

CHAPITRE

Structures algébriques

Extrait du programme officiel :

L'étude des structures algébriques permet d'approfondir plusieurs points abordés en première année : arithmétique de \mathbb{Z} et de $\mathbb{K}[X]$, congruences, algèbre linéaire, groupe symétrique, groupes issus de l'algèbre linéaire et de la géométrie des espaces euclidiens. Ce chapitre gagne à être illustré par de nombreux exemples.

Le paragraphe relatif aux polynômes permet de revenir sur l'étude menée en première année, dans un cadre étendu et dans un esprit plus algébrique, mettant l'accent sur la notion d'idéal.

Sans soulever de difficulté, on signalera que les notions d'algèbre linéaire étudiées en MPSI s'étendent au cas où le corps de base est un sous-corps de \mathbb{C} .

CONTENUS

CAPACITÉS & COMMENTAIRES

a) Groupes et sous-groupes

Groupe. Produit fini de groupes.

Exemples issus de l'algèbre et de la géométrie.

Sous-groupe. Caractérisation.

Intersection de sous-groupes.

Sous-groupes du groupe $(\mathbb{Z}, +)$.

b) Morphismes de groupes

Morphisme de groupes.

Exemples : signature, déterminant.

Image et image réciproque d'un sous-groupe par un morphisme. Image et noyau d'un morphisme. Condition d'injectivité d'un morphisme.

Exemple : groupe spécial orthogonal d'un espace euclidien.

Isomorphisme de groupes. Réciproque d'un isomorphisme.

e) Anneaux

Anneau. Produit fini d'anneaux.

Les anneaux sont unitaires.

Sous-anneaux. Morphisme d'anneaux. Image et noyau d'un morphisme. Isomorphisme d'anneaux.

Anneau intègre. Corps. Sous-corps.

Les corps sont commutatifs.

f) Idéaux d'un anneau commutatif

Idéal d'un anneau commutatif. Le noyau d'un morphisme d'anneaux est un idéal.

Relation de divisibilité dans un anneau commutatif intègre.

Interprétation de la divisibilité en termes d'idéaux.

Idéaux de \mathbb{Z} .

h) Anneaux de polynômes à une indéterminée

Dans ce paragraphe, K est un sous-corps de \mathbb{C} .

Idéaux de $K[X]$.

PGCD de deux polynômes.

Par convention, le PGCD est unitaire.
Extension au cas d'une famille finie.

Relation de Bézout. Lemme de Gauss.

\Leftrightarrow I : algorithme d'Euclide étendu sur les polynômes, recherche simultanée du PGCD et des coefficients de Bézout.

Irréductible de $K[X]$. Existence et unicité de la décomposition en facteurs irréductibles.

Les étudiants doivent connaître les irréductibles de $\mathbb{C}[X]$ et $\mathbb{R}[X]$.
L'étude des polynômes sur un corps fini est hors programme.

i) Algèbres

Algèbre.

Les algèbres sont unitaires.
Exemples : $\mathbb{K}[X]$, $\mathcal{L}(E)$, $\mathcal{M}_n(\mathbb{K})$, $\mathcal{F}(X, \mathbb{K})$.

Sous-algèbre.

Morphisme d'algèbres.



TABLE DES MATIÈRES

STRUCTURES ALGÈBRIQUES

I	Groupes et sous-groupes	2
1	Structure de groupe	2
2	Puissances ou itérées d'un élément	3
3	Régularité	4
4	Groupe produit	5
5	Sous-groupes	5
a	Définition et caractérisation	5
b	Intersection et réunion	7
c	Sous-groupes de $(\mathbb{Z}, +)$	7
6	Morphismes	8
a	Définition	8
b	Noyau et image	9
c	Isomorphismes	10
II	Anneaux et Corps	11
1	Anneaux	11
2	Groupe des inversibles	11
3	Calculs dans un anneau	12
4	Corps	13
5	Intégrité	13
6	Anneau produit	14
7	Sous-anneau et sous-corps	15
8	Morphismes d'anneaux	17
III	Idéal d'un anneau commutatif	18
1	Généralités	18
2	Somme et intersection d'idéaux	19
3	Idéal principal	19
4	Divisibilité dans un anneau intègre	20
IV	La structure d'algèbre	20
1	Algèbre et sous-algèbre	20
2	Morphismes d'algèbres	21
V	Complément : sous-groupes de $(\mathbb{R}, +)$	22

I GROUPES ET SOUS-GROUPES

1 Structure de groupe

Remarque : Quelques rappels :

- **Loi de composition interne** sur un ensemble E : toute application $\star : \begin{matrix} E \times E & \longrightarrow & E \\ (x, y) & \longmapsto & x \star y \end{matrix}$.
- 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

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

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

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

Sur E^E pour \circ , l'élément neutre est id_E .

★ $(\exists g \in E^E, f \circ g = g \circ f = \text{id}_E) \iff f$ bijective (ie inversible pour \circ).

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

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

- 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 : Groupe

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

(G1) \star est une loi de composition interne sur G

(G2) \star est associative

(G3) G admet un élément neutre pour \star

(G4) 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

En particulier, un groupe n'est jamais vide.

Exemples

E1 – $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes commutatifs de neutre 0.

E2 – 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.

