Structures algébriques

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

$$\star : \left| \begin{array}{ccc} E\times E & \longrightarrow & E \\ (x,y) & \longmapsto & x\star y \end{array} \right. .$$

Définition : associativité, commutativité

Une loi de composition interne $\star$ sur un ensemble E 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

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

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.

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.

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* $\mathrm{sym}(\mathrm{sym}(x)) = x$.

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**.

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

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

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

Notation

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

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.

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.*

Corollaire

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

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

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

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.

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 $(G, \star)$.

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

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 $(G,\star)$.

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

Notation

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

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 $G \neq \{0\}$, $a = \min(G \cap \mathbb{N}^*)$.

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

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

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**.

Propriété

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

Propriété

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

Propriété

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

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

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

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

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

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* $\operatorname{Im} f = G'$.

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 $(G, \star)$.

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 $(G', \bullet)$.*

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 $(G, \star)$.

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

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

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.**

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.

Propriété : Groupe des inversibles

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

3 Calculs dans un anneau

Propriété

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

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

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 $+$.

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

Propriété

Soit $(A,+,\times)$ un anneau intègre, $n \in \mathbb{N}^*$ et $(a_1,\ldots,a_n) \in A^n$.
Si pour tout $k \in [\![1,n]\!]$, $a_k \neq 0_A$, alors $a_1 \times \cdots \times a_n \neq 0_A$.

Propriété

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

Propriété

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

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.

Propriété

Si $(A,+,\times)$ et $(B,+,\times)$ sont deux anneaux, alors $U_{A\times B}=U_A\times U_B$.
De plus, si $(a,b)\in U_{A\times B}$, alors $(a,b)^{-1}=(a^{-1},b^{-1})$.

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.

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

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

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,

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

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.

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.

Définition : 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.

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

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.

Propriété

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

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.

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.*

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.

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 $(a)\subset(b)$.

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 $b=qa$.

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$\}$.

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 $\deg R < \deg B$.

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

Théorème

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

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 $A \wedge B$.

Propriété : Relation de Bézout

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

Propriété : Caractérisation

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

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

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

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.

Théorème : de Bézout

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

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

Corollaire

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

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

(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 $A_1 \wedge B_1 = 1$.

Théorème : Lemme de Gauß

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

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.

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 $A_1\mathbb{K}[X] + \cdots + A_n\mathbb{K}[X] = D\mathbb{K}[X]$.

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 $\implies$ 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 $A_1 \cdots A_n | B$.*

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 $P = UV \implies U$ ou V inversible.

Les autres polynômes sont dits **réductibles**.

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 $k \in \mathbb{N}$, $\lambda \in \mathbb{K}^*$, $P_1, \dots, P_k$ irréductibles deux à deux distincts unitaires, $\alpha_1, \dots, \alpha_k \in \mathbb{N}^*$.

Alors $\lambda = \operatorname{cd} A$, $P_1, \dots, P_k$ sont les diviseurs irréductibles unitaires de A.

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

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

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

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

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

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

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

2 Morphismes d'algèbres

Définition : Morphisme d'algèbre

Soit $(\mathcal{A}, +, \times, \cdot)$, $(\mathcal{B}, +, \times, \cdot)$ et $f : \mathcal{A} \to \mathcal{B}$.

On dit que f est un **morphisme d'algèbres** lorsque

(MAl1) f est linéaire,

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

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