Chapitre 19

Structures algébriques

Plan du chapitre

Hypothèse

Dans tout ce chapitre, E est un ensemble, et $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.

1 Vocabulaire introductif

1.1 Loi de composition interne

Définition 19.1 – 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.

Étant donné une l.c.i. notée $\top : E \times E \to E$, on notera $x \top y$ au lieu de $\top(x,y)$.

Méthode

Pour montrer qu'une application $\top$ est une l.c.i. sur E, il faut montrer que cette application est bien définie : que pour tous $x, y \in E$, l'expression $x \top y$ a un sens et appartient bien à E.

Exemple 1.
- Les lois $+$, $-$ et $\times$ sont des l.c.i. sur $\mathbb{Z}$ car ces applications sont bien définies de $\mathbb{Z} \times \mathbb{Z}$ dans $\mathbb{Z}$. Idem pour $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.
- La loi $-$ n'est pas une l.c.i. sur $\mathbb{N}$, car cette application n'est pas bien définie de $\mathbb{N} \times \mathbb{N}$ dans $\mathbb{N}$: par exemple $2-3 \notin \mathbb{N}$.
- La loi $/$ (division) n'est pas une l.c.i. sur $\mathbb{R}$ car, par exemple, $2/0$ n'a pas de sens. Par contre la loi $/$ est une l.c.i. sur $\mathbb{R}_+^*$.

Exemple 2. On pose $E =]-1,1[$ et on définit l'application $*$ par :

$$\begin{aligned} * : E \times E &\to E \\ (x,y) &\mapsto \frac{x+y}{1+xy} \end{aligned}$$

Montrer que $*$ est bien définie, donc que $*$ est une l.c.i. sur E.

1.2 Commutativité, associativité

Définition 19.2 – 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 $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.
- Barrer ce qui ne convient pas : la l.c.i. $-$ sur $\mathbb{Z}$ **est / n'est pas** commutative et **est / n'est pas** associative. Idem pour $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.
- Pour tout ensemble Ω, la réunion $\cup$ et l'intersection $\cap$ sont des l.c.i. commutatives et associatives sur l'ensemble $E = \mathscr{P}(\Omega)$.

Exemple 4. On reprend l'Exemple 2, avec $E =]-1,1[$ et l'application $*$. Montrer que $*$ est commutative.

Vérifier brièvement que l'application $*$ est associative.

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 $x_1 \top x_2 \top \ldots \top x_n$ sans ambiguité.

Théorème 19.3

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 19.4

Deux éléments x et y de 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 5. Soit f et g les fonctions de $\mathbb{C}^{\mathbb{C}}$ définies par $f(z) = z^2$ et $g(z) = \bar{z}$. Montrer que f et g commutent.

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.

1.3 Élément neutre

Définition 19.5 – 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

$$\forall x \in E \quad \begin{cases} x \top e = x \\ e \top x = x \end{cases}$$

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

Il faut bien vérifier que $x \top e = x$ ET que $e \top x = x$, et ce pour tout $x \in E$. Cependant, si la loi $\top$ est **commutative**, il est suffisant de vérifier que $x \top e = x$.

Démonstration. Démontrons l'unicité.

□

Exemple 6.

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

Méthode

Pour montrer qu'une loi $\top$ admet un élément neutre, il faut partir de la relation $x \top e = x$ pour en déduire la valeur de e qui convient. Attention à vérifier aussi $e \top x = x$ si $\top$ n'est pas commutative !

Exemple 7. On reprend l'Exemple 2, avec $E =]-1, 1[$ et l'application $*$. Montrer que $*$ admet un élément neutre, qu'on notera e.

1.4 Élément symétrisable

Définition 19.6 – Élément symétrisable

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

$$\exists y \in E \qquad \begin{cases} x \top y = e \\ y \top x = e \end{cases}$$

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

Il faut bien vérifier que $x \top y = e$ ET que $y \top x = e$. Cependant, si la loi $\top$ est **commutative**, il est suffisant de vérifier que $x \top y = e$. Bien entendu, la valeur de y dépendra de x.

