Structures algébriques usuelles : rappels et compléments

Lundi 3 novembre 2025

Table des matières

Table des matières

1. Rappels sur les groupes et les anneaux

1.1. Structure de groupe

1.1. Structure de groupe

Definition 1

On dit qu'un ensemble $(G, *)$ est un *groupe* lorsque :

- $*$ est une loi de composition interne associative sur G
- $(G, *)$ possède un élément neutre (nécessairement unique) e : $\forall x \in G, \ e * x = x * e = x$
- Tout élément $x \in G$ possède un symétrique $y \in G$ (nécessairement unique) pour $*$: $x * y = y * x = e$.

Si $*$ est commutative, on dit que $(G, *)$ est un groupe *commutatif* ou *abélien*

Remarques :

- ...

1.1. Structure de groupe

Proposition 1

Étant donnés deux groupes $(G_1, *_1)$ et $(G_2, *_2)$ d'éléments neutres e_1 et e_2, la *loi produit* $*$ définie sur $G_1 \times G_2$ par :

$$(x_1, x_2) * (y_1, y_2) = (x_1 *_1 y_1, x_2 *_2 y_2)$$

confère à $G_1 \times G_2$ une structure de groupe, avec pour élément neutre (e_1, e_2). $G_1 \times G_2$ est appelé *groupe produit*.

Remarque :

Se généralise à n groupes. En particulier, si G est un groupe, G^n aussi (exemples : $\mathbb{Z}^n$, $\mathbb{R}^n$, etc ...).

1.2. Sous-groupes et morphismes de groupes

1.2. Sous-groupes et morphismes de groupes

Definition 2

Soit $(G, *)$ un groupe d'élément neutre e. On dit qu'une partie H de G est un sous-groupe de G lorsque :

- $e \in H$
- H est stable pour $*$: pour tout $x, y \in H$, on a $x * y \in H$
- H est stable par symétrisation : pour tout $x \in H$, on a $x^{-1} \in H$.

Remarque :

...

Proposition 2

Si H est un sous-groupe de $(G, *)$ d'élément neutre e, alors la loi induite par $*$ sur H (notée encore $*$) est une loi de composition interne et $(H, *)$ est un groupe d'élément neutre e.

1.2. Sous-groupes et morphismes de groupes

Proposition 3

Une partie H de $\mathbb{Z}$ est un sous groupe de $(\mathbb{Z}, +)$ **ssi** il existe $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.

Exercice 1

Soit H un sous-groupe de $(\mathbb{R}, +)$. Montrer que l'une **ou** l'autre des deux situations suivantes se présente :

- H est dense dans $\mathbb{R}$
- Il existe $\alpha \geqslant 0$ tel que $H = \alpha\mathbb{Z}$.

1.2. Sous-groupes et morphismes de groupes

Definition 3

Soient $(G, *)$ et $(G', *')$ deux groupes d'éléments neutre e et e'. On appelle *morphisme de groupes* de G dans G', toute application f de G dans G' qui vérifie :

$$\forall (x, y) \in G^2, \quad f(x * y) = f(x) *' f(y).$$

Remarques :

- ...

1.2. Sous-groupes et morphismes de groupes

Proposition 4

Soit $(G, *)$ et $(G', *')$ deux groupes d'éléments neutre e et e', et soit $f : G \to G'$ un morphisme.

- Si H est un sous-goupe de G, $f(H)$ est un sous-groupe de G'. En particulier $f(G)$ est un sous-groupe de G' appelé *image* de f et noté $\mathrm{Im}(f)$. On a $\mathrm{Im}(f) = G'$ **ssi** f est surjectif.
- Si H' est un sous-groupe de G', $f^{-1}(H')$ est un sous-groupe de G. En particulier $f^{-1}(\{e'\})$ est un sous-groupe de G appelé *noyau* de f et noté $\mathrm{Ker}(f)$. On a $\mathrm{Ker}(f) = \{e\}$ **ssi** f est injectif.

1.3. Structure d'anneau

1.3. Structure d'anneau

Definition 4

Soit A un ensemble muni de deux lois de composition internes $+$ et $\times$. On dit que $(A, +, \times)$ est un *anneau* lorsque :

- $(A, +)$ est un groupe commutatif,
- $\times$ est associative.
- A possède un élément neutre 1_A pour $\times$.
- $\times$ est distributive par rapport à $+$.

On dit que l'anneau est commutatif si $\times$ est commutative.

Remarques :

- ...