E3 – (\mathbb{Q}^*, \times) , (\mathbb{Q}_+^*, \times) , (\mathbb{R}^*, \times) , (\mathbb{R}_+^*, \times) et (\mathbb{C}^*, \times) sont des groupes commutatifs de neutre 1.

E4 – 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

Définition : 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

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

Remarques

R1 – Autrement dit, $x^n = \underbrace{\star_{k=1}^n x}_{n \text{ fois}}$.

R2 – En notation additive,

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

Propriétés

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 $(x^n)^{-1} = (x^{-1})^n$.

Démonstration

(i) Par récurrence sur m (par exemple) à n fixé et par associativité.

(ii) Par récurrence sur m à n fixé.

(iii) Par récurrence sur n .

(iv) On calcule avec la propriété précédente $x^n \star (x^{-1})^n = (x \star x^{-1})^n = e$ et de même $(x^{-1})^n \star x^n = e$.

□

Notation

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

Remarque

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

3 Régularité

Soit¹ E un ensemble muni d'une loi de composition interne associative \star et possédant un élément neutre e .

Définition : 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.

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

Propriété

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

Démonstration

Si x est inversible et si $x \star a = x \star b$, alors

$$a = (x^{-1} \star x) \star a = x^{-1} \star (x \star a) = x^{-1} \star (x \star b) = (x^{-1} \star x) \star b = b$$

par associativité. □

Corollaire

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

Corollaire

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 $\psi_a : \begin{cases} G & \longrightarrow & G \\ x & \longmapsto & x \star a \end{cases}$ sont bijectives.

Démonstration

On vérifie que $\varphi_a \circ \varphi_{a^{-1}} = \varphi_{a^{-1}} \circ \varphi_a = \text{id}_G$ et $\psi_a \circ \psi_{a^{-1}} = \psi_{a^{-1}} \circ \psi_a = \text{id}_G$. □

Corollaire

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

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

Démonstration

Il s'agit de la surjectivité des deux applications précédentes. □

Remarque

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

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

\star	1	j	j^2
1	1	j	j^2
j	j	j^2	1
j^2	j^2	1	j

4 Groupe produit

Propriété : 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.

Démonstration

- Le fait que \top soit une loi de composition interne sur $G \times H$ provient du fait que \star et Δ le sont sur G et H respectivement.
- Un calcul facile mais pénible à écrire permet de vérifier que les associativités de \star et Δ donnent celle de \top .
- Si e_G et e_H sont les éléments neutres de G et H , alors (e_G, e_H) est bien neutre sur $G \times H$.
- Si $g \in G$ et $h \in H$ d'inverses g^{-1} et h^{-1} , alors (g^{-1}, h^{-1}) est l'inverse de (g, h) .

□

Remarque

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 $G_1 \times \dots \times G_p$,

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

5 Sous-groupes



Définition et caractérisation

Définition : 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.
 On note parfois $H < G$.

Propriété : Sous-groupes triviaux

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

Propriétés

- 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) .

Démonstration

- (i) Soient e_H et e_G les éléments neutres respectifs. Alors $e_H \star e_G = e_H = e_H \star e_H$ car $e_H \in G$ et e_G neutre sur G d'une part, et e_H neutre sur H d'autre part. Puis, par régularité à gauche de e_H dans G , $e_G = e_H$.
- (ii) Si $x \in H$, alors x a un symétrique $\text{sym}_H(x) \in H \subset G$ tel que $x \star \text{sym}_H(x) = \text{sym}_H(x) \star x = e_H = e_G$ et donc par unicité, x inversible dans G et $\text{sym}_G(x) = \text{sym}_H(x)$.

□

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

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

Remarque

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

Démonstration

- (i) \implies (ii) : si $H < G$, $H \subset G$, $H \neq \emptyset$, H stable par \star (lci) et, d'après la propriété précédente, H est bien stable par inverse.
- (ii) \implies (iii) : facile.
- (iii) \implies (i) : si on a (iii), alors $H \subset G$. La loi \star est associative sur G donc a fortiori, elle l'est aussi sur H . Comme H est non vide, on a $x \in H$ avec $x \star x^{-1} = e_G \in H$. Alors pour tout $x \in H$, $e_G \star x^{-1} = x^{-1} \in H$. e_G est neutre pour \star sur G donc l'est aussi sur H . L'inverse x^{-1} d'un élément de $x \in H$ dans G est dans H , donc tout élément de H est symétrisable dans H . Donc (H, \star) est bien un sous-groupe de (G, \star) . □

Remarque

Un sous-groupe d'un groupe abélien est facilement encore commutatif.

Exemples

- E1 – $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ sont des sous-groupes (additifs et abéliens) de $(\mathbb{C}, +)$.
- E2 – \mathbb{R}^D où $D \neq \emptyset$ est un sous-groupe additif abélien de $(\mathbb{C}^D, +)$.
- E3 – $\mathbb{Q}^*, \mathbb{Q}_+^*, \mathbb{R}^*, \mathbb{R}_+^*, \mathbb{U}, \mathbb{U}_n$ 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 $n \in \mathbb{N}^*$, $\mathbb{U}_n = \{z \in \mathbb{C}, z^n = 1\} = \left\{ e^{\frac{2ik\pi}{n}}, k \in \llbracket 0, n-1 \rrbracket \right\}$.)

b Intersection et réunion

Propriété

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) .

