3

Structures algébriques

Extrait du programme officiel :

CONTENUS	CAPACITÉS & COMMENTAIRES
a) Compléments sur les groupes	
Intersection de sous-groupes.	
~~Sous-groupe engendré par une partie. Partie génératrice d'un groupe.~~	
Sous-groupes du groupe $(\mathbb{Z}, +)$.	
~~Groupe $(\mathbb{Z}/n\mathbb{Z}, +)$. Générateurs de $\mathbb{Z}/n\mathbb{Z}$.~~	
~~Groupe monogène, groupe cyclique.~~	~~Groupe des racines n-ièmes de l'unité.~~
~~Tout groupe monogène infini est isomorphe à $(\mathbb{Z}, +)$. Tout groupe monogène fini de cardinal n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.~~	
~~Ordre d'un élément d'un groupe.~~ ~~Si x est d'ordre fini d et si e désigne le neutre de G, alors, pour tout $n \in \mathbb{Z}$, $x^n = e \iff d \mid n$.~~	~~L'ordre de x est le cardinal du sous-groupe de G engendré par x.~~
~~L'ordre d'un élément d'un groupe fini divise le cardinal du groupe.~~	~~La démonstration n'est exigible que pour G commutatif.~~
b) Compléments sur les anneaux	
Produit fini d'anneaux.	
Idéal d'un anneau commutatif.	Noyau d'un morphisme d'anneaux commutatifs.
Idéal engendré par un élément.	Notation xA.
Divisibilité dans un anneau commutatif intègre.	Interprétation en termes d'idéaux.
c) Idéaux de $\mathbb{Z}$	
Idéaux de $\mathbb{Z}$.	
~~Définition du PGCD de $n \geqslant 2$ entiers relatifs en termes d'idéaux, relation de Bézout.~~	~~Lien avec le programme de première année.~~
f) Algèbres	
Algèbre.	Les algèbres sont unitaires. Exemples : $\mathbb{K}[X]$, $\mathscr{L}(E)$, $\mathscr{M}_n(\mathbb{K})$, $\mathscr{F}(X, \mathbb{K})$.
Sous-algèbre.	
Morphisme d'algèbres.	

Table des matières

I GROUPES ET SOUS-GROUPES

1 Structure de groupe (MP2I)

Remarque : Quelques rappels

R 1 – ■ **Loi de composition interne** sur un ensemble E : toute application $\star : \begin{array}{|ccc} E\times E & \longrightarrow & E \\ (x,y) & \longmapsto & x\star y \end{array}$.

■ Elle est dite
  ⋆ **associative** lorsque
$$\forall (x,y,z)\in E^3,\quad (x\star y)\star z = x\star(y\star z)$$
  (que l'on peut alors noter $x\star y\star z$.)
  ⋆ **commutative** lorsque
$$\forall (x,y)\in E^2,\quad x\star y = y\star x.$$

■ 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
E 1 – 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
E 2 – Sur E^E pour $\circ$, l'élément neutre est id_E.
  ⋆ $(\exists g\in E^E,\ f\circ g = g\circ f = \mathrm{id}_E) \iff f$ bijective (ie inversible pour $\circ$).
  ⋆ $(\exists g\in E^E,\ f\circ g = \mathrm{id}_E) \iff f$ surjective.
  ⋆ $(\exists g\in E^E,\ g\circ f = \mathrm{id}_E) \iff f$ 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 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

R 2 – En particulier, un groupe n'est jamais vide.

Exemple

E 3 – $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes commutatifs de neutre 0.

E 4 – Si D est un ensemble non vide, $(\mathbb{R}^D, +)$ et $(\mathbb{C}^D, +)$ et en particulier $\left(\mathbb{R}^{\mathbb{N}}, +\right)$ et $\left(\mathbb{C}^{\mathbb{N}}, +\right)$ sont des groupes commutatifs, de neutre la fonction / suite nulle.

E 5 – $(\mathbb{Q}^*, \times)$, $(\mathbb{Q}_+^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{R}_+^*, \times)$ et $(\mathbb{C}^*, \times)$ sont des groupes commutatifs de neutre 1.

