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.	$\leftrightarrows$ 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 : $\mathbb{K}[X]$, $\mathscr{L}(E)$, $\mathscr{M}_n(\mathbb{K})$, $\mathscr{F}(X,\mathbb{K})$.
Sous-algèbre.	
Morphisme d'algèbres.	

TABLE DES MATIÈRES

I GROUPES ET SOUS-GROUPES

1 Structure de groupe

Définition : loi de composition interne

Soit E un ensemble non vide.

On appelle **loi de composition interne** sur E toute application $\star$: $\begin{array}{ccc} E\times E & \longrightarrow & E \\ (x,y) & \longmapsto & x\star y \end{array}$.

Définition : associativité, commutativité

Une loi de composition interne $\star$ sur un ensemble E 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
$$\forall (x,y) \in E^2,\ \ x \star y = y \star x.$$

Définition : Élément neutre

Soit $\star$ une loi de composition interne sur E et e un élément de E.
On dit que e est **élément neutre** pour $\star$ si pour tout $x \in E$, $x \star e = e \star x = x$.

Propriété : Unicité de l'élément neutre

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

Démonstration

$e = e \star e' = e'$ car e est neutre à gauche et e' est neutre à droite. □

Remarque

- **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.

Définition : Éléments symétrisables

Soit $\star$ une loi de composition interne sur E, admettant un élément neutre $e \in E$.
Un élément x de E est dit **symétrisable** pour $\star$ si on a $y \in E$ tel que $x \star y = y \star x = e$.

Définition - Propriété : Unicité du symétrique

Si $\star$ est une loi de composition interne associative sur E, alors pour tout $x \in E$ symétrisable, l'élément y de E tel que $x \star y = y \star x = e$ est unique et appelé **symétrique** de x pour $\star$ dans E.

Démonstration

Si y, y' conviennent, alors $y' = y' \star (x \star y) = (y' \star x) \star y = y$. □

Remarques

R 1 –
- **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 $y^{-1} \star x$?

R 2 – L'élément neutre e (lorsqu'il existe) est toujours symétrisable, de symétrique lui-même, car $e \star e = e$.

R 3 – Être symétrisable à gauche ou à droite ne suffit pas.

Exemple

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

- $\left(\exists g \in E^E,\ f\circ g = g\circ f = \mathrm{id}_E\right) \iff f$ bijective (ie inversible pour $\circ$).
- $\left(\exists g \in E^E,\ f\circ g = \mathrm{id}_E\right) \iff f$ surjective.
- $\left(\exists g \in E^E,\ g\circ f = \mathrm{id}_E\right) \iff f$ injective.

R 4 – Vu la démonstration, si on a un symétrique à gauche et un symétrique à droite, ils sont égaux et l'élément est symétrisable.

Propriété

Soit $\star$ une loi de composition interne associative sur E.
Si x et y sont symétrisables, alors

- *$x\star y$ l'est aussi. De plus, $\mathrm{sym}(x\star y) = \mathrm{sym}(y)\star\mathrm{sym}(x)$.*
- *$\mathrm{sym}(x)$ l'est aussi et $\mathrm{sym}(\mathrm{sym}(x)) = x$.*

Remarque

Avec des notations multiplicatives, $(x\cdot y)^{-1} = y^{-1}\cdot x^{-1}$ et $\left(x^{-1}\right)^{-1} = x$.

Démonstration

$(x\star y)\star(\mathrm{sym}(y)\star\mathrm{sym}(x)) = e$ par associativité, et de même $(\mathrm{sym}(y)\star\mathrm{sym}(x))\star(x\star y) = e$, d'où la conclusion, par unicité du symétrique.
Puis $\mathrm{sym}(x)\star x = x\star\mathrm{sym}(x) = e$. □

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

E 1 – $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ et $(\mathbb{C},+)$ sont des groupes commutatifs de neutre 0.
E 2 – Si D est un ensemble non vide, $\left(\mathbb{R}^D,+\right)$ et $\left(\mathbb{C}^D,+\right)$ 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 3 – $(\mathbb{Q}^*,\times)$, $(\mathbb{Q}_+^*,\times)$, $(\mathbb{R}^*,\times)$, $(\mathbb{R}_+^*,\times)$ et $(\mathbb{C}^*,\times)$ sont des groupes commutatifs de neutre 1.
E 4 – 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

Définition : Itérées d'un élément

Soir 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

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

R 2 – 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

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

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

Propriété

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. □

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 $\varphi_a : \left|\begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & a \star x \end{array}\right.$ *et* $\psi_a : \left|\begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & x \star a \end{array}\right.$ *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

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.

