

Structures algébriques usuelles

Schéma du chapitre

- I) Structure de groupe
 - 1) Groupes
 - 2) Produit fini de groupes
 - 3) L'ensemble $\mathbb{Z}/n\mathbb{Z}$
 - 4) Sous-groupes
 - 5) Sous-groupe engendré par une partie
 - 6) Morphisme de groupes
 - 7) Groupes monogènes. Groupes cycliques
 - 8) Ordre d'un élément
- II) Structure d'anneau
 - 1) Rappels et compléments de SUP
 - 2) produit fini d'anneaux
 - 3) Sous-anneaux
 - 4) Morphisme d'anneaux
 - 5) Noyau et image d'un morphisme d'anneaux
 - 6) Sous-corps
 - 7) L'anneau $\mathbb{Z}/n\mathbb{Z}$
 - 8) Idéal d'un anneau commutatif
 - 9) Divisibilité dans un anneau commutatif intègre
 - 10) Théorème chinois
 - 11) Indicatrice d'Euler
 - 12) Théorème d'Euler
- III) Anneaux de polynômes à une indéterminée
 $\mathbb{K}$ est un sous-corps de $\mathbb{C}$
 - 1) Préambule
 - 2) Idéaux de l'anneau $\mathbb{K}[X]$
 - 3) PGCD de deux polynômes
 - 4) Irréductibles de $\mathbb{K}[X]$
- IV) Structure d'algèbre
 $\mathbb{K}$ est un sous-corps de $\mathbb{C}$
 - 1) Algèbre
 - 2) Sous-algèbre
 - 3) Morphisme d'algèbre

Structures algébriques usuelles

I) Structure de groupe

1) Groupes

La déf d'un groupe est vue au SUP.

Exemples de groupes :

- $\mathbb{R}, \mathbb{Z}, \mathbb{C}$ gr additifs neutre 0.
- $\mathbb{C}^*, \mathbb{R}^*,]0, +\infty[$ gr multiplicatifs de neutre 1.
- $\mathbb{U}, \mathbb{U}_n$
- $(S_E, \circ)$ et $(S_n, \circ)$
- $(GL(E), \circ)$ et $(GL_n(\mathbb{K}), \times)$, où E est $\mathbb{K}$ -espace vectoriel.

2) Produit fini de groupes

Soient $(G_1, *_1), \dots, (G_n, *_n)$ des groupes.

- loi produit définie sur le produit cartésien $G_1 \times \dots \times G_n$:

$$(x_1, \dots, x_n) * (y_1, \dots, y_n) = (x_1 *_1 y_1, \dots, x_n *_n y_n)$$

Prop :

Si $(G_1, *_1), \dots, (G_n, *_n)$ des groupes d'éléments neutres respectifs $e_1, \dots, e_n$, alors $G_1 \times \dots \times G_n$ est un groupe de neutre le n-uplet $(e_1, \dots, e_n)$.

Il est à noter que :

- si $(G_1, *_1), \dots, (G_n, *_n)$ sont abéliens alors $G_1 \times \dots \times G_n$ l'est aussi.
- L'inverse de $(x_1, \dots, x_n)$ est $(x_1, \dots, x_n)^{-1} = (x_1^{-1}, \dots, x_n^{-1})$

Exemples :

- $(\mathbb{C}, +)$ est un groupe, alors $(\mathbb{C}^n, +)$ est un groupe de neutre $(0, \dots, 0)$ pour la loi :

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n)$$

- $(\mathbb{C}, +)$ et $(\mathbb{C}^*, \times)$ sont des groupes. Alors $\mathbb{C} \times \mathbb{C}^*$ est un groupe pour la loi $\star$:

$$(a, b) \star (c, d) = (a + c, bd)$$

3) L'ensemble $\mathbb{Z}/n\mathbb{Z}$

Prop :

La congruence $\equiv$ est une relation d'équivalence sur $\mathbb{Z}$.

NB :

- $\bar{a}$, la classe d'équivalence de a, est donnée par :

$$\bar{a} = \{a + kn/k \in \mathbb{Z}\}$$

- $\bar{a} = \bar{b} \Leftrightarrow a \equiv b[n]$
- $\bar{a} = \bar{0} \Leftrightarrow n/a$, par exemple :

$$\forall k \in \mathbb{Z}, \overline{kn} = \overline{0};$$

$$\overline{n} = \overline{0}$$

Notation :

L'ensemble quotient de $\mathbb{Z}$ est noté $\mathbb{Z}/n\mathbb{Z}$.

NB :

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{a}/a \in \mathbb{Z}\}$$

Prop :

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \dots, \overline{n-1}\}$$

Par exemple :

$$\mathbb{Z}/2\mathbb{Z} = \dots \text{ et } \mathbb{Z}/4\mathbb{Z} = \dots$$

Prop :

$$\begin{cases} a \equiv b [n] \\ c \equiv d [n] \end{cases} \Rightarrow \begin{cases} a + c \equiv b + d [n] \\ ac \equiv bd [n] \end{cases}$$

Conséquences :

$$\text{i) } \begin{cases} \overline{a} = \overline{b} \\ \overline{c} = \overline{d} \end{cases} \Rightarrow \begin{cases} \overline{a+c} = \overline{b+d} \\ \overline{ac} = \overline{bd} \end{cases}$$

ii) Deux ici se définissent sur $\mathbb{Z}/n\mathbb{Z}$; la somme et le produit :

$$\overline{a+b} = \overline{a} + \overline{b} \text{ et } \overline{a \times b} = \overline{a} \times \overline{b}$$

Exemples :

On est dans $\mathbb{Z}/5\mathbb{Z}$. Complétons les deux tableaux suivants :

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$					
$\overline{1}$					
$\overline{2}$					
$\overline{3}$					
$\overline{4}$					

et

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$					
$\overline{1}$					
$\overline{2}$					
$\overline{3}$					
$\overline{4}$					

Prop :

$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien de neutre $\overline{0}$, et de cardinal n .

4) **Sous-groupes**

La déf et la caractérisation d'un sous-groupe sont vues au SUP.

NB :

$\{e\}$ et G sont des sous groupes triviaux de G .