E 6 – 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 $|E| \geqslant 3$, ce groupe n'est pas commutatif.
Si $n \in \mathbb{N} \setminus \{0, 1\}$, et $E = [\![1, n]\!]$, on note $\mathfrak{S}_n = \mathfrak{S}([\![1, n]\!])$.
$(\mathfrak{S}_n, \circ)$ 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

R 3 – Autrement dit, $x^n = \bigstar_{k=1}^{n} x = \underbrace{x \star \cdots \star x}_{n \text{ fois}}$.

R 4 – 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 $(x^n)^{-1} = (x^{-1})^n$.

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 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[1] 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
$$\forall a, b \in E, \quad x \star a = x \star b \Longrightarrow a = b$$
- **à droite** lorsque
$$\forall a, b \in E, \quad a \star x = b \star x \Longrightarrow a = b$$

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.

Démonstration

Si x est inversible et si $x \star a = x \star b$, alors
$$a = \left(x^{-1} \star x\right) \star a = x^{-1} \star (x \star a) = x^{-1} \star (x \star b) = \left(x^{-1} \star x\right) \star b = b$$
par associativité.

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

Corollaire 1 : Régularité dans un groupe

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

Corollaire 2 : Bijectivité des translations

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

Les applications $\varphi_a : \begin{array}{|ccc} G & \longrightarrow & G \\ x & \longmapsto & a \star x \end{array}$ *et* $\psi_a : \begin{array}{|ccc} G & \longrightarrow & G \\ x & \longmapsto & x \star a \end{array}$ *(appelées translations à gauche et à droite) sont bijectives.*

Démonstration

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

Corollaire 3

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

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

Démonstration

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

Remarque

R 6 – 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

E 7 – Si on considère le groupe des racines cubique de l'unité : $\mathbb{U}_3 = \{1, \mathrm{j}, \mathrm{j}^2\}$ 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 (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.

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

R7 – Cela se généralise à un nombre de groupes quelconque $\left(G_1, \underset{1}{\star}\right), \dots, \left(G_p, \underset{p}{\star}\right)$ avec pour tout $(x_1, \dots, x_p)$ et $(y_1, \dots, y_p)$ dans $G_1 \times \cdots \times G_p$,

$$(x_1, \dots, x_p) \top (y_1, \dots, y_p) = \left(x_1 \underset{1}{\star} y_1, \dots, x_p \underset{p}{\star} y_p\right).$$

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 $\left(H, \star|_{H^2}\right)$ 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 $(G, \star)$.

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 $\operatorname{sym}_H(x) \in H \subset G$ tel que $x \star \operatorname{sym}_H(x) = \operatorname{sym}_H(x) \star x = e_H = e_G$ et donc par unicité, x inversible dans G et $\operatorname{sym}_G(x) = \operatorname{sym}_H(x)$. ■

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) $\begin{cases} H\subset G \\ H\neq\varnothing \quad (e_G\in H) \\ H \text{ est stable par } \star \ : \ \forall x,y\in H,\ \ x\star y\in H \\ H \text{ est stable par inverse } : \ \forall x\in H,\ \ x^{-1}\in H \end{cases}$

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

Remarque

R 8 – En notation additive, (ii) devient $\begin{cases} H\subset G \\ H\neq\varnothing \quad (0_G\in H) \\ H \text{ est stable par } \star \ : \ \forall x,y\in H,\ \ x+y\in H \\ H \text{ est stable par opposé } : \ \forall x\in H,\ \ -x\in H \end{cases}$ et (iii) devient $\begin{cases} H\subset G,\ H\neq\varnothing \quad (0_G\in H) \\ \forall x,y\in H,\ \ x-y\in H \end{cases}$

Démonstration

- $(i)\Longrightarrow(ii)$: si $H<G$, $H\subset G$, $H\neq\varnothing$, H stable par $\star$ (Ici) et, d'après la propriété précédente, H est bien stable par inverse.
- $(ii)\Longrightarrow(iii)$: facile.
- $(iii)\Longrightarrow(i)$: 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 est bien un sous-groupe de $(G,\star)$. ■

Remarque

R 9 – Un sous-groupe d'un groupe abélien est facilement encore commutatif.

Exemple

E 8 – $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ sont des sous-groupes (additifs et abéliens) de $(\mathbb{C},+)$.

