

Structures algébriques

1 GROUPES ET SOUS-GROUPES

1 Structure de groupe (MP2I)

Remarque : Quelques rappels

R1 – ■ **Loi de composition interne** sur un ensemble E : toute application

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

■ Elle est dite

★ **associative** lorsque

$$\forall (x, y, z) \in E^3, (x \star y) \star z = x \star (y \star z)$$

(que l'on peut alors noter $x \star y \star z$.)

★ **commutative** lorsque

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

■ On dit que e est **élément neutre** pour \star si pour tout $x \in E$, $x \star e = e \star x = x$.

Exercice 1

S'il existe, l'élément neutre est unique.

★ **Notation additive** : $0x = e$ avec e souvent noté 0 ou 0_E appelé élément nul.

★ **Notation multiplicative** : $x^0 = e$ avec e souvent noté 1 ou 1_E appelé élément unité.

■ Un élément x de E est dit **symétrisable** pour \star si on a $y \in E$ tel que $x \star y = y \star x = e$.

Exercice 2

S'il existe, y est unique.

★ **Notation additive** : on parle d'opposé, noté $-x$. Pour $x + (-y)$, on note $x - y$.

★ **Notation multiplicative** : on parle d'inverse, noté x^{-1} .

⚠ $\frac{x}{y}$ n'a pas de sens en général : cela désigne $x \star y^{-1}$ ou $y^{-1} \star x$?

Exemple

E1 – L'élément neutre e (lorsqu'il existe) est toujours symétrisable, de symétrique lui-même.

Être symétrisable à gauche ou à droite ne suffit pas.

Exemple

E2 – Sur E^E pour \circ , l'élément neutre est id_E .
 $(\exists g \in E^E, f \circ g = g \circ f = \text{id}_E) \iff$

$$\star (\exists g \in E^E, f \circ g = \text{id}_E) \iff$$

$$\star (\exists g \in E^E, g \circ f = \text{id}_E) \iff$$

■ Soit \star une loi de composition interne associative sur E notée multiplicativement.

Si x et y sont symétrisables, alors

★ $x \star y$ l'est aussi. De plus,
 $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$.

★ x^{-1} l'est aussi et $(x^{-1})^{-1} = x$.

Définition 1 : Groupe

On appelle **groupe** tout couple (G, \star) où G est un ensemble tel que

- (i) \star est une loi de composition interne sur G
- (ii) \star est associative
- (iii) G admet un élément neutre pour \star
- (iv) Tout élément de G admet un symétrique dans G pour \star .

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



Remarque

R2 – En particulier, un groupe n’est jamais vide.

Exemple

E3 – $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes commutatifs de neutre 0.

E4 – Si D est un ensemble non vide, $(\mathbb{R}^D, +)$ et $(\mathbb{C}^D, +)$ et en particulier $(\mathbb{R}^{\mathbb{N}}, +)$ et $(\mathbb{C}^{\mathbb{N}}, +)$ sont des groupes commutatifs, de neutre la fonction / suite nulle.

E5 – (\mathbb{Q}^*, \times) , (\mathbb{Q}_+^*, \times) , (\mathbb{R}^*, \times) , (\mathbb{R}_+^*, \times) et (\mathbb{C}^*, \times) sont des groupes commutatifs de neutre 1.

E6 – Si E est un ensemble non vide, on note $\mathfrak{S}(E)$ l’ensemble des permutations de E (bijection de E sur E). Alors $(\mathfrak{S}(E), \circ)$ est un groupe d’élément neutre id_E .

Si $|E| \geq 3$, ce groupe n’est pas commutatif.

Si $n \in \mathbb{N} \setminus \{0, 1\}$, et $E = \llbracket 1, n \rrbracket$, on note $\mathfrak{S}_n = \mathfrak{S}(\llbracket 1, n \rrbracket)$.

(\mathfrak{S}_n, \circ) est appelé **groupe symétrique d’ordre n** (et contient $n!$ éléments).

2 Puissances ou itérées d’un élément (MP2I)

Définition 2 : Itérées d’un élément

Soit E un ensemble muni d’une loi de composition interne \star (notée multiplicativement) **associative** et possédant un élément neutre e .

Pour tout $x \in E$ et tout $n \in \mathbb{N}$, on définit récursivement

$$x^n = \begin{cases} e & \text{si } n = 0 \\ x^{n-1} \star x & \text{sinon.} \end{cases}$$

Remarque

R3 – Autrement dit, $x^n = \underbrace{\star_{k=1}^n x}_{n \text{ fois}}$

R4 – En notation additive,

$$n \cdot x = \begin{cases} 0 & \text{si } n = 0 \\ (n-1) \cdot x + x & \text{sinon.} \end{cases}$$

Propriétés 1

Soient $x, y \in E$ et $n, m \in \mathbb{N}$.

(i) $x^{n+m} = x^n \star x^m = x^m \star x^n$.

(ii) $(x^n)^m = x^{nm} = (x^m)^n$.

(iii) Si $x \star y = y \star x$, $(x \star y)^n = x^n \star y^n$.

(iv) Si x est inversible, x^n est inversible et $(x^n)^{-1} = (x^{-1})^n$.

Notation 1

Si $x \in E$ inversible et $n \in \mathbb{N}$, on note x^{-n} l’élément $(x^{-1})^n$.

Remarque

R5 – Les propriétés (i) à (iii) restent vraies pour $n, m \in \mathbb{Z}$ lorsque x et y sont inversibles.

3 Régularité

Soit E un ensemble muni d’une loi de composition interne associative \star et possédant un élément neutre e .