Proposition 5

Étant donnés deux anneaux A_1 et A_2, On peut munir l'ensemble produit $A_1 \times A_2$ de deux lois $+$ et $\times$:

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$$

$$(x_1, x_2) \times (y_1, y_2) = (x_1 \times y_1, x_2 \times y_2)$$

Cela confère à $A_1 \times A_2$ une structure d'anneau, avec pour éléments neutres additifs et multiplicatifs $(0, 0)$ et $(1, 1)$. $A_1 \times A_2$ est appelé *anneau produit*.

Remarque :

Se généralise à n anneaux.

1.4. Sous-anneaux et morphismes d'anneaux

1.4. Sous-anneaux et morphismes d'anneaux

Definition 5

On appelle *sous-anneau* d'un anneau $(A, +, \times)$ un sous-groupe de $(A, +)$ qui est stable par $\times$ et qui contient 1_A. Muni des lois induites, un sous-anneau est un anneau.

Definition 6

Soient $(A, +, \times)$ et $(B, +, \times)$ deux anneaux. On dit que $f : A \to B$ est un *morphisme d'anneau* si :

1. $\forall (x, y) \in A^2, \quad f(x + y) = f(x) + f(y)$,
2. $\forall (x, y) \in A^2, \quad f(x \times y) = f(x) \times f(y)$
3. $f(1_A) = 1_B$.

Remarques :

- ...

Exercice 2

Déterminer les endomorphismes de $\mathbb{Z}$:

a) En tant que groupe pour $+$

b) En tant qu'anneau pour $+$ et $\times$.

1.5. Anneau intègre et corps, groupe des inversibles

Definition 7

On dit qu'un anneau A est *intègre* lorsqu'il est non nul, commutatif, et qu'il vérifie :

$$\forall a, b \in A, \quad ab = 0 \Rightarrow a = 0 \text{ ou } b = 0$$

Remarques :

- Tout $a \neq 0$ est *régulier* :

$$ax = ay \Rightarrow x = y \qquad \text{et} \qquad xa = ya \Rightarrow x = y$$

- a inversible $\Rightarrow$ a régulier. Réciproque fausse.

Exemples :

$\mathbb{Z}$, $\mathbb{K}[X]$ sont intègres, $\mathcal{M}_n(\mathbb{K})$ non.

Exercice 3

Montrer qu'une matrice $A \in \mathcal{M}_n(\mathbb{K})$ est inversible **ssi** elle est régulière dans $\mathcal{M}_n(\mathbb{K})$.

1.5. Anneau intègre et corps, groupe des inversibles

Proposition 6

L'ensemble $A^\times$ des éléments inversibles de A est un groupe pour la loi $\times$.

Definition 8

L'ensemble $A^\times$ s'appelle *groupe des inversibles*, ou encore *groupe des unités* de A. On peut le noter aussi $U(A)$.

Exemples :

- $\mathbb{Z}^\times =$
- $\mathbb{K}[X]^\times =$
- $\mathcal{M}_n(\mathbb{K})^\times =$

Definition 9

Un anneau A est un *corps* lorsque c'est un anneau non nul, commutatif, et dans lequel tout élément non nul est inversible. On a alors $A^\times = A^* = A\backslash\{0\}$.

Exemples :

$\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{K}(X)$.

1.6. Structure de $\mathbb{Z}/n\mathbb{Z}$

1.6. Structure de $\mathbb{Z}/n\mathbb{Z}$

Definition 10

Soit $n \in \mathbb{N}$. On dit que a est *congru à b modulo n* lorsque $a - b \in n\mathbb{Z}$. On note alors $a \equiv b \quad [n]$.

Proposition 7

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

Definition 11

Pour $n \in \mathbb{N}$, on note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence pour la relation de congruence modulo n.
Pour $k \in \mathbb{Z}$, on note $\overline{k}$ (ou $\dot{k}$) la classe de k pour cette relation.

1.6. Structure de $\mathbb{Z}/n\mathbb{Z}$

Proposition 8

Pour $n \in \mathbb{N}^*$, $\mathbb{Z}/n\mathbb{Z}$ est un ensemble fini de cardinal n, et on a :

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

Remarque :

Cas $n = 0$?

1.6. Structure de $\mathbb{Z}/n\mathbb{Z}$

Proposition 9

La relation de congruence modulo n sur $\mathbb{Z}$ est compatible avec sa structure d'anneau :

- Si $a_1 \equiv b_1$ et $a_2 \equiv b_2$, $a_1 + a_2 \equiv b_1 + b_2$
- Si $a \equiv b$, $-a \equiv -b$.
- si $a_1 \equiv b_1$ et $a_2 \equiv b_2$, alors $a_1 a_2 \equiv b_1 b_2$

Definition 12

Soit $n \in \mathbb{N}$. Pour tout $u, v \in \mathbb{Z}/n\mathbb{Z}$:

$$u + v = \overline{a + b}, \quad \text{où} \quad u = \bar{a} \text{ et } v = \bar{b},$$

$$uv = \overline{ab}, \quad \text{où} \quad u = \bar{a} \text{ et } v = \bar{b},$$

ce qui ne dépend pas des représentants a et b choisis dans $\mathbb{Z}$.