E 9 – $\mathbb{R}^D$ où $D\neq\varnothing$ est un sous-groupe additif abélien de $(\mathbb{C}^D,+)$.

E 10 – $\mathbb{Q}^*$, $\mathbb{Q}_+^*$, $\mathbb{R}^*$, $\mathbb{R}_+^*$, $\mathbb{U}$, $\mathbb{U}_n$ 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 $n\in\mathbb{N}^*$, $\mathbb{U}_n=\{z\in\mathbb{C},\ z^n=1\}=\left\{\mathrm{e}^{\frac{2ik\pi}{n}},\ k\in[\![0,n-1]\!]\right\}$.)

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 $(G,\star)$.

Démonstration

- $(H_i)_{i\in I} \subset G$ car $\forall\, i \in I,\ \ H_i \subset G$.
- $(H_i)_{i\in I} \neq \varnothing$ 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 3 : Réunion de sous-groupes

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

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

- $\Longleftarrow$: ok
- $\Longrightarrow$: 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 $(\mathbb{Z},+)$ (MPI)

Notation 2

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

Remarque

R 10 – 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 $a\mathbb{Z}$ 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 $p\in G\cap\mathbb{N}^*\neq\varnothing$, soit $p<0$ et alors $-p\in G\cap\mathbb{N}^*\neq\varnothing$.
    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 $0\leqslant r<a$.

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 (MP2I)

a Définition

Définition 5 : Morphisme de groupe

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

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

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

E 11 – $\ln : (\mathbb{R}_+^*, \times) \to (\mathbb{R}, +)$ isomorphisme de groupes.

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

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

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

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

E 15 – $\det : (\mathscr{GL}(E), \circ) \to (\mathbb{R}^*, \times)$ et $\det : (\mathscr{GL}_n(\mathbb{K}), \times) \to (\mathbb{R}^*, \times)$ 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 7 : Image du neutre et du symétrique par un morphisme de groupes

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

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

Démonstration

$f(e_G) = f(e_G \star e_G) = f(e_G) \star f(e_G)$ donc comme $f(e_G)$ est inversible, $f(e_G) = e_{G'}$.
$f(x) \bullet f(\mathrm{sym}(x)) = f(x \star \mathrm{sym}(x)) = f(e_G) = e_{G'}$
et $f(\mathrm{sym}(x)) \star f(x) = f(\mathrm{sym}(x) \star x) = f(e_G) = e_{G'}$

Propriété 8 : Image d'une itérée

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

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 9 : Composée de morphismes

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

b Noyau et image

Définition 6 : Image et noyau d'un morphisme

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

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

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

  Ainsi, $x\in\operatorname{Ker} f \iff f(x)=e_{G'}$.
- On appelle **image** de f l'ensemble

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

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

Exemple

E 16 – $f:\left|\begin{array}{ccc}(\mathbb{R},+) & \longrightarrow & (\mathbb{U},\times)\\ \theta & \longmapsto & \mathrm{e}^{\mathrm{i}\theta}\end{array}\right.$: $\operatorname{Ker} f=2\pi\mathbb{Z}$.

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

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

- *f est injectif si et seulement si $\operatorname{Ker} f=\{e_G\}$.*
- *f est surjectif si et seulement si $\operatorname{Im} f=G'$.*

Remarque

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

Démonstration

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

$$e'_G=f(x)\bullet\left(f(x')\right)^{-1}=f(x)\bullet f\left(x'^{-1}\right)=f\left(x\star x'^{-1}\right)$$

  donc $x\star x'^{-1}\in\operatorname{Ker} f$ 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,

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

Exemple

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

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

Soit $f : (G, \star) \to (G', \bullet)$ 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 $(G', \bullet)$:
  - ⋆ $f(H) \subset G'$
  - ⋆ $f(H) \neq \varnothing$ car $H \neq \varnothing$
  - ⋆ Si $y, y' \inf(H)$, on a $x, x' \in H$ tels que $y = f(x)$ et $y' = f(x')$. f étant un morphisme de groupes,

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

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

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

Soit $f : (G, \star) \to (G', \bullet)$ un morphisme de groupes.
Alors $\operatorname{Ker} f$ est un sous-groupe de $(G, \star)$ et $\operatorname{Im} f$ est un sous-groupe de $(G', \bullet)$.