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

Exemple

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

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 $\left(G_1, \underset{1}{\star}\right), \ldots, \left(G_p, \underset{p}{\star}\right)$ avec pour tout $(x_1, \ldots, x_p)$ et $(y_1, \ldots, y_p)$ dans $G_1 \times \cdots \times G_p$,

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

5 Sous-groupes

a 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 $\left(H, \star|_{H^2}\right)$ 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 $\mathrm{sym}_H(x)\in H\subset G$ tel que $x\star\mathrm{sym}_H(x)=\mathrm{sym}_H(x)\star x=e_H=e_G$ et donc par unicité, x inversible dans G et $\mathrm{sym}_G(x)=\mathrm{sym}_H(x)$. □

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

(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

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 $\star$ (loi) 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 $(H,\star)$ est bien un sous-groupe de $(G,\star)$. □

Remarque

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

Exemples

E 1 – $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ sont des sous-groupes (additifs et abéliens) de $(\mathbb{C},+)$.

E 2 – $\mathbb{R}^D$ où $D \neq \varnothing$ est un sous-groupe additif abélien de $\left(\mathbb{C}^D,+\right)$.

E 3 – $\mathbb{Q}^*$, $\mathbb{Q}_+^*$, $\mathbb{R}^*$, $\mathbb{R}_+^*$, $\mathbb{U}$, $\mathbb{U}_n$ pour $n \in \mathbb{N}^*$ sont des sous-groupes multiplicatifs abéliens de $\left(\mathbb{C}^*,\times\right)$.
(On rappelle que $\mathbb{U} = \{z \in \mathbb{C},\ |z| = 1\}$ et pour $n \in \mathbb{N}^*$, $\mathbb{U}_n = \{z \in \mathbb{C},\ z^n = 1\} = \left\{e^{\frac{2ik\pi}{n}},\ k \in [\![0, n-1]\!]\right\}$.)

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 $\forall\, i \in I,\ \ H_i \subset G$.
- $(H_i)_{i\in I} \neq \varnothing$ 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

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 $(\mathbb{Z},+)$

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 $a\mathbb{Z}=\{\ldots,-2a,-a,0,a,2a,\ldots\}$, 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 $p\in G\cap\mathbb{N}^*\neq\varnothing$, 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

a Définition

Définition

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

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

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

E 1 – $\ln : \left(\mathbb{R}_+^*, \times\right) \to (\mathbb{R}, +)$ isomorphisme de groupes.

E 2 – $\exp : (\mathbb{R}, +) \to \left(\mathbb{R}_+^*, \times\right)$ isomorphisme de groupes.

E 3 – $\left|\begin{array}{ccc} (\mathbb{R}, +) & \longrightarrow & (\mathbb{U}, \times) \\ \theta & \longmapsto & \mathrm{e}^{\mathrm{i}\theta} \end{array}\right.$ morphisme de groupes (non injectif).

E 4 – 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

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

E 5 – $\det : (\mathcal{GL}(E), \circ) \to \left(\mathbb{R}^*, \times\right)$ et $\det : (\mathcal{GL}_n(\mathbb{K}), \times) \to \left(\mathbb{R}^*, \times\right)$ 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 $f : (G, \star) \to \left(G', \bullet\right)$ est un morphisme de groupes, alors $f(e_G) = e_{G'}$ et pour tout $x \in G$, $f\left(\mathrm{sym}(x)\right) = \mathrm{sym}(f(x))$.

Remarque

En notation multiplicative : $f\left(x^{-1}\right) = \left(f(x)\right)^{-1}$.
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, $f(e_G) = e_{G'}$.
$f(x) \bullet f(\mathrm{sym}(x)) = f\left(x \star \mathrm{sym}(x)\right) = f(e_G) = e_{G'}$
et $f(\mathrm{sym}(x)) \star f(x) = f\left(\mathrm{sym}(x) \star x\right) = f(e_G) = e_{G'}$ □

Propriété

En notation multiplicative, si $f : (G, \star) \to \left(G', \bullet\right)$ 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

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

b Noyau et image

Définition

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

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

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

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

Exemple

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

Propriété

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

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

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

Propriété

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 $f\left(e_G\right) = e_{G'} \in H'$.
  - ⋆ Si $x, x' \inf^{(-1)}(H')$, f étant un morphisme de groupes, $f\left(x \star x'^{-1}\right) = \underbrace{f(x)}_{\in H'} \bullet \underbrace{f(x')}_{\in H'}^{-1} \in H'$, donc $x \star x'^{-1} \in f^{(-1)}(H')$. □

