp f(y)$$

On peut également dire que f est un morphisme de $(G,\top)$ dans $(G',\perp)$: ceci permet de préciser quelles sont les l.c.i. de G et de G' pour lesquelles f est un morphisme de groupes. Il arrive parfois qu'on omette les lois $\top$ et $\perp$ et qu'on écrive : " f est un morphisme de G dans G' ".

Définition 18.17

Soit $(G,\top)$ et $(G',\perp)$ deux groupes. Soit $f : G \to G'$ un morphisme de groupes. On dit que :

- f est un isomorphisme (de groupes) si f est bijective.
- f est un endomorphisme (de G) si $(G,\top) = (G',\perp)$, i.e. f est un morphisme de $(G,\top)$ dans $(G,\top)$.
- f est un automorphisme (de G) si f est un isomorphisme et un endomorphisme (de G).

Exemple 14. Montrer que les fonctions suivantes sont des morphismes de groupes. Sont-ce des isomorphismes ? Des endomorphismes ? Des automorphismes ?

$$\begin{array}{ccc} f : (\mathbb{Z},+) \to (\mathbb{R}_+^*,\times) & g : (\mathbb{R}_+^*,\times) \to (\mathbb{R},+) & h : (\mathbb{C},+) \to (\mathbb{C},+) \\ n \mapsto 2^n & x \mapsto \ln x & z \mapsto \overline{z} \end{array}$$

1. Traitons f : soit $m,n \in \mathbb{Z}$. Tout d'abord, il est clair que $f(n) = 2^n \in \mathbb{R}_+^*$ donc f est bien définie. De plus,

$$f(m+n) = 2^{m+n} = 2^m 2^n = f(m) \times f(n)$$

donc f est un morphisme de groupes. f n'est pas un endomorphisme (donc pas un automorphisme) car $\mathbb{Z} \neq \mathbb{R}_+^*$. Supposons par l'absurde que f soit bijective. Alors f serait surjective, et en particulier, $\pi \in f(\mathbb{Z})$. Donc il existerait $n \in \mathbb{Z}$ tel que $\pi = 2^n$. Comme $2^n \in \mathbb{Q}$, on en déduit que π est rationnel. Contradiction. Donc f n'est pas bijective et par suite, f n'est pas un isomorphisme.

Théorème 18.18

Soit G, G' deux groupes d'éléments neutres respectifs e, e'. Soit $f : G \to G'$ un morphisme de groupes. *Avec la notation multiplicative* :

1. $f(e) = e'$
2. $\forall x \in G \qquad f(x^{-1}) = f(x)^{-1}$
3. $\forall x \in G \qquad \forall n \in \mathbb{Z} \qquad f(x^n) = f(x)^n$

Démonstration. On ne prouve que les deux premières assertions, la troisième étant une récurrence immédiate.

□

Exemple 15. Comme l'application ln : $(\mathbb{R}_+^*, \times) \to (\mathbb{R}, +)$ est un morphisme de groupes, on a :

1. 2. 3.

2.6 Noyau et image d'un morphisme

Théorème 18.19

Soit G, G' deux groupes et $f : G \to G'$ un morphisme de groupes.

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

Pour rappel :

$$f(H) := \ldots\ldots\ldots\ldots \subset G' \qquad f^{-1}(H') := \ldots\ldots\ldots\ldots \subset G$$

□

Définition 18.20 – Noyau

Soit G, G' deux groupes d'éléments neutres respectifs e, e'. Soit $f : G \to G'$ un morphisme de groupes. On appelle noyau de f, noté $\mathrm{Ker} f$, l'ensemble

$$\mathrm{Ker} f := \left\{x \in G \mid f(x) = e'\right\} = f^{-1}\left(\left\{e'\right\}\right)$$

Théorème 18.21

Avec les mêmes notations que la définition :

1. $\mathrm{Ker} f$ est un sous-groupe de G.
2. $\mathrm{Ker} f = \{e\}$ si et seulement si f est injective.

Démonstration. Montrons la première assertion : $\{e'\}$ est un sous-groupe de G', donc $f^{-1}\left(\{e'\}\right) = \mathrm{Ker} f$ est un sous-groupe de G par la proposition 18.19. Montrons maintenant la seconde assertion.

□

Exemple 16. Montrer que $(2\pi\mathbb{Z}, +)$ est un groupe en utilisant le morphisme de groupes

$$f : (\mathbb{R}, +) \to (\mathbb{C}^*, \times)$$
$$x \mapsto e^{ix}$$

L'application f est-elle injective ?