Exemples :

- $\mathbb{U}$, $\mathbb{U}_n$ et $]0, +\infty[$ sont des sgr de $(\mathbb{C}^*, \times)$
- $O(n)$, l'ensemble des matrices orthogonale, est un ssgr de $(GL_n(\mathbb{R}), \times)$.
- $SO(n)$, l'ensemble des matrices orthogonales positives, est un ssgr de $O(n)$.
- $O(E)$, l'ensemble des isométries de E (càd endomorphismes orthogonaux de E), est un ssgr de $(GL(E), \circ)$; où E est un espace euclidien.
- $SO(E)$, l'ensemble des isométries directes, est un ssgr de $O(E)$

Prop :

Un ssgr est aussi un groupe.

Prop :

Les ssgr de $(\mathbb{Z}, +)$ sont exactement les $n\mathbb{Z}$ avec $n \in \mathbb{N}$; où $n\mathbb{Z} = \{nk/k \in \mathbb{Z}\}$

Prop :

L'intersection d'une famille de ssgr est un ssgr :

Si tous les F_i sont des ssgr de G , alors $\bigcap_{i \in I} F_i$ l'est aussi.

NB :

la réunion de 2 ssgr n'est en général pas un ssgr. Toutefois, on a :

$$H \cup K \text{ est un ssgr} \Leftrightarrow (H \subset K \text{ ou } K \subset H)$$

Démo : En exercice.

NB :

C'est le même résultat et la même démonstration pour les sous-espaces vectoriels; la réunion de deux sev n'est en général pas un sev. On a toutefois :

Soient H et K deux sev d'un $\mathbb{K}$ -esp vectoriel E .

$$H \cup K \text{ est un sev de } E \Leftrightarrow (H \subset K \text{ ou } K \subset H)$$

5) **Sous-groupe engendré par une partie**

$(G, \cdot)$ sera un groupe.

Déf :

Soit A une partie de G .

Le sous-groupe de G engendré par A est l'intersection de tous les sous-groupes de G contenant A .

On le note $\langle A \rangle$.

NB :

$$\langle A \rangle = \bigcap_{H \in I} H$$

où $I = \{H \text{ ssgr de } G/A \subset H\}$; l'ensemble des sous-groupes contenant A .

NB :

i) $\langle A \rangle$ est un sous-groupe de G (comme intersection de ssgrs)

ii) $\langle A \rangle$ contient A .

iii) Si K est un ssgr de G contenant A alors $\langle A \rangle \subset K$

iv) i), ii) et iii) se résument dans la proposition suivante :

Prop :

$\langle A \rangle$ est le plus petit sous-groupe de G contenant A .

Vocab :

Si $G = \langle A \rangle$, A est dite *partie génératrice* de G . On dit aussi que G est *engendré* par A .

– Ainsi A est une *partie génératrice* du groupe $\langle A \rangle$

Prop :

Soit A une partie d'un groupe $(G, \cdot)$.

Si tout élément de G s'écrit comme produit d'éléments de A alors A est une partie génératrice de G ; càd que G est engendré par A .

Par exemple :

a) S_n est engendré par les cycles.

b) S_n est engendré par les transpositions.

Rappel :

Toute permutation de S_n s'écrit comme produit de cycles (resp.transpositions).

Prop :

Soit $a \in G$.

$$\langle a \rangle = \{a^k / k \in \mathbb{Z}\}$$

Notation et vocabulaire :

Soit $a \in G$.

$\{a^k / k \in \mathbb{Z}\}$ se note aussi $\langle a \rangle$ et s'appelle *le sous-groupe engendré par a* .

NB :

Si $(G, +)$ est additif, on a

$$\langle a \rangle = \{ka / k \in \mathbb{Z}\}$$

Par exemple dans le groupe $(\mathbb{Z}, +)$, on a $\langle n \rangle = \{kn / k \in \mathbb{Z}\}$ qui se note $n\mathbb{Z}$.

NB :

Soient a et b deux éléments de G .

Si $ab = ba$ ou si G est commutatif, on a :

$$\langle \{a, b\} \rangle = \{a^p b^q / p, q \in \mathbb{Z}\}$$

6) **Morphisme de groupes****Déf :**

On appelle morphisme du groupe (G_1, T_1) vers le groupe (G_2, T_2) toute application f définie de G_1 vers G_2 vérifiant

$$\forall x, y \in G, f(xT_1y) = f(x)T_2f(y)$$

Vocabulaire :

i) Si f est un morphisme de G vers lui-même, on dit que f est un *endomorphisme* de G .

ii) Un morphisme bijectif est dit *isomorphisme*.

iii) Un endomorphisme bijectif de G est dit *automorphisme* de G .

iv) Deux groupes sont dits *isomorphes* s'il existe un isomorphisme entre eux.

Exemples :

- a) Soit $n \geq 2$.
L'application $z \mapsto z^n$ est un endomorphisme de $(\mathbb{C}^*, \times)$.
- b) L'application $z \mapsto |z|$ est un endomorphisme de $(\mathbb{C}^*, \times)$.
- c) L'application $\exp : z \mapsto e^z$ est un morphisme de $(\mathbb{C}, +)$ vers $(\mathbb{C}^*, \times)$.
- d) L'application $\ln : x \mapsto \ln x$ est un morphisme de $(\mathbb{R}^{+*}, \times)$ vers $(\mathbb{R}, +)$.
Il est clair alors que $(\mathbb{R}^{+*}, \times)$ et $(\mathbb{R}, +)$ sont isomorphes.
- e) i) L'application $\det : A \mapsto \det(A)$ est un morphisme de $(GL_n(\mathbb{K}), \times)$ vers $(\mathbb{K}^*, \times)$.
ii) L'application $\det : A \mapsto \det(A)$ est un morphisme de $(O(n), \times)$ vers $(\mathbb{R}^*, \times)$.
iii) L'application $\det : f \mapsto \det(f)$ est un morphisme de $(O(E), \circ)$ vers $(\mathbb{R}^*, \times)$, où E est un espace euclidien.
- f) Soit $a \in G$ fixé, où $(G, \cdot)$ est un groupe.
L'application $m \mapsto a^m$ est un morphisme du groupe $(\mathbb{Z}, +)$ vers le groupe $(G, \cdot)$.
- g) La *signature* est un morphisme du groupe $(S_n, \circ)$ vers le groupe $\{-1, 1\}$.