Propriété

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

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

Exemples

E 1 – $f : \left|\begin{array}{ccc} (\mathbb{R}, +) & \longrightarrow & (\mathbb{C}^*, \times) \\ \theta & \longmapsto & \mathrm{e}^{\mathrm{i}\theta} \end{array}\right.$ 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 2 – $f : \left|\begin{array}{ccc} (\mathbb{C}^*, \times) & \longrightarrow & (\mathbb{C}^*, \times) \\ z & \longmapsto & z^n \end{array}\right.$ 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 $k \in \mathbb{Z} \mapsto \mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}}$.

E 3 – Si $(E, |)$ est un espace euclidien, le noyau du morphisme $\det : (\mathcal{O}(E), \circ) \mapsto (\{\pm 1\}, \times)$ est le groupe $\mathcal{SO}(E)$.

C Isomorphismes

Propriété

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

« 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

E 1 – $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$, $\left(\mathbb{C}^D,+,\times\right)$ et $\left(\mathbb{R}^D,+,\times\right)$ (avec $D \neq \varnothing$), $\left(\mathbb{C}^{\mathbb{N}},+,\times\right)$ et $\left(\mathbb{R}^{\mathbb{N}},+,\times\right)$ sont des anneaux commutatifs.

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

Remarques

R 1 – 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 2 – 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 3 – Si $A \neq \{0_1\}$, alors 0_A n'est pas inversible (pour $\times$).

R 4 – 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

E 1 – $U_{\mathbb{R}} = \mathbb{R}^*$

E 2 – $U_{\mathbb{Z}} = \{-1, 1\} \neq \mathbb{Z}^*$

E 3 – $U_{\mathbb{C}^{\mathbb{N}}} = \{\text{suites jamais nulles}\}$

E 4 – $U_{\mathbb{C}^D} = \{\text{fonctions jamais nulles}\}$

E 5 – $U_{\mathcal{M}_n(\mathbb{K})} = \mathcal{GL}_n(\mathbb{K})$

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. □

3 Calculs dans un anneau

Propriété

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

- *Si $a\times b=b\times a$,*
$$(ab)^n=a^nb^n.$$
- ***Formule du binôme de Newton** : Si $a\times b=b\times a$,*
$$(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^kb^{n-k}.$$
- ***Factorisation**[a] **de** a^n-b^n : Si $a\times b=b\times a$*
$$\begin{aligned}a^n-b^n&=(a-b)\left(a^{n-1}+a^{n-2}b+a^{n-3}b^2\ldots+ab^{n-2}+b^{n-1}\right)\\&=(a-b)\sum_{k=0}^{n-1}a^kb^{n-1-k}.\end{aligned}$$
- ***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,

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

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

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

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

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 $k \in [\![1,n]\!]$, $a_k \neq 0_A$, alors $a_1 \times \cdots \times a_n \neq 0_A$.

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 $a \neq 0_K$, 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 $\left(A_1, \underset{(1)}{+}, \underset{(1)}{\times}\right), \ldots, \left(A_p, \underset{(p)}{+}, \underset{(p)}{\times}\right)$ avec pour tout $(x_1, \ldots, x_p)$ et $(y_1, \ldots, y_p)$ dans $A_1 \times \cdots \times A_p$,

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

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

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

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

Définition : Sous-anneau

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

- $B \subset A$
- $1_A \in B$
- $\left(B, +|_{B^2}, \times|_{B^2}\right)$ 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 $\left(\begin{smallmatrix} a & 0 \\ 0 & 0 \end{smallmatrix}\right)$ 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 : Caractérisation des sous-anneaux

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

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

ou, de manière équivalente,

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

ou encore

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

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 $1_A \in B$. □

Exemples

E 1 – 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 2 – $\mathcal{T}_n^+(\mathbb{K})$ est un sous-anneau de $(\mathcal{M}_n(\mathbb{K}),+,\times)$

E 3 – 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 : 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 : 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,

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

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

Définition : 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

(MA1) $\forall\,(a,b) \in A^2,\ \ f(a+b) = f(a) \oplus f(b)$
(ie $f : (A,+) \to (A',\oplus)$ morphisme de groupes)

(MA2) $\forall\,(a,b) \in A^2,\ \ f(a \times b) = f(a) \otimes f(b)$

(MA3) $f(1_A) = 1_{A'}$

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

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

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

Remarques

R 1 – 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 2 – En général, $\operatorname{Ker} f$ n'est pas un sous-anneau de A. C'est un sous-groupe additif stable par multiplication.