Remarque. Un même élément x peut a priori avoir plusieurs symétriques. Néanmoins, très souvent, ce symétrique est unique, et on le note en général x', ou $-x$, ou encore x^{-1} (selon la loi ou la notation imposée par l'énoncé, cf section 2.2).

Exemple 8.

- Pour la l.c.i. $+$ dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, l'élément neutre est 0. De plus, tout élément x est symétrisable, et son symétrique est $y = -x$.
- Pour la l.c.i. $+$ dans $\mathbb{N}$, seul l'élément 0 est symétrisable : son propre symétrique est lui-même.
- Pour la l.c.i. $\times$ dans $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, l'élément neutre est 1. De plus, tout élément *non nul* x est symétrisable, et son symétrique est $y = x^{-1}$.
- Pour la l.c.i. $\times$ dans $\mathbb{Z}$, seuls les éléments 1 et -1 sont symétrisables : ils sont leur propre symétrique.

Méthode

Pour montrer qu'un élément x est symétrisable pour $\top$, il faut partir de la relation $x \top y = e$ pour en déduire la valeur de y qui convient. Attention à vérifier aussi $y \top x = e$ si $\top$ n'est pas commutative !

Exemple 9. On reprend l'Exemple 2, avec $E =]-1, 1[$ et l'application $*$. Montrer que tout élément de E est symétrisable pour $*$.

2 Groupes

2.1 Définition et propriétés générales

Définition 19.7 – 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).

Bien vérifier que l'élément neutre e, tout comme l'élément symétrique de x appartiennent bien à G !

Groupes usuels :

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes commutatifs. Mais $(\mathbb{N}, +)$ n'est pas un groupe car, par exemple, 3 n'est pas symétrisable pour $+$ dans $\mathbb{N}$.
- $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{R}_+^*, \times)$ 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 $\times$: aucun élément y de $\mathbb{N}^*$ ou de $\mathbb{Z}^*$ ne vérifie $2y = 1$.
- $(\mathbb{K}^{\mathbb{N}}, +)$ et $(\mathbb{K}^{\mathbb{R}}, +)$ sont des groupes (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...

Remarque. Pour les groupes usuels ci-dessus, par abus de langage, on sous-entend parfois la loi $\top$ et on dira simplement que G est un groupe. Par exemple on parlera du groupe $\mathbb{Z}$ ou encore du groupe $\mathbb{R}^*$ pour désigner $(\mathbb{Z}, +)$ et $(\mathbb{R}^*, \times)$ respectivement. On emploiera parfois cet abus pour des groupes non usuels également.

Exemple 10.
- $(\mathbb{N}, \times)$, $(\mathbb{Z}, \times)$, $(\mathbb{Q}, \times)$, $(\mathbb{R}, \times)$ et $(\mathbb{C}, \times)$ ne sont pas des groupes car :

- On reprend l'Exemple 2, avec $E =]-1, 1[$ et l'application $*$. Alors $(E, *)$ est un groupe commutatif (cf exemples précédents).

Théorème 19.8

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

La loi d'un groupe peut être notée $\top$ ou $*$, mais bien souvent on emploie les notations $+$ et $\times$, car ces deux lois sont associées à des notations usuelles pour l'élément neutre et l'élément symétrique, qui permettront de mener des calculs de manière similaire à ce qu'on fait avec des nombres réels ou complexes.

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

Notations et règles de calcul (notations additives et multiplicatives)