Démonstration

- $(H_i)_{i \in I} \subset G$ car $\forall i \in I, H_i \subset G$.
- $(H_i)_{i \in I} \neq \emptyset$ car $\forall i \in I, e_G \in H_i$.
- Si $x, y \in (H_i)_{i \in I}$, alors $\forall i \in I, x \star y^{-1} \in H_i$ donc $x \star y^{-1} \in \bigcap_{i \in I} H_i$. □

Exercice

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

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

- \Leftarrow : ok
- \Rightarrow : Si $H \cup K$ sous- groupe de G et $H \not\subset K$, on va montrer que $K \subset H$.
On a $h \in H \setminus K$.



Soit $k \in K$. Alors $k \star h \in H \cup K$ par stabilité de \star sur $H \cup G$.
 Si $k \star h \in K$, alors $h = k^{-1} \star (k \star h) \in K$, ce qui n'est pas possible.
 C'est donc que $k \star h \in H$ et donc $k = (k \star h) \star h^{-1} \in H$.
 Finalement, on a bien $K \subset H$.

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

Notation

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

Remarque

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

Les sous-groupes G de $(\mathbb{Z}, +)$ sont exactement les $a\mathbb{Z}$ pour $a \in \mathbb{N}$.
 De plus, si $G \neq \{0\}$, $a = \min(G \cap \mathbb{N}^*)$.

Démonstration

- On a déjà que, si $a \in \mathbb{N}$, $a\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$ par la caractérisation.
 - Réciproquement, considérons G un sous-groupe de $(\mathbb{Z}, +)$.
 - ★ Soit $G = \{0\}$ et alors $G = a\mathbb{Z}$ avec $a = 0$.
 - ★ Soit $G \neq \{0\}$ et on peut trouver $p \in G \setminus \{0\}$. Soit $p > 0$ et alors $p \in G \cap \mathbb{N}^* \neq \emptyset$, soit $p < 0$ et alors $-p \in G \cap \mathbb{N}^* \neq \emptyset$.
 On peut donc introduire $a = \min(G \cap \mathbb{N}^*)$.
 Montrons que $G = a\mathbb{Z}$ par double inclusion.
 - $a \in G$, puis par stabilité et récurrence, pour tout $n \in \mathbb{N}$, $na \in G$ et par stabilité par passage à l'opposé, $-an \in G$. Finalement, $a\mathbb{Z} \subset G$.
 - Réciproquement, si $x \in G \subset \mathbb{Z}$, par division euclidienne, on a $(q, r) \in \mathbb{Z}^2$ tel que $x = aq + r$ et $0 \leq r < a$.
 Or $x \in G$ et $aq \in a\mathbb{Z} \subset G$ donc, comme on a un sous-groupe $r = x - aq \in G \cap \mathbb{N}$. Mais comme $r < a = \min(G \cap \mathbb{N}^*)$, $r \notin \mathbb{N}^*$ et donc $r = 0$.
 Finalement, $x = aq \in a\mathbb{Z}$.
- On a donc bien $G = a\mathbb{Z}$. □

6 Morphismes

a **Définition**

Définition

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

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

Définition

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**.

Exemples

E1 – $\ln : (\mathbb{R}_+^*, \times) \rightarrow (\mathbb{R}, +)$ isomorphisme de groupes.

E2 – $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}_+^*, \times)$ isomorphisme de groupes.

E3 – $\begin{cases} (\mathbb{R}, +) & \rightarrow & (\mathbb{U}, \times) \\ \theta & \mapsto & e^{i\theta} \end{cases}$ morphisme de groupes (non injectif).

E4 – Si $n \in \mathbb{N}^*$, $\sigma \in \mathfrak{S}_n$, $\varepsilon(\sigma)$ sa signature ^a, alors $\varepsilon : (\mathfrak{S}_n, \circ) \rightarrow (\{-1, 1\}, \times)$ est un morphisme de groupes, c'est-à-dire

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

E5 – $\det : (\mathcal{GL}(E), \circ) \rightarrow (\mathbb{R}^*, \times)$ et $\det : (\mathcal{GL}_n(\mathbb{K}), \circ) \rightarrow (\mathbb{R}^*, \times)$ sont des morphismes de groupes.

a. 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.

Propriété

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

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 $f(-x) = (f(x))^{-1}$.

Démonstration

$f(e_G) = f(e_G \star e_G) = f(e_G) \star f(e_G)$ donc comme $f(e_G)$ est inversible, $f(e_G) = e_{G'}$.

$f(x) \bullet f(\text{sym}(x)) = f(x \star \text{sym}(x)) = f(e_G) = e_{G'}$

et $f(\text{sym}(x)) \star f(x) = f(\text{sym}(x) \star x) = f(e_G) = e_{G'}$ □

Propriété

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

Démonstration

Par récurrence pour $k \in \mathbb{N}$, puis par passage à l'inverse et d'après la propriété précédente pour $k \in \mathbb{Z}^-$. □

Propriété

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.

b

Noyau et image

Définition

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

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

$$\text{Ker } f = f^{(-1)}(\{e_{G'}\}) = \{x \in G \mid f(x) = e_{G'}\} \subset G.$$

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

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

$$\text{Im } f = f(G) = \{f(x), x \in G\} \subset G'.$$

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



Exemple

$$f : \begin{cases} (\mathbb{R}, +) & \longrightarrow & (\mathbb{U}, \times) \\ \theta & \longmapsto & e^{i\theta} \end{cases} : \text{Ker } f = 2\pi\mathbb{Z}.$$

Propriété

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 $\text{Im } f = G'$.

