

Chapitre 17

Structures algébriques.

Sommaire.

1	Loi de composition interne sur un ensemble.	1
1.1	Définitions et propriétés.	1
1.2	Éléments symétrisables.	2
1.3	Itérés.	3
1.4	Notations multiplicatives et additives.	3
2	Structure de groupe.	4
2.1	Définition et exemples.	4
2.2	Sous-groupes.	5
2.3	Morphismes de groupes.	6
3	Structure d’anneau.	8
3.1	Définitions et règles de calcul.	8
3.2	Groupe des inversibles dans un anneau.	8
3.3	Nilpotents dans un anneau.	9
3.4	Sous-anneaux, morphismes d’anneaux.	9
3.5	Anneaux intègres.	10
4	Structure de corps.	10
4.1	Définitions et exemples.	10
4.2	Notation fractionnaire dans un corps.	11
4.3	Corps des fractions d’un anneau intègre.	11
5	Exercices.	11

Les propositions marquées de ★ sont au programme de colles.

1 Loi de composition interne sur un ensemble.

1.1 Définitions et propriétés.

Définition 1: et 2

On appelle **loi de composition interne** sur un ensemble E (on écrire l.c.i.) une application

$$\star : \begin{cases} E \times E & \rightarrow & E \\ (x, y) & \mapsto & x \star y \end{cases}$$

On notera que l'image de (x, y) par \star est notée $x \star y$ plutôt que $\star(x, y)$.

Soit E un ensemble et \star une l.c.i. sur E .

- La loi \star est dite **associative** si $\forall (x, y, z) \in E^3, (x \star y) \star z = x \star (y \star z)$.
- De deux éléments x et y de E , on dit qu'ils **commutent** pour \star lorsque $x \star y = y \star x$. On dit que la loi \star est **commutative** si $\forall (x, y) \in E^2, x \star y = y \star x$.
- On appelle **élément neutre** pour \star tout élément $e \in E$ tel que $\forall x \in E, x \star e = x$ et $e \star x = x$.

Définition 2: Vocabulaire hors-programme.

Un couple (E, \star) , où E est un ensemble et \star une l.c.i. sur E est appelé **magma**.

On dit que ce magma est associatif si \star est associative, commutatif si \star est commutative, et **unifère** s'il existe dans E un élément neutre pour \star .

Proposition 3

Dans un magma unifère, il y a unicité du neutre.

Preuve :

Soient e et e' des éléments neutres d'un magma unifère (E, \star) .

On a $e \star e' = e = e'$ car e et e' sont neutres pour \star donc $e = e'$.

Définition 4: Partie stable.

Soit (E, \star) un magma et $A \in \mathcal{P}(E)$. On dit que A est **stable** par \star si

$$\forall (x, y) \in A^2, x \star y \in A.$$

Définition 5: Loi induite.

Soit (E, \star) un magma et $A \in \mathcal{P}(E)$ stable par \star . La restriction de \star à A^2 :

$$\star : \begin{cases} A \times A & \rightarrow & A \\ (x, y) & \mapsto & x \star y \end{cases}$$

est une l.c.i. sur A : on l'appelle loi induite par \star sur A .

Exemple 6: Ensembles de nombres.

- $+$ est une l.c.i. associative, commutative avec 0 comme neutre sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
- \times est une l.c.i. associative, commutative, de neutre 1 sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
- $-$ est une l.c.i. non associative, non commutative et sans neutre sur \mathbb{Z} . \mathbb{N} n'est pas stable par $-$.

Exemple 7: Ensemble des parties

Soit E un ensemble. L'intersection \cap et la réunion \cup définissent des l.c.i. sur $\mathcal{P}(E)$.

- Le magma $(\mathcal{P}(E), \cap)$ est associatif, commutatif et unifère, avec E pour neutre.
- Le magma $(\mathcal{P}(E), \cup)$ est associatif, commutatif et unifère, avec \emptyset pour neutre.

Exemple 8: Ensembles de fonctions et composition.

Soit E un ensemble. La composition \circ est une l.c.i. sur E^E , l'ensemble des fonctions de E vers E .

Le magma (E^E, \circ) est associatif et unifère : il admet id_E pour neutre. Si $|E| \geq 2$, il n'est pas commutatif.

L'ensemble des fonctions injectives est stable par \circ , de même pour l'ensemble des fonctions surjectives, bijectives.

Définition 9: Distributivité d'une loi par rapport à une autre.

Soit E un ensemble muni de deux l.c.i. \oplus et \otimes .

On dit que \otimes est **distributive par rapport à \oplus** si

$$\forall (x, y, z) \in E^3 \quad : \quad \begin{cases} x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z) \\ (y \oplus z) \otimes x = (y \otimes x) \oplus (z \otimes x) \end{cases}$$

(Si la loi \oplus n'est pas commutative, il est primordial de vérifier les deux égalités.)

Exemple 10

- Dans $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, la multiplication \times est distributive par rapport à l'addition $+$.
- Dans $\mathcal{P}(E)$, \cap est distributive par rapport à \cup .
- Dans $\mathcal{P}(E)$, \cup est distributive par rapport à \cap .

1.2 Éléments symétrisables.

Définition 11: Élément symétrisable.

Soit (E, \star) un magma unifère de neutre e , et $x \in E$.

On dit que x est **symétrisable** (ou **inversible**) s'il existe un élément x' dans E tel que

$$x \star x' = e \quad \text{et} \quad x' \star x = e.$$

Proposition 12: Unicité du symétrique / de l'inverse.

Soit (E, \star) un magma associatif et unifère de neutre e .

Si x est un élément de E symétrisable, il existe un unique x' dans E tel que $x \star x' = x' \star x = e$.

On appelle cet élément le **symétrique** de x (ou son inverse), et on le note x^{-1} .

Preuve :

Soit $x \in E$ et $x', x'' \in E$ tels que :

$$\begin{cases} x \star x' = x' \star x = e, \\ x \star x'' = x'' \star x = e \end{cases}$$

On a alors $x' \star x \star x'' = (x' \star x) \star x'' = x'' = x'' \star x = x' \star (x \star x'') = x'$ donc $x' = x''$.

Exemple 13

- Les inversibles de (\mathbb{Z}, \times) sont -1 et 1 .
- Les inversibles de (\mathbb{R}, \times) sont les réels non nuls. (admis)

Solution :

On vérifie facilement que -1 et 1 sont inversibles.

Soit $p \in \mathbb{Z} \setminus \{-1, 0, 1\}$. Supposons par l'absurde qu'il existe $q \in \mathbb{Z}$ tel que $pq = qp = 1$.

Alors $|p| \geq 2$ et $|q| \geq 1$ donc $|p||q| \geq 2 \cdot 1$ donc $|pq| \geq 2$ donc $1 \geq 2$, absurde.

Exemple 14

Les inversibles du magma (E^E, \circ) sont les bijections $f : E \rightarrow E$, d'inverse f^{-1} .

Proposition 15

Soit (E, \star) un magma associatif et unifère, et $x, y \in E$.