Démonstration

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

Exemple

E 18 – $f : \left| \begin{array}{ccc} (\mathbb{R}, +) & \longrightarrow & (\mathbb{C}^*, \times) \\ \theta & \longmapsto & e^{i\theta} \end{array} \right.$ étant un morphisme de groupes, $\operatorname{Im} f = \mathbb{U}$ est un sous-groupe de $(\mathbb{C}^*, \times)$ et $\operatorname{Ker} f = 2\pi\mathbb{Z}$ est un sous-groupe de $(\mathbb{R}, +)$.
$\mathbb{U}$ est aussi le noyau du morphisme $|\cdot| : \mathbb{C}^* \to \mathbb{R}^*$.

E 19 – $f : \left| \begin{array}{ccc} (\mathbb{C}^*, \times) & \longrightarrow & (\mathbb{C}^*, \times) \\ z & \longmapsto & z^n \end{array} \right.$ étant un morphisme de groupes, $\operatorname{Ker} f = \mathbb{U}_n$ est un sous-groupe de $(\mathbb{C}^*, \times)$. C'est aussi l'image du morphisme $k \in \mathbb{Z} \mapsto e^{\frac{2ik\pi}{n}}$.

C Isomorphismes

Propriété 12 : Réciproque d'un isomorphisme

Soit $f:(G,\star)\to(G',\bullet)$ 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,

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

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 $D\neq\varnothing$), $\left(\mathbb{C}^{\mathbb{N}},+,\times\right)$ et $\left(\mathbb{R}^{\mathbb{N}},+,\times\right)$ sont des anneaux commutatifs.

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

Remarque

R 14 – 0_A est **absorbant** :

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

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

R 18 – On parle parfois d'unités de A, d'où la notation...

Exemple

E 22 – $U_{\mathbb{R}} = \mathbb{R}^*$

E 23 – $U_{\mathbb{Z}} = \{-1, 1\} \neq \mathbb{Z}^*$

E 24 – $U_{\mathbb{C}^{\mathbb{N}}} = \{\text{suites jamais nulles}\}$

E 25 – $U_{\mathbb{C}^D} = \{\text{fonctions jamais nulles}\}$

E 26 – $U_{\mathcal{M}_n(\mathbb{K})} = \mathcal{GL}_n(\mathbb{K})$

Propriété 13 : Groupe des inversibles

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

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. ■

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 $a \times b = b \times a$,*
$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$
- ***Factorisation**[a] **de $a^n - b^n$** : Si $a \times b = b \times a$*
$$\begin{aligned} a^n - b^n &= (a-b)\left(a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1}\right) \\ &= (a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k}. \end{aligned}$$
- ***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

R 19 – Si a et b ne commutent pas,
$$\begin{aligned} (ab)^n &= abab\cdots ab \\ (a+b)^2 &= a^2 + ab + ba + b^2 \\ (a+b)^3 &= a^3 + a^2b + aba + ba^2 + ab^2 + bab + b^2a + b^3 \end{aligned}$$
etc.

Démonstration

- Par récurrence sur n.
- **Formule du binôme** :
  - ⋆ **Preuve par dénombrement** :
$$(a+b)^n = \underbrace{(a+b)(a+b)\cdots(a+b)}_{n \text{ fois}}$$
    En développant, on obtient des termes de la forme $x_1x_2\cdots x_n$ avec $x_i = a$ ou b. Si on veut k termes a, on $\binom{n}{k}$ choix, et le terme vaut a^kb^{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 $n-1$,
$$\begin{aligned} (a+b)^n = (a+b)(a+b)^{n-1} &= (a+b)\sum_{k=0}^{n-1}\binom{n-1}{k}a^kb^{n-1-k} \\ &= \sum_{k=0}^{n-1}\binom{n-1}{k}a^{k+1}b^{n-k-1} + \sum_{k=0}^{n-1}\binom{n-1}{k}a^kb^{n-k} \end{aligned}$$
    (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 cœfficients avec $k<0$.