Exemple

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

Propriété

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 : Morphisme de corps

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

Remarque

Avec (i) et (ii), $f\left(1_{\mathbb{K}}\right) = \left(f\left(1_{\mathbb{K}}\right)\right)^2$ et comme $\mathbb{K}'$ est intègre, $f\left(1_{\mathbb{K}}\right)$ 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

E 1 – $\mathrm{id}_{\mathbb{C}}$, $z \mapsto \overline{z}$ sont des automorphismes (involutifs) du corps $\mathbb{C}$.
E 2 – 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

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

E 1 – $2\mathbb{Z}$ est un idéal de $(\mathbb{Z},+,\times)$.
E 2 – 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 $f : (A,+,\times) \to (A',\oplus,\otimes)$ un morphisme d'anneau. 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

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

Exercice

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

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 $ax = ax_I + ay_I \in I+J$.
- $I+J$ 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

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 cœfficients 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 $(a) \cap (b) = \{$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 MPSI dans $\mathbb{Z}$.
Un avantage de cette définition du PGCD est de donner directement la relation de Bézout.
Nous détaillons la démarche ci-après dans le cas des polynômes et réviserons l'arithmétique sur $\mathbb{Z}$ en fin d'année.

IV ARITHMÉTIQUE SUR $\mathbb{K}[X]$

Dans cette partie, $\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$, comme, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

1 L'anneau $\mathbb{K}[X]$

Théorème

$(\mathbb{K}[X],+,\times)$ est un anneau commutatif et intègre.
Son groupe des inversibles est $U_{\mathbb{K}[X]} = \mathbb{K}_0[X] \setminus \{0\} = \{$polynômes constants non nuls$\}$.

Démonstration

- La structure d'anneau commutatif a été vue en classe de MPSI.
  L'élément neutre pour $+$ est le polynôme nul, celui pour $\times$ est le polynôme constant 1
- Si P est inversible pour $\times$, alors on a Q tel que $PQ = 1$ et alors $\deg P + \deg Q = 0$ donc $\deg P = \deg Q = 0$. La réciproque est bien sûr vraie, avec, pour $P = \lambda \neq 0$, $P^{-1} = \lambda^{-1} = \dfrac{1}{\lambda}$.
- Si $PQ = 0$ alors $\deg(PQ) = \deg P + \deg Q = -\infty$ donc $\deg P = -\infty$ ou $\deg Q = -\infty$, d'où l'intégrité. □

Corollaire

Si $P,Q \in \mathbb{K}[X]$, P et Q sont associés si et seulement s'il existe $\lambda \in \mathbb{K}^*$ tel que $P = \lambda Q$.

2 $\mathbb{K}[X]$ est un anneau euclidien

Théorème : Division euclidienne polynomiale

Soient $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. Alors il existe un unique couple $(Q,R) \in \mathbb{K}[X]$ tel que $A = BQ + R$ et $\deg R < \deg B$.

Remarque : Algorithme

C'est celui que l'on utilise en posant la division. On s'intéresse au terme de plus haut degré dans A que l'on compense en multipliant B par un monôme, et on recommence en soustrayant.

Exemple

Poser une division quelconque.

Démonstration

- **Existence** : Soit $d = \deg B$, $B = b_0 + \cdots + b_d X^d$ avec $b_d \neq 0$. Si $d = 0$, le couple $(A/b_0, 0)$ convient. Sinon, on raisonne par récurrence forte sur $n = \deg A$, $A = a_0 + \cdots + a_n X^n$.
  - ⋆ Si $n < d$, $(0, A)$ convient.
  - ⋆ Si le résultat est vrai pour tout polynôme de degré au plus $n-1$, alors on écrit $A = \dfrac{a_n}{b_d} X^{n-d} B + A_1$ avec $\deg A_1 \leqslant n-1$.
    Par hypothèse de récurrence, on a $(Q_1, R) \in \mathbb{K}[X]$ tels que $A = BQ_1 + R$ et $\deg R < \deg B$.
    Alors $\left(Q_1 + \dfrac{a_n}{b_d} X^{n-d}, R\right)$ convient.
- **Unicité** : Si (Q_1, R_1) et (Q_2, R_2) conviennent, alors $B(Q_1 - Q_2) = R_2 - R_1$. Vu les degrés, on en tire $Q_1 = Q_2$, puis $R_1 = R_2$. □

3 $\mathbb{K}[X]$ est anneau principal

Théorème

L'anneau $\mathbb{K}[X]$ est principal.