1. Si x est symétrisable, x^{-1} l'est aussi et $(x^{-1})^{-1} = x$.
2. Si x et y sont symétrisables, $x \star y$ l'est aussi et

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

Preuve :

1.
- Supposons que x est symétrisable, alors $x \star x^{-1} = x^{-1} \star x = e : (x^{-1})^{-1} = x$.
2.
- Supposons x et y symétrisables. Alors :

$$\begin{cases} (x \star y) \star (y^{-1} \star x^{-1}) = x \star (y \star y^{-1}) \star x^{-1} = x \star x^{-1} = e, \\ (y^{-1} \star x^{-1}) \star (x \star y) = y^{-1} \star (x^{-1} \star x) \star y = y^{-1} \star y = e. \end{cases}$$

Donc $x \star y$ est inversible, d'inverse $y^{-1} \star x^{-1}$.

1.3 Itérés.

On fixe pour tout ce paragraphe un magma (E, \star) associatif et unifère de neutre e .

Définition 16: Itérés d'un élément.

- Soit $x \in E$.
1. Pour $n \in \mathbb{N}$, on définit x^n par récurrence sur n . — On pose $x^0 = e$.
— Pour tout $n \in \mathbb{N} : x^{n+1} = x^n \star x$.
 2. Si x est inversible et $n \in \mathbb{N}^*$, on pose $x^{-n} = (x^{-1})^n$.

Proposition 17: Propriétés des itérés.

$$\forall x \in E, \forall (m, n) \in \mathbb{N}^2, x^m \star x^n = x^{m+n} \quad \text{et} \quad (x^m)^n = x^{mn}.$$

Si x est inversible, les identités ci-dessus sont vraies pour $(m, n) \in \mathbb{Z}^2$.

Preuve :

Soit un élément x de E .

Soit $m \in \mathbb{N}$ fixé. Pour $n \in \mathbb{N}$, on note $\mathcal{P}(n) : \ll x^m \star x^n = x^{m+n} \gg$.

Initialisation. On a $x^m \star x^0 = x^l \star e = x^{m+0}$.

Hérédité. Soit $n \in \mathbb{N} \mid \mathcal{P}(n)$. Alors $x^m \star x^{n+1} = x^m \star x^n \star x = x^{m+n} \star x = x^{m+n+1}$.

Conclusion. Par récurrence, $\forall n \in \mathbb{N}, \mathcal{P}(n)$.

Soit $m \in \mathbb{N}$ fixé. Pour $n \in \mathbb{N}$, on note $\mathcal{Q}(n) : \ll (x^m)^n = x^{m \cdot n} \gg$.

Initialisation. On a $(x^m)^0 = e = x^{m \cdot 0}$.


Hérédité. Soit $n \in \mathbb{N} \mid \mathcal{Q}(n)$. Alors $(x^m)^{n+1} = (x^m)^n \star x^m = x^{mn} \star x^m = x^{mn+m} = x^{m(n+1)}$.

Conclusion. Par récurrence, $\forall n \in \mathbb{N}, \mathcal{Q}(n)$.

Exemple 18: Itérés d'éléments qui commutent.

Soient x et y deux éléments deux E qui commutent. Alors

$$\forall (m, n) \in \mathbb{N}^2, x^m \star y^n = y^n \star x^m \quad \text{et} \quad (x \star y)^n = x^n \star y^n.$$

 Les identités ci-dessus sont FAUSSES en général lorsque x et y ne commutent pas.

1.4 Notations multiplicatives et additives.

Utiliser la **notation multiplicative**, lorsqu'on travaille avec un magma (E, \star) consiste à ne pas écrire \star lorsqu'on calcule l'image d'un couple $(x, y) \in E^2$. Concrètement, on note alors xy à la place de $x \star y$.

Lorsqu'on travaille avec un magma associatif, commutatif et unifère, on pourra utiliser la notation $+$ pour la l.c.i. Le vocabulaire sur les notations introduits plus haut est alors adapté à cette **notation additive**, comme explicité dans le tableau ci-dessous.

notation l.c.i.	\star	cot	$+$
image de (x, y)	$x \star y$	xy	$x + y$
notation neutre	e	e	0
on dit	symétrisable	inversible	symétrisable
on dit	symétrique	inverse	opposé
notation symétrique	x^{-1}	x^{-1}	-x
notation itéré	x^n	x^n	nx

2 Structure de groupe.

2.1 Définition et exemples.

Définition 19

On appelle **groupe** un magma associatif et unifère dans lequel tout élément est symétrisable.

Plus précisément, un groupe est la donnée d'un couple (G, \star) où G est un ensemble et \star une l.c.i. tels que

- \star est associative.
- il existe dans G un élément e neutre pour \star .
- tout élément de G est symétrisable.

Si de surcroît \star est commutative, on dit que le groupe (G, \star) est **abélien** (ou commutatif).

Remarque. Un groupe n'est jamais vide car il contient au moins son élément neutre.

Proposition 20: Ensembles de nombres.

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

Exemple 21: Ce ne sont pas des groupes.

- $(\mathbb{N}, +)$ n'est pas un groupe car 1 n'est pas symétrisable.
- (\mathbb{Z}^*, \times) n'est pas un groupe car 2 n'est pas inversible dans \mathbb{Z} .
- $(\mathbb{C}, +)$ n'est pas un groupe car 0 n'a pas d'inverse dans \mathbb{C} .

Exemple 22: Vérifier les axiomes de groupe sur une loi artificielle.

On pose $G = \mathbb{R}^* \times \mathbb{R}$. Pour $(a, b) \in G$ et $(a', b') \in G$ on définit

$$(a, b) \star (a', b') = (aa', ab' + b).$$

Montrer que (G, \star) est un groupe.

Solution :

On vérifie chacun des points de la définition de groupe...

\star est-elle une l.c.i. dans G ? G est-il associatif ? Unifère ? Symétrisable ?

Définition 23

Soit E un ensemble non-vide. On appelle **permutation** de E une bijection $\sigma : E \rightarrow E$.

On note S_E l'ensemble des permutations de E .

Proposition 24: ★

(S_E, \circ) est un groupe, appelé **groupe des permutations** de E , ou groupe symétrique de E .

Dès que E contient au moins 3 éléments, le groupe S_E n'est pas abélien.

Preuve :

Soient $\sigma, \sigma' \in S_E$. On a $\sigma \circ \sigma' : E \rightarrow E$ une bijection comme composée.

- \circ est une l.c.i. sur E .
- Associativité.** On sait déjà que $(\mathcal{F}(E, E), \circ)$ est associatif.
- Unifère.** $\text{id}_E \in S_E$ est neutre pour \circ .
- Symétrie.** Si $f \in S_E$, c'est une bijection alors $f^{-1} \in S_E$ et est le symétrique de f .

Supposons que $|E| \geq 3$. Soient $a, b, c \in E$ différents.

On définit σ telle que $\sigma(a) = b$, $\sigma(b) = c$, $\sigma(c) = a$ et $\sigma(x) = x$ pour $x \in E \setminus \{a, b, c\}$.

On définit σ' telle que $\sigma'(a) = b$, $\sigma'(b) = a$ et $\sigma'(x) = x$ pour $x \in E \setminus \{a, b\}$.

On a $\sigma' \circ \sigma(a) = a$ et $\sigma \circ \sigma'(a) = c$ donc $\sigma' \circ \sigma \neq \sigma \circ \sigma'$: pas commutatif.

Proposition 25: Produit de deux groupes.

Soient (G, \star) et (G', \top) deux groupes. On note e le neutre de G et e' celui de G' .