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

$$(a-b)\sum_{k=0}^{n-1}a^k b^{n-1-k} = \sum_{k=0}^{n-1}\left(a^{k+1}b^{n-(k+1)} - a^k b^{n-k}\right)$$
(a et b commutent, associativité, distributivité)
$$= a^n b^0 - a^0 b^n = a^n - b^n$$
(somme télescopique)

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

E 27 – $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ 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

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

Exemple

E 28 – $\mathbb{R},\mathbb{Z},\mathbb{C},\mathbb{Q}$ 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 $k\in[\![1,n]\!]$, $a_k\neq 0_A$, *alors* $a_1\times\cdots\times a_n\neq 0_A$.

Démonstration

Par contraposée et récurrence. ■

Propriété 16 : Régularité dans un anneau intègre

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

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 17 : Intégrité d'un corps

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

Démonstration

Si $ab=0_{\mathbb{K}}$ et si $a\neq 0_K$, 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 (MPI)

Propriété 18 : Anneau produit

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

$$(a,b)+(a',b')=(a\dotplus a',b\oplus b')$$
$$(a,b)\times(a',b')=(a\dot\times a',b\otimes b')$$

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 $\dotplus$ 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

R 20 – Cela se généralise à un nombre d'anneaux quelconque $\left(A_1, \underset{(1)}{+}, \underset{(1)}{\times}\right), \dots, \left(A_p, \underset{(p)}{+}, \underset{(p)}{\times}\right)$ avec pour tout $(x_1, \dots, x_p)$ et $(y_1, \dots, y_p)$ dans $A_1 \times \dots \times A_p$,

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

$$(x_1, \dots, x_p) + (y_1, \dots, y_p) = \left(x_1 \underset{(1)}{\times} y_1, \dots, x_p \underset{(p)}{\times} y_p\right)$$

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

Démonstration

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

et on a bien alors $(a, b)^{-1} = \left(a^{-1}, b^{-1}\right)$. ■

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

Remarque

R 21 – 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

E 29 – Soit, dans l'anneau des matrices 2×2, l'ensemble B des matrices $\left(\begin{smallmatrix} a & 0 \\ 0 & 0 \end{smallmatrix}\right)$ pour $a \in \mathbb{K}$. Alors $(B, +, \times)$ est un anneau d'unité $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \neq I_2$.

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,

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

ou encore

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

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 $1_A \in B$. ■

Exemple

E 30 – **Anneau des entiers de Gauss**[a] : $\mathbb{Z}[\mathrm{i}] = \mathbb{Z} + \mathrm{i}\mathbb{Z}$ est un sous-anneau de $(\mathbb{C},+,\times)$.

E 31 – $\mathcal{T}_n^+(\mathbb{K})$ est un sous-anneau de $(\mathcal{M}_n(\mathbb{K}),+,\times)$

E 32 – L'ensemble $\mathcal{B}(\mathbb{R})$ des fonctions bornées est un sous-anneau de $\left(\mathbb{R}^{\mathbb{R}},+,\times\right)$.

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 $1+2+\cdots+100$. 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 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 $\left(\mathbb{L}, +|_{\mathbb{L}^2}, \times|_{\mathbb{L}^2}\right)$ 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,

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

Démonstration

Le sens $\Longrightarrow$ ne pose pas de problème. Pour le sens $\Longleftarrow$, 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 (MP2I)

Définition 14 : Morphisme d'anneaux

Soient $(A,+,\times)$ et $(A',\oplus,\otimes)$ deux anneaux.
$f:(A,+,\times)\to(A',\oplus,\otimes)$ 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 $f:(A,+)\to(A',\oplus)$ 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.

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

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

Remarque

R 22 – 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 $\operatorname{Ker} f=\{0_A\}$.

R 23 – En général, $\operatorname{Ker} f$ n'est pas un sous-anneau de A. C'est un sous-groupe additif stable par multiplication... Nous les étudions juste après !

Exemple

E 33 – $f:\left|\begin{array}{ccc}\mathbb{R}[X] & \longrightarrow & \mathbb{C}\\ P & \longmapsto & \tilde{P}(\mathrm{i})\end{array}\right.$; $\operatorname{Ker} f=(X^2+1)\,\mathbb{R}[X]$ n'est pas un sous-anneau de $\mathbb{R}[X]$.