Définition 18.22 – Image

Soit G, G' deux groupes d'éléments neutres respectifs e, e'. Soit $f : G \to G'$ un morphisme de groupes. On appelle image de f, noté $\mathrm{Im} f$, l'ensemble

$$\mathrm{Im} f := \{f(x) \mid x \in G\} = f(G)$$

Théorème 18.23

Avec les mêmes notations que la définition :

1. $\mathrm{Im} f$ est un sous-groupe de G'.
2. $\mathrm{Im} f = G'$ si et seulement si f est surjectif.

Démonstration. Montrons la première assertion : G est un sous-groupe de G, donc $f(G)$ est un sous-groupe de G' par la proposition 18.19.
La seconde assertion est tautologique : par définition, $\mathrm{Im} f = f(G)$ et on a vu au chapitre 6 que $f(G) = G'$ si et seulement si f est surjective. □

Exemple 17. Montrer que $(\mathbb{U}, \times)$ est un groupe en utilisant le morphisme de groupes

$$\begin{aligned} f : (\mathbb{R}, +) &\to (\mathbb{C}^*, \times) \\ x &\mapsto e^{ix} \end{aligned}$$

Est-ce que f est surjective ?

2.7 Groupe produit

Dans ce qui suit, on a choisi la notation g_1, g_2 pour deux éléments d'un groupe G et h_1, h_2 pour deux éléments d'un groupe H. Ce ne sont pas des applications (sauf si G et/ou H contiennent des applications)

Théorème 18.24 – Groupe produit

Soit $(G, \top)$ et $(H, \perp)$ deux groupes. On peut définir une l.c.i. $*$ sur $G \times H$, dite loi produit par :

$$\forall (g_1, h_1), (g_2, h_2) \in G \times H \qquad (g_1, h_1) * (g_2, h_2) = (g_1 \top g_2, h_1 \perp h_2)$$

- $(G \times H, *)$ est un groupe, dit groupe produit de G et H.
- Son élément neutre est (e_G, e_H), où e_G, e_H sont les éléments neutre de G, H respectivement.
- Si $(x, y) \in G \times H$, alors, en notation multiplicative : $(x, y)^{-1} = (x^{-1}, y^{-1})$.
- Enfin, si G, H sont abéliens, alors $G \times H$ l'est aussi.

Attention, il n'y a pas de notation dédiée pour la loi produit : on peut la noter $*$, $\times$, ou encore $\otimes$...

Démonstration. On va montrer les trois premières assertions en montrons que $(G \times H, *)$ est un groupe. Montrons **G1.**, i.e. $*$ est une l.c.i. sur $G \times H$. Soit (g_1, h_1) et (g_2, h_2) deux couples de $G \times H$. On a

$$(g_1, h_1) * (g_2, h_2) = (g_1 \top g_2, h_1 \perp h_2) \in G \times H \qquad \text{car} \begin{cases} g_1 \top g_2 \in G \\ h_1 \perp h_2 \in H \end{cases}$$

Ainsi, $*$ est une l.c.i. sur $G \times H$. On peut vérifier (mais c'est fastidieux) que $*$ est associative. Montrons que $G \times H$ vérifie **G3.** et **G4.**

□

Exemple 18. $(\mathbb{R},+)$ et $(\mathbb{R}^*,\times)$ sont des groupes donc on peut munir $\mathbb{R}\times\mathbb{R}^*$ de la loi produit

$$(x,y)\circledast(x',y') := (x+x', yy')$$

Dans ce cas, l'élément neutre est $(0,1)$ et le symétrique d'un élément (x,y) est $(-x,y^{-1})$.

3 Anneaux

3.1 Anneau

Définition 18.25 – monoïde, hors programme

Soit M un ensemble. On dit que $(M,\top)$ est un monoïde si :

M1. $\top$ est une l.c.i. sur M.

M2. $\top$ est associative : $\forall a,b,c\in M \quad a\top(b\top c)=(a\top b)\top c$.

M3. M possède un élément neutre (pour $\top$) : $\exists e\in M \quad \forall a\in G \quad a\top e=e\top a=a$.

Autrement dit, un monoïde vérifie les mêmes propriétés qu'un groupe sauf la condition que chaque élément doit être symétrisable : ce n'est pas nécessaire pour être un monoïde.