Pour (x, x') et (y, y') deux éléments de $G \times G'$, on pose

$$(x, x') \heartsuit (y, y') = (x \star y, x' \top y').$$

Muni de la l.c.i. \heartsuit , le produit cartésien $G \times G'$ est un groupe, de neutre (e, e') .

Preuve :

On vérifie chacun des points de la définition de groupe...

Proposition 26: Produit de n groupes.

Soient G_1, \dots, G_n n groupes (les l.c.i. étant sous-jacentes et notées multiplicativement).
Pour (x_1, \dots, x_n) et (y_1, \dots, y_n) deux éléments $G_1 \times \dots \times G_n$, on pose

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

Muni de la l.c.i. \heartsuit , le produit cartésien $G_1 \times \dots \times G_n$ est un groupe, de neutre (e_1, \dots, e_n) .

2.2 Sous-groupes.

Définition 27

Soit (G, \star) un groupe et H une partie de G .
On dit que H est un **sous-groupe** de G si H est stable par \star et si (H, \star) est un groupe.

Proposition 28: Élément neutre et inverses dans un sous-groupe.

Soit (G, \star) un groupe et H un sous-groupe de G .
1. L'élément neutre du groupe H n'est autre que celui de G .
2. Soit $x \in H$. L'inverse de x dans le groupe (H, \star) et celui dans le groupe (G, \star) sont égaux.

Preuve :

- [1.] Soit e le neutre de G . On a $\forall x \in G, e \star x = x \star e = x$ donc $\forall x \in H, e \star x = x \star e = x$ car $H \subset G$.
Par unicité du neutre dans H , on a e neutre de H .
[2.] Soit $x \in H$. On note x' l'inverse de x dans H et x'' dans G .
Alors $x' \star x = x \star x' = e$ et $x'' \star x = x \star x'' = e$, donc par unicité du neutre dans G , $x' = x''$.

Théorème 29: Caractérisation des sous-groupes.

Soit (G, \star) un groupe de neutre e et $H \subset G$. On équivale entre :

1. H est un sous-groupe de G .
2. $\begin{cases} \bullet e \in H, \\ \bullet \forall (x, y) \in H^2, x \star y^{-1} \in H \end{cases}$
3. $\begin{cases} \bullet e \in H \\ \bullet \forall (x, y) \in H^2, x \star y \in H \\ \bullet \forall x \in H, x^{-1} \in H \end{cases}$

Remarque. On utilisera presque **toujours** cette caractérisation.

Preuve :

- [1] \implies [2] Supposons H sous-groupe de G . Alors H est stable par \star et (H, \star) est un groupe.
— $\bullet e$ est le neutre de G , c'est aussi celui de H donc $e \in H$.
— \bullet Soit $(x, y) \in H^2$. y^{-1} est l'inverse de y et $y^{-1} \in H$, alors $x \star y^{-1} \in H$ par stabilité de H par \star .
[2] \implies [3] Supposons $e \in H$ et $\forall (x, y) \in H^2, x \star y^{-1} \in H$.
— $\bullet e \in H$ donc $e \in H$.
— \bullet Soient $(x, y) \in H^2 : x \star y = x \star (y^{-1})^{-1} \in H$ par hypothèse.
— \bullet Soit $x \in H$, on a $x^{-1} = e \star x^{-1} \in H$ car $e, x \in H$.
[3] \implies [1] Supposons $e \in H, \forall (x, y) \in H^2, x \star y \in H$ et $\forall x \in H, x^{-1} \in H$.
— $\bullet H$ est stable par \star car $\forall (x, y) \in H^2, x \star y \in H$ et \star est l.c.i. sur H par déf.
— $\bullet \star$ est associative sur H car elle l'est sur G .
— $\bullet H$ est unifère car e est neutre et $e \in H$.
— \bullet tout élément de H est symétrisable car $\forall x \in H, x^{-1} \in H$.

Proposition 30: Sous-groupes usuels.

1. $(\mathbb{Q}, +)$ est un sous-groupe de $(\mathbb{R}, +)$, qui est lui-même un sous-groupe de $(\mathbb{C}, +)$.
2. \mathbb{R}_+^* est un sous-groupe de (\mathbb{R}^*, \times) .
3. \mathbb{U} et \mathbb{U}_n sont des sous-groupes de (\mathbb{C}^*, \times) .

Exemple 31: Une intersection de sous-groupes est un sous-groupe. ★

Soient H et H' deux sous-groupes d'un groupe (G, \star) . Montrer que $H \cap H'$ est sous-groupe de G .

Solution :

- Soit e le neutre de G , on a alors $e \in H$ et $e \in H'$ car sous-groupes donc $e \in H \cap H'$.
- Soient $x, y \in H \cap H'$.
— On a $x \in H$ et $y \in H$ donc $x \star y^{-1} \in H$ car H est un groupe.
— On a $x \in H'$ et $y \in H'$ donc $x \star y^{-1} \in H'$ car H' est un groupe.
— Alors $x \star y^{-1} \in H \cap H'$.

Exemple 32: Une union de sous-groupes n'est pas toujours un sous-groupe.

Montrer que $\mathbb{U}_2 \cup \mathbb{U}_3$ n'est pas un sous-groupe de (\mathbb{C}^*, \times) .

On note $H = \bigcup_{n \in \mathbb{N}^*} \mathbb{U}_n$. Montrer que H est un sous-groupe de (\mathbb{C}^*, \times) .

Solution :

1. On a $\mathbb{U}_2 \cup \mathbb{U}_3 = \{-1, 1, j, j^2\}$ et $-1 \times j = -j \notin \mathbb{U}_2 \cup \mathbb{U}_3$: pas stable par \times .
 2. On a $1 \in H$ car $1 \in \mathbb{U}_1$.
- Soient $z, \tilde{z} \in H : \exists k, \tilde{k} \in \mathbb{N}^* \mid z \in \mathbb{U}_k$ et $\tilde{z} \in \mathbb{U}_{\tilde{k}}$ donc $(z \cdot \tilde{z})^{k\tilde{k}} = (z^k)^{\tilde{k}}(\tilde{z}^{\tilde{k}})^k = 1$ donc $z\tilde{z} \in \mathbb{U}_{k\tilde{k}} \subset H$.
 - Soit $z \in H : \exists p \in \mathbb{N}^* \mid z \in \mathbb{U}_p$, or \mathbb{U}_p est un groupe donc $z^{-1} \in \mathbb{U}_p \subset H$.

Exemple 33: Centre d'un groupe. ★

Soit (G, \star) un groupe. On note

$$Z(G) = \{x \in G \mid \forall a \in G, x \star a = a \star x\}.$$

Montrer que $Z(G)$ est un sous-groupe de G .

Solution :

- Soit e le neutre de G . On a $\forall a \in G, e \star a = a \star e = a$ donc $e \in Z(G)$.
 - Soient $a, b \in Z(G)$ et $x \in G$. On a $(a \star b) \star x = a \star x \star b = x \star (a \star b)$ donc $a \star b \in Z(G)$.
 - Soient $x \in Z(G)$ et $a \in G$. On a $x^{-1} \star a = (a^{-1} \star x)^{-1} = (x \star a^{-1})^{-1} = a \star x^{-1}$ donc $x^{-1} \in Z(G)$.
- Par caractérisation, le centre d'un groupe est un sous-groupe.