Propriété 22 : des morphismes d'anneaux

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

(i) *Si a est inversible dans A, alors $f(a)$ l'est dans B et $f\left(a^{-1}\right)=\left(f(a)\right)^{-1}$.*

(ii) *Si f est un isomorphisme alors $f^{-1}:(B,\oplus,\otimes)\to(A,+,\times)$ est aussi un isomorphisme d'anneau.*

(iii) *Si $g:(B,\oplus,\otimes)\to(C,\dot{+},\dot{\times})$ est aussi un morphisme d'anneau, alors $g\circ f:(A,+,\times)\to(C,\dot{+},\dot{\times})$ l'est encore.*

Démonstration

(i) $f(a)f\left(a^{-1}\right)=f\left(aa^{-1}\right)=f(1_A)=1_{A'}$ et de même $f\left(a^{-1}\right)f(A)=1_{A'}$.

(ii) Même principe que pour les morphismes de groupes.

(iii) Simple vérification. ■

Définition 15 : Morphisme de corps

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

Remarque

R 24 – Avec (i) et (ii), $f(1_\mathbb{K})=\left(f(1_\mathbb{K})\right)^2$ 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

E 34 – $\mathrm{id}_\mathbb{C}$, $z\mapsto\overline{z}$ sont des automorphismes (involutifs) du corps $\mathbb{C}$.

E 35 – 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 $x\notin\operatorname{Ker} f$, donc $\operatorname{Ker} f=\{0_\mathbb{K}\}$.

III 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) I est un sous-groupe de $(A,+)$

(ii) $\forall a\in A,\quad \forall x\in I,\quad ax\in I$.

Remarque

R 25 – Finalement, I est un **idéal** de $(A,+,\times)$ lorsque
- $I\subset A$
- $I\neq\varnothing$
- $\forall x,y\in I,\quad x-y\in I$
- $\forall a\in A,\quad \forall x\in I,\quad ax\in I.$

Comme $-1_A\in A$, on peut se contenter de
- $I\subset A$
- $I\neq\varnothing$
- $\forall x,y\in I,\quad x+y\in I$

- $\forall a \in A, \quad \forall x \in I, \quad ax \in I.$

Exemple

E 36 – $2\mathbb{Z}$ est un idéal de $(\mathbb{Z}, +, \times)$.

E 37 – L'ensemble des suites convergeant vers 0 est un idéal de l'anneau des suites bornées.

Remarque

R 26 – Si un idéal contient l'unité 1_A ou plus généralement un élément inversible, il est égal à A tout entier.

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.

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 24 : Noyau d'un morphisme d'anneaux

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

Démonstration

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

■

Remarque

R 27 – $\operatorname{Im} f$ est un sous-anneau de $(A', \oplus, \otimes)$.
En général, $\operatorname{Ker} A$ n'est pas un sous-anneau de $(A, +, \times)$.

Exercice 4

Montrer que si $f : (A, +, \times) \to (A', \oplus, \otimes)$ 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

R 28 – 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 $ax=ax_I+ay_I\in I+J$.
- $I+J$ 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 26 : Idéal engendré par un élément

Soit $x\in A$. On note

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

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

Remarque

R 29 – 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 cœfficients 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) C'est un anneau intègre.
  (ii) Tous ses idéaux sont principaux.

Théorème 1 : Principalité de $\mathbb{Z}$

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

R 30 – 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

R 31 – 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 $aA=bB$ si et seulement s'il existe $q\in U_A$ tel que $b=qa$.

Exemple

E 38 – Dans $\mathbb{Z}$, a,b sont associés si et seulement si $a=\pm b$.

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 $(a)\cap(b) = \{$multiples communes à a 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 $(\mathscr{A}, +, \times, \cdot)$ est une $\mathbb{K}$-algèbre lorsque

- $(\mathscr{A}, +, \cdot)$ est une $\mathbb{K}$-espace vectoriel,
- $(\mathscr{A}, +, \times)$ est un anneau,
- *Pseudo-associativité* : $\forall \lambda \in \mathbb{K},\quad \forall x, y \in \mathscr{A}$,

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

Exemple

E 39 – $(\mathbb{C}, +, \times, \cdot)$ est une $\mathbb{R}$-algèbre et une $\mathbb{C}$-algèbre.