Définition 3 : Régularité

Soit $x \in E$. On dit que x est **régulier** (ou **simplifiable**)

■ **à gauche** lorsque

$$\forall a, b \in E, x \star a = x \star b \implies a = b$$

■ **à droite** lorsque

$$\forall a, b \in E, a \star x = b \star x \implies a = b$$

On dit que x est **régulier** lorsqu’il l’est à gauche et à droite.

Propriété 1 : Régularité d’un inversible

Tout élément inversible de (E, \star) est régulier.

Corollaire 1 : Régularité dans un groupe

Si (G, \star) est un groupe, alors tout élément de G est régulier.

1. On dit que (E, \star) est un **monoïde**.

Corollaire 2 : Bijektivité des translations

Si (G, \star) est une groupe et $a \in G$ fixé.

Les applications $\varphi_a : \begin{cases} G \longrightarrow G \\ x \longmapsto a \star x \end{cases}$ et

$\psi_a : \begin{cases} G \longrightarrow G \\ x \longmapsto x \star a \end{cases}$ (appelées translations à gauche et à droite) sont bijectives.

Corollaire 3

Si (G, \star) est une groupe et $a \in G$ fixé.

$G = \{a \star x, x \in G\} = \{x \star a, x \in G\}$.

Remarque

R6 – Cela signifie que dans la table de la loi \star du groupe G , chaque élément de G apparaît une et une seule fois sur chaque ligne et sur chaque colonne.

Exemple

E7 – Si on considère le groupe des racines cubique de l'unité : $\mathbb{U}_3 = \{1, j, j^2\}$ muni de la loi \times , quelle est sa table ?

4 Groupe produit (MP2I)

Propriété 2 : Groupe produit

Soit (G, \star) et (H, Δ) des groupes.

Pour tout (g, h) et (g', h') dans $G \times H$, on pose

$$(g, h) \top (g', h') = (g \star g', h \Delta h').$$

Alors $(G \times H, \top)$ a une structure de groupe.

Si, de plus, les lois \star et Δ sont commutatives, alors \top l'est.

Remarque

R7 – Cela se généralise à un nombre de groupes quelconque $(G_1, \star_1), \dots, (G_p, \star_p)$ avec pour tout (x_1, \dots, x_p) et (y_1, \dots, y_p)

dans $G_1 \times \dots \times G_p$,

$$(x_1, \dots, x_p) \top (y_1, \dots, y_p) = \left(x_1 \star_1 y_1, \dots, x_p \star_p y_p \right).$$

5 Sous-groupes

a Définition et caractérisation (MP2I)

Définition 4 : Sous-groupe

Soit (G, \star) groupe. On note $\star|_{H^2}$ la restriction à H^2 de la loi \star .

On dit que H est un **sous-groupe** de (G, \star) si $H \subset G$ et $(H, \star|_{H^2})$ est un groupe.

Propriété 3 : Sous-groupes triviaux

Soit (G, \star) groupe. G et $\{e_G\}$ sont des sous-groupes de (G, \star) appelés **sous-groupes triviaux**.

Propriétés 2

Soit H un sous-groupe de (G, \star) .

- (i) (H, \star) possède le même élément neutre que (G, \star) .
- (ii) Si $x \in H$, alors x a même inverse dans (H, \star) et dans (G, \star) .

Propriété 4 : caractérisation des sous-groupes

Soit (G, \star) un groupe (multiplicatif). Les propositions suivantes sont équivalentes :

- (i) H est un sous-groupe de (G, \star)
- (ii) $\left\{ \begin{array}{l} H \subset G \\ H \neq \emptyset \quad (e_G \in H) \\ H \text{ est stable par } \star : \\ \quad \forall x, y \in H, \quad x \star y \in H \\ H \text{ est stable par inverse} : \\ \quad \forall x \in H, \quad x^{-1} \in H \end{array} \right.$



$$(iii) \begin{cases} H \subset G \\ H \neq \emptyset \quad (e_G \in H) \\ \forall x, y \in H, x \star y^{-1} \in H \end{cases}$$

Remarque

R8 – En notation additive, (ii) devient

$$\begin{cases} H \subset G \\ H \neq \emptyset \quad (0_G \in H) \\ H \text{ est stable par } \star : \forall x, y \in H, x + y \in H \\ H \text{ est stable par opposé} : \forall x \in H, -x \in H \end{cases}$$

et (iii) devient

$$\begin{cases} H \subset G, H \neq \emptyset \quad (0_G \in H) \\ \forall x, y \in H, x - y \in H \end{cases}$$

Remarque

R9 – Un sous-groupe d’un groupe abélien est facilement encore commutatif.

Exemple

- E8** – $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ sont des sous-groupes (additifs et abéliens) de $(\mathbb{C}, +)$.
- E9** – \mathbb{R}^D où $D \neq \emptyset$ est un sous-groupe additif abélien de $(\mathbb{C}^D, +)$.
- E10** – $\mathbb{Q}^*, \mathbb{Q}_+^*, \mathbb{R}^*, \mathbb{R}_+^*, \mathbb{U}, \mathbb{U}_n$ pour $n \in \mathbb{N}^*$ sont des sous-groupes multiplicatifs abéliens de (\mathbb{C}^*, \times) . (On rappelle que $\mathbb{U} = \{z \in \mathbb{C}, |z|=1\}$ et pour $n \in \mathbb{N}^*$, $\mathbb{U}_n = \{z \in \mathbb{C}, z^n = 1\} = \{e^{\frac{2ik\pi}{n}}, k \in \llbracket 0, n-1 \rrbracket\}$.)

b Intersection et réunion (MPI)

Propriété 5 : Intersection de sous-groupes

Soit (G, \star) un groupe et $(H_i)_{i \in I}$ une famille de sous-groupes de (G, \star) . Alors $\bigcap_{i \in I} H_i$ est un sous-groupe de (G, \star) .