Exemple 19. $(\mathbb{Z},\times)$, $(\mathbb{Q},\times)$, $(\mathbb{R},\times)$ et $(\mathbb{C},\times)$ sont des monoïdes.
Si X est un ensemble, $(\mathscr{P}(X),\cap)$ et $(\mathscr{P}(X),\cup)$ sont des monoïdes.

Définition 18.26 – Anneau

Soit A un ensemble. On dit que $(A,+,\times)$ est un anneau si :

A1. $(A,+)$ est un groupe abélien.

A2. $(A,\times)$ est un monoïde. ($\times$ est une l.c.i. associative, et A admet un élément neutre pour $\times$)

A3. $\times$ est distributive par rapport à $+$, c'est-à-dire :

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

- L'élement neutre pour $+$ est noté 0_A et appelé élément nul.
- L'élément neutre pour $\times$ est noté 1_A et appelé élément unité.
- Pour tout $x \in A$, son symétrique par rapport à $+$ est noté $-x$ et est appelé l'opposé de x.

Définition 18.27

Soit $(A,+,\times)$ un anneau et $a \in A$. On dit que a est inversible si a est symétrisable par rapport à $\times$, càd :

$$\exists b \in A \qquad ab = ba = 1_A$$

Dans ce cas, un tel $b \in A$ qui vérifie ces égalités est unique. On le note a^{-1} et on dit que c'est l'inverse de x.

Ainsi, **si a est inversible**, alors a^{-1} a un sens et $aa^{-1} = a^{-1}a = 1_A$.

Anneaux usuels.

- $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ sont des anneaux commutatifs.
  - Dans $\mathbb{Q},\mathbb{R},\mathbb{C}$ tout élément non nul x est inversible et $x^{-1} = \dfrac{1}{x}$.
  - Dans $\mathbb{Z}$ seuls -1 et 1 sont inversibles et chacun est égal à son propre inverse.
- $(\mathbb{R}^{\mathbb{N}},+,\times)$ est un anneau commutatif.
  $0_{\mathbb{R}^{\mathbb{N}}}$ est la suite de terme général $u_n = 0$
  $1_{\mathbb{R}^{\mathbb{N}}}$ est la suite de terme général $u_n = 1$
- $(\mathbb{R}^{\mathbb{R}},+,\times)$ est un anneau commutatif.
  $0_{\mathbb{R}^{\mathbb{R}}}$ est la fonction $x \mapsto 0$
  $1_{\mathbb{R}^{\mathbb{R}}}$ est la fonction $x \mapsto 1$.

Exemple 20. Montrer que $u \in \mathbb{R}^{\mathbb{N}}$ est inversible si et seulement si $u_n \neq 0$ pour tout $n \in \mathbb{N}$.

3.2 Sous-anneau

On rappelle que la notion de sous-ensemble stable par l.c.i. et de loi induite a été vue à la définition 18.12.

Définition 18.28

Soit $(A,+,\times)$ un anneau. Une partie $B \subset A$ est dite un sous-anneau de A si B est stable par les l.c.i. $+$ et $\times$, et que $(B,+_B,\times_B)$ est un anneau, où $+_B,\times_B$ sont les lois induites par $+,\times$ sur B.

Comme pour les groupes, on fait souvent un abus de notation en notant $+$ et $\times$ les lois induites $+_B$ et $\times_B$. Pour vérifier que $(B,+,\times)$ est un anneau, il faudrait donc vérifier les propriétés **A1.** à **A3.**. En pratique, on utilise la caractérisation suivante :

Théorème 18.29

Soit $(A,+,\times)$ un anneau. Une partie $B \subset A$ est un sous-anneau de A si et seulement si :

1. $1_A \in B$
2. $\forall x,y \in B \quad x-y \in B$
3. $\forall x,y \in B \quad xy \in B$

On notera que A n'intervient pas dans les assertions 1–2–3, et qu'il suffit de vérifier que $B \subset A$, qui est une "condition zéro".

Démonstration. On vérifie que les assertions **A1.** à **A3.** sont vraies pour B.

2 Montrons que $(B,\times)$ est un monoïde.

(a) Par 3, $\times$ est une l.c.i. sur B

(b) Par 1, B possède un élément neutre pour $\times$.

(c) Il reste à montrer que $\times$ est associative. Pour tous $x,y,z \in B$, montrons que $x(yz) = (xy)z$. Or, $x,y,z \in A$ et $\times$ est associative sur A, donc cette égalité est vraie. Ainsi $\times$ est associative sur B. Finalement $(B,\times)$ est un monoïde.