Soit $a\in E$ et $m,n\in\mathbb{Z}$.	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 : noté $-a$ $a+(-a)=(-a)+a=0_E$	Inverse : noté a^{-1} $aa^{-1}=a^{-1}a=1_E$
Itéré n-ième de a (a symétrisable si $n\leq -1$)	$na=\begin{cases}\underbrace{a+\ldots+a}_{n\text{ fois}} & \text{si } n\geq 1\\ 0a=0_E & \text{si } n=0\\ \underbrace{(-a)+\ldots+(-a)}_{n\text{ fois}} & \text{si } n\leq -1\end{cases}$	$a^n=\begin{cases}\underbrace{a\cdots a}_{n\text{ fois}} & \text{si } n\geq 1\\ a^0=1_E & \text{si } n=0\\ \underbrace{a^{-1}\cdots a^{-1}}_{n\text{ fois}} & \text{si } n\leq -1\end{cases}$
Symétrique de l'itéré (a symétrisable)	$-(na)=n(-a)=(-n)a$	$(a^n)^{-1}=(a^{-1})^n=a^{-n}$
Si a n'est pas symétrisable, les lignes suivantes ne sont valides que pour $m,n\in\mathbb{N}$.		
Opération sur l'itéré	$na+ma=(n+m)a$	$a^na^m=a^{n+m}=a^na^m$
Itéré de l'itéré	$n(ma)=(nm)a$	$(a^n)^m=a^{nm}=(a^m)^n$

Toutes ces règles de calcul sont similaires aux réels, c'est ce qui fait l'attrait de ces notations. Prudence cependant, toutes les opérations dans $\mathbb{R}$ ne sont pas permises ! Notamment l'associativité et la commutativité ne vont pas de soi.

En notation multiplicative, on n'a pas toujours $ab = ba$ (la commutativité de $\cdot$ n'est pas automatique). Par contre, la notation additive $a+b$ n'est employée que pour une l.c.i. commutative (ce qui n'exclut pas de devoir la vérifier si nécessaire).

Exemple 11 (Notation multiplicative et composition)**.** On pose $E = \mathbb{R}^{\mathbb{R}}$. On munit l'ensemble E de la l.c.i. $\circ$ (composition), avec la notation muliplicative :

- Plutôt que d'écrire $g \circ f$, on écrira gf (cela ne désigne *pas* la fonction $x \mapsto g(x) \times f(x)$!).
- Son élément neutre est id_E, mais on le notera 1_E. On a donc $1_E f = f 1_E = f$.
- f est symétrisable pour $\circ$ si et seulement s'il existe (une unique fonction) $g \in E$ telle que

$$fg = gf = 1_E \qquad (\text{i.e. } f \circ g = g \circ f = \mathrm{id}_E)$$

  cela revient à dire que f est bijective et que g est l'application réciproque de f. On notera f^{-1} l'application g, et on aura $ff^{-1} = f^{-1}f = 1_E$. Cette notation coïncide bien avec celle vue dans le chapitre des applications.
- Pour tout $n \in \mathbb{N}^*$, f^n désignera l'application $f \circ f \circ \cdots \circ f$ (cela ne désigne *pas* la fonction $x \mapsto f(x)^n$!).
- On a alors les règles de calcul $f^n f^m = f^{n+m}$, ou encore $(f^n)^m = f^{nm}$, etc.

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 19.9

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 :

Démonstration.

□

Définition 19.10 – 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 19.11

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

Exemple 12. Soit $(G, \cdot)$ un groupe et $a, b \in G$. Résoudre l'équation $x^{-1}a = ab$ d'inconnue $x \in G$.

2.4 Sous-groupes

Définition 19.12

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

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

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

Dans ce cas, $\top_H$ est une l.c.i. sur H et est appelée la loi induite (par $\top$) sur H. Très souvent, on note encore $\top$ la l.c.i. $\top_H$ bien qu'il y ait ambiguité. Par ailleurs, la notation $\top_H$ n'est pas officielle.

Lemme 19.13

Avec les notations ci-dessus :

- Si $\top$ est associative (resp. commutative), alors $\top_H$ l'est aussi.
- Si e est un élément neutre de E, et que $e \in H$, alors e est aussi un élément neutre pour $\top_H$.
- Soit $x \in H$. Si x est symétrisable pour $\top$, et que son symétrique x' vérifie $x' \in H$, alors x est aussi symétrisable pour $\top_H$ (de symétrique x').

Définition 19.14

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, grâce au Lemme 19.13 ci-dessus, on peut (et on doit) utiliser une des caractérisations qui suivent :

Théorème 19.15 – 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 :

1.
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 .....