Exercice 3 : Réunion de sous-groupes

Soit (G, \star) un groupe, H, K sont des sous-groupes de (G, \star) , alors

$$H \cup K \text{ sous-groupe de } G \iff H \subset K \text{ ou } K \subset H.$$

c Sous-groupes de $(\mathbb{Z}, +)$ (MPI)

Notation 2

Pour tout $a \in \mathbb{Z}$, on note $a\mathbb{Z} = \{ak, k \in \mathbb{Z}\}$.

Remarque

R10 – On vérifie avec la caractérisation que $a\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$. Avec $a\mathbb{Z} = \{\dots, -2a, -a, 0, a, 2a, \dots\}$, il s’agit du plus petit sous-groupe (au sens de l’inclusion) contenant a . On dit qu’il est engendré par a (sur le même principe que les Vect en algèbre linéaire.)

Propriété 6 : Sous-groupes de $(\mathbb{Z}, +)$

Les sous-groupes G de $(\mathbb{Z}, +)$ sont exactement les

6 Morphismes (MP2I)

a Définition

Définition 5 : Morphisme de groupe

Soient (G, \star) et (G', \bullet) deux groupes. $f : (G, \star) \rightarrow (G', \bullet)$ est un **morphisme de groupes** si et seulement si

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

Lorsque $(G, \star) = (G', \bullet)$, on parle d’**endomorphisme** de groupes.

Lorsque f est bijective, on parle d’**isomorphisme**.

Lorsqu’il existe un isomorphisme entre G et G' , on dit que G et G' sont **isomorphes**.

Lorsque f est bijective et $G = G'$, on parle d’**automorphisme**.

Exemple

E11 – $\ln : (\mathbb{R}_+^*, \times) \rightarrow (\mathbb{R}, +)$ isomorphisme de groupes.

E 12 – $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}_+^*, \times)$ isomorphisme de groupes.

E 13 – $\begin{cases} (\mathbb{R}, +) & \longrightarrow & (\mathbb{U}, \times) \\ \theta & \longmapsto & e^{i\theta} \end{cases}$ morphisme de groupes (non injectif).

E 14 – Si $n \in \mathbb{N}^*$, $\sigma \in \mathfrak{S}_n$, $\varepsilon(\sigma)$ sa signature $^\sigma$, alors $\varepsilon : (\mathfrak{S}_n, \circ) \rightarrow (\{-1, 1\}, \times)$ est un morphisme de groupes, c'est-à-dire

$$\forall \sigma, \sigma' \in \mathfrak{S}_n, \varepsilon(\sigma \circ \sigma') = \varepsilon(\sigma) \times \varepsilon(\sigma').$$

E 15 – $\det : (\mathcal{GL}(E), \circ) \rightarrow (\mathbb{R}^*, \times)$ et $\det : (\mathcal{GL}_n(\mathbb{K}), \circ) \rightarrow (\mathbb{R}^*, \times)$ sont des morphismes de groupes.

α . C'est-à-dire $(-1)^{I(\sigma)}$ où $I(\sigma)$ est le nombre d'inversions de σ ou encore $(-1)^N$ si σ s'écrit comme produit (composée) de N transpositions.

b Noyau et image

Définition 6 : Image et noyau d'un morphisme

Soit $f : (G, \star) \rightarrow (G', \bullet)$ un morphisme de groupes.

- On appelle **noyau** de f l'ensemble

$$\text{Ker } f =$$

Ainsi, $x \in \text{Ker } f \iff f(x) = e_{G'}$.

- On appelle **image** de f l'ensemble

$$\text{Im } f =$$

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

Propriété 7 : Image du neutre et du symétrique par un morphisme de groupes

Si $f : (G, \star) \rightarrow (G', \bullet)$ est un morphisme de groupes, alors $f(e_G) = e_{G'}$ et pour tout $x \in G$, $f(\text{sym}(x)) = \text{sym}(f(x))$.

Remarque

R 11 – En notation multiplicative : $f(x^{-1}) = (f(x))^{-1}$.

En notation additive : $f(-x) = -f(x)$.

On peut avoir un mix des deux : par exemple, si c'est additif au départ et multiplicatif à l'arrivée, ça devient $f(-x) = (f(x))^{-1}$.

Exemple

E 16 – $f : \begin{cases} (\mathbb{R}, +) & \longrightarrow & (\mathbb{U}, \times) \\ \theta & \longmapsto & e^{i\theta} \end{cases}$

Propriété 10 : Caractérisations de l'injectivité et de la surjectivité

Soit $f : (G, \star) \rightarrow (G', \bullet)$ un morphisme de groupe.

- f est injectif si et seulement si $\text{Ker } f = \{e_{G'}\}$.
- f est surjectif si et seulement si $\text{Im } f = G'$.

Propriété 8 : Image d'une itérée

En notation multiplicative, si $f : (G, \star) \rightarrow (G', \bullet)$ est un morphisme de groupes, pour tout $x \in G$ et pour tout $k \in \mathbb{Z}$, $f(x^k) = (f(x))^k$.

Remarque

R 12 – Ainsi, f est injective si et seulement si $f(x) = e_{G'} (= f(e_G)) \implies x = e_G$!