3 Il faut enfin montrer que, sur B, $\times$ est distributive sur $+$, c'est-à-dire :

$$\forall x,y,z \in B \qquad x(y+z) = xy+xz \qquad \text{et} \qquad (y+z)x = yx+zx$$

Or, $x,y,z \in A$ et comme A est un anneau, les relations ci-dessus sont vérifiées. D'où le résultat. □

Exemple 21.
- $\mathbb{Z},\mathbb{D},\mathbb{Q}$ sont des sous-anneaux de $(\mathbb{R},+,\times)$.
- $\mathbb{Z},\mathbb{D},\mathbb{Q},\mathbb{R}$ sont des sous-anneaux de $(\mathbb{C},+,\times)$.
- L'ensemble des suites réelles convergentes est un sous-anneau de $(\mathbb{R}^{\mathbb{N}},+,\times)$.

- L'ensemble des fonctions polynômiales est un sous-anneau de $(\mathbb{R}^{\mathbb{R}}, +, \times)$.

3.3 Calcul dans un anneau

Sur un anneau $(A, +, \times)$, on peut définir une l.c.i. $-$ par[2] :

$$\text{pour tous } a, b \in A, \qquad a - b := a + (-b)$$

On dispose alors des règles de calcul usuelles : pour tous $a, b, c \in A$,

- $a0_A = 0_A a = 0_A$ (0_A est absorbant pour $\times$)
- $-(ab) = (-a)b = a(-b)$
- $a(b-c) = ab - (ac)$ (distributivité de $\times$ sur $-$)

□

Grâce à ces formules, on peut écrire sans ambiguité "$-ab$" : c'est aussi bien $-(ab)$, i.e. l'opposé de ab, que $(-a)b$, i.e. l'opposé de a multiplié par b. On peut donc réécrire les deux dernières formules :

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

Théorème 18.30 – Calcul dans un anneau

Soit $(A, +, \times)$ un anneau. Alors pour tous $a, b \in A$ et $n \in \mathbb{N}$,

$$\boxed{ab = ba} \implies (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

et si $n \in \mathbb{N}^*$,

$$\boxed{ab = ba} \implies a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^k b^{n-1-k} \qquad = \left(\sum_{k=0}^{n-1} a^k b^{n-1-k} \right) (a-b)$$

2. On peut aussi définir la l.c.i. $-$ sur un groupe $(G, +)$.

Exemple 22. Soit $(A,+,\times)$ un anneau. Soit $a \in A$ et $n \in \mathbb{N}$ tels que $a^n = 0$. Montrer que $1_A - a$ est inversible et calculer son inverse.

Remarque (Cas $1_A = 0_A$)**.** La définition d'un anneau $(A,+,\times)$ n'exclut pas la possibilité que $1_A = 0_A$. Dans ce cas, pour tout $x \in A$,

$$x = x1_A = x0_A = 0_A$$

si bien que tout élément de A est égal à 0_A. Autrement dit, $A = \{0_A\}$. On dit alors que A est un anneau trivial.

3.4 Morphismes d'anneaux

Définition 18.31 – Morphisme d'anneaux

Soit $(A,+,\times)$ et $(A',\oplus,\otimes)$ deux anneaux. Une application $f : A \to A'$ est appelée un morphisme (d'anneaux) si

$$\forall a,b \in A \qquad f(a+b) = f(a) \oplus f(b)$$
$$\forall a,b \in A \qquad f(a \times b) = f(a) \otimes f(b)$$
$$f(1_A) = 1_{A'}$$

On dit aussi que f est un morphisme de $(A,+,\times)$ dans $(A',\oplus,\otimes)$, pour préciser quelles sont les l.c.i. de A et de A' pour lesquelles f est un morphisme d'anneaux. Parfois on omet les lois $+,\times$ et $\oplus,\otimes$: on se contente d'écrire "f est un morphisme de A dans A' ".

Définition 18.32

Soit $(A,+,\times)$ et $(A',\oplus,\otimes)$ deux anneaux. Soit $f : A \to A'$ un morphisme d'anneaux. On dit que :

- f est un isomorphisme (d'anneaux) si f est bijective.
- f est un endomorphisme (de A) si $(A,+,\times) = (A',\oplus,\otimes)$.
- f est un automorphisme (de A). si f est un isomorphisme et un endormorphisme (de A).