Proposition 34: Sous-groupes de $(\mathbb{Z}, +)$ (programme de spé). ★★

Pour $n \in \mathbb{N}$, on note $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$.

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

Preuve :

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

- • $0 \in n\mathbb{Z}$ car $0 = n0$.
- • Soient $p, p' \in n\mathbb{Z} : \exists k, k' \in \mathbb{Z} \mid p = kn$ et $p' = k'n$, alors $p + p' = (k + k')n \in n\mathbb{Z}$.
- • Soit $p \in \mathbb{Z} : \exists k \in \mathbb{Z} \mid p = kn$ donc $p^{-1} = -p = (-k)n \in n\mathbb{Z}$.

Par caractérisation, c'est bien un sous-groupe de \mathbb{Z} .

Soit H un sous-groupe de \mathbb{Z} . Montrons qu'il existe $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.

→ Cas particulier : $H = \{0\}$, alors $H = 0\mathbb{Z}$. Supposons $H \neq \{0\}$ pour la suite.

On a alors $H \cap \mathbb{N}^*$ une partie non-vide de \mathbb{N}^* . Notons n son plus petit élément. Montrons que $H = n\mathbb{Z}$.

\supseteq Soit $p \in n\mathbb{Z} : \exists k \in \mathbb{Z} \mid p = nk : p$ est itéré de n avec $n \in H$ donc $p \in H$.

\subseteq Soit $p \in H : \exists!(q, r) \in \mathbb{Z}^2 \mid p = nq + r$ et $0 \leq r < n$ (division euclidienne).

- Alors $r = p - nq$ avec $p \in H$ et $nq \in H$ donc $r \in H$.
- Supposons $r \neq 0$, alors $r \in H \cap \mathbb{N}^*$, or $n = \min(H \cap \mathbb{N}^*)$ et $r < n$: absurde !
- Donc $r = 0$ et $p = nq$ donc $p \in n\mathbb{Z}$.

Par double-inclusion, $H = n\mathbb{Z}$.

Exemple 35: (*) Sous-groupes de $(\mathbb{R}, +)$.

Pour $a \in \mathbb{R}_+$, on note $a\mathbb{Z} = \{ak \mid k \in \mathbb{Z}\}$.

Soit H un sous-groupe de $(\mathbb{R}, +)$. Ou bien il existe $a \in \mathbb{R}_+$ tel que $H = a\mathbb{Z}$, ou bien H est dense dans \mathbb{R} .

2.3 Morphismes de groupes.

Définition 36

Soient (G, \star) et (G', \top) deux groupes.

On appelle **morphisme de groupe** de G dans G' toute application $f : G \rightarrow G'$ telle que

$$\forall (x, y) \in G^2, f(x \star y) = f(x) \top f(y).$$

Si de surcroît f est bijective, on dit qu'une telle application f est un **isomorphisme** de groupes.

Un morphisme d'un groupe G vers lui même est appelé **endomorphisme** de G .

Si un tel endomorphisme est bijectif, on parle d'**automorphisme** de G .

Définition 37

On dit que deux groupes sont **isomorphes** s'il existe un isomorphisme de l'un vers l'autre.

Exemple 38

- L'exponentielle réelle est un isomorphisme de $(\mathbb{R}, +)$ dans (\mathbb{R}^*, \times) .
- L'exponentielle complexe est un morphisme de groupes de $(\mathbb{C}, +)$ dans (\mathbb{C}^*, \times) .
- $t \mapsto e^{it}$ est un morphisme de groupes de $(\mathbb{R}, +)$ dans (\mathbb{U}, \times) .
- Le logarithme népérien est un isomorphisme de groupes de (\mathbb{R}^*, \times) dans $(\mathbb{R}, +)$.

Exemple 39

Justifier que les groupes $(\mathbb{R}^2, +)$ et $(\mathbb{C}, +)$ sont isomorphes.

Solution :

On pose $f : (a, b) \mapsto a + ib$. Soient (a, b) et (a', b') dans \mathbb{R}^2 .

$$\begin{aligned} f((a, b) + (a', b')) &= f((a + a', b + b')) = (a + a') + i(b + b') = a + ib + a' + ib' \\ &= f(a, b) + f(a', b'). \end{aligned}$$

La fonction f est un morphisme de groupes de $(\mathbb{R}^2, +)$ dans $(\mathbb{C}, +)$.

Elle est bijective par unicité de la forme algébrique : c'est un isomorphisme. Les groupes sont donc isomorphes.

Proposition 40: ★

Soient G et G' deux groupes de neutres respectifs e et e' , et $f : G \rightarrow G'$ un morphisme de groupes.

1. $f(e) = e'$.
2. $\forall x \in G, f(x^{-1}) = f(x)^{-1}$.
3. $\forall x \in G, \forall p \in \mathbb{Z}, f(x^p) = f(x)^p$.
4. Si H est un sous-groupe de G , alors $f(H)$ est un sous-groupe de G' .
5. Si H' est un sous-groupe de G' , alors $f^{-1}(H')$ est un sous-groupe de G .
6. Si f est un isomorphisme de G vers G' , alors f^{-1} est un isomorphisme de G' vers G .

Preuve :

1. On a $f(e) = f(e \cdot e) = f(e) \cdot f(e) = f(e)^{-1} \cdot f(e) \cdot f(e) = f(e)^{-1} \cdot f(e) = e'$.
2. Soit $x \in G$. On a $f(x \cdot x^{-1}) = f(x)f(x^{-1}) = f(e) = e'$ donc par unicité de l'inverse $f(x)^{-1} = f(x^{-1})$.
3. Soit $x \in G$. Par récurrence sur $p \in \mathbb{N}$.
— **Initialisation.** $f(x^0) = f(e) = e' = f(x)^0$.
— **Hérédité.** Soit $p \in \mathbb{N} \mid f(x^p) = f(x)^p$. Alors $f(x^{p+1}) = f(x^p \cdot x) = f(x)^p f(x) = f(x)^{p+1}$.
4. ★ Soit H un sous-groupe de G .
— • $e' \in f(H)$ car $e \in H$.
— • Soient $y, \tilde{y} \in f(H)$, d'antécédents $x, \tilde{x} : y\tilde{y}^{-1} = f(x)f(\tilde{x})^{-1} = f(x \cdot \tilde{x}^{-1}) \in f(H)$.
Par caractérisation, $f(H)$ est un sous-groupe de G' .
5. ★ Soit H' un sous-groupe de G' .
— • $e \in f^{-1}(H)$ car $e' \in H'$.
— • Soient $x, \tilde{x} \in f^{-1}(H) : f(x\tilde{x}^{-1}) = f(x)f(\tilde{x})^{-1} \in H$ par stabilité puisque $f(x)$ et $f(\tilde{x})^{-1}$ dans H .
Par caractérisation, $f^{-1}(H')$ est un sous-groupe de G .
6. Soit f un isomorphisme de G vers G' . Sa réciproque f^{-1} existe.
— Soient $y, y' \in G' : f^{-1}(yy') = f^{-1}(f(f^{-1}(y))f(f^{-1}(y')))) = f^{-1}(f(f^{-1}(y)f^{-1}(y')))) = f^{-1}(y)f^{-1}(y')$.