Remarque

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

Démonstration

- Remarquons qu'on a toujours $e_G \in \text{Ker } f$ car $f(e_G) = e_{G'}$.
Si f est injectif, alors $x \in \text{Ker } f \iff f(x) = e_{G'} = f(e_G) \iff x = e_G$, donc $\text{Ker } f = \{e_G\}$.
Si $\text{Ker } f = \{e_G\}$ et si $f(x) = f(x')$, alors (en notation multiplicative)

$$e_{G'} = f(x) \bullet (f(x'))^{-1} = f(x) \bullet f(x'^{-1}) = f(x \star x'^{-1})$$

donc $x \star x'^{-1} \in \text{Ker } f$ donc $x \star x'^{-1} = e_G$ donc $x = x'$.
 f est bien injectif.

- La caractérisation est valable pour les fonctions en général. Par définition,

$$f \text{ est surjective} \iff \text{Im } f = \{f(x), x \in G\} = G'$$

□

Exemple

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

Propriété

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) .

Démonstration

- $f(H)$ est un sous groupe de (G', \bullet) :
 - ★ $f(H) \subset G'$
 - ★ $f(H) \neq \emptyset$ car $H \neq \emptyset$
 - ★ Si $y, y' \in f(H)$, on a $x, x' \in H$ tels que $y = f(x)$ et $y' = f(x')$. f étant un morphisme de groupes,

$$y \bullet y'^{-1} = f(x) \bullet f(x')^{-1} = f(\underbrace{x \star x'^{-1}}_{\in H}) \in f(H).$$

- $f^{(-1)}(H')$ est un sous groupe de G :
 - ★ $f^{(-1)}(H') \subset G$
 - ★ $f^{(-1)}(H') \neq \emptyset$ car $e_G \in f^{(-1)}(H')$ car $f(e_G) = e_{G'} \in H'$.
 - ★ Si $x, x' \in f^{(-1)}(H')$, f étant un morphisme de groupes, $f(x \star x'^{-1}) = \underbrace{f(x)}_{\in H'} \bullet \underbrace{f(x')^{-1}}_{\in H'} \in H'$, donc $x \star x'^{-1} \in f^{(-1)}(H')$. □

Propriété

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) .

Démonstration

- $\text{Ker } f = f^{-1}(\{e_{G'}\})$ avec $\{e_{G'}\}$ sous-groupe de (G', \bullet)
- $\text{Im } f = f(G)$ avec G sous-groupe de (G, \star) .

□

Exemples

E1 – $f : \begin{array}{l} (\mathbb{R}, +) \longrightarrow (\mathbb{C}^*, \times) \\ \theta \longmapsto e^{i\theta} \end{array}$ étant un morphisme de groupes, $\text{Im } f = \mathbb{U}$ est un sous-groupe de (\mathbb{C}^*, \times) et $\text{Ker } f = 2\pi\mathbb{Z}$ est un sous-groupe de $(\mathbb{R}, +)$.

\mathbb{U} est aussi le noyau du morphisme $|\cdot| : \mathbb{C}^* \rightarrow \mathbb{R}^*$.

E2 – $f : \begin{array}{l} (\mathbb{C}^*, \times) \longrightarrow (\mathbb{C}^*, \times) \\ z \longmapsto z^n \end{array}$ étant un morphisme de groupes, $\text{Ker } f = \mathbb{U}_n$ est un sous-groupe de (\mathbb{C}^*, \times) . C'est aussi l'image du morphisme $k \in \mathbb{Z} \mapsto e^{\frac{2ik\pi}{n}}$.

E3 – Si $(E, |)$ est un espace euclidien, le noyau du morphisme $\det : (\mathcal{O}(E), \circ) \rightarrow (\{\pm 1\}, \times)$ est le groupe $\mathcal{SO}(E)$.

C**Isomorphismes****Propriété**

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) .

Démonstration

f^{-1} est bijective, et si $y, y' \in G'$, alors, comme f est un morphisme de groupes,

$$f^{-1}(y \bullet y') = f^{-1}(f(f^{-1}(y)) \bullet f(f^{-1}(y'))) = f^{-1}(f(f^{-1}(y) \star f^{-1}(y'))) = f^{-1}(y) \star f^{-1}(y').$$

□

Remarque

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

II ANNEAUX ET CORPS**1 Anneaux****Définition : 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

$$\forall (x, y, z) \in E^3, \quad x \star (y \top z) = (x \star y) \top (x \star z) \text{ et } (y \top z) \star x = (y \star x) \top (z \star x).$$

Définition : Anneau

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

(A1) $(A, +)$ est un groupe abélien. L'élément neutre est noté 0_A .

(A2) \times est une loi de composition interne associative admettant un élément neutre appelé unité de A , noté 1_A .

(A3) \times est distributive sur $+$.



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

Exemples

E1 – $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$, $(\mathbb{C}^D, +, \times)$ et $(\mathbb{R}^D, +, \times)$ (avec $D \neq \emptyset$), $(\mathbb{C}^{\mathbb{N}}, +, \times)$ et $(\mathbb{R}^{\mathbb{N}}, +, \times)$ sont des anneaux commutatifs.