Démonstration. Soit $H \subset G$ qui vérifie 1–2–3. Par 2, H est stable par $\top$ donc $\top_H$ est bien définie, d'où **G1.**. Comme $\top$ est associative, $\top_H$ l'est aussi par le Lemme 19.13, d'où **G2.**. Par 1 et le Lemme 19.13, e est élement neutre de H, d'où **G3.**. Enfin, par **G4.** et le Lemme 19.13, on en déduit que tout élément x de H est symétrisable pour $\top_H$. Ainsi, $(H, \top_H)$ est bien un groupe. □

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 13.

- $2\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.
- $\mathbb{N}$ n'est pas un sous-groupe de $\mathbb{Z}$ car $1 \in \mathbb{N}$ mais $-1 \notin \mathbb{N}$ (assertion 3 non vérifiée).
- $\mathbb{R}_-^*$ n'est pas un sous-groupe de $\mathbb{R}^*$ car $(-2) \times (-2) \notin \mathbb{R}_-^*$ (assertion 2 non vérifiée).

Méthode

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 19.15, cf exemples ci-dessus.

On peut condenser les assertions 2 et 3 de la propriété 19.15 ci-dessus en une seule :

Théorème 19.16 – 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 :

1.

2.

Exemple 14. 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 19.15 et 19.16, 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 :

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

(et idem pour la propriété 19.15). 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 $x_0 x_0^{-1} \in H$, 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 $\top$.

Exemple 15. Montrer que $(\mathbb{U},\times)$ est un groupe.

Corollaire 19.17

Si H est un sous-groupe d'un groupe commutatif, alors H est aussi un groupe commutatif.

Démonstration. Cela découle du Lemme 19.13. □

Exemple 16. Comme $(\mathbb{C}^*,\times)$ est un groupe commutatif, il en va de même pour $(\mathbb{U},\times)$.

2.5 Morphismes de groupes

Définition 19.18 – 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 19.19

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

$$f : (\mathbb{Z},+) \to (\mathbb{Z},+) \qquad n \mapsto 2n$$

$$g : (\mathbb{R}_+^*,\times) \to (\mathbb{R},+) \qquad x \mapsto \ln x$$

Théorème 19.20

Soit G et G' deux groupes d'éléments neutres respectifs e et 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 18. 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 19.21

Soit G et 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 :

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

Démonstration.

□

Définition 19.22 – 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 19.23

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 le Théorème 19.21. Montrons maintenant la seconde assertion.

- Sens réciproque : supposons f injective. Comme $f(e) = e'$, il est clair que $e \in \mathrm{Ker} f$. Montrons l'autre inclusion, à savoir $\mathrm{Ker} f \subset \{e\}$. Soit $x \in \mathrm{Ker} f$. Alors $f(x) = e' = f(e)$ et comme f est injective, $x = e$. Ainsi, $x \in \{e\}$ et on a bien l'inclusion recherchée. D'où $\mathrm{Ker} f = \{e\}$.
- Sens direct : supposons $\mathrm{Ker} f = \{e\}$ et montrons que f est injective. Soit $x, y \in G$ tels que $f(x) = f(y)$. Alors :

$$f(x) f(y)^{-1} = e'$$

et comme f est un morphisme, on en déduit $f(xy^{-1}) = e'$. Ainsi, $xy^{-1} \in \mathrm{Ker} f = \{e\}$. Donc, $xy^{-1} = e$, ou encore $x = y$. Donc (par arbitraire sur x, y), f est injective.

□

Exemple 19. 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 19.24 – 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 19.25

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 le Théorème 19.21.

La seconde assertion est tautologique : par définition, $\mathrm{Im} f = f(G)$ et on a vu au chapitre sur les applications que $f(G) = G'$ si et seulement si f est surjective. □

Exemple 20. 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 19.26 – Groupe produit

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

$$\forall (g_1,h_1),(g_2,h_2)\in G\times H \qquad (g_1,h_1)\otimes(g_2,h_2)=(g_1g_2,h_1h_2)$$

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

Attention, la notation $\otimes$ est loin d'être universelle pour désigner une loi produit : on peut aussi noter $*$, voire même $\times$, comme les lois de G et H !