Définition 41

Soient G et G' deux groupes de neutres respectifs e et e' , et $f : G \rightarrow G'$ un morphisme de groupes.

1. On appelle **noyau** de f et on note $\text{Ker } f$ l'ensemble

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

2. On appelle **image** de f et on note $\text{Im } f$ l'ensemble

$$\text{Im } f = \{y \in G' \mid \exists x \in G : y = f(x)\}.$$

Proposition 42: ★★

Soient G et G' deux groupes de neutres respectifs e et e' , et $f : G \rightarrow G'$ un morphisme de groupes.

1. $\text{Ker } f$ est un sous-groupe de G et

$$f \text{ est injective} \iff \text{Ker } f = \{e\}.$$

2. $\text{Im } f$ est un sous-groupe de G' et

$$f \text{ est surjective} \iff \text{Im } f = G'.$$

Preuve :

1. On a $\text{Ker } f = f^{-1}(\{e'\})$ donc $\text{Ker } f$ est un sous-groupe de G comme image réciproque du sous-groupe $\{e'\}$.
 \implies Supposons f injective.
— • $e \in \text{Ker } f$ car $\text{Ker } f$ est un sous-groupe de G .
— • Soit $x \in \text{Ker } f$. Alors $f(x) = f(e) = e'$ et par injectivité de f , $x = e$.
Par double inclusion, $\text{Ker } f = \{e\}$.
 \impliedby Supposons $\text{Ker } f = \{e\}$. Soient $x, x' \in G$ tels que $f(x) = f(x')$.
On a $f(x)f(x)^{-1} = f(x')f(x)^{-1}$ donc $e' = f(x')f(x)^{-1} = f(x'x^{-1})$.
Alors $x'x^{-1} \in \text{Ker } f : x'x^{-1} = e$, on multiplie par x à droite : $x' = x$.
2. $\text{Im } f = f(G)$ est l'image d'un sous-groupe de G par un morphisme, c'est un sous-groupe de G' .
On a déjà l'équivalence, vraie pour n'importe quelle application de $\mathcal{F}(G, G')$.

3 Structure d’anneau.

3.1 Définitions et règles de calcul.

Définition 43

On appelle **anneau** tout triplet $(A, +, \times)$, où A est un ensemble et $+$ et \times des l.c.i telles que

- $(A, +)$ est un groupe abélien, de neutre 0_A .
- (A, \times) est un magma associatif et unifère, de neutre 1_A .
- \times est distributive par rapport à $+$.

Les lois $+$ et \times sont appelées respectivement **addition** et **multiplication** de l’anneau A .
Si de surcroît \times est commutative, on dit que l’anneau A est commutatif.

Exemple 44: Ensembles de nombres.

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

Exemple 45: Anneau de fonctions.

On rappelle que, pour X une partie de \mathbb{R} , $\mathcal{F}(X, \mathbb{R})$, ensemble des fonctions définies sur X et à valeurs réelles a été muni d’une addition et d’une multiplication de la manière suivante :

$$\forall f, g \in \mathcal{F}(X, \mathbb{R}), \quad f + g = \begin{cases} X & \rightarrow \mathbb{R} \\ x & \mapsto f(x) + g(x) \end{cases} \quad \text{et} \quad f \times g : \begin{cases} X & \rightarrow \mathbb{R} \\ x & \mapsto f(x)g(x) \end{cases}$$

Le triplet $(\mathcal{F}(X, \mathbb{R}), +, \times)$ est un anneau commutatif.
L’élément neutre pour $+$ est la fonction nulle sur X .
L’élément neutre pour \times est la fonction constante sur X égale à 1.
En particulier, $(\mathbb{R}^{\mathbb{N}}, +, \times)$ est un anneau commutatif : celui des suites.

Exemple 46: Pas des anneaux.

- $(2\mathbb{Z}, +, \times)$ n’est pas un anneau car il n’y a pas de neutre pour \times .
- $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \circ)$ n’est pas un anneau car \circ n’est pas distributive par rapport à $+$.

Proposition 47

Soit $(A, +, \times)$ un anneau. En utilisant la notation multiplicative pour la loi \times ,

1. $\forall a \in A, \quad 0_A \times a = a \times 0_A = 0_A$.
2. $\forall (a, b) \in A^2, \quad a(-b) = (-a)b = -(ab)$.
3. $\forall (a, b) \in A^2, \quad (-a)(-b) = ab$.
4. $\forall (a, b) \in A^2, \quad \forall n \in \mathbb{Z}, \quad a(nb) = (na)b = n(ab)$.

Proposition 48: Identités remarquables : si ça commute, d’accord.

Soit $(A, +, \times)$ un anneau et $(a, b) \in A^2$.

1. Si $ab = ba$, alors $\forall n \in \mathbb{N}, \quad (a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$.
2. Si $ab = ba$, alors $\forall n \in \mathbb{N}^*, \quad a^n - b^n = (a - b) \sum_{k=0}^{n-1} a^k b^{n-k-1}$.

Preuve :

Exactement les mêmes preuves que lorsqu’on $A = \mathbb{R}$.

3.2 Groupe des inversibles dans un anneau.

Définition 49

Dans un anneau $(A, +, \times)$, les **inversibles** sont les éléments de A inversibles pour la loi \times .
L’ensemble des éléments de A qui sont inversibles sera noté $U(A)$.

Exemple 50

- $U(\mathbb{Z}) = \{-1, 1\}$.
- $U(\mathbb{R}) = \mathbb{R}^*$.
- Pour $X \subset \mathbb{R}$, $U(\mathcal{F}(X, \mathbb{R}))$ est l’ensemble des fonctions ne s’annulant pas sur X .

Proposition 51

Si $(A, +, \times)$ est un anneau, $(U(A), \times)$ est un groupe. On l’appelle **groupe des inversibles**.
On a notamment

$$\forall (a, b) \in (U(A))^2, \quad ab \in U(A) \quad \text{et} \quad (ab)^1 = b^{-1}a^{-1}.$$

3.3 Nilpotents dans un anneau.

Définition 52

Dans un anneau $(A, +, \times)$, on dit d'un élément $a \in A$ qu'il est **nilpotent** s'il possède une puissance nulle, c'est à dire :

$$\exists p \in \mathbb{N}^* \mid a^p = 0_A.$$

Exemple 53

Soit $(A, +, \times)$ un anneau et $(a, b) \in A^2$.

1. Montrer que si a est nilpotent, et si b commute avec a , alors ab est nilpotent.
2. Montrer que si ab est nilpotent, alors ba est nilpotent.

Solution :

1.
- Soit a nilpotent : $\exists p \in \mathbb{N}^* \mid a^p = 0_A$. Alors $(ab)^p = a^p b^p = 0_A b^p = 0_A$.
2.
- Soient $a, b \in A$ tel que $\exists p \in \mathbb{N}^* \mid (ab)^p = 0_A$. Alors $(ba)^{p+1} = b(ab)^p a = b 0_A a = 0_A$?

Exemple 54

Soit $(A, +, \times)$ un anneau non réduit à $\{0_A\}$ et $a \in A$ nilpotent d'ordre p .