E2 – $(\mathcal{M}_n(\mathbb{R}), +, \times)$ et $(\mathcal{M}_n(\mathbb{C}), +, \times)$ sont des anneaux non commutatifs si $n \geq 2$.

Remarques

R1 – 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.

R2 – Si $1_A = 0_A$, alors pour tout $a \in A$, $a = a \times 1_A = a \times 0_A = 0_A$, donc $A = \{0_A\}$.

R3 – Si $A \neq \{0_1\}$, alors 0_A n'est pas inversible (pour \times).

R4 – Pour tout $a, b \in A$, $-ab = (-a) \times b = a \times (-b)$.

2 Groupe des inversibles

Définition

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

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

Exemples

E1 – $U_{\mathbb{R}} = \mathbb{R}^*$

E2 – $U_{\mathbb{Z}} = \{-1, 1\} \neq \mathbb{Z}^*$

E3 – $U_{\mathbb{C}^{\mathbb{N}}} = \{\text{suites jamais nulles}\}$

E4 – $U_{\mathbb{C}^D} = \{\text{fonctions jamais nulles}\}$

E5 – $U_{\mathcal{M}_n(\mathbb{K})} = \mathcal{GL}_n(\mathbb{K})$

Propriété : Groupe des inversibles

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

Démonstration

On a déjà l'associativité, l'élément neutre car A est un anneau. Comme de plus, tout élément inversible est lui même inversible et comme le produit de deux éléments inversibles l'est encore, on a bien une structure de groupe. \square

3 Calculs dans un anneau

Propriété

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 $a \times b = b \times a$,

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

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

$$\begin{aligned} a^n - b^n &= (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 \dots + ab^{n-2} + b^{n-1}) \\ &= (a-b) \sum_{k=0}^{n-1} a^k b^{n-1-k}. \end{aligned}$$

- **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

Si a et b ne commutent pas,

$$\begin{aligned} (ab)^n &= abab \dots ab \\ (a+b)^2 &= a^2 + ab + ba + b^2 \\ (a+b)^3 &= a^3 + a^2b + aba + ba^2 + ab^2 + bab + b^2a + b^3 \end{aligned}$$

etc.

Démonstration

- Par récurrence sur n .
- **Formule du binôme** :

- ★ **Preuve par dénombrement** :

$$(a+b)^n = \underbrace{(a+b)(a+b) \dots (a+b)}_{n \text{ fois}}$$

En développant, on obtient des termes de la forme $x_1 x_2 \dots x_n$ avec $x_i = a$ ou b . Si on veut k termes a , on $\binom{n}{k}$ chois, et le terme vaut $a^k b^{n-k}$ car a et b commutent.

- ★ **Preuve par récurrence** sur n , c'est simple si $n = 0$ ou 1 . Si c'est vrai pour $n-1$,

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

(associativité, distributivité, a et b commutent, dans la seconde somme)



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

(changement d'indice $k \mapsto k-1$)

$$= \sum_{k=0}^n \binom{n-1}{k-1} a^k b^{n-k} + \sum_{k=0}^n \binom{n-1}{k} a^k b^{n-k}$$

(les termes ajoutés sont nuls)

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

(associativité, distributivité,

Donc $(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$ d'après la formule de Pascal étendue au coefficients avec $k < 0$.

- **Factorisation de $a^n - b^n$:**

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

(a et b commutent, associativité, distributivité)

$$= a^n b^0 - a^0 b^n = a^n - b^n$$

(somme télescopique)

□

4 Corps

Définition

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

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

5 Intégrité

Définition : 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

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

Exemple

$\mathbb{R}, \mathbb{Z}, \mathbb{C}, \mathbb{Q}$ 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

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 $a_1 \times \dots \times a_n \neq 0_A$.

Démonstration

Par contraposée et récurrence. □

Propriété

Soit $(A, +, \times)$ un anneau intègre.
Tout élément non nul de A est régulier (ie simplifiable) pour \times

Démonstration

Si $a, b, c \in A$ et $a \neq 0_A$ tels que $ab = ac$, alors $a(b - c) = 0_A$ et donc $b - c = 0_A$ soit $b = c$. □

Propriété

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

Démonstration

Si $ab = 0_{\mathbb{K}}$ et si $a \neq 0_{\mathbb{K}}$, alors a est inversible et $b = a^{-1}ab = a^{-1}0_{\mathbb{K}} = 0_{\mathbb{K}}$ car $0_{\mathbb{K}}$ est un élément absorbant.
Pour la réciproque, $(\mathbb{Z}, +, \times)$ est un anneau commutatif intègre qui n'est pas un corps. □

6 Anneau produit

Propriété : Groupe produit

Soit $(A, \dot{+}, \dot{\times})$ et (B, \oplus, \otimes) des anneaux.
Pour tout (a, b) et (a', b') dans $A \times B$, on pose

$$(a, b) + (a', b') = (a \dot{+} a', b \oplus b')$$

$$(a, b) \times (a', b') = (a \dot{\times} a', b \otimes b')$$

Alors $(A \times B, +, \times)$ a une structure d'anneau.
Si, de plus, les lois $\dot{\times}$ et \otimes sont commutatives, alors \times l'est.