Prop :

- 1) La composée de deux morphismes (resp. endomorphismes) (resp. isomorphismes) est un morphisme (resp. endomorphisme) (resp. isomorphisme).
- 2) La réciproque d'un isomorphisme est un isomorphisme.

NB :

$(\text{Aut}(G), \circ)$ est un groupe ; où $\text{Aut}(G)$ est l'ensemble des automorphismes de G .

Exercice :

Soit $(G, \cdot)$ un groupe.

- a) Pour $a \in G$, notons τ_a l'application définie de G vers lui-même par

$$\tau : x \mapsto axa^{-1}$$

Montrer que τ_a est un automorphisme de G .

- b) Montrer que l'application $\Phi : a \mapsto \tau_a$ est un morphisme du groupe G vers le groupe $(\text{Aut}(G), \circ)$.

Prop

Soit f un morphisme du groupe G vers G' . Soient e et e' les éléments neutres respectifs. On a :

- 1) $f(e) = e'$
- 2) $\forall x \in G, f(x^{-1}) = f(x)^{-1}$
- 3) $\forall x \in G, \forall m \in \mathbb{Z}, f(x^m) = f(x)^m$

Prop :

L'image directe (resp.réciproque) d'un sous-groupe par un morphisme de groupes est un sous-groupe.

Définition et proposition : (Noyau et image d'un morphisme)

Soit f un morphisme du groupe G vers G' . Soit e' l'élément neutre de G' .

- 1) Le *noyau* de f est

$$\ker(f) = f^{-1}(\{e'\}) = \{x \in G / f(x) = e'\}$$

- 2) L'*image* de f est

$$\text{Im}(f) = f(G) = \{f(x) / x \in G\}$$

- 3) $\ker(f)$ et $\text{Im}(f)$ sont des sous-groupes resp de G et G' .

NB :

Résultats analogues à ceux pour une application linéaire ; où les images directes et réciproques de sev sont des sev, puis on déduit que le noyau et l'image sont des sev.

Exercice :

Considérons le morphisme de $(\mathbb{C}, +)$ vers $(\mathbb{C}^*, \times)$ défini par $\exp : z \mapsto e^z$. Montrer que

$$\text{Im}(\exp) = \mathbb{C}^* \text{ et } \ker(\exp) = 2\pi i\mathbb{Z}$$

Prop :

Soit f un morphisme du groupe G vers G' . Soit e le neutre de G .

- 1) f est injectif $\Leftrightarrow \ker(f) = \{e\}$
- 2) f est surjectif $\Leftrightarrow \text{Im}(f) = G'$

7) **Groupes monogènes. Groupes cycliques****Déf :**

- i) Un groupe G est dit *monogène* s'il existe un élément $a \in G$ tel que $G = \langle a \rangle$.
 a est dit dans ce cas *un générateur* de G .
- ii) Un groupe monogène fini est dit groupe *cyclique*.

Exemples :

- i) $(\mathbb{U}_n, \times)$ est cyclique et $e^{\frac{2\pi i}{n}}$ en est un générateur.
- ii) $(\mathbb{Z}, +)$ est monogène et 1 en est un générateur.
- iii) $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique et $\bar{1}$ en est un générateur.

NB :

Tout groupe monogène est commutatif.

La réciproque est en général fausse :

Contre-exemple :

$(\mathbb{C}, +)$ est commutatif mais non monogène (*Démo par l'absurde*)

Conséquence :

Pour $n \geq 3$, $(S_n, \circ)$ n'est pas cyclique.

Clé à retenir :

Soit H un sous-groupe de G . Soit $a \in G$. On a

$$\langle a \rangle \subset H \Leftrightarrow a \in H$$

Prop :

$\overline{m}$ est générateur de $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow m \wedge n = 1$

Démo :

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} = \langle \overline{m} \rangle &\Leftrightarrow \mathbb{Z}/n\mathbb{Z} \subset \langle \overline{m} \rangle \\ &\Leftrightarrow \langle \overline{1} \rangle \subset \langle \overline{m} \rangle \\ &\Leftrightarrow \overline{1} \in \langle \overline{m} \rangle \\ &\Leftrightarrow \exists k \in \mathbb{Z} \text{ tel que } \overline{1} = \overline{km} \\ &\Leftrightarrow \exists k, l \in \mathbb{Z} \text{ tels que } nl + km = 1 \\ &\Leftrightarrow m \wedge n = 1 \text{ (Bezout)} \end{aligned}$$

Prop :

1) Tout groupe monogène infini est isomorphe à $(\mathbb{Z}, +)$

2) Tout groupe cyclique de cardinal n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$

Démo :

Posons $G = \langle a \rangle$ et e son élément neutre. Considérons l'application suivante :

$$\begin{aligned} f : (\mathbb{Z}, +) &\rightarrow G \\ m &\mapsto a^m \end{aligned}$$

f est bien un morphisme de groupes surjectif.

i) Si f est injective. Alors f est un isomorphisme de groupes, et donc G est isomorphe à $(\mathbb{Z}, +)$.

ii) Si f n'est pas injective. Alors $\ker(f) = n\mathbb{Z}$ où $n \in \mathbb{N}^*$.

Signalons alors qu'on a :

$$a^k = e \Leftrightarrow n/k$$

Montrons que G est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

Considérons l'application naturelle suivante :

$$\begin{aligned} \Phi : \mathbb{Z}/n\mathbb{Z} &\rightarrow G \\ \overline{k} &\mapsto a^k \end{aligned}$$

Φ est un isomorphisme, en effet :

a) Φ est une application injective, en effet :

$$\begin{aligned}\bar{k} = \bar{l} &\Leftrightarrow n/(k-l) \\ &\Leftrightarrow a^{k-l} = e \\ &\Leftrightarrow a^k = a^l \\ &\Leftrightarrow \Phi(k) = \Phi(l)\end{aligned}$$

b) Φ est surjective par construction.

c) Φ est clairement un morphisme de groupes

Conclusion : Φ est un isomorphisme.