Démonstration

C'est un anneau intègre. Montrons que ses idéaux sont tous principaux.
Soit I un idéal de $\mathbb{K}[X]$.

- Si $I = \{0\}$ alors $I = 0\mathbb{K}[X] = (0)$.
- Sinon, l'ensemble $E = \{\deg P, P \in I, P \neq 0\}$ est une partie non vide de $\mathbb{N}$ donc admet un minimum. Soit $P_0 \in I$ réalisant ce minimum. On montre que $I = (P_0)$.
  - ⋆ On a déjà $P_0 \in I$ donc par définition d'un idéal, $(P_0) = P_0\mathbb{K}[X] \subset I$.
  - ⋆ Si, réciproquement, $P \in I$, effectuons la division euclidienne par P_0 : on a $(Q,R) \in \mathbb{K}[X]^2$ tel que $P = P_0Q + R$ et $\deg R < \deg P_0$.
    Alors $R = P - P_0Q \in I$ et $\deg R < \min E$ donc $R = 0$ et $P = P_0Q \in (P_0)$.

□

Remarque

Les idéaux de $\mathbb{Z}$ et $\mathbb{K}[X]$ sont donc principaux, c'est-à-dire engendré par un élément. Tous les générateurs sont associés.
Donc dans le cas d'un idéal non nul, quitte à choisir un générateur positif (dans $\mathbb{Z}$) ou unitaire (dans $\mathbb{K}[X]$) on a de plus unicité de celui-ci.

4 PGCD de deux polynômes

Définition : PGCD

Soient $A, B \in \mathbb{K}[X]$ non tous les deux nuls.
$I = (A) + (B) = A\mathbb{K}[X] + B\mathbb{K}[X] = \{AU + BV,\ U, V \in \mathbb{K}[X]\}$ est un idéal non réduit à zéro de $\mathbb{K}[X]$.
Son unique générateur unitaire est appelé pgcd de A et B, noté $A \wedge B$.

Remarque

La définition s'étend au cas où $A = B = 0$ en posant $A \wedge B = 0$ car $(0) + (0) = (0)$ même si alors, on ne peut plus dire que $A \wedge B$ est unitaire.

Propriété : Relation de Bézout

Si $A, B \in \mathbb{K}[X]$, on peut trouver $U, V \in \mathbb{K}[X]$ tels que $AU + BV = A \wedge B$.

Démonstration

$A \wedge B \in A \wedge B\mathbb{K}[X] = A\mathbb{K}[X] + B\mathbb{K}[X]$. □

Propriété : Caractérisation

Soit $(A, B) \neq (0, 0)$.

$$D = A \wedge B \iff \begin{cases} D \text{ est unitaire} \\ D|A \text{ et } D|B \\ \forall C \in \mathbb{K}[X],\ (C|A \text{ et } C|B) \Longrightarrow C|D \end{cases}$$

Il s'agit donc du plus grand diviseur unitaire au sens de la division.

Démonstration

($\Longrightarrow$) Si $D = A \wedge B$ alors D est unitaire et $AK[X] + B\mathbb{K}[X] = D\mathbb{K}[X]$ donc $A, B \in D\mathbb{K}[X]$ soit $D|A$ et $D|B$.
Et si $C|A$ et $C|B$, alors, comme on a $U, V \in \mathbb{K}[X]$ tels que $AU + BV = A \wedge B$, $C|A \wedge B$.

($\Longleftarrow$) Si D est un diviseur commun unitaire plus grand que tous les autres au sens de la division, alors D divise $AU + BV = A \wedge B$, et comme $A \wedge B$ est un diviseur commun, il divise D.
D et $A \wedge B$ étant associés et unitaires, ils sont égaux. □

Remarques

R 1 – Les diviseurs de D sont alors exactement les diviseurs communs à A et à B.

R 2 – Les racines des pgcd sont exactement les racines communes de A et B, de multiplicité le minimum des multiplicités.

Exercice

Soit $A = X^5 - X^4 + 2X^3 + 1$ et $B = X^4 - X^3 + 3X^2 - 2X + 2$.

1. À l'aide de l'algorithme d'Euclide, déterminer $D = A \wedge B$.
2. En déduire $(U, V) \in \mathbb{R}[X]^2$ tel que $AU + BV = D$.