Propriété 9 : Composée de morphismes

Si $f : (G, \star) \rightarrow (G', \bullet)$ et $g : (G', \bullet) \rightarrow (G'', \Delta)$ sont des morphismes de groupes, alors $g \circ f$ en est encore un.

Exemple

E 17 – La fonction f de l'exemple précédent est donc non injective car $\text{Ker } f = 2\pi\mathbb{Z} \neq \{0\}$.



Propriété 11 : Images directe et réciproque d'un sous-groupe

Soit $f : (G, \star) \rightarrow (G', \bullet)$ un morphisme de groupes.

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

Corollaire 4 : Cas particulier du noyau et de l'image

Soit $f : (G, \star) \rightarrow (G', \bullet)$ un morphisme de groupes.

Alors $\text{Ker } f$ est un sous-groupe de (G, \star) et $\text{Im } f$ est un sous-groupe de (G', \bullet) .

Exemple

E 18 - $f : \begin{matrix} (\mathbb{R}, +) & \longrightarrow & (\mathbb{C}^*, \times) \\ \theta & \longmapsto & e^{i\theta} \end{matrix}$

E 19 - $f : \begin{matrix} (\mathbb{C}^*, \times) & \longrightarrow & (\mathbb{C}^*, \times) \\ z & \longmapsto & z^n \end{matrix}$

C Isomorphismes

Propriété 12 : Réciproque d'un isomorphisme

Soit $f : (G, \star) \rightarrow (G', \bullet)$ un isomorphisme de groupes.

Alors f^{-1} est un isomorphisme du groupe (G', \bullet) sur le groupe (G, \star) .

Remarque

R 13 - « Être isomorphe à » est une relation d'équivalence sur l'ensemble des groupes.

II ANNEAUX ET CORPS

1 Anneaux (MP2I)

Définition 7 : Distributivité

Soit E un ensemble et \star et \top deux lois de composition interne sur E , on dit que \star est **distributive** sur \top lorsque $\forall (x, y, z) \in E^3$,

$$x \star (y \top z) = (x \star y) \top (x \star z),$$

$$(y \top z) \star x = (y \star x) \top (z \star x).$$

Définition 8 : Anneau

On dit que $(A, +, \times)$ est un **anneau** lorsque

- (i) $(A, +)$ est un groupe abélien. L'élément neutre est noté 0_A .
- (ii) \times est une loi de composition interne associative admettant un élément neutre appelé unité de A , noté 1_A .
- (iii) \times est distributive sur $+$.

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

Exemple

E 20 - $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$, $(\mathbb{C}^D, +, \times)$ et $(\mathbb{R}^D, +, \times)$ (avec $D \neq \emptyset$), $(\mathbb{C}^{\mathbb{N}}, +, \times)$ et $(\mathbb{R}^{\mathbb{N}}, +, \times)$ sont des anneaux commutatifs.

E 21 - $(\mathcal{M}_n(\mathbb{R}), +, \times)$ et $(\mathcal{M}_n(\mathbb{C}), +, \times)$ sont des anneaux non commutatifs si $n \geq 2$.

Remarque

R 14 - 0_A est **absorbant** :

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

En effet, $0_A = a \times (0_A + 0_A) = a \times 0_A + a \times 0_A$ donc $a \times 0_A = 0_A$. Idem à droite.

R 15 - Si $1_A = 0_A$, alors pour tout $a \in A$, $a = a \times 1_A = a \times 0_A = 0_A$, donc $A = \{0_A\}$.

R 16 - Si $A \neq \{0_1\}$, alors 0_A n'est pas inversible (pour \times).

R 17 - Pour tout $a, b \in A$, $-ab = (-a) \times b = a \times (-b)$.

2 Groupe des inversibles (MP2I)

Définition 9

Soit $(A, +, \times)$ un anneau.
 $a \in A$ est dit **inversible** si et seulement s'il est symétrisable pour \times .
 Son symétrique est appelé **inverse** de a , noté a^{-1} .
 On note U_A ou $U(A)$ ou A^\times l'ensemble des inversibles de A .

Remarque

R18 – On parle parfois d'unités de A , d'où la notation...

Exemple

- E22 – $U_{\mathbb{R}} =$
- E23 – $U_{\mathbb{Z}} =$
- E24 – $U_{\mathbb{C}^{\mathbb{N}}} =$
- E25 – $U_{\mathbb{C}^D} =$
- E26 – $U_{\mathcal{M}_n(\mathbb{K})} =$

Propriété 13 : Groupe des inversibles

Si $(A, +, \times)$ anneau, alors (U_A, \times) est un groupe appelé **groupe des inversibles** de A .

3 Calculs dans un anneau (MP2I)

Propriété 14

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

- Si $a \times b = b \times a$,

$$(ab)^n = a^n b^n.$$

- **Formule du binôme de Newton** : Si $a \times b = b \times a$,

$$(a + b)^n =$$

■ **Factorisation^a de $a^n - b^n$** : Si $a \times b = b \times a$

$$a^n - b^n =$$

$$=$$

■ **Somme géométrique** : En particulier, pour tout $x \in A$;

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

a. parfois appelée formule de Bernoulli

Remarque

R19 – Si a et b ne commutent pas,

$$(ab)^n = abab \cdots ab$$

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

$$(a + b)^3 = a^3 + a^2b + aba + ba^2 + ab^2 + bab + b^2a + b^3$$

etc.