1. Montrer que a n'est pas inversible.
2. Montrer que $1_A - a$ est inversible et exprimer son inverse.

Solution :

1.
- Supposons a inversible. Alors a^p l'est aussi, $1_A = a^{-p} a^p = a^{-p} 0_A = 0_A$, absurde.
2.
- $(1_A - a) \sum_{k=0}^{p-1} a^k = 1_A - a^p = 1_A$, de même a droite.

3.4 Sous-anneaux, morphismes d'anneaux.

Proposition 55

Soit $(A, +, \times)$ un anneau et $B \subset A$. On dit que B est un **sous-anneau** de A si

- $\forall (a, b) \in B^2, a - b \in B$.
- $\forall (a, b) \in B^2, ab \in B$.
- $1_A \in B$.

Muni des lois induites par $+$ et \times , B est un anneau.

Preuve :

Montrons que $(B, +)$ est un groupe abélien.

— *bullet* $1_A \in B$ donc $1_A - 1_A \in B$ donc $0_A \in B$.

— • $\forall (a, b) \in B, a - b \in B$.

Par caractérisation c'est un sous groupe, abélien car $(A, +)$ l'est.

Montrons que (B, \times) est un magma unifère et associatif.

— • B est stable par \times .

— • Associatif car \times l'est dans A .

— • Unifère car $1_A \in B$ et est neutre pour \times .

\times se distribue déjà sur $+$ dans A , donc aussi dans B .

Exemple 56

- A est un sous-anneau de A . Si $0_A \neq 1_A$, alors $\{0_A\}$ n'est pas un sous-anneau de A .
- Montrer que \mathbb{Z} est le seul sous-anneau de \mathbb{Z} .

Exemple 57: Anneau de Gauss. ★

Soit l'ensemble

$$\mathbb{Z}[i] = \{a + ib \mid (a, b) \in \mathbb{Z}^2\}.$$

Montrer que $(\mathbb{Z}[i], +, \times)$ est un anneau commutatif et déterminer ses éléments inversibles.

Solution :

Vérifions qu'il s'agit d'un sous-anneau de $(\mathbb{C}, +, \times)$.

Soit $(z, z') \in \mathbb{Z}[i] : \exists!(a, b) \in \mathbb{Z}^2 \mid z = a + ib$ et $\exists!(a', b') \in \mathbb{Z}^2 \mid z' = a' + ib'$.

— • $1 = 1 + 0i$ et $(1, 0) \in \mathbb{Z}^2$ donc $1 \in \mathbb{Z}[i]$.

— • On a $z - z' = (a - a') + i(b - b')$ donc $z - z' \in \mathbb{Z}[i]$.

— • On a $zz' = (aa' - bb') + i(ab' + a'b)$ donc $zz' \in \mathbb{Z}[i]$.

Donc c'est bien un anneau.

Soit un inversible $z = a + ib$ de $\mathbb{Z}[i]$. On a $zz' = 1$ donc $|zz'| = 1$ donc $|z||z'| = 1$.

On a que $|z|$ et $|z'|$ sont entiers donc $|z| = |z'| = 1$, donc $z \in \{\pm 1, \pm i\}$.

On vérifie facilement que c'est exactement l'ensemble des inversibles de $\mathbb{Z}[i]$.

Définition 58

Soient $(A, +, \times)$ et $(A', +, \times)$ deux anneaux.
On appelle **morphisme d'anneaux** de A dans A' toute application $f : A \rightarrow A'$ telle que

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

Si de surcroît f est bijective, on dit qu'une telle application f est un **isomorphisme** d'anneaux.

Exemple 59

La conjugaison

$$\text{conj} : \begin{cases} \mathbb{C} & \rightarrow & \mathbb{C} \\ z & \mapsto & \bar{z} \end{cases}$$

est un isomorphisme de l'anneau $(\mathbb{C}, +, \times)$ dans lui-même.

3.5 Anneaux intègres.

Définition 60

Soit $(A, +, \times)$ un anneau. On dit d'un élément a de A qu'il est un **diviseur de zéro** si $a \neq 0_A$ et s'il existe un élément b dans $A \setminus \{0_A\}$ tel que $ab = ba = 0_A$.

Exemple 61

- Dans l'anneau $(\mathbb{Z}, +, \times)$, il n'y a pas de diviseurs de zéro.
- Dans l'anneau $(\mathbb{R}^{\mathbb{R}}, +, \times)$, il existe des diviseurs de zéro.

Définition 62

On appelle anneau **intègre** tout anneau commutatif sans diviseurs de zéro. Dans un tel anneau,

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

Exemple 63

\mathbb{Z} est un anneau intègre, l'anneau $\mathbb{K}[X]$ des polynômes aussi, mais pas celui des matrices $M_n(\mathbb{K})$ ($n \geq 2$).

4 Structure de corps.

4.1 Définitions et exemples.

Définition 64

On appelle **corps** tout anneau commutatif $(K, +, \times)$ non réduit à $\{0_K\}$ dans lequel tout élément non nul est inversible.

Proposition 65

Tout corps est un anneau intègre, la réciproque est fausse.

Preuve :

Soit $(K, +, \times)$ un corps. C'est un anneau commutatif.
Supposons qu'il existe un diviseur de zéro, noté $x \in K$.
Alors $x \neq 0_K$ et $\exists y \in K \setminus \{0_K\} \mid xy = 0_K$ et $yy^{-1} = 1_K$ donc $y^{-1}xy = y^{-1}0_K$ donc $x = 0_K$. Absurde.

Exemple 66: ★

Soit

$$\mathbb{Q}[\sqrt{2}] = \left\{ x \in \mathbb{R} \mid \exists (a, b) \in \mathbb{Q}^2, x = a + b\sqrt{2} \right\}.$$

Montrer que $\mathbb{Q}[\sqrt{2}]$ est un corps.

Solution :

— • $\mathbb{Q}[\sqrt{2}]$ est un sous-anneau de $(\mathbb{R}, +, \times)$.
— • $\mathbb{Q}[\sqrt{2}]$ est commutatif car \mathbb{R} l'est.
Soit $x \in \mathbb{Q}[\sqrt{2}]$ non nul, $\exists (a, b) \in \mathbb{Q}^2 \mid x = a + b\sqrt{2}$.
Alors $(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$ donc $(a + b\sqrt{2}) \times \left(\frac{a}{a^2 - 2b^2} + \frac{b}{a^2 - 2b^2}\sqrt{2} \right) = 1$.
Notons $c = \frac{a}{a^2 - 2b^2}$ et $d = \frac{b}{a^2 - 2b^2}$. On a $c + d\sqrt{2}$ inverse de $a + b\sqrt{2}$. Montrons que $a^2 - 2b^2 \neq 0$.
Supposons que $a^2 - 2b^2 = 0$, alors $a^2 = 2b^2$ et si $b = 0$, alors $a = 0$, impossible.
Si $b \neq 0$, alors $\frac{a^2}{b^2} = 2$ donc $\left| \frac{a}{b} \right| = \sqrt{2}$, absurde car $\sqrt{2} \notin \mathbb{Q}$.
Alors $\mathbb{Q}[\sqrt{2}]$ est un corps.