Définition

$A, B \in \mathbb{K}[X]$ sont dits **premiers entre eux** lorsque $A \wedge B = 1$, c'est-à-dire lorsque les seuls diviseurs communs sont les polynômes constants non nuls.

Remarque

Lorsque c'est le cas, ils n'ont pas de racine commune dans $\mathbb{K}$. La réciproque est fausse.

Théorème : de Bézout

Soit $A, B \in \mathbb{K}[X]$.

$$A \wedge B = 1 \Longleftrightarrow \exists\, U, V \in \mathbb{K}[X],\quad AU + BV = 1$$

Démonstration

($\Longrightarrow$) Connu

($\Longleftarrow$) S'il existe $U, V \in \mathbb{K}[X]$ tel que $AU + BV = 1$, alors $1 \in (A \wedge B)$ donc $(A \wedge B) = \mathbb{K}[X] = (1)$. □

Corollaire

Soient $A, B, C \in \mathbb{K}[X]$.

(i) $A \wedge BC = 1 \Longleftrightarrow A \wedge B = A \wedge C = 1$

(ii) Si $D = A \wedge B$, *on a* $A_1, B_1 \in \mathbb{K}[X]$ *tels que* $A = DA_1$, $B = DB_1$ *et* $A_1 \wedge B_1 = 1$.

Remarque

(i) s'étend à un produit quelconque (fini) de polynômes.

Démonstration

□

Théorème : Lemme de Gauß

Soient $A, B, C \in \mathbb{K}[X]$.
Si $A|BC$ et $A \wedge B = 1$, alors $A|C$.

Démonstration

□

Propriété : Cas des polynômes scindés

*Si A ou B est **scindé**,*
$A \wedge B = 1 \iff A$ et B n'ont pas de racine commune.

Remarque

C'est toujours vrai si $\mathbb{K} = \mathbb{C}$.

Démonstration

- ($\Longrightarrow$) : Pas de facteur $(X - a)$ commun.
- ($\Longleftarrow$) : Si A et B n'ont pas de racine commune, un diviseur de A et de B, nécessairement constant ou scindé n'a pas de racine, donc est constant. □

5 PGCD d'une famille finie de polynômes

Soit $n \in \mathbb{N} \setminus \{0,1\}$.

Définition : pgcd de n polynômes

Soient $(A_1,\dots,A_n) \in (\mathbb{K}[X])^n \setminus \{(0,\dots,0)\}$. On note $D = A_1 \wedge A_2 \wedge \cdots \wedge A_n = \bigwedge_{k=1}^{n} A_k$ l'unique polynôme unitaire tel que $A_1\mathbb{K}[X] + \cdots + A_n\mathbb{K}[X] = D\mathbb{K}[X]$.

Remarques

R1 – Comme pour deux polynômes, il s'agit du plus grand diviseur commun unitaire au sens de la division (et aussi du degré).

R2 – La définition s'étend à $0 \wedge \cdots \wedge 0 = 0$.

Propriété

(i) ***Associativité*** *: $A \wedge B \wedge C = (A \wedge B) \wedge C = A \wedge (B \wedge C)$.*

(ii) Les diviseurs communs à $A_1,\dots,A_n$ sont exactement les diviseurs de $\bigwedge_{k=1}^{n} A_k$.

(iii) ***Relation de Bézout*** *: On a $U_1,\dots,U_n \in \mathbb{K}[X]$ tels que $A_1U_1 + \cdots A_nU_n = \bigwedge_{k=1}^{n} A_k$.*

Définition : Polynômes premiers entre eux dans leur ensemble

$A_1,\dots,A_n$ sont dits **premiers entre eux dans leur ensemble** lorsque $\bigwedge_{k=1}^{n} A_k = 1$, c'est-à-dire que le seul diviseur unitaire commun à tous les A_k est 1.

$A_1,\dots,A_n$ sont dits **premiers entre eux deux à deux** lorsque $\forall\, i \neq j,\ \ A_i \wedge A_j = 1$.

Propriété

Premiers entre eux deux à deux $\Longrightarrow$ premiers entre eux dans leur ensemble, mais la réciproque est fausse pour plus de deux polynômes.

Théorème : de Bézout

$A_1,\dots,A_n$ sont premiers entre eux dans leur ensemble si et seulement si on a $U_1,\dots,U_n$ tels que $A_1U_1 + \cdots + A_nU_n = 1$.