8) **Ordre d'un élément**

Déf :

Soit $(G, \cdot)$ un groupe de neutre e . Soit $a \in G$.

1) a est dit *d'ordre fini* si et seulement s'il existe $n \in \mathbb{N}^*$ tel que $a^n = e$

2) Dans ce cas, *l'ordre de a* est le plus petit entier $n \in \mathbb{N}^*$ vérifiant $a^n = e$.

Cas d'un groupe additif $(G, +)$:

1) a est dit *d'ordre fini* si et seulement s'il existe $n \in \mathbb{N}^*$ tel que $na = 0$

2) Dans ce cas, *l'ordre de a* est le plus petit entier n vérifiant $na = 0$.

Exemples :

1) Dans $(\mathbb{Z}/6\mathbb{Z}, +)$, on a $o(\bar{1}) = 6$, $o(\bar{2}) = 3$, $o(\bar{3}) = 2$.

2) Dans $(\mathbb{Z}, +)$, tout élément $p \in \mathbb{Z}^*$ n'est d'ordre fini.

3) Dans un groupe $(G, \cdot)$ quelconque de neutre e , on a :

i) $o(e) = 1$

ii) On a même l'équivalence

$$o(x) = 1 \Leftrightarrow x = e$$

4) Dans $(\mathbb{C}^*, \times)$, on a :

i) $o(i) = 4$

ii) $o\left(e^{\frac{2\pi i}{n}}\right) = n$

iii) 2015 n'est pas d'ordre fini.

5) Dans $(G, \cdot)$ quelconque de neutre e . Si on a $o(a) = n$ alors On a :

i) $a^n = e$

ii) $\forall k \in \mathbb{Z}, a^{nk} = e$

En général, on a :

Prop :

Supposons $o(a) = n$, on a :

1) $a^k = e \Leftrightarrow n/k$

$$2) a^k = a^l \Leftrightarrow n/(k-l) \Leftrightarrow k \equiv l[n]$$

Démo :

$$1) a^k = e \Leftrightarrow n/k, \text{ en effet :}$$

($\Leftarrow$) OK

($\Rightarrow$) Supposons $a^k = e$.

La division euclidienne de k par n implique l'existence de $(q, r) \in \mathbb{Z}^2$ tel que

$$k = nq + r \text{ et } 0 \leq r < n$$

On a :

$$k = nq + r \Rightarrow a^r = e$$

$$\Rightarrow r = 0 \text{ par définition de } r$$

$$\Rightarrow k = nq$$

2) Vient de 1)

Prop

Si $o(a)=n$ alors $\langle a \rangle$, le sous-groupe engendré par a , est de cardinal n .

On a précisément : $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$

Prop

Supposons que G est un groupe fini et $\text{card}(G)=n$. Alors on a :

$$1) \forall a \in G, a^n = e$$

2) Tout élément a de G est d'ordre fini, et on a $o(a)/n$

Démo :

Le programme se limite à la démonstration dans le cas commutatif.

1) Soit $a \in G$.

$$\text{On a } \prod_{x \in G} x = \prod_{x \in G} ax \text{ car } \{ax/x \in G\} = G.$$

$$\text{D'où } \prod_{x \in G} x = a^n \prod_{x \in G} x$$

$$\text{Et donc } a^n = e$$

2) Vient de 1)

II) Structure d'anneau

1) Rappels et compléments de SUP

Les notions suivantes sont déjà vues au SUP, *revoyez-les* :

Anneau-Anneau intègre-Corps-Élément inversible dans un anneau-Calcul dans un anneau

Rappelons ici quelques points importants :

Exemples d'anneaux :

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{K}[X], \mathbb{K}(X), M_n(\mathbb{K}), (L(E), +, \circ), F(X, \mathbb{K})$ en particulier $\mathbb{K}^{\mathbb{N}}$

Calcul dans un anneau :

$(A, +, \times)$ un anneau et $a, b \in A$ tels que $\mathbf{ab=ba}$. On a :

- i. $(ab)^n = a^n b^n$
- ii. $(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$: **Binôme de Newton**
- iii. $a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^k b^{n-1-k}$: **Egalité de Bernoulli**

Prop :

$(U(A), \times)$, l'ensemble des éléments inversibles de A , est un groupe.

NB :

$U(A)$ se note aussi $A^\times$.

$U(A)$ s'appelle le *groupe des unités* de A .

Exemples d'éléments inversibles :

- i. L'anneau $(M_n(\mathbb{K}), +, \times)$:
 $U(M_n(\mathbb{K})) = GL_n(\mathbb{K})$ et $(GL_n(\mathbb{K}), \times)$ est le groupe de ses éléments inversibles. C'est en fait le *groupe linéaire d'ordre n*
- ii. L'anneau $(\mathbb{K}, +, \times)$:
 $U(\mathbb{K}) = \mathbb{K}^*$ et $(\mathbb{K}^*, \times)$ est le groupe de ses éléments inversibles.
- iii. L'anneau $(\mathbb{Z}, +, \times)$:
 $U(\mathbb{Z}) = \{-1, 1\}$ et $(\{-1, 1\}, \times)$ est le groupe de ses éléments inversibles.

Prop :

Dans un anneau intègre, on a

$$ab = 0 \Leftrightarrow (a = 0 \text{ ou } b = 0)$$

Exemples d'anneaux intègres :

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{K}[X], \mathbb{K}(X)$

Exemples d'anneaux non intègres :

- 1) $M_2(\mathbb{R})$, car $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ et les deux matrices sont non nulles.
 - 2) $\mathbb{Z}/8\mathbb{Z}$, car $\bar{2} \times \bar{4} = \bar{0}$ et les deux éléments sont non nuls.
 - 3) $(\mathbb{R}^{\mathbb{R}}, +, \times)$. Donner deux fonctions convenables.
- (En exo chez-vous)

Déf :

a est *nilpotent* si et ss'il existe $n \in \mathbb{N}^*$ tel que $a^n = 0$

L'indice de nilpotence de a est le plus petit entier p tel que $a^p = 0$

Exemples :

- Dans $\mathbb{Z}/8\mathbb{Z}$, $\bar{2}^3 = \bar{0}$ et $\bar{2}$ est nilpotent d'indice 3.
- Dans $M_2(\mathbb{R})$, $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = 0$; ainsi $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ est nilpotent d'indice 2.