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

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

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.**

- Montrons G3. Soit $(x,y)\in G\times H$. On a
$$(e_G,e_H)*(x,y)=(e_G\top x,e_H\bot y)=(x,y)$$
et de même $(x,y)*(e_G,e_H)=(x,y)$. Ainsi, (e_G,e_H) est bien élément neutre.
- Montrons G4. On a
$$(x^{-1},y^{-1})*(x,y)=(x^{-1}\top x,y^{-1}\bot y)=(e_G,e_H)$$
et de même $(x,y)*(x^{-1},y^{-1})=(e_G,e_H)$. Ainsi, (x,y) est bien symétrisable et $(x,y)^{-1}=(x^{-1},y^{-1})$.
- Montrons enfin la dernière assertion. Si $\top$ et $\bot$ sont commutatives, alors
$$(g_1,h_1)*(g_2,h_2)=(g_1\top g_2,h_1\bot h_2)=(g_2\top g_1,h_2\bot h_1)=(g_2,h_2)*(g_1,h_1)$$
donc $*$ est commutative.

□

Exemple 21. $(\mathbb{R},+)$ et $(\mathbb{R}^*,\times)$ sont des groupes donc on peut munir l'ensemble $E=\mathbb{R}\times\mathbb{R}^*$ de la loi produit

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

Dans ce cas, l'élément neutre de E est ..... et le symétrique d'un élément (x,y) de E est .....

3 Anneaux

3.1 Anneau

Définition 19.27 – 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 : $\forall a,b,c\in M \qquad a\top(b\top c)=(a\top b)\top c$.

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

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 22. $(\mathbb{Z},\times)$, $(\mathbb{Q},\times)$, $(\mathbb{R},\times)$ et $(\mathbb{C},\times)$ sont des monoïdes.
Étant donné un ensemble Ω quelconque, $(\mathscr{P}(\Omega),\cap)$ et $(\mathscr{P}(\Omega),\cup)$ sont des monoïdes.

Définition 19.28 – 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 19.29

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 a.

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

Dans un anneau, il n'est jamais garanti qu'un élément donné soit inversible !

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 23. Déterminer une condition nécessaire et suffisante pour qu'une suite u de l'anneau $\mathbb{R}^{\mathbb{N}}$ soit inversible.

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 19.12.

Définition 19.30

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 19.31

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. □

1. Montrons que $(B,+)$ est un groupe abélien. On va montrer que c'est un sous-groupe de $(A,+)$.
   - Par les assertions 1 et 2, en prenant $x=y=1_A$, on a $x-y=1_A-1_A=0_A \in B$ donc B contient l'élément neutre pour la loi $+$.
   - De plus, comme on a 2, on vérifie que $(B,+)$ est un sous-groupe de $(A,+)$ donc un groupe (proposition 19.16).
   - Enfin, $(B,+)$ est un sous-groupe du groupe abélien $(A,+)$, donc $(B,+)$ est abélien.

   Finalement $(B,+)$ est un groupe abélien.
2. Montrons que $(B,\times)$ est un monoïde.
   - Par 3, $\times$ est une l.c.i. sur B
   - Par 1, B possède un élément neutre pour $\times$.
   - Comme $\times$ est associative sur A et que $B \subset A$, on en déduit que $\times$ est associative sur B.
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, on a en particulier $x,y,z \in A$ et comme A est un anneau, les relations ci-dessus sont vérifiées. D'où le résultat.

Exemple 24.
- $\mathbb{Z}$, $\mathbb{D}$ et $\mathbb{Q}$ sont des sous-anneaux de $(\mathbb{R},+,\times)$.
- $\mathbb{Z}$, $\mathbb{D}$, $\mathbb{Q}$ et $\mathbb{R}$ sont des sous-anneaux de $(\mathbb{C},+,\times)$.
- On note C l'ensemble des suites réelles convergentes. C 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 $-$)

Démonstration.

□

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 19.32 – Formules du binôme et $a^n - b^n$, version anneaux

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

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

Ne pas oublier que a et b doivent *commuter* pour appliquer ces formules !

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

Exemple 25. 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 19.33 – 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 dans A', pour préciser les anneaux de départ et d'arrivée. On omettra en général les lois $+,\times$ et $\oplus,\otimes$.