4 Corps (MP2I)

Définition 10 : Corps

Soit \mathbb{K} un ensemble, $+, \times$ deux lois de composition internes sur \mathbb{K} . On dit que $(\mathbb{K}, +, \times)$ est un **corps** lorsque

- $(\mathbb{K}, +, \times)$ est un anneau commutatif.
- $\mathbb{K} \setminus \{0_{\mathbb{K}}\}$ est non vide et tous ses éléments sont inversibles (c'est-à-dire $\mathbb{K} \neq \{0_{\mathbb{K}}\}$ et $U_{\mathbb{K}} = \mathbb{K}^\times = \mathbb{K} \setminus \{0_{\mathbb{K}}\}$.)

ou, de manière équivalente,

- $(\mathbb{K}, +)$ est un groupe abélien,
- $(\mathbb{K} \setminus \{0_{\mathbb{K}}\}, \times)$ est un groupe,
- \times est commutative et distributive sur $+$.

Exemple

E27 – $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ munis des lois $+$ et \times sont des corps, mais pas \mathbb{Z} .



5 Intégrité (MP2I)

Définition 11 : Anneau intègre

Un anneau $(A, +, \times)$ est dit **intègre** si

- A est commutatif,
- $A \neq \{0_A\}$ c'est-à-dire $1_A \neq 0_A$,
- A n'admet aucun diviseur de zéro, c'est-à-dire

$$\forall a, b \in A, a \times b = 0_A \implies a = 0_A \text{ ou } b = 0_A.$$

Exemple

E28 – $\mathbb{R}, \mathbb{Z}, \mathbb{C}, \mathbb{Q}$ sont des anneaux intègres. $\mathbb{R}^{\mathbb{N}}$ et plus généralement \mathbb{R}^D avec D contenant au moins deux éléments ne le sont pas.

Propriété 15 : Généralisation

Soit $(A, +, \times)$ un anneau intègre, $n \in \mathbb{N}^*$ et $(a_1, \dots, a_n) \in A^n$.

Si pour tout $k \in \llbracket 1, n \rrbracket$, $a_k \neq 0_A$, alors $a_1 \times \dots \times a_n \neq 0_A$.

Propriété 16 : Régularité dans un anneau intègre

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

Tout élément non nul de A est régulier (ie simplifiable) pour \times

Propriété 17 : Intégrité d'un corps

Tout corps est un anneau commutatif intègre. La réciproque est fausse.

6 Anneau produit (MPI)

Propriété 18 : Anneau produit

Soit $(A, +, \times)$ et (B, \oplus, \otimes) des anneaux.

Pour tout (a, b) et (a', b') dans $A \times B$, on pose

$$(a, b) + (a', b') = (a + a', b \oplus b')$$

$$(a, b) \times (a', b') = (a \times a', b \otimes b')$$

Alors $(A \times B, +, \times)$ a une structure d'anneau.

Si, de plus, les lois \times et \otimes sont commutatives, alors \times l'est.

Remarque

R20 – Cela se généralise à un nombre d'anneaux quelconque $(A_1, +_{(1)}, \times_{(1)}), \dots, (A_p, +_{(p)}, \times_{(p)})$ avec pour tout (x_1, \dots, x_p) et (y_1, \dots, y_p) dans $A_1 \times \dots \times A_p$,

$$(x_1, \dots, x_p) + (y_1, \dots, y_p) = (x_1 +_{(1)} y_1, \dots, x_p +_{(p)} y_p)$$

$$(x_1, \dots, x_p) \times (y_1, \dots, y_p) = (x_1 \times_{(1)} y_1, \dots, x_p \times_{(p)} y_p)$$

Propriété 19 : Inversion dans un anneau produit

Si $(A, +, \times)$ et $(B, +, \times)$ sont deux anneaux, alors $U_{A \times B} = U_A \times U_B$.

De plus, si $(a, b) \in U_{A \times B}$, alors $(a, b)^{-1} = (a^{-1}, b^{-1})$.

7 Sous-anneau et sous-corps (MP2I)

Définition 12 : Sous-anneau

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

- $B \subset A$
- **Important** : $1_A \in B$
- $(B, +|_{B^2}, \times|_{B^2})$ est un anneau.

Remarque

R21 – Une partie peut avoir une structure d’anneau pour les lois induites sans avoir la même unité (ce n’est pas un sous-anneau au sens de la définition précédente.) C’est le cas trivialement de $\{0_A\}$.

Exemple

E29 – Soit, dans l’anneau des matrices 2×2 , l’ensemble B des matrices $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ pour $a \in \mathbb{K}$. Alors $(B, +, \times)$ est un anneau d’unité $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq I_2$.

Définition 13 : Sous-corps

Soit $(\mathbb{K}, +, \times)$ un corps. On dit que $(\mathbb{L}, +, \times)$ est un sous-corps de $(\mathbb{K}, +, \times)$ lorsque $\mathbb{L} \subset \mathbb{K}$ et $(\mathbb{L}, +|_{\mathbb{L}^2}, \times|_{\mathbb{L}^2})$ est un corps.