Exercice :

Soit a un élément nilpotent d'indice $n \in \mathbb{N}^*$. Montrer que $(1 - a)$ est inversible et préciser $(1 - a)^{-1}$ en fonction des puissances de a .

Exemples de corps :

$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{K}(X)$, le corps des fractions rationnelles à coefficients dans $\mathbb{K}$

NB :

- i. Tout corps est intègre.
- ii. Un anneau est par définition *unitaire*
- iii. Un corps est par définition *commutatif*

2) Produit fini d'anneaux

Soient $(A_1, +, \times), \dots, (A_n, +, \times)$ des anneaux.

Considérons les deux lois $+$ et $\times$ définies naturellement sur le produit cartésien $A_1 \times \dots \times A_n$ par

$$\begin{cases} (a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n) \\ (a_1, \dots, a_n) \times (b_1, \dots, b_n) = (a_1 \times b_1, \dots, a_n \times b_n) \end{cases}$$

Prop :

- 1) $(A_1 \times \dots \times A_n, +, \times)$ est un anneau et que

$$0_{A_1 \times \dots \times A_n} = (0_{A_1}, \dots, 0_{A_n}) \text{ et } 1_{A_1 \times \dots \times A_n} = (1_{A_1}, \dots, 1_{A_n})$$

- 2) $(a_1, \dots, a_n)$ est inversible $\Leftrightarrow a_1, \dots, a_n$ le sont.

Dans ce cas $(a_1, \dots, a_n)^{-1} = (a_1^{-1}, \dots, a_n^{-1})$

- 3) $U(A_1 \times \dots \times A_n) = U(A_1) \times \dots \times U(A_n)$

- 4) *En particulier*, si $(A, +, \times)$ est un anneau, alors $(A^n, +, \times)$ l'est aussi et on

$$U(A^n) = (U(A))^n$$

Par exemple :

- 1) Considérons l'anneau $(\mathbb{C}^2, +, \times)$, on a $U(\mathbb{C}^2) = (\mathbb{C}^*)^2$

- 2) Dans l'anneau $(\mathbb{Z}^2, +, \times)$ on a $U(\mathbb{Z}^2) = \{-1, 1\}^2 = \{(1, 1), (-1, -1), (-1, 1), (1, -1)\}$

3) Sous-anneaux**Déf :**

Soit $(A, +, \times)$ un anneau. Soit B une partie de A .

B est dite *sous-anneau* de A si et ssi

$$\begin{cases} a) 1 \in B \\ b) \forall x, y \in B, x - y \in B \\ c) \forall x, y \in B, x \times y \in B \end{cases}$$

NB :

— Il faut vérifier que 1 qui est dans B , n'est pas 0 ;

—un sous-anneau contient par définition 1.

Prop :

Un sous-anneau est à son tour un anneau.

Exercice d'application :

Les ensembles suivants sont-ils des anneaux ?

- 1) L'ensemble des suites réelles convergentes.
- 2) L'ensemble des suites réelles convergentes vers zéro.
- 3) $2\mathbb{Z}$
- 4) $\mathbb{Z}[i] = \{a + bi/a, b \in \mathbb{Z}\}$. Il s'appelle ¹

4) **Morphisme d'anneaux**

Déf :

Soit f une application définie d'un anneau A vers un anneau B .

f est dite *morphisme d'anneaux* si et ssi

- 1) $f(1)=1$
- 2) $\forall x, y \in A, f(x + y) = f(x) + f(y)$
- 3) $\forall x, y \in A, f(x \times y) = f(x) \times f(y)$

Vocabulaire :

- 1) Un morphisme d'anneaux *bijectif* est dit *isomorphisme* d'anneaux.
- 2) Deux anneaux sont dits *isomorphes* s'il existe un morphisme d'anneaux entre eux.

Prop :

- 1) La *composée* de deux morphismes d'anneaux est un morphisme d'anneaux.
- 2) La *composée* de deux isomorphismes d'anneaux est un isomorphisme d'anneaux.
- 3) La *reciproque* d'un isomorphisme d'anneaux est un isomorphisme d'anneaux.

Prop :

Soit f un morphisme d'anneaux de A vers B . On a :

- 1) $f(0)=0$
- 2) $\forall x \in A, \forall n \in \mathbb{N}, f(x^n) = (f(x))^n$
- 3) $\forall x \in A, \forall m \in \mathbb{Z}, f(mx) = mf(x)$
- 4) Si $x \in A$ est inversible alors son image $f(x)$ l'est aussi, et on a $(f(x))^{-1} = f(x^{-1})$

5) **Noyau et image d'un morphisme d'anneaux**

Déf :(noyau et image) ²

Soit f un morphisme d'anneaux de A vers B .

1. anneau de Gauss

2. Mêmes définitions que pour un morphisme de groupes ou application linéaire.

1) *Le noyau* de f :

$$\ker(f) = \{x \in A / f(x) = 0\} = f^{-1}\{0\}$$

2) *L'image* de f :

$$\operatorname{Im}(f) = \{f(x) / x \in A\} = f(A)$$

Prop :

Soit f un morphisme d'anneaux de A vers B . On a :

1) $\operatorname{Im}(f)$ est un sous-anneau de B

2) f est injective $\Leftrightarrow \ker(f) = \{0\}$

3) f est surjective $\Leftrightarrow \operatorname{Im}(f) = B$

NB :

$\ker(f)$ n'est en général pas un sous-anneau de A . En fait, il sera un **idéal** ; voir plus tard.

6) **Sous-corps**

Déf :

Soit $(K, +, \times)$ un corps. Soit B une partie de K .

B est dite *sous-corps* de K si et ssi

$$\left\{ \begin{array}{l} a) 1 \in B \\ b) \forall x, y \in B, x - y \in B \\ c) \forall x, y \in B, x \times y \in B \\ d) \forall x \in B \setminus \{0\}, x^{-1} \in B \end{array} \right.$$

Prop : Un sous-corps est à son tour un corps.