Démonstration

- On a bien $(A \times B, +)$ groupe (produit) abélien.
- \times est bien une loi de composition interne sur $A \times B$.
Un calcul facile mais pénible à écrire permet de vérifier que les associativités de $\dot{\times}$ et \otimes donnent celle de \times .
Un calcul facile mais pénible à écrire permet de vérifier que les distributivités de $\dot{\times}$ sur $\dot{+}$ et \otimes sur \oplus donnent celle de \times sur $+$.
- Si 1_A et 1_B sont les unités de A et B , alors $(1_A, 1_B)$ est bien neutre sur $A \times B$. □

Remarque

Cela se généralise à un nombre d'anneaux quelconque $\left(A_1, \begin{smallmatrix} + \\ (1) \end{smallmatrix}, \begin{smallmatrix} \times \\ (1) \end{smallmatrix}\right), \dots, \left(A_p, \begin{smallmatrix} + \\ (p) \end{smallmatrix}, \begin{smallmatrix} \times \\ (p) \end{smallmatrix}\right)$ avec pour tout (x_1, \dots, x_p) et (y_1, \dots, y_p) dans $A_1 \times \dots \times A_p$,

$$(x_1, \dots, x_p) + (y_1, \dots, y_p) = \left(x_1 \begin{smallmatrix} + \\ (1) \end{smallmatrix} y_1, \dots, x_p \begin{smallmatrix} + \\ (p) \end{smallmatrix} y_p\right)$$

$$(x_1, \dots, x_p) \times (y_1, \dots, y_p) = \left(x_1 \begin{smallmatrix} \times \\ (1) \end{smallmatrix} y_1, \dots, x_p \begin{smallmatrix} \times \\ (p) \end{smallmatrix} y_p\right)$$



Propriété

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 $(a, b)^{-1} = (a^{-1}, b^{-1})$.

Démonstration

$$\begin{aligned} (a, b) \in U_{A \times B} &\iff \exists (c, d) \in A \times B, (a, b) \times (c, d) = (c, d) \times (a, b) = (1_A, 1_B) \\ &\iff \exists (c, d) \in A \times B, ac = ca = 1_A \text{ et } bd = db = 1_B \\ &\iff (a, b) \in U_A \times U_B \end{aligned}$$

et on a bien alors $(a, b)^{-1} = (a^{-1}, b^{-1})$. □

7 Sous-anneau et sous-corps

Définition : Sous-anneau

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

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

Remarque

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

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 $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq I_2$.

Propriété : Caractérisation des sous-anneaux

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

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

ou, de manière équivalente,

$$\left\{ \begin{array}{l} B \subset A \\ 1_A \in B \\ \forall x, y \in B, x + y \in B, -x \in B \text{ et } x \times y \in B \end{array} \right.$$

ou encore

$$\left\{ \begin{array}{l} B \subset A \\ 1_A \in B \\ \forall x, y \in B, x - y \in B \text{ et } x \times y \in B \end{array} \right.$$

Démonstration

Même principe que pour les sous-groupes, la présence de 1_A n'étant automatique que si B possède un élément inversible, d'où la nécessité d'imposer $1_A \in B$. □

Exemples

- E1 – **Anneau des entiers de Gauss**^a : $\mathbb{Z}[i] = \mathbb{Z} + i\mathbb{Z}$ est un sous-anneau de $(\mathbb{C}, +, \times)$.
- E2 – $\mathcal{F}_n^+(\mathbb{K})$ est un sous-anneau de $(\mathcal{M}_n(\mathbb{K}), +, \times)$
- E3 – L'ensemble $\mathcal{B}(\mathbb{R})$ des fonctions bornées est un sous-anneau de $(\mathbb{R}^{\mathbb{R}}, +, \times)$.

a.



Carl Friedrich Gauss (Brunswick 1777 - Göttingen 1855) est un mathématicien, astronome et physicien allemand. Surnommé *le prince des mathématiciens*, il est considéré comme l'un des plus grands mathématiciens de tous les temps. Gauss était un génie particulièrement précoce : à 7 ans (ou 10 selon les sources), il donne la formule calculant $1 + 2 + \dots + 100$. À 19 ans, il fut le premier à démontrer la loi de réciprocité quadratique. Parmi ses autres prouesses, on peut citer la démonstration du théorème fondamental de l'algèbre, dans sa thèse en 1799, l'invention de la théorie des congruences, la résolution de problèmes de construction à la règle et au compas... Il est considéré comme le fondateur de la géométrie différentielle.

Définition : 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 : 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,

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

Démonstration

Le sens \implies ne pose pas de problème. Pour le sens \impliedby , on a bien un sous-anneau dont tous les éléments non nuls sont inversibles car $1_{\mathbb{K}} = xx^{-1} \in \mathbb{L}$. □

8 Morphismes d'anneaux

Définition : 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

- (MA1) $\forall (a, b) \in A^2, \quad f(a + b) = f(a) \oplus f(b)$
(ie $f : (A, +) \rightarrow (A', \oplus)$ morphisme de groupes)
- (MA2) $\forall (a, b) \in A^2, \quad f(a \times b) = f(a) \otimes f(b)$
- (MA3) $f(1_A) = 1_{A'}$

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 .



Remarques

R1 – 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 $\text{Ker } f = \{0_A\}$.