4.2 Notation fractionnaire dans un corps.

Soit $(K, +, \times)$ un corps, $a \in K$ et $b \in K^*$. On note $ab^{-1} = \frac{a}{b}$.
Pour $(a, c) \in K^2$ et $(b, d) \in (K^*)^2$, on peut vérifier que

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd} \qquad \frac{a}{b} = \frac{c}{d} \iff ad = bc \qquad \frac{1}{a} = a^{-1}.$$

4.3 Corps des fractions d’un anneau intègre.

Théorème 67

Pour tout anneau intègre A , il existe un unique corps commutatif K contenant A et vérifiant

$$\forall x \in K, \exists (a, b) \in A \times A^* \mid x = \frac{a}{b}.$$

Le corps K est appelé **corps des fractions** de l’anneau A .

Exemple. Le corps des fractions de \mathbb{Z} n’est autre que \mathbb{Q} .

5 Exercices.

Groupes, sous-groupes, morphismes de groupes.

Exercice 1: ♦♦♦

Soit (E, \star) un magma associatif fini.
Démontrer qu’il existe dans E un élément idempotent, c’est-à-dire un élément x tel que $x^2 = x$.

Solution :

Soit $x \in E$. On considère la suite (u_n) telle que $u_0 = 1$ et $\forall n \in \mathbb{N}, u_{n+1} = u_n^2$. Soit $n \in \mathbb{N}$.
Puisque E est fini, $\exists p > q \in \mathbb{N} \mid u_{2p} = u_{2q}$ donc $x^{2p} = x^{2q}$.
Alors on pose $n = p - q$ et $a = x^{2p}$. Ainsi : $a^{2^n} = a$.
Si $n = 1$, a est idempotent. Sinon, on a:

$$a^{2^n-1} a^{2^n-1} = a^{2^{n+1}-2} = a^{2^n} a^{2^n-2} = a a^{2^n-2} = a^{2^n-1}$$

Donc a^{2^n-1} est idempotent.

Exercice 2: ♦♦♦

Pour x et y dans $] - 1, 1[$, on pose $x \star y = \frac{x+y}{1+xy}$. Montrer que $(] - 1, 1[, \star)$ est un groupe abélien.

Solution :

Soit $y \in] - 1, 1[$. On pose $f_y : x \mapsto \frac{x+y}{1+xy}$ définie sur $] - 1, 1[$. On a $f'_y : x \mapsto \frac{1-y^2}{(1+xy)^2}$.

x	-1	1
$f'_y(x)$		$+$
f_y	-1	1

Donc $] - 1, 1[$ est stable part \star , c’est bien une l.c.i.
— Le neutre est 0.
— On peut vérifier l’associativité par calcul direct.
— Pour $x \in] - 1, 1[$, $x \star y = \frac{x+y}{1+xy} = \frac{y+x}{1+yx} = y \star x$.
— Tout élément x admet un symétrique $-x$.
On a bien vérifié tous les points de la définition de groupe abélien.

Exercice 3: ♦♦♦

Soient (G, \star) un groupe et H un sous-groupe de G . Pour $a \in G$, on pose

$$aHa^{-1} = \{a \star h \star a^{-1}, h \in H\}.$$

Montrer que aHa^{-1} est un sous-groupe de G .

Solution :

Soit e le neutre de G et de H . On fixe $a \in G$.
— • On a $e \in H$ et $e \star e \star e^{-1} = e$ donc $e \in aHa^{-1}$.
— • Soient $x, y \in H$. On a $x \star y = axa^{-1}aya^{-1}a^{-1} = axy^{-1}a^{-1} \in aHa^{-1}$ car $xy^{-1} \in H$ car H est un groupe.
Par caractérisation, aHa^{-1} est un sous-groupe de G .

Exercice 4: ♦♦♦

Soit $(a_n)_{n \in \mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$. Posons

$$H = \{x \in \mathbb{R} \mid \cos(a_n x) \rightarrow 1\}.$$

Montrer que H est un sous-groupe de $(\mathbb{R}, +)$.

Solution :

- • On a $\cos(a_n 0) = \cos(0) = 1$ donc $0 \in H$.
- • Soient $x, y \in H$. On a

$$\begin{aligned} \cos(a_n(x - y)) &= \cos(a_n x - a_n y) = \cos(a_n x) \cos(a_n y) + \sin(a_n x) \sin(a_n y) \rightarrow 1 \\ \text{car } \sin(a_n x) \sin(a_n y) &= \sqrt{1 - \cos^2(a_n x)} \sqrt{1 - \cos^2(a_n y)} \rightarrow 0. \end{aligned}$$

Par caractérisation, H est un sous-groupe de $(\mathbb{R}, +)$.

Exercice 5: ♦♦♦

Soit l'ensemble d'applications

$$G = \{x \mapsto ax + b, a \in \mathbb{R}^*, b \in \mathbb{R}\}.$$

En vous appuyant sur un groupe connu, montrer que (G, \circ) est un groupe.

Solution :

Montrons que (G, \circ) est sous-groupe de $(S_{\mathbb{R}}, \circ)$.

- • $\text{id}_{\mathbb{R}} \in G$ car $\forall x \in \mathbb{R}, \text{id}_{\mathbb{R}}(x) = 1x + 0$.
- • Soient $f : x \mapsto ax + b, g : x \mapsto mx + p \in G$. Alors:

$$\forall x \in \mathbb{R}, f \circ g^{-1}(x) = a\left(\frac{x - p}{m}\right) + b = \frac{a}{m}x + \frac{bm - ap}{m}.$$

Par caractérisation, G est un sous-groupe de $S_{\mathbb{R}}$.

Exercice 6: ♦♦♦

Soit G un groupe noté multiplicativement, et H et K deux sous-groupes de G . On définit

$$HK = \{x \in G \mid \exists h \in H, \exists k \in K, x = hk\}.$$

Démontrer que HK est un sous-groupe de G si et seulement si $HK = KH$.

Solution :

\Rightarrow Supposons HK sous-groupe de G .

\subset Soit $x \in HK : \exists h \in H, \exists k \in K \mid x = hk$ donc $x^{-1} = k^{-1}h^{-1} \in KH$ donc $x \in KH$.

\supset Soit $x \in KH : \exists k \in K, \exists h \in H \mid x = kh$ donc $x^{-1} = h^{-1}k^{-1} \in HK$ donc $x \in HK$.

On a l'égalité des ensembles.

\Leftarrow Supposons $HK = KH$.

— • On a $1_G = 1_H 1_K$ donc $1_G \in HK$.

— • Soient $x = hk, x' = h'k' \in HK$. $xx' = hkh'k'$ or $kh' \in KH$ et $KH = HK$ donc $\exists \tilde{h}, \tilde{k} \in H \times K \mid kh' = \tilde{h}\tilde{k}$.

Ainsi, $x\tilde{x} = h\tilde{h}\tilde{k}k' \in HK$.

— • Soit $x = hk \in HK$. On a $x^{-1} = k^{-1}h^{-1} \in KH = HK$ donc $x^{-1} \in HK$.

Par caractérisation, HK est sous-groupe de G .

Exercice 7: ♦♦♦

Soit G un groupe noté multiplicativement. Pour $a \in G$, on pose $\tau_a : x \mapsto ax$.

1. Pour tout $a \in G$, montrer que $\tau_a \in S_G$.
2. Montrer que $\delta : a \mapsto \tau_a$ est un morphisme injectif de G dans S_G .