Exemples : $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$

7) **L'anneau $\mathbb{Z}/n\mathbb{Z}$**

Prop : Soit $n \geq 2$.

1) $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif de neutres $\bar{0}$ et $\bar{1}$

2) $\bar{m}$ est inversible dans $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow m \wedge n = 1$

3) $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps $\Leftrightarrow p$ est un nombre premier

Démo :

1) OK

2) On a :

$$\begin{aligned} \bar{m} \text{ est inversible dans } \mathbb{Z}/n\mathbb{Z} &\Leftrightarrow \exists u \in \mathbb{Z} \text{ tel que } \bar{m} \times \bar{u} = \bar{1} \\ &\Leftrightarrow \exists u, v \in \mathbb{Z} \text{ tels que } mu + nv = 1 \\ &\Leftrightarrow m \wedge n = 1 \text{ (Bezout)} \end{aligned}$$

3) $(\Rightarrow)$

Supposons que $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps. Vérifions que p est

premier.

Raisonnons par l'absurde et supposons que p n'est pas premier.

Alors il existe $n, k \in \mathbb{N}$ tels que $p = nk$ et $2 \leq n, k \leq p-1$

D'où $\bar{n} \times \bar{k} = \bar{0}$ (dans $\mathbb{Z}/p\mathbb{Z}$)

Or $\bar{k}$ et $\bar{n}$ sont inversibles dans le corps $\mathbb{Z}/p\mathbb{Z}$ car non nuls.

Alors leur produit, qui est $\bar{0}$ est aussi inversible. Ce qui est absurde.

($\Leftarrow$)

Soit $\bar{m} \neq \bar{0}$. Montrons que $\bar{m}$ est inversible dans l'anneau $\mathbb{Z}/p\mathbb{Z}$.

On a

$$\begin{aligned}\bar{m} \neq \bar{0} &\Leftrightarrow p \nmid m \\ &\Leftrightarrow p \wedge m = 1 \\ &\Leftrightarrow \bar{m} \text{ est inversible}\end{aligned}$$

Exercice : (Résolution de l'équation $\bar{a} \times \bar{x} = \bar{b}$)

Résoudre dans $\mathbb{Z}$ les équations suivantes :

1) $6x + 5 \equiv 0 \pmod{13}$

2) $6x \equiv 2 \pmod{8}$

3) $6x \equiv 3 \pmod{8}$

8) Idéal d'un anneau commutatif

$(A, +, \times)$ sera dans ce paragraphe un anneau commutatif de neutre 1.

Déf : Soit $I \subset A$.

I est un *idéal* de A si et ssi les trois conditions suivantes sont satisfaites :

- 1) $0 \in I$
- 2) $\forall x, y \in I, x + y \in I$
- 3) $\forall x \in I, \forall y \in A, x \times y \in I$

NB :

- a) $\forall x \in I, -x \in I$ (vient de 3))
- b) I est un sous-groupe de $(A, +)$
- c) $\{0\}$ et A sont des idéaux de A

Prop :

- 1) Les idéaux de $(\mathbb{Z}, +, \times)$ sont les $n\mathbb{Z}$.
- 2) Soit I un idéal de A . On a

$$I = A \Leftrightarrow 1 \in I$$

- 3) Le noyau d'un morphisme d'anneaux est un idéal.
- 4) L'intersection de deux idéaux est un idéal.

- 5) La somme de deux idéaux est un idéal ; avec la notation naturelle suivante

$$I + J = \{x + y/x \in I \text{ et } y \in J\}$$

N.B : Soient I et J deux idéaux de A.

- 1) $I \cap J$ est le plus grand idéal de A contenu dans I et J.
- 2) $I + J$ est le plus petit idéal de A contenant I et J.

Prop et déf : Soit $a \in A$.

- 1) $aA = \{ax/x \in A\}$ est un idéal de A.
 - 2) aA s'appelle *l'idéal engendré par a*.
 - 3) aA est le plus petit idéal de A contenant a.
- 9) **Divisibilité dans un anneau commutatif intègre**
 ($A, +, \times$) sera dans ce paragraphe un anneau commutatif intègre.

Déf : Soient $a, b \in A$

- 1) a *divise* b si et ss'il existe $c \in A$ tel que $b = ca$.
- 2) On note $a|b$

Propriétés immédiates : Soient $a, b, c \in A$.

- 1) $1|a, a|a, a|0$
- 2) $a|b \Leftrightarrow b \in aA \Leftrightarrow bA \subset aA$
- 3) $(a|b \text{ et } a|c) \Rightarrow a|(b + c)$
- 4) $(a|b \text{ et } b|c) \Rightarrow a|c$

Déf : a et b sont dits *associés* si et ssi $a|b$ et $b|a$

Prop : Les assertions suivantes sont équivalentes

- 1) a et b sont associés
- 2) $aA = bA$
- 3) $\exists u \in U(A) / a = bu$
- 4) $\exists v \in U(A) / b = av$

NB :

- 1) L'association est une relation d'équivalence sur A.
- 2) Soient $a, b \in \mathbb{Z}$. On a

$$a \text{ et } b \text{ sont associés} \Leftrightarrow |a| = |b| \Leftrightarrow a = \pm b$$

- 3) Soient $P, Q \in \mathbb{K}[X]$. On a

$$P \text{ et } Q \text{ sont associés} \Leftrightarrow \exists \lambda \in \mathbb{K}^*, P = \lambda Q$$

10) **Théorème chinois****Prop :**(Théorème chinois)

Si $m \wedge n = 1$ alors $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes par l'isomorphisme naturel

$$\begin{aligned} \mathbb{Z}/mn\mathbb{Z} &\rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \bar{k} &\mapsto (\hat{k}, \tilde{k}) \end{aligned}$$

Démo :Notons $f : \bar{k} \mapsto (\hat{k}, \tilde{k})$

f est bien une application (facile)

f est un morphisme d'anneaux (facile)

f est injective, en effet :

$$\begin{aligned} f(\bar{k}) = (\hat{0}, \tilde{0}) &\Rightarrow \hat{k} = \hat{0} \text{ et } \tilde{k} = \tilde{0} \\ &\Rightarrow m|k \text{ et } n|k \\ &\Rightarrow mn|k \text{ (car } m \wedge n = 1) \\ &\Rightarrow \bar{k} = \bar{0} \end{aligned}$$

Enfin f est bijective puisque l'ensemble de départ et celui d'arrivée ont le même cardinal mn .