Propriété 21 : Caractérisation des sous-corps

$(\mathbb{L}, +, \times)$ est un sous-corps de $(\mathbb{K}, +, \times)$ si et seulement si

$$\begin{cases} \mathbb{L} \subset \mathbb{K} \\ (\mathbb{L}, +) \text{ est un sous-groupe de } (\mathbb{K}, +) \\ (\mathbb{L} \setminus \{0_{\mathbb{K}}\}, \times) \text{ est un sous-groupe de } (\mathbb{K} \setminus \{0_{\mathbb{K}}\}, \times) \end{cases}$$

ou, de manière équivalente,

$$\begin{cases} \mathbb{L} \subset \mathbb{K} \\ \mathbb{L} \setminus \{0_{\mathbb{K}}\} \neq \emptyset \quad (1_{\mathbb{K}} \in \mathbb{L}) \\ \forall x, y \in \mathbb{L}, \quad x - y \in \mathbb{L} \\ \forall x, y \in \mathbb{L} \setminus \{0_{\mathbb{K}}\}, \quad xy^{-1} \in \mathbb{L} \end{cases}$$

Propriété 20 : Caractérisation des sous-anneaux

B est un sous-anneau de $(A, +, \times)$ si et seulement si

$$\begin{cases} B \subset A \\ (B, +) \text{ est un sous-groupe de } (A, +) \\ B \text{ est stable par } \times : \forall x, y \in B, \quad x \times y \in B \\ 1_A \in B \end{cases}$$

ou, de manière équivalente,

$$\begin{cases} B \subset A \\ 1_A \in B \\ \forall x, y \in B, \quad x + y \in B, \quad -x \in B \text{ et } x \times y \in B \end{cases}$$

ou encore

$$\begin{cases} B \subset A \\ 1_A \in B \\ \forall x, y \in B, \quad x - y \in B \text{ et } x \times y \in B \end{cases}$$

Exemple

E30 – **Anneau des entiers de Gauß** : $\mathbb{Z}[i] = \mathbb{Z} + i\mathbb{Z}$ est un sous-anneau de $(\mathbb{C}, +, \times)$.

E31 – $\mathcal{T}_n^+(\mathbb{K})$ est un sous-anneau de $(\mathcal{M}_n(\mathbb{K}), +, \times)$

E32 – L’ensemble $\mathcal{B}(\mathbb{R})$ des fonctions bornées est un sous-anneau de $(\mathbb{R}^{\mathbb{R}}, +, \times)$.

8 Morphismes d’anneaux (MP2I)

Définition 14 : Morphisme d’anneaux

Soient $(A, +, \times)$ et (A', \oplus, \otimes) deux anneaux. $f : (A, +, \times) \rightarrow (A', \oplus, \otimes)$ est un **morphisme d’anneaux** si et seulement si

- (i) $\forall (a, b) \in A^2, \quad f(a + b) = f(a) \oplus f(b)$
(ie $f : (A, +) \rightarrow (A', \oplus)$ morphisme de groupes)
- (ii) $\forall (a, b) \in A^2, \quad f(a \times b) = f(a) \otimes f(b)$
- (iii) $f(1_A) = 1_{A'}$

On parle aussi, d’**endomorphisme**, d’**isomorphisme** et d’**automorphisme** d’anneaux.

$\text{Ker } f = f^{(-1)}(\{0_{A'}\}) = \{a \in A \mid f(a) = 0_{A'}\}$ est le **noyau** de f .

$\text{Im } f = f(A) = \{f(x), x \in A\}$ est l’**image** de f .



Remarque

R22 – Comme on a en particulier un morphisme de groupes additifs, on peut utiliser les propriétés de ceux-ci :

- $f(0_A) = 0_{A'}$,
- Pour tout $a \in A$, $f(-a) = -f(a)$,
- f est injective si et seulement si $\text{Ker } f = \{0_A\}$.

R23 – En général, $\text{Ker } f$ n'est pas un sous-anneau de A . C'est un sous-groupe additif stable par multiplication... Nous les étudions juste après!

Exemple

E33 – $f : \begin{cases} \mathbb{R}[X] & \rightarrow \mathbb{C} \\ P & \mapsto \tilde{P}(i) \end{cases}$

Propriété 22 : des morphismes d'anneaux

Soit $f : (A, +, \times) \rightarrow (B, \oplus, \otimes)$ est un morphisme d'anneaux.

- (i) Si a est inversible dans A , alors $f(a)$ l'est dans B et $f(a^{-1}) = (f(a))^{-1}$.
- (ii) Si f est un isomorphisme alors $f^{-1} : (B, \oplus, \otimes) \rightarrow (A, +, \times)$ est aussi un isomorphisme d'anneau.
- (iii) Si $g : (B, \oplus, \otimes) \rightarrow (C, \dot{+}, \dot{\times})$ est aussi un morphisme d'anneau, alors $g \circ f : (A, +, \times) \rightarrow (C, \dot{+}, \dot{\times})$ l'est encore.

Définition 15 : Morphisme de corps

Soient $(\mathbb{K}, +, \times)$ et $(\mathbb{K}', \oplus, \otimes)$ deux corps.
 $f : (\mathbb{K}, +, \times) \rightarrow (\mathbb{K}', \oplus, \otimes)$ est un **morphisme de corps** si et seulement s'il s'agit d'un morphisme d'anneaux.

Remarque

R24 – Avec (i) et (ii), $f(1_{\mathbb{K}}) = (f(1_{\mathbb{K}}))^2$ et comme \mathbb{K}' est intègre, $f(1_{\mathbb{K}})$ vaut $1_{\mathbb{K}'}$ ou $0_{\mathbb{K}'}$. S'il vaut $0_{\mathbb{K}'}$ et si (ii) est vérifiée, alors $f \equiv 0_{\mathbb{K}'}$.

Exemple

E34 – $\text{id}_{\mathbb{C}}$, $z \mapsto \bar{z}$ sont des automorphismes (involutifs) du corps \mathbb{C} .

E35 – Tout morphisme de corps est injectif.



IDÉAL D'UN ANNEAU COMMUTATIF (MPI)

1 Généralités

Définition 16 : Idéal

Soit $(A, +, \times)$ un anneau commutatif et $I \subset A$. On dit que I est un **idéal** de $(A, +, \times)$ lorsque

- (i)
- (ii)

Remarque

R25 – Finalement, I est un **idéal** de $(A, +, \times)$ lorsque

- $0_A \in I$
- $\forall x, y \in I, x - y \in I$
- $\forall a \in A, \forall x \in I, ax \in I$.