R2 – En général, $\text{Ker } f$ n'est pas un sous-anneau de A . C'est un sous-groupe additif stable par multiplication.

Exemple

$$f : \begin{cases} \mathbb{R}[X] & \longrightarrow & \mathbb{C} \\ P & \longmapsto & \tilde{P}(i) \end{cases} ; \text{Ker } f = (X^2 + 1)\mathbb{R}[X] \text{ n'est pas un sous-anneau de } \mathbb{R}[X].$$

Propriété

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.

Démonstration

- (i) $f(a)f(a^{-1}) = f(aa^{-1}) = f(1_A) = 1_{A'}$ et de même $f(a^{-1})f(a) = 1_{A'}$.
- (ii) Même principe que pour les morphismes de groupes.
- (iii) Simple vérification. □

Définition : 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

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 $f \equiv 0_{\mathbb{K}'}$.

Exemples

- E1 – $\text{id}_{\mathbb{C}}$, $z \mapsto \bar{z}$ sont des automorphismes (involutifs) du corps \mathbb{C} .
- E2 – Tout morphisme de corps est injectif, car si $x \neq 0_{\mathbb{K}}$, x est inversible donc $f(x)$ est inversible, donc $f(x) \neq 0_{\mathbb{K}'}$ donc $x \notin \text{Ker } f$, donc $\text{Ker } f = \{0_{\mathbb{K}}\}$.

III IDÉAL D'UN ANNEAU COMMUTATIF

1 Généralités

Définition : Idéal

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

- (I1) I est un sous-groupe de $(A, +)$
- (I2) $\forall a \in A, \forall x \in I, ax \in I$.

Remarque

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

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

Exemples

E1 – $2\mathbb{Z}$ est un idéal de $(\mathbb{Z}, +, \times)$.

E2 – L'ensemble des suites bornées est un idéal de l'anneau des suites bornées.

Remarque

Si un idéal contient l'unité 1_A ou plus généralement un élément inversible, il est égal à A tout entier.

Propriété

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.

Démonstration

Simple vérification. Dans le cas d'un corps, comme tous les éléments non nuls sont inversibles, s'il y en a un dans I , en le multipliant par son inverse on obtient $1_A \in I$ puis $I = A$. □

Propriété

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

Démonstration

- $0_A \in \text{Ker } f \neq \emptyset$
 - Si $x, y \in \text{Ker } f$, $f(x - y) = f(x) - f(y) = 0_{A'}$ donc $x - y \in \text{Ker } f$.
 - Si $x \in \text{Ker } f$ et $a \in A$, $f(ax) = f(a)f(x) = 0_{A'}$ donc $ax \in \text{Ker } f$.
-

Remarque

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

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

Exercice

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

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

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

Démonstration

- (i) • $I + J$ est un idéal :
- ★ $0_A = 0_A + 0_A \in I + J$
 - ★ Si $x, y \in I + J$, on a $(x_I, x_J), (y_I, y_J) \in I \times J$ tels que $x = x_I + x_J$ et $y = y_I + y_J$.
Alors $x + y = (x_I + y_I) + (x_J + y_J) \in I + J$.
 - ★ Si $x = x_I + x_J \in I + J$ et $a \in A$ alors $ax = ax_I + ay_J \in I + J$.
- $I + J$ contient I et J car ceux-ci contiennent 0_A .
 - Si K est un idéal de A contenant I et J , alors par stabilité par $+$, $I + J \subset K$.
- (ii) • $I \cap J$ est un idéal :
- ★ $0_A \in I \cap J$
 - ★ Si $x, y \in I \cap J$, $x + y \in I \cap J$.
 - ★ Si $x \in I \cap J$ et $a \in A$ alors $ax \in I \cap J$.
- $I \cap J$ est contenu dans I et J .
 - Si K est un idéal de A contenu dans I et J , alors $K \subset I \cap J$.

□

3 Idéal principal

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

Propriété

Soit $x \in A$. On note

$$(x) = xA = \{xa, a \in A\}.$$

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

Remarque

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'élément est l'ensemble des combinaisons linéaires (finies) de ces éléments, à coefficients dans A .

Définition : 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
 - (AP1) C'est un anneau intègre
 - (AP2) Tous ses idéaux sont principaux.

Théorème

L'anneau \mathbb{Z} est principal.

Démonstration

C'est un anneau intègre et ses idéaux qui sont aussi ses sous-groupes sont tous principaux.

□

Remarque

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 : 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 : Caractérisation avec les idéaux

Soient $a, b \in A$.

b divise a si et seulement si $a \in (b)$ si et seulement si $(a) \subset (b)$.

Remarque

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

Propriété

Soient $a, b \in A$.

a et b sont associés si et seulement si $(a) = (b)$ si et seulement s'il existe $q \in U_A$ tel que $b = qa$.

Exemple

Dans \mathbb{Z} , a, b sont associés si et seulement si $a = \pm b$.

Remarque

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 MPSI dans \mathbb{Z} .

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

IV LA STRUCTURE D'ALGÈBRE

1 Algèbre et sous-algèbre

Définition : 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* : $\forall \lambda \in \mathbb{K}, \forall x, y \in \mathcal{A}, \lambda \cdot (x \times y) = (\lambda \cdot x) \times y = x \times (\lambda \cdot y)$.