Solution :

1. Soit $a \in G$. On a τ_a bijective car $\tau_{a^{-1}}$ est sa réciproque, et de G vers G car $a \in G$.

2. Soient $a, b \in G$. On a $\delta(ab) = \tau_{ab} = \tau_a \circ \tau_b = \delta(a)\delta(b)$.

Supposons $\delta(a) = \delta(b)$. Alors pour $x \in G$, $ax = bx$ donc $axx^{-1} = bxx^{-1}$ donc $a = b$. C'est un morphisme injectif.

Exercice 8: ♦♦♦

Soit G un groupe. Montrer qu'une partie H finie, non vide et stable par la loi de G est nécessairement un sous-groupe de G .

Solution :

Soit H une telle partie et $x \in H$. On note e le neutre de G .

Puisque H est fini, $\exists k > q \in \mathbb{N} \mid x^k = x^q$ donc $x^{k-q} = e$ donc $e \in H$ comme itéré de x .

On a d'ailleurs $x^{-1} = x^{k-q-1} \in H$.

Par hypothèse, H est stable par la loi de G donc c'est un sous-groupe.

Exercice 9: ♦♦◇

Soit (G, \cdot) un groupe. On note $\text{Aut}(G)$ l'ensemble des automorphismes de G .

Pour $g \in G$, on note σ_g l'application $x \mapsto gxg^{-1}$.

1. Démontrer que $(\text{Aut}(G), \circ)$ est un groupe.
2. Montrer que pour tout $g \in G$, $\sigma_g \in \text{Aut}(G)$.
3. Démontrer que l'application $\sigma : g \mapsto \sigma_g$ est un morphisme de groupes de G dans $\text{Aut}(G)$.
4. Montrer que $\text{Ker}(\sigma) = Z(G)$, où $Z(G)$ est le centre de G .

Solution :

[1.] Montrons que c'est un sous-groupe de S_G .

— • On a $\text{id}_G \in \text{Aut}(G)$.

— • Soient $\varphi, \psi \in \text{Aut}(G)$. On a $\varphi \circ \psi^{-1}$ bijective de G dans G car φ et ψ le sont donc $\varphi\psi^{-1} \in \text{Aut}(G)$.

Par caractérisation, c'est un sous-groupe de S_G .

[2.] Soit $g \in G$. On a σ_g bijective car $\sigma_{g^{-1}}$ est sa réciproque. Soient $x, y \in G$.

C'est un morphisme car $\sigma_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \sigma_g(x)\sigma_g(y)$.

C'est un endomorphisme car $\forall x \in G$, $gxg^{-1} \in G$ par stabilité.

[3.] Soient $g, h, x \in G$. On a $\sigma(gh)(x) = \sigma_{gh}(x) = ghxh^{-1}g^{-1} = \sigma_g\sigma_h(x) = \sigma(g)\sigma(h)(x)$.

[4.] \subseteq Soient $x \in \text{Ker}(\sigma)$ et $g \in G$. On a $\sigma(x) = \text{id}_G$ donc $xgx^{-1} = g$ donc $xg = gx$ par comp. à droite.

\supseteq Soient $x \in Z(G)$, $g \in G$. On a $gx = xg$ donc $g = xgx^{-1} = \sigma_x(g) = \sigma(x)(g)$ donc $\sigma_x = \text{id}_G$ donc $x \in \text{Ker}(\sigma)$.

Par double inclusion, $\text{Ker}(\sigma) = Z(G)$.

Exercice 10: ♦♦♦

Soit (G, \cdot) un groupe fini et χ un morphisme de groupes non constant de (G, \cdot) dans (\mathbb{C}^*, \times) . Calculer

$$S = \sum_{x \in G} \chi(x).$$

Solution :

Soit $\tilde{x} \in G$ tel que $\chi(\tilde{x}) \neq 1$ (existe car χ non constant).

On pose $\sigma_{\tilde{x}} : x \mapsto x\tilde{x}$, c'est une bijection de G dans G . Alors :

$$\chi(\tilde{x})S = \sum_{x \in G} \chi(\tilde{x})\chi(x) = \sum_{x \in G} \chi(x\tilde{x}) \stackrel{\sigma_{\tilde{x}}}{=} \sum_{x \in G} \chi(x) = S.$$

Alors $S(\chi(\tilde{x}) - 1) = 0$. Donc $S = 0$.

Anneaux, corps.

Exercice 11: ♦♦◇

Montrer que dans un anneau, la somme de deux éléments nilpotents qui commutent est nilpotent.

Solution :

Soient a, b deux éléments nilpotents d'ordre p et q . On a:

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

Pour $k \geq p$, on a $a^k = 0$. Pour $k \leq p$, on a $p + q - k \geq q$ donc $b^{p+q-k} = 0$.

Dans tous les cas, les termes de la somme sont nuls. Donc $(a + b)^{p+q} = 0$.

Exercice 12: ♦♦♦

Soit $(A, +, \times)$ un anneau. On suppose qu'il existe deux éléments a, b de A tels que

$$ab + ba = 1_A \quad \text{et} \quad a^2b + ba^2 = a$$

1. Montrer que $a^2b = ba^2$ et $2aba = a$.
2. Montrer que a est inversible et que $a^{-1} = 2b$.

Solution :

[1.] $a^2b + aba = a$ et $aba + ba^2 = a$ donc $a^2b = ba^2$ d'après la première équation.

Alors $a^2b + ba^2 + 2aba = 2a$ donc $a + 2aba = 2a$ donc $2aba = a$.

[2.] On a $a^2b + aba = a$ donc $a + aba = a + ba^2$ donc $aba = ba^2$; et $ba^2 + aba = a$ donc $aba = ab^2$.

On a alors $a = 2aba = 2a^2b = 2ba^2$ donc $ab = ba = 2ba^2b$. Or $ab + ba = 1_A$ et $ab = ba$ donc $2ab = 2ba = 1_A$.

Exercice 13: ♦♦♦

Soit E un ensemble. On définit sur E la différence symétrique

$$\Delta : \begin{cases} E \times E & \rightarrow & E \\ (A, B) & \mapsto & A \Delta B = (A \cup B) \setminus (A \cap B) \end{cases}$$

1. Montrer que $(\mathcal{P}(E), \Delta)$ est un groupe commutatif.
2. Montrer que $(\mathcal{P}(E), \Delta, \cap)$ est un anneau commutatif.
3. Démontrer que si E possède au moins deux éléments, alors l'anneau $(\mathcal{P}(E), \Delta, \cap)$ n'est pas intègre.

Exercice 14: ♦♦♦

On appelle anneau de Boole un anneau A dans lequel $\forall x \in A, x^2 = x$.

1. Montrer que $(\{0, 1\}, +, \times)$ est un anneau de Boole, (avec $+$ telle que $1 + 1 = 0$).
2. Montrer que pour un ensemble E , $(\mathcal{P}(E), \Delta, \cap)$ est un anneau de Boole.
3. Donner un exemple d'anneau de Boole infini.
4. Démontrer que pour tout élément x d'un anneau de Boole, $x + x = 0_A$ puis démontrer qu'un anneau de Boole est toujours commutatif.
5. Démontrer qu'il n'existe pas d'anneau de Boole à trois éléments.

Exercice 15: ♦♦♦

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

Démontrer que A est un corps si et seulement si il possède exactement un élément nilpotent et exactement deux éléments idempotents (éléments x tels que $x^2 = x$).