Exemple 23. L'application $z \mapsto \bar{z}$ est un automorphisme de l'anneau $(\mathbb{C},+,\times)$.

L'application $(u_n) \mapsto \lim u_n$ est un morphisme de l'anneau des suites convergentes dans $\mathbb{R}$.

4 Inversibles d'un anneau, corps

4.1 Éléments inversibles d'un anneau

Définition 18.33 – Élément inversible

Soit $(A,+,\times)$ un anneau. L'ensemble des éléments inversibles de A sera noté $\mathrm{Inv}(A)$.

Attention, la notation $\mathrm{Inv}(A)$ n'est pas officielle et est à manier avec précaution. On trouve aussi la notation $A^\times$.

Si A n'est pas trivial, alors $0_A \notin \mathrm{Inv}(A)$: en effet si (par l'absurde) 0_A était inversible, alors en notant b son inverse :

$$0_A b = 1_A \qquad \text{mais aussi} \qquad 0_A b = 0_A$$

donc $1_A = 0_A$, ce qui est une contradiction car A est non trivial. Donc $0_A \notin \mathrm{Inv}(A)$. En particulier, si A n'est pas trivial, alors $(A,\times)$ n'est pas un groupe car 0_A n'est pas inversible.

Remarque. Soit B un sous-anneau de A et $a \in \mathrm{Inv}(A)$. Ainsi, a est inversible **dans l'anneau** $(A,+,\times)$, càd :

$$\exists b \in A \qquad ab = ba = 1_A$$

Il est possible que $a \notin \mathrm{Inv}(B)$. En effet, pour avoir $a \in \mathrm{Inv}(B)$, il faut que a soit inversible **dans l'anneau** $(B,+,\times)$, et donc il faut que

$$\exists b \in \boxed{B} \qquad ab = ba = 1_A$$

En pratique, si $a \in \mathrm{Inv}(A)$, alors on a $\quad a \in \mathrm{Inv}(B) \iff a^{-1} \in B$.

Exemple 24. 2 est inversible dans $(\mathbb{Q},+,\times)$ d'inverse $\dfrac{1}{2}$. Mais 2 n'est pas inversible dans $(\mathbb{Z},+,\times)$.

Théorème 18.34

Soit $(A,+,\times)$ un anneau. Alors $(\mathrm{Inv}(A),\times)$ est un groupe, appelé groupe des inversibles de A.

Démonstration. On vérifie les propriétés **G1.** à **G4.** :

□

Exemple 25. Le groupe des inversibles de $(\mathbb{Z},+,\times)$ est $\{-1,1\}$.
Le groupe des inversibles de $\mathbb{Q},\mathbb{R},\mathbb{C}$ est $\mathbb{Q}^*,\mathbb{R}^*,\mathbb{C}^*$ respectivement.
Le groupe des inversibles de $\mathbb{R}^{\mathbb{N}}$ est l'ensemble des suites (u_n) qui ne s'annulent pas : on a alors $(u_n)^{-1}=\left(\frac{1}{u_n}\right)$.

4.2 Calcul dans un anneau (inversibilité)

Théorème 18.35

Soit A un anneau. Si $\boxed{a\in \mathrm{Inv}(A)}$, alors a est régulier :

$$\forall x,y\in A \qquad ax=ay \implies x=y \qquad \text{et} \qquad xa=ya \implies x=y$$

Il est essentiel que a soit inversible. Contre-exemple : si $a=0_A$ et $x\neq y$, on a $x0_A=y0_A$ mais pas $x=y$.

Définition 18.36 – Diviseur de zéro

Soit $(A,+,\times)$ un anneau. On appelle diviseur de zéro tout élément $a\in A\setminus\{0_A\}$ tel que

$$\exists b\in A\setminus\{0_A\} \qquad ab=0_A$$

Définition 18.37 – Anneau intègre

Soit $(A,+,\times)$ un anneau. On dit que A est un anneau intègre si :

I1. $A\neq\{0_A\}$

I2. A est commutatif.

I3. $\forall a,b\in A \qquad (\quad ab=0_A \implies \quad a=0_A \quad \text{ou} \quad b=0_A \quad)$

La condition **I3.** est équivalente à dire que A ne contient pas de diviseur de zéro.

Exemple 26. Les anneaux $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ sont intègres.
Dans un anneau intègre, "si un produit est nul, (au moins) un des facteurs du produit est nul". Cela est vrai sur $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$, mais ce n'est pas automatique ! Cf les exemples ci-dessous.