E 40 – $\left(\mathbb{K}^X, +, \times, \cdot\right)$ est une $\mathbb{K}$-algèbre.

E 41 – $\left(\mathbb{K}^{\mathbb{N}}, +, \times, \cdot\right)$ est une $\mathbb{K}$-algèbre.

E 42 – $(\mathbb{K}[X], +, \times, \cdot)$ est une $\mathbb{K}$-algèbre.

E 43 – $(\mathbb{K}(X), +, \times, \cdot)$ est une $\mathbb{K}$-algèbre.

E 44 – Si E est un $\mathbb{K}$-espace vectoriel, $(\mathscr{L}(E), +, \circ, \cdot)$ est une $\mathbb{K}$-algèbre.

E 45 – Si $n \in \mathbb{N}^*$, $(\mathscr{M}_n(\mathbb{K}), +, \times, \cdot)$ 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 $(\mathscr{A}, +, \times, \cdot)$ est une $\mathbb{K}$-algèbre. $\mathscr{B}$ est une sous-algèbre de $(\mathscr{A}, +, \times, \cdot)$ lorsque

(i) $\mathscr{B} \subset \mathscr{A}$

(ii) $1_A \in \mathscr{B}$

(iii) $\forall x, y \in \mathscr{B},\quad \forall \lambda \in \mathbb{K},\quad x+\lambda y \in \mathscr{B}$

(iv) $\forall x, y \in \mathscr{B},\quad \forall \lambda \in \mathbb{K},\quad x\times y \in \mathscr{B}$

Exemple

E 46 – $\mathbb{K}[X]$ est une sous-algèbre de $\mathbb{K}(X)$.

E 47 – $\mathscr{C}^k(I, \mathbb{K})$ est une sous-algèbre de $\mathbb{K}^I$.

E 48 – L'ensemble des suites convergentes est une sous-algèbre de $\mathbb{K}^{\mathbb{N}}$.

E 49 – L'ensemble $\mathbb{K}[x]$ des fonctions polynomiales est une sous-algèbre de $\mathbb{K}^{\mathbb{K}}$.

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

Définition 20 : Polynôme en un élément d'une algèbre

Si $P = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{K}[X]$ et $x \in \mathscr{A}$, on pose

$$P(x) = \sum_{k=0}^{n} a_k x^k = a_0 1_{\mathscr{A}} + a_1 x + \cdots + a_n x^n.$$

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

2 Morphismes d'algèbres

Définition 21 : Morphisme d'algèbre

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

(i) f est linéaire ie $\forall x, y \in \mathscr{A}, \quad \forall \lambda \in \mathbb{K}, \quad f(x + \lambda y) = f(x) + \lambda f(y)$

(ii) $\forall x, y \in \mathscr{A}, \quad f(x \times y) = f(x) \times f(y)$

(iii) $f(1_{\mathscr{A}}) = 1_{\mathscr{B}}$.

Exemple

E 50 – Si $X \neq \varnothing$, $\mathscr{A}$ une $\mathbb{K}$-algèbre, $a \in X$, $u_a : \left| \begin{array}{ccc} \mathscr{A}^X & \longrightarrow & \mathscr{A} \\ f & \longmapsto & f(a) \end{array} \right.$ est un morphisme de $\mathbb{K}$-algèbres. (morphisme d'évaluation).

E 51 – $f : \left| \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{K}[x] \\ P & \longmapsto & \tilde{P} \end{array} \right.$ est un isomorphisme d'algèbre si $\mathbb{K}$ est infini, et $g : \left| \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{K}(X) \\ P & \longmapsto & \frac{P}{1} \end{array} \right.$ est un morphisme d'algèbres injectif.

E 52 – $f : \left| \begin{array}{ccc} \mathbb{K} & \longrightarrow & \mathscr{M}_1(\mathbb{K}) \\ x & \longmapsto & (x) \end{array} \right.$ est un isomorphisme de $\mathbb{K}$-algèbres.

Propriété 30

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

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

Démonstration

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

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

Remarque

R 32 – En particulier, deux polynômes en $x \in \mathscr{A}$ 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 $\alpha\leqslant x<2\alpha$. 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 $q\alpha\leqslant x<(q+1)\alpha$.
      En déduire que $x=q\alpha$.
      iii. Conclure.