Comme $-1_A \in A$, on peut se contenter de

- $0_A \in I$
- $\forall x, y \in I, x + y \in I$
- $\forall a \in A, \forall x \in I, ax \in I$.

Exemple

E36 – $2\mathbb{Z}$ est un idéal de $(\mathbb{Z}, +, \times)$.

E37 – L'ensemble des suites bornées est un idéal de l'anneau des suites bornées.

Remarque

R26 – Si un idéal contient l'unité 1_A ou plus généralement un élément inversible, il est égal à

Propriété 23 : Idéaux triviaux

Soit $(A, +, \times)$ un anneau commutatif. $\{0_A\}$ et A sont des idéaux (triviaux) de $(A, +, \times)$.

Ce sont les seuls idéaux si de plus $(A, +, \times)$ est un corps.

Propriété 24 : Noyau d'un morphisme d'anneaux

Soit $f : (A, +, \times) \rightarrow (A', \oplus, \otimes)$ un morphisme d'anneaux. Alors $\text{Ker } f$ est un idéal de $(A, +, \times)$.

Remarque

R27 – $\text{Im } f$ est un sous-anneau de (A', \oplus, \otimes) .

En général, $\text{Ker } f$ n'est pas un sous-anneau de $(A, +, \times)$.

Exercice 4

Montrer que si $f : (A, +, \times) \rightarrow (A', \oplus, \otimes)$ est un morphisme d'anneaux :

- L'image réciproque d'un sous-anneau de A' est un sous-anneau de A .
- L'image directe d'un sous-anneau de A est un sous-anneau de A' .
- L'image réciproque d'un idéal de A' par f est un idéal de A .
- L'image directe d'un idéal de A par f est un idéal de $f(A)$.

2 Somme et intersection d'idéaux

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

Propriété 25 : Somme et intersection d'idéaux

Soient I, J des idéaux de A . On note

$$I + J = \{x + y, x \in I, y \in J\}$$

(i) $I + J$ est un idéal.

Il s'agit du plus petit idéal de A (au sens de l'inclusion) contenant les idéaux I et J .

(ii) $I \cap J$ est un idéal.

Il s'agit du plus grand idéal de A (au sens de l'inclusion) contenu dans les idéaux I et J .

Remarque

R28 – Ce résultat s'étend facilement à une somme et une intersection d'un nombre fini quelconque d'idéaux de A .

3 Idéal principal

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

Propriété 26 : Idéal engendré par un élément

Soit $x \in A$. On note

$$(x) = xA =$$

C'est un idéal de A , appelé **idéal engendré** par x .

Remarque

R29 – C'est aussi le plus petit idéal contenant x , et donc l'intersection de tous les idéaux contenant x par unicité du plus petit élément.

Cette notion se généralise à plus d'un élément, un peu comme avec les Vect en algèbre linéaire.

Ainsi, l'idéal engendré par un nombre quelconque d'éléments est l'ensemble des combinaisons linéaires (finies) de ces éléments, à coefficients dans A .

Définition 17 : Idéal et anneau principal

- Tout idéal de la forme (x) (donc engendré par un seul élément) est dit **principal**.
- Un anneau commutatif est dit **principal** lorsque
 - (i)
 - (ii)

Théorème 1 : Principauté de \mathbb{Z}

L'anneau \mathbb{Z} est principal.



Remarque

R30 – Les idéaux de \mathbb{Z} sont donc principaux, c'est-à-dire engendré par un élément. Tous les générateurs sont associés. Donc, quitte à choisir un générateur positif (ou nul), on a de plus unicité de celui-ci.

4 Divisibilité dans un anneau intègre

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

Définition 18 : Divisibilité

Soient $a, b \in A$.

On dit que b **divise** a ou que a est multiple de b lorsqu'il existe $q \in A$ tel que $a = bq$. On note $b|a$.

a et b sont dit associés lorsque $a|b$ et $b|a$.

Propriété 27 : Caractérisation avec les idéaux

Soient $a, b \in A$.

b divise a si et seulement si $a \in bA$ si et seulement si $aA \subset bA$.

Remarque

R31 – Soit encore ssi tous les multiples de a sont des multiples de b .

Propriété 28

Soient $a, b \in A$.

a et b sont associés si et seulement si $aA = bA$ si et seulement si

Exemple

E38 – Dans \mathbb{Z} , a, b sont associés si et seulement si

Dans un anneau (commutatif intègre) principal, on définit les PGCD et PPCM de deux éléments a, b de la manière suivante :

- on appelle PGCD de a et b tout $d \in A$ qui engendre l'idéal $(a) + (b) = \{au + bv, u, v \in A\}$ ie tel que $(a) + (b) = (d)$.
- on appelle PPCM de a et b tout $m \in A$ qui engendre l'idéal $(a) \cap (b) = \{\text{multiples communes à } a \text{ et à } b\}$ ie tel que $(a) \cap (b) = (m)$.

On vérifie alors facilement, que ces sont des plus grand diviseur commun et plus petit multiple commun au sens de la division ce qui permet aussi de retrouver la définition vu en MP2I dans \mathbb{Z} .

Un avantage de cette définition du PGCD est de donner directement la relation de Bézout.