Définition 19.34

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 26.
- L'application $z \mapsto \overline{z}$ 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

Théorème 19.35

Soit A un anneau et soit a et b deux éléments **inversibles** de a.

- Le produit ab est aussi inversible et $(ab)^{-1} = b^{-1}a^{-1}$.
- a^{-1} est inversible et $(a^{-1})^{-1} = a$.

Démonstration. La preuve est très similaire à celle du Théorème 19.9. □

Comme déjà dit, rien ne permet de dire qu'un élément quelconque d'un anneau A est inversible ou non. On peut mentionner que 1_A est inversible et est son propre inverse puisque $1_A 1_A = 1_A$. En revanche, dès que A est non trivial, on peut montrer que 0_A n'est pas inversible car il n'existe aucun $b \in A$ tel que $0_A b = 1_A$.

Notation. Soit $(A, +, \times)$ un anneau. L'ensemble des éléments inversibles de A sera noté $\mathrm{Inv}(A)$ dans ce cours. Cette notation n'est pas officielle. On trouve aussi la notation $A^\times$...

Théorème 19.36

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**.. On s'appuie sur le Lemme 19.13 et le Théorème 19.35 :

□

Exemple 27. Le groupe des inversibles de $(\mathbb{Z}, +, \times)$ est $\{-1, 1\}$, qui est bien un groupe pour $\times$.
Les groupes des inversibles des anneaux $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ 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 19.37

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 $a = 0_A$, on a toujours $0_A x = 0_A y$ mais pas nécessairement $x = y$.

Définition 19.38 – 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 19.39 – 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 28. Les anneaux $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont intègres.
Dans un anneau intègre, "si un produit est nul, (au moins) un des facteurs du produit est nul". Cela est vrai sur $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, mais ce n'est pas automatique ! Cf les exemples ci-dessous.

Exemple 29. Montrons que $(\mathbb{R}^2, +, \times)$ n'est pas intègre. On a $(0,1) \times (1,0) = (0,0)$ alors que $(0,1)$ et $(1,0)$ ne sont pas égaux à $0_{\mathbb{R}^2}$, qui vaut (0,0). Ainsi $(0,1)$ et $(1,0)$ sont des diviseurs de zéro. D'où $(\mathbb{R}^2, +, \times)$ n'est pas intègre.

Exemple 30. $(\mathbb{R}^{\mathbb{R}}, +, \times)$ 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 19.40

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

Démonstration.

□

4.3 Corps

Définition 19.41

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 31. $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps. $\mathbb{Z}$ n'est pas un corps car, par exemple, 2 est un élément non nul de $\mathbb{Z}$ qui n'est pas inversible.

Théorème 19.42

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 19.39. Soit $a, b \in \mathbb{K}$ tels que $ab = 0_\mathbb{K}$. Montrons que $a = 0_\mathbb{K}$ ou $b = 0_\mathbb{K}$. 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 19.43 – 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 19.44 – 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 32. $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$, qui est lui-même un sous-corps de $\mathbb{C}$.

5 Méthodes pour les exercices

Méthode

Pour montrer qu'un ensemble E est un groupe, on peut :

1. **Montrer que c'est le sous-groupe d'un groupe usuel.**
2. **Vérifier si E n'est pas égal à $\mathrm{Inv}(A)$ pour un anneau usuel A** (il faut que la loi de E soit $\times$)**.**
3. Montrer que $E=\mathrm{Im}\,f$ ou $E=\mathrm{Ker}\,f$ avec $f:G\to G'$ un morphisme de groupes.
4. Montrer que $E=f(H)$ ou $E=f^{-1}(H')$ avec H et H' des sous-groupes de G et G'.
5. Si E s'écrit comme un produit de deux groupes, vérifier si E est le groupe produit de ces deux groupes.
6. En dernier recours, vérifier **G1.** à **G4.**.

Méthode

Pour montrer qu'un ensemble E est un anneau, on peut :

1. **Montrer que c'est le sous-anneau d'un anneau usuel.**
2. En dernier recours, vérifier **A1.** à **A3.**.