Propriété

Si $A_1,\dots,A_n$ sont premiers entre eux ***deux à deux*** *et divisent B, alors $A_1 \cdots A_n | B$.*

Remarque : Application

Si $x_1,\dots,x_n$ sont racines de P d'ordre au moins $m_1,\dots,m_n$ alors $(X-x_1)^{m_1}\cdots(X-x_n)^{m_n} \mid P$ car les $(X-x_i)^{m_i}$ sont premiers entre eux deux à deux (scindés sans racine commune).

6 Polynômes irréductibles

Définition : Polynôme irréductible

On appelle **polynôme irréductible** tout polynôme $P \in \mathbb{K}[X]$ **non constant** dont les seuls diviseurs sont les λ et λP pour $\lambda \in \mathbb{K}^*$, c'est-à-dire tels que $P = UV \Longrightarrow U$ ou V inversible.
Les autres polynômes sont dits **réductibles**.

Remarques

R 1 – Tout polynôme de degré 1 est irréductible.

R 2 – Les polynômes irréductibles de $\mathbb{C}[X]$ sont exactement les polynômes de degré 1 (d'après le théorème de d'Alembert - Gauß).

R 3 – Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 sans racine réelle (en passant par $\mathbb{C}$).

R 4 – Si P est irréductible dans $\mathbb{K}$ et $\deg P \geqslant 2$, P n'a pas de racine dans $\mathbb{K}$. La réciproque est fausse.

R 5 – P est réductible dans $\mathbb{K}[X]$ ss'il admet un diviseur Q tel que $0 < \deg Q < \deg P$.

Théorème : Décomposition en produit d'irréductibles

Tout $A \in \mathbb{K}[X] \setminus \{0\}$ s'écrit de manière unique à l'ordre des facteurs près sous la forme

$$A = \lambda P_1^{\alpha_1} \cdots P_k^{\alpha_k}$$

où $k \in \mathbb{N}$, $\lambda \in \mathbb{K}^*$, $P_1, \ldots, P_k$ irréductibles deux à deux distincts unitaires, $\alpha_1, \ldots, \alpha_k \in \mathbb{N}^*$.
Alors $\lambda = \operatorname{cd} A$, $P_1, \ldots, P_k$ sont les diviseurs irréductibles unitaires de A.

Démonstration

Comme dans $\mathbb{Z}$ pour l'unicité.
L'existence se démontre par récurrence sur $n = \deg A$.
Si $n = 0$ ou $n = 1$, c'est immédiat.
Si c'est vrai jusqu'au degré $n-1$, soit A est irréductible et il n'y a rien à faire d'autre que de factoriser le cœfficient dominant, soit ce n'est pas le cas, et on écrit $A = UV$ avec $\deg U < n$ et $\deg V < n$, on applique deux fois l'hypothèse de récurrence et celle-ci s'établit. □

Remarques

R 1 – La décomposition en irréductibles dans $\mathbb{C}$ redonne le fait que tout polynôme à cœfficient complexe est constant ou scindé. Elle est de la forme

$$P = \lambda (X - x_1)^{m_1} \cdots (X - x_n)^{m_n}.$$

R 2 – Les décompositions en irréductibles dans $\mathbb{R}[X]$ sont donc de la forme

$$P = \lambda (X - x_1)^{m_1} \cdots (X - x_n)^{m_n} \left(X^2 + a_1 X + b_1\right)^{\ell_1} \cdots \left(X^2 + a_k X + b_k\right)^{\ell_k}$$

avec pour tout i, $\Delta_k = a_k^2 - 4b_k < 0$.

R 3 – Pour décomposer en irréductibles dans $\mathbb{R}[X]$, on peut décomposer dans $\mathbb{C}[X]$ puis rassembler les $X - \alpha$ et $X - \overline{\alpha}$ si $\alpha \in \mathbb{C} \setminus \mathbb{R}$.

Exemples

E 1 – Décomposition en irréductibles de $X^n - 1$.

E 2 – Décomposition en irréductibles de $X^4 + 1$.

Propriété

Si $A = \lambda P_1^{\alpha_1} \cdots P_k^{\alpha_k}$ et $B = \mu P_1^{\beta_1} \cdots P_k^{\beta_k}$ décompositions en irréductibles (avec exposants éventuellement nuls), alors

$$A \wedge B = P_1^{\min(\alpha_1,\beta_1)} \cdots P_k^{\min(\alpha_k,\beta_k)}.$$

7 PPCM (Complément)

Définition

Le PPCM de deux polynômes A, B non nuls est l'unique générateur unitaire $A \vee B$ de l'idéal $A\mathbb{K}[X] \cap B\mathbb{K}[X]$ des multiples communs à A et à B.