Résolution des systèmes de congruence de type

$$\begin{cases} x \equiv a \ [m] \\ x \equiv b \ [n] \end{cases}$$

où x l'inconnue dans $\mathbb{Z}$, a, b, m et n des entiers de $\mathbb{Z}$ avec $m \wedge n = 1$ Notons (Σ) ce système $\begin{cases} x \equiv a \ [m] \\ x \equiv b \ [n] \end{cases}$ **Résumé de la résolution :**

- 1) On trouve un couple $(u, v) \in \mathbb{Z}^2$ vérifiant la relation de Bezout $mu + nv = 1$.
- 2) $x_0 = a(nv) + b(mu)$ est bien une solution particulière de (Σ)
- 3) La solution générale de (Σ) est de la forme

$$x = x_0 + kmn \text{ avec } k \in \mathbb{Z}$$

Exercice d'application :Résoudre dans $\mathbb{Z}$ les systèmes suivants :

- 1) $\begin{cases} x \equiv 2 \ [6] \\ x \equiv 3 \ [11] \end{cases}$
- 2) $\begin{cases} x \equiv 2 \ [6] \\ x \equiv 3 \ [11] \\ x \equiv 4 \ [7] \end{cases}$

$$3) \begin{cases} 8x \equiv 4 \pmod{10} \\ 9x \equiv 3 \pmod{21} \end{cases}$$

11) **Indicatrice d'Euler****Déf :** (Fonction indicatrice d'Euler)C'est l'application $\varphi : \mathbb{N}^* \rightarrow \mathbb{N}^*$ définie par

$$\varphi(n) = \text{card}(\{1 \leq k \leq n \mid k \wedge n = 1\})$$

Exemples : $\varphi(8) = \dots; \varphi(p) = \dots$ où p est un nombre premier.**Prop :** $\varphi(n)$ est le nombre de générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$, et c'est aussi le nombre d'éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.**Prop :**

1) $m \wedge n = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$

2) $\varphi(p^r) = p^r - p^{r-1}$, où p un nombre premier et $r \in \mathbb{N}^*$.

3) Si $n = \prod_{i=1}^s p_i^{r_i}$ est la décomposition de n en facteurs premiers

$$\text{alors } \varphi(n) = n \prod_{i=1}^s \left(1 - \frac{1}{p_i}\right)$$

Démo :

1) $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes alors

$$\underbrace{\text{card}(U(\mathbb{Z}/mn\mathbb{Z}))}_{=\varphi(mn)} = \text{card}(U(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}))$$

Or $U(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) = U(\mathbb{Z}/m\mathbb{Z}) \times U(\mathbb{Z}/n\mathbb{Z})$

$$\text{Alors } \text{card}(U(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})) = \underbrace{\text{card}(U(\mathbb{Z}/m\mathbb{Z}))}_{=\varphi(m)} \times \underbrace{\text{card}(U(\mathbb{Z}/n\mathbb{Z}))}_{=\varphi(n)}$$

D'où $\boxed{\varphi(mn) = \varphi(m)\varphi(n)}$

2) Notons $A = \{1 \leq k \leq p^r \mid k \wedge p^r = 1\}$

Il s'agit de montrer que $\text{card}(A) = p^r - p^{r-1}$

Il est clair que $\text{card}(A) = p^r - \text{card}(\{1 \leq k \leq p^r \mid k \wedge p^r \neq 1\})$

On a $k \wedge p^r = 1 \Leftrightarrow k \wedge p = 1 \Leftrightarrow p \nmid k$

$$\text{D'où } \text{card}(A) = p^r - \underbrace{\text{card}(\{1 \leq k \leq p^r \mid p \mid k\})}_{=p^{r-1}}$$

car le nombre de multiples de p compris entre 1 et p^r est p^{r-1}

3) On a :

$$\begin{aligned}
 \varphi(n) &= \varphi\left(\prod_{i=1}^s p_i^{r_i}\right) = \prod_{i=1}^s \varphi(p_i^{r_i}) \\
 &= \prod_{i=1}^s p_i^{r_i} \left(1 - \frac{1}{p_i}\right) \\
 &= \prod_{i=1}^s p_i^{r_i} \times \prod_{i=1}^s \left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^s \left(1 - \frac{1}{p_i}\right)
 \end{aligned}$$

Exemple : $\varphi(72) = \dots$

12) **Théorème d'Euler**

Prop : (Théorème d'Euler)

$$a \wedge n = 1 \Rightarrow a^{\varphi(n)} \equiv 1 [n]$$

Démo :

$$\begin{aligned}
 a \wedge n = 1 &\Rightarrow \bar{a} \in U(\mathbb{Z}/n\mathbb{Z}) \\
 &\Rightarrow \bar{a}^{\varphi(n)} = \bar{1} \text{ car } \text{card}(U(\mathbb{Z}/n\mathbb{Z})) = \varphi(n) \\
 &\Rightarrow a^{\varphi(n)} \equiv 1 [n]
 \end{aligned}$$

Corollaire :

Soit p un nombre premier. On a :

$$a \not\equiv 0 [p] \Rightarrow a^{p-1} \equiv 1 [p]$$

Démo :

$$\begin{aligned}
 a \not\equiv 0 [p] &\Rightarrow p \nmid a \\
 &\Rightarrow a \wedge p = 1 \text{ car } p \text{ premier} \\
 &\Rightarrow a^{\varphi(p)} \equiv 1 [p] \text{ (thm d'Euler)} \\
 &\Rightarrow a^{p-1} \equiv 1 [p] \text{ car } p \text{ premier}
 \end{aligned}$$

III) **Anneaux de polynômes à une indéterminée**

$\mathbb{K}$ sera un sous-corps de $\mathbb{C}$, par exemple $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$

1) **Préambule :**

- $(K[X], +, \times)$ est un anneau *commutatif intègre* de neutres 0 et 1. Ainsi, on peut parler de divisibilité et d'association.
- Les éléments inversibles de l'anneau $(K[X], +, \times)$ sont les polynômes constants non nuls ; càd

$$U(K[X]) = K^*$$

- P et Q sont *associés* $\Leftrightarrow \exists \lambda \in K^* / Q = \lambda P$

- On a aussi la division euclidienne tout comme vue au sup.