Exemple 27. $(\mathbb{R}^2,+,\times)$ n'est pas intègre car $(0,1)\times(1,0)=(0,0)$ alors que $(0,1)$ et $(1,0)$ ne sont pas égaux à $0_{\mathbb{R}^2}=(0,0)$. Ainsi $(0,1)$ et $(1,0)$ sont des diviseurs de zéro.

Exemple 28. $(\mathbb{R}^{\mathbb{R}},+,\times)$ n'est pas intègre. En effet, si on pose $f:x\mapsto\begin{cases}0 & x\leq 0\\ |x| & x\geq 0\end{cases}$ et $g:x\mapsto\begin{cases}|x| & x\leq 0\\ 0 & x\geq 0\end{cases}$
alors $fg\equiv 0$ mais $f\not\equiv 0$ et $g\not\equiv 0$. Ainsi, f et g sont des diviseurs de zéro.

Théorème 18.38

Dans un anneau intègre A, tout élément différent de 0_A est régulier.

Démonstration. Soit $a \in A \setminus \{0_A\}$. Montrons pour commencer que a est régulier à gauche. Soit $x, y \in A$. Alors

$$\begin{aligned} ax = ay &\implies a(x-y) = 0_A \\ &\implies a = 0_A \text{ ou } x-y = 0_A \qquad \text{car } A \text{ est intègre} \\ &\implies x-y = 0_A \qquad\qquad\quad \text{car } a \neq 0_A \\ &\implies x = y \end{aligned}$$

Donc a est régulier à gauche. De même, a est régulier à droite, donc est régulier. □

4.3 Corps

Définition 18.39

Un anneau $(\mathbb{K}, +, \times)$ est appelé un corps si :

K1. $\mathbb{K} \neq \{0_\mathbb{K}\}$

K2. $\mathbb{K}$ est commutatif.

K3. Tout élément non nul de $\mathbb{K}$ est inversible.

On note en général $\mathbb{K}^* := \mathbb{K} \setminus \{0_\mathbb{K}\}$ le groupe des inversibles de $\mathbb{K}$.

Exemple 29. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps. $\mathbb{Z}$ n'est pas un corps car, par exemple, $2 \in \mathbb{Z}$ n'est pas inversible.

Théorème 18.40

Tout corps est un anneau intègre. La réciproque est fausse (contre-exemple : $\mathbb{Z}$).

Démonstration. Soit $\mathbb{K}$ un corps. Il suffit de vérifier la condition **I3.** de la Définition 18.37. Soit $a, b \in \mathbb{K}$ tels que $ab = 0_\mathbb{K}$. Si $a = 0_\mathbb{K}$, alors l'assertion est vérifiée. Si $a \neq 0_\mathbb{K}$, alors a est inversible, donc

$$a^{-1}ab = a^{-1}0_\mathbb{K} = 0_\mathbb{K}$$

si bien que $b = 0_\mathbb{K}$. D'où le résultat. □

Définition 18.41 – Sous-corps, hors programme ?

Soit $(\mathbb{K}, +, \times)$ un corps. Une partie $\mathbb{L} \subset \mathbb{K}$ est un sous-corps de $\mathbb{K}$ si $\mathbb{L}$ est stable par les l.c.i. $+$ et $\times$, et que $(\mathbb{L}, \oplus, \otimes)$ est un corps, où $\oplus, \otimes$ sont les lois induites par $+, \times$ sur $\mathbb{L}$.

À nouveau, on commet l'abus de notation en confondant les lois induites $\oplus, \otimes$ avec les lois $+, \times$.

Théorème 18.42 – Hors programme ?

Soit $(\mathbb{K}, +, \times)$ un corps. Une partie $\mathbb{L} \subset \mathbb{K}$ est un sous-corps de $\mathbb{K}$ si et seulement si :

1. $\mathbb{L} \neq \{0_\mathbb{K}\}$ et $\mathbb{L} \neq \varnothing$ (ou de manière équivalente $\mathbb{L} \setminus \{0_\mathbb{K}\} \neq \varnothing$)
2. $\forall x, y \in \mathbb{L} \quad x - y \in \mathbb{L}$
3. $\forall x, y \in \mathbb{L} \times \mathbb{L}^* \quad xy^{-1} \in \mathbb{L}$

Exemple 30. $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$, qui est lui-même un sous-corps de $\mathbb{C}$.

5 Méthodes pour les exercices

Méthode

Apprendre son cours.