On a donc $A\mathbb{K}[X] \cap B\mathbb{K}[X] = (A \vee B)\mathbb{K}[X]$.

On peut poser $0 \vee 0 = 0$.

Propriété

(i) Il s'agit du plus petit multiple unitaire commun à A et à B au sens de la division.

(ii) Si $A = \lambda P_1^{\alpha_1} \cdots P_k^{\alpha_k}$ et $B = \mu P_1^{\beta_1} \cdots P_k^{\beta_k}$ décompositions en irréductibles (avec exposant éventuellement nuls), alors

$$A \vee B = P_1^{\max(\alpha_1,\beta_1)} \cdots P_k^{\max(\alpha_k,\beta_k)}.$$

(iii) On a toujours que AB et $(A \wedge B)(A \vee B)$ sont associés (donc égaux à normalisation près).

V LA STRUCTURE D'ALGÈBRE

1 Algèbre et sous-algèbre

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

Exemples

E 1 – $(\mathbb{C}, +, \times, \cdot)$ est une $\mathbb{R}$-algèbre et une $\mathbb{C}$-algèbre.

E 2 – $\left(\mathbb{K}^X, +, \times, \cdot\right)$ est une $\mathbb{K}$-algèbre.

E 3 – $\left(\mathbb{K}^{\mathbb{N}}, +, \times, \cdot\right)$ est une $\mathbb{K}$-algèbre.

E 4 – $(\mathbb{K}[X], +, \times, \cdot)$ est une $\mathbb{K}$-algèbre.

E 5 – $(\mathbb{K}(X), +, \times, \cdot)$ est une $\mathbb{K}$-algèbre.

E 6 – Si E est un $\mathbb{K}$-espace vectoriel, $(\mathscr{L}(E), +, \circ, \cdot)$ est une $\mathbb{K}$-algèbre.

E 7 – 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 : 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

(SAl1) $\mathscr{B}\subset\mathscr{A}$

(SAl2) $1_A\in\mathscr{B}$

(SAl3) $\forall x,y\in\mathscr{B},\ \forall\lambda\in\mathbb{K},\ x+\lambda y\in\mathscr{B}$

(SAl4) $\forall x,y\in\mathscr{B},\ \forall\lambda\in\mathbb{K},\ x\times y\in\mathscr{B}$

Exemples

E 1 – $\mathbb{K}[X]$ est une sous-algèbre de $\mathbb{K}(X)$.

E 2 – $\mathscr{C}^k(I,\mathbb{K})$ est une sous-algèbre de $\mathbb{K}^I$.

E 3 – L'ensemble des suites convergentes est une sous-algèbre de $\mathbb{K}^{\mathbb{N}}$.

E 4 – 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

Si $P=a_0+a_1X+\cdots+a_nX^n\in\mathbb{K}[X]$ et $x\in\mathscr{A}$, on pose $P(x)=\sum_{k=0}^{n}a_kx^k=a_0 1_{\mathscr{A}}+a_1x+\cdots+a_nx^n$.

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

2 Morphismes d'algèbres

Définition : 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

(MAl1) f est linéaire ie, $\forall x,y\in\mathscr{A},\ \forall\lambda\in\mathbb{K},\ f(x+\lambda y)=f(x)+\lambda f(y)$

(MAl2) $\forall x,y\in\mathscr{A},\ f(x\times y)=f(x)\times f(y)$

(MAl3) $f(1_{\mathscr{A}})=1_{\mathscr{B}}$.

Exemples

E 1 – Si $X\neq\varnothing$, $\mathscr{A}$ une $\mathbb{K}$-algèbre, $a\in X$, alors $u_a:\left|\begin{array}{ccc}\mathscr{A}^X&\longrightarrow&\mathscr{A}\\ f&\longmapsto&f(a)\end{array}\right.$ est un morphisme de $\mathbb{K}$-algèbres. (morphisme d'évaluation).

E 2 – $f:\left|\begin{array}{ccc}\mathbb{K}[X]&\longrightarrow&\mathbb{K}[x]\\ P&\longmapsto&\tilde{P}\end{array}\right.$ 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 3 – $f:\left|\begin{array}{ccc}\mathbb{K}&\longrightarrow&\mathscr{M}_1(\mathbb{K})\\ x&\longmapsto&(x)\end{array}\right.$ est un isomorphisme de $\mathbb{K}$-algèbres.

Propriété

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 :

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

□

Remarque

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