IV LA STRUCTURE D'ALGÈBRE (MPI)

1 Algèbre et sous-algèbre

Définition 19 : Structure d'algèbre

On dit que $(\mathcal{A}, +, \times, \cdot)$ est une \mathbb{K} -algèbre lorsque

- $(\mathcal{A}, +, \cdot)$ est une \mathbb{K} -espace vectoriel,
- $(\mathcal{A}, +, \times)$ est un anneau,
- *Pseudo-associativité* :

$$\lambda \cdot (x \times y) = (\lambda \cdot x) \times y = x \times (\lambda \cdot y).$$

Exemple

E39 – $(\mathbb{C}, +, \times, \cdot)$ est une \mathbb{R} -algèbre et une \mathbb{C} -algèbre.

E40 – $(\mathbb{K}^X, +, \times, \cdot)$ est une \mathbb{K} -algèbre.

E41 – $(\mathbb{K}^{\mathbb{N}}, +, \times, \cdot)$ est une \mathbb{K} -algèbre.

E42 – $(\mathbb{K}[X], +, \times, \cdot)$ est une \mathbb{K} -algèbre.

E43 – $(\mathbb{K}(X), +, \times, \cdot)$ est une \mathbb{K} -algèbre.

E44 – Si E est un \mathbb{K} -espace vectoriel, $(\mathcal{L}(E), +, \circ, \cdot)$ est une \mathbb{K} -algèbre.

E45 – Si $n \in \mathbb{N}^*$, $(\mathcal{M}_n(\mathbb{K}), +, \times, \cdot)$ est une \mathbb{K} -algèbre.

On a aussi une notion de sous-algèbre : c'est simultanément un sous-espace vectoriel et un sous-anneau, donc stable par combinaisons linéaires et par produit et contenant l'unité.

Propriété 29 : Caractérisation des sous-algèbres

Soit $(\mathcal{A}, +, \times, \cdot)$ est une \mathbb{K} -algèbre. \mathcal{B} est une sous-algèbre de $(\mathcal{A}, +, \times, \cdot)$ lorsque

- (i)
- (ii)
- (iii)
- (iv)

Exemple

- E46 – $\mathbb{K}[X]$
- E47 – $\mathcal{C}^k(I, \mathbb{K})$
- E48 – L'ensemble des suites convergentes
- E49 – L'ensemble $\mathbb{K}[x]$ des fonctions polynomiales

L'intérêt principal des algèbres est de pouvoir évaluer un polynôme à coefficients dans \mathbb{K} en un élément d'une \mathbb{K} -algèbre :

Définition 20 : Polynôme en un élément d'une algèbre

Si $P = a_0 + a_1X + \dots + a_nX^n \in \mathbb{K}[X]$ et $x \in \mathcal{A}$, on pose

$$P(x) =$$

Attention à ne pas oublier l'unité de \mathcal{A} !

2 Morphismes d'algèbres

Définition 21 : Morphisme d'algèbre

Soit $(\mathcal{A}, +, \times, \cdot)$, $(\mathcal{B}, +, \times, \cdot)$ et $f : \mathcal{A} \rightarrow \mathcal{B}$. On dit que f est un **morphisme d'algèbres** lorsque

- (i) f est linéaire ie
- (ii)
- (iii)

Exemple

E50 – Si $X \neq \emptyset$, \mathcal{A} une \mathbb{K} -algèbre, $a \in X$,

$$u_a : \begin{cases} \mathcal{A}^X & \longrightarrow \mathcal{A} \\ f & \longmapsto f(a) \end{cases}$$

E51 – $f : \begin{cases} \mathbb{K}[X] & \longrightarrow \mathbb{K}[x] \\ P & \longmapsto \tilde{P} \end{cases}$

E52 – $f : \begin{cases} \mathbb{K} & \longrightarrow \mathcal{M}_1(\mathbb{K}) \\ x & \longmapsto (x) \end{cases}$

Propriété 30

Soit $(\mathcal{A}, +, \times, \cdot)$ une \mathbb{K} -algèbre et $x \in \mathcal{A}$.

Alors l'application $f : \begin{cases} \mathbb{K}[X] & \longrightarrow \mathcal{A} \\ P & \longmapsto P(x) \end{cases}$

est un morphisme de \mathbb{K} -algèbres.

Remarque

R32 – En particulier, deux polynômes en $x \in \mathcal{A}$ commutent toujours.

V COMPLÉMENT : SOUS-GROUPES DE $(\mathbb{R}, +)$

Théorème 2 : Hors-Programme

Soit G est un sous-groupe de $(\mathbb{R}, +)$. Alors G est soit dense dans \mathbb{R} , soit discret (de la forme $\alpha\mathbb{Z}$).

Exercice 5

1. Traiter le cas où $G = \{0\}$.
2. On suppose dorénavant que $G \neq \{0\}$.
 - (a) Montrer que $G \cap \mathbb{R}_+^*$ est non vide. En déduire que $G \cap \mathbb{R}_+^*$ admet une borne inférieure. On note α cette borne inférieure.
 - (b) On suppose dans cette question que $\alpha = 0$.
Montrer que pour tout $\delta > 0$, il existe $x \in G$ tel que $0 < x < \delta$. En déduire que G est dense dans \mathbb{R} .
 - (c) On suppose dans cette question que $\alpha > 0$.
 - i. Montrer qu'il existe $x \in G$ tel que $\alpha \leq x < 2\alpha$. En déduire que $x = \alpha$, puis que $\alpha\mathbb{Z} \subset G$.
 - ii. Soit réciproquement $x \in G$. Montrer que l'on peut trouver $q \in \mathbb{Z}$ tel que $q\alpha \leq x < (q+1)\alpha$. En déduire que $x = q\alpha$.
 - iii. Conclure.