2) **Idéaux de l'anneau $\mathbb{K}[X]$**

Prop :

I est un idéal de $(K[X], +, \times)$ si et ssi I est de la forme $AK[X]$

Démo :

1) Si I est de la forme $AK[X]$ alors c'est un idéal de $K[X]$, car c'est l'idéal engendré par A .

2) Réciproquement, soit I un idéal de $K[X]$.

Montrons qu'il est de la forme $AK[X]$.

Cas 1 : Si $I = \{0\}$, c'est évident, avec $A=0$.

Cas 2 : Si $I \neq \{0\}$.

Soit $A \in I \setminus \{0\}$ de degré minimal. On a $I = AK[X]$, en effet :

a) Pour $AK[X] \subset I$. C'est clair car I idéal contenant A .

b) Pour $I \subset AK[X]$:

Soit $P \in I$. Montrons que $P \in AK[X]$

Par division euclidienne de P par A on obtient

$$P = AQ + R \text{ avec } \deg(R) < \deg(A)$$

On a $R = \underbrace{P - AQ}_{\in I}$ donc $R \in I$

Ainsi $R \in I$ et $\deg(R) < \deg(A)$

Alors par définition de A , R est nul, et donc $P = AQ$ et par suite $P \in AK[X]$.

Prop :

Soit I est un idéal **non nul** de $(K[X], +, \times)$.

1) Il existe un **unique** polynôme **unitaire** A_0 tel que $I = A_0\mathbb{K}[X]$.

2) A_0 est de degré **minimal** parmi les polynômes **non nuls** de I .

3) **PGCD de deux polynômes**

Théorème et définition :

Soient A et $B \in \mathbb{K}[X]$ non nuls. Il existe un unique polynôme unitaire $D \in \mathbb{K}[X]$ tel que

$$A.\mathbb{K}[X] + B.\mathbb{K}[X] = D.\mathbb{K}[X]$$

D s'appelle le PGCD de A et B , et se note $D = A \wedge B$

NB :

Supposons $D = A \wedge B$. On a alors :

$$D|A, D|B, \text{ et si } (C|A, C|B) \text{ alors } C|D$$

Prop : $D = A \wedge B \Rightarrow (\exists U, V \in \mathbb{K}[X] \text{ tels que } D = AU + BV)$

NB :

On définit d'une manière analogue le PGCD de plusieurs polynômes.

Déf :

A et B sont dits premiers entre eux si et ssi $A \wedge B = 1$.

Autrement dit :

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

Prop :

Si $a \neq b$ alors $(X - a)$ et $(X - b)$ sont premiers entre eux.

Prop :

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

Prop : (théorème de Gauss)

$(A|BC \text{ et } A \wedge B = 1) \Rightarrow A|C$

NB :

La recherche des coefficients de Bezout se fait de la même manière que pour les entiers relatifs.

4) **Irréductibles de $\mathbb{K}[X]$**

La définition d'un polynôme irréductible dans $\mathbb{K}[X]$ est la même que celle vue au sup.

Les polynômes de degré 1 sont irréductibles dans $\mathbb{K}[X]$.

On a de même encore la décomposition d'un polynôme non constant en produit de facteurs irréductibles :

$$P = \alpha \prod_{i=1}^n P_i^{r_i}$$

où les P_i sont unitaires, irréductibles et distincts deux à deux.

Et que cette décomposition est unique à ordre près.

On rappelle que les polynômes irréductibles dans $\mathbb{C}[X]$ sont ceux de degré 1. Et les polynômes irréductibles dans $\mathbb{R}[X]$ sont ceux de degré 1 et ceux de degré 2 à discriminant strictement négatif.

IV) **Structure d'algèbre**

$\mathbb{K}$ est un sous-corps de $\mathbb{C}$

1) **Algèbre**

Déf : $(A, +, \cdot, \times)$ est une **K-algèbre** si et ssi les conditions suivantes sont satisfaites :

a) $(A, +, \cdot)$ est un K-espace vectoriel.

b) $(A, +, \times)$ est un anneau.

c) $\forall x, y \in A, \forall \lambda, \mu \in K, (\lambda x) \times (\mu y) = (\lambda \mu)(x \times y)$

Exemples usuels d'algèbres :

$(K[X], +, \cdot, \times), (L(E), +, \cdot, \circ), (M_n(K), +, \cdot, \times), (F(X, K), +, \cdot, \times)$

2) **Sous-algèbre****Déf :**Soit $B \subset A$, où $(A, +, \cdot, \times)$ est une algèbre. B est une *sous-algèbre* de A si et ssi

$$\begin{aligned} 1 &\in B \\ \forall x, y \in B, \forall \lambda \in K, (\lambda x + y) &\in B \\ \forall x, y \in B, x \times y &\in B \end{aligned}$$

Prop :Toute sous-algèbre est une algèbre (pour les lois héritées de A)3) **Morphisme d'algèbre****Prop :**Soient A et B deux algèbres et $f : A \mapsto B$ une application. f est dite *morphisme d'algèbres* si et ssi

$$\begin{aligned} f(1) &= 1 \\ \forall x, y \in A, \forall \lambda \in K, f(\lambda x + y) &= \lambda f(x) + f(y) \\ \forall x, y \in A, f(x \times y) &= f(x) \times f(y) \end{aligned}$$

Prop :Soient A et B deux algèbres et $f : A \mapsto B$ un morphisme d'algèbres.1) $Im(f)$ est une *sous-algèbre* de B .2) $Ker(f)$ est un *idéal* de A .