Exemples

E1 – $(\mathbb{C}, +, \times, \cdot)$ est une \mathbb{R} -algèbre et une \mathbb{C} -algèbre.

E2 – $(\mathbb{K}^X, +, \times, \cdot)$ est une \mathbb{K} -algèbre.

E3 – $(\mathbb{K}^{\mathbb{N}}, +, \times, \cdot)$ est une \mathbb{K} -algèbre.

E4 – $(\mathbb{K}[X], +, \times, \cdot)$ est une \mathbb{K} -algèbre.

E5 – $(\mathbb{K}(X), +, \times, \cdot)$ est une \mathbb{K} -algèbre.



- E6 – Si E est un \mathbb{K} -espace vectoriel, $(\mathcal{L}(E), +, \circ, \cdot)$ est une \mathbb{K} -algèbre.
- E7 – Si $n \in \mathbb{N}^*$, $(\mathcal{M}_n(\mathbb{K}), +, \times, \cdot)$ est une \mathbb{K} -algèbre.

Propriété : 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

- (SAI1) $\mathcal{B} \subset \mathcal{A}$
- (SAI2) $1_{\mathcal{A}} \in \mathcal{B}$
- (SAI3) $\forall x, y \in \mathcal{B}, \forall \lambda \in \mathbb{K}, x + \lambda y \in \mathcal{B}$
- (SAI4) $\forall x, y \in \mathcal{B}, \forall \lambda \in \mathbb{K}, x \times y \in \mathcal{B}$

Exemples

- E1 – $\mathbb{K}[X]$ est une sous-algèbre de $\mathbb{K}(X)$.
- E2 – $\mathcal{C}^k(I, \mathbb{K})$ est une sous-algèbre de \mathbb{K}^I .
- E3 – L'ensemble des suites convergentes est une sous-algèbre de $\mathbb{K}^{\mathbb{N}}$.
- E4 – L'ensemble $\mathbb{K}[x]$ des fonctions polynomiales est une sous-algèbre de $\mathbb{K}^{\mathbb{K}}$.

Définition

Si $P = a_0 + a_1X + \dots + a_nX^n \in \mathbb{K}[X]$ et $x \in \mathcal{A}$, on pose $P(x) = \sum_{k=0}^n a_k x^k = a_0 1_{\mathcal{A}} + a_1 x + \dots + a_n x^n$.

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

2 Morphismes d'algèbres

Définition : 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

- (MAI1) f est linéaire ie, $\forall x, y \in \mathcal{A}, \forall \lambda \in \mathbb{K}, f(x + \lambda y) = f(x) + \lambda f(y)$
- (MAI2) $\forall x, y \in \mathcal{A}, f(x \times y) = f(x) \times f(y)$
- (MAI3) $f(1_{\mathcal{A}}) = 1_{\mathcal{B}}$.

Exemples

E1 – Si $X \neq \emptyset, \mathcal{A}$ une \mathbb{K} -algèbre, $a \in X$, alors $u_a : \begin{matrix} \mathcal{A}^X & \longrightarrow & \mathcal{A} \\ f & \longmapsto & f(a) \end{matrix}$ est un morphisme de \mathbb{K} -algèbres. (morphisme d'évaluation).

E2 – $f : \begin{matrix} \mathbb{K}[X] & \longrightarrow & \mathbb{K}[x] \\ P & \longmapsto & \tilde{P} \end{matrix}$ est un isomorphisme d'algèbre si \mathbb{K} est infini, et $g : \begin{matrix} \mathbb{K}[X] & \longrightarrow & \mathbb{K}(X) \\ P & \longmapsto & \frac{P}{1} \end{matrix}$ est un morphisme d'algèbres injectif.

E3 – $f : \begin{matrix} \mathbb{K} & \longrightarrow & \mathcal{M}_1(\mathbb{K}) \\ x & \longmapsto & (x) \end{matrix}$ est un isomorphisme de \mathbb{K} -algèbres.

Propriété

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

Alors l'application $f : \begin{array}{l} \mathbb{K}[X] \longrightarrow \mathcal{A} \\ P \longmapsto P(x) \end{array}$ est un morphisme de \mathbb{K} -algèbres.

Démonstration

Soit $P = \sum_{k \geq 0} a_k X^k, Q = \sum_{k \geq 0} b_k X^k \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$. L'associativité et la distributivité des lois sur \mathcal{A} , toutes les sommes étant finies, permettent d'écrire :

- $(P + \lambda Q)(x) = \sum_{k \geq 0} (a_k + \lambda b_k) x^k = \sum_{k \geq 0} a_k x^k + \lambda \sum_{k \geq 0} b_k x^k = P(x) + \lambda Q(x).$
- $(PQ)(x) = \sum_{k, \ell \geq 0} a_k b_\ell x^k = \left(\sum_{k \geq 0} a_k x^k \right) \times \left(\sum_{\ell \geq 0} b_\ell x^\ell \right) = P(x) \times Q(x).$
- $f(1_{\mathbb{K}[X]}) = f(X^0) = x^0 = 1_{\mathcal{A}}.$

□

Remarque

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

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

Soit G est un sous-groupe de $(\mathbb{R}, +)$.

Alors G est soit dense dans \mathbb{R} , soit discret (de la forme $\alpha\mathbb{Z}$).

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.