1.6. Structure de $\mathbb{Z}/n\mathbb{Z}$

Proposition 10

Muni de l'addition définie ci-dessus, $\mathbb{Z}/n\mathbb{Z}$ est un groupe commutatif d'élément neutre $\overline{0}$.
L'application $\phi : k \mapsto \overline{k}$ est un morphisme de surjectif de groupes, de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$, appelé *surjection canonique*, et de noyau $n\mathbb{Z}$.

Exemples :

- Pour $n = 0$, ϕ est un isomorphisme : $\mathbb{Z}/0\mathbb{Z} \simeq \mathbb{Z}$.
- Pour $n = 1$, on a $\mathrm{Ker}(\phi) = \mathbb{Z}$ et $\mathbb{Z}/1\mathbb{Z} = \{\overline{0}\}$ est le groupe trivial à un seul élément.
- Pour $n = 2$, on a $\mathrm{Ker}(\phi) = 2\mathbb{Z}$ (ensemble des entiers pairs) et $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$: il s'agit de l'unique groupe à 2 éléments, à isomorphisme près.

Exercice 4

Soit $f : \mathbb{Z} \to \mathbb{Q}^*$ défini par $f(k) = (-1)^k$.

a) Montrer que f définit un morphisme de groupes de $(\mathbb{Z}, +)$ vers $(\mathbb{Q}^*, \times)$

b) Déterminer $\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$.

c) Montrer que $\mathrm{Im}(f) \simeq \mathbb{Z}/2\mathbb{Z}$.

1.6. Structure de $\mathbb{Z}/n\mathbb{Z}$

Proposition 11

Muni de l'addition et de la multiplication précedemment définies, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif d'éléments neutres $\overline{0}$ et $\overline{1}$. L'application $\phi : k \mapsto \overline{k}$ est un morphisme surjectif d'anneaux, de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$, appelé *surjection canonique*, et de noyau $n\mathbb{Z}$.

Remarque :

Cas $n = 0$ et $n = 1$?

Table des matières

2. Compléments sur les groupes

2.1. Sous-groupe engendré par une partie

Proposition 12

Toute intersection de sous-groupes de G est un sous-groupe de G.

Definition 13

Soit $A \subset G$.

- on appelle *sous-groupe engendré* par A l'intersection de tous les sous-groupes de G contenant A. On le note $\langle A \rangle$.
- On dit que A est une *partie génératrice* de G lorsque $\langle A \rangle = G$.

Remarques :

- ...

2.1. Sous-groupe engendré par une partie

Exemples :

- Le sous-groupe engendré par e est le sous-groupe trivial $\{e\}$.
- Dans le groupe $(\mathbb{Z}, +)$, si $n \in \mathbb{N}^*$, alors $\langle n \rangle = n\mathbb{Z}$.
- En particulier, 1 est un générateur de $\mathbb{Z}$.
- L'ensemble $\mathcal{T}$ des transpositions de $[\![1, n]\!]$ est une partie génératrice du groupe symétrique S_n.
- L'ensemble des matrices de $\mathcal{M}_n(\mathbb{K})$ associées à des opérations élémentaires (dilatation, transvection, permutation) est une partie génératrice de $GL_n(\mathbb{K})$.
- L'ensemble des réflexions d'un espace euclidien E est une partie génératrice du groupe orthogonal $O(E)$ (voir chapitre ultérieur).

2.2. Groupes engendrés par un élément

2.2. Groupes engendrés par un élément

Proposition 13

Si $a \in G$, le sous-groupe de G engendré par a est :

$$\langle a \rangle = \{a^k, k \in \mathbb{Z}\} \quad \text{ou} \quad \langle a \rangle = \{k\,a, k \in \mathbb{Z}\} \quad \text{(en notation additive)}$$

Definition 14

- On dit que G est un groupe *monogène* lorsqu'il est engendré par un seul élément : il existe $a \in G$ tel que $G = \langle a \rangle$.
- On dit que G est un groupe *cyclique* lorsqu'il est monogène et fini.

Tout élément a qui engendre G est appelé un *générateur*.

Exemples :

$(\mathbb{Z}, +)$, $(\mathbb{Z}/n\mathbb{Z}, +)$.

2.2. Groupes engendrés par un élément

Proposition 14

Supposons G monogène. Alors :

- Si G est infini, $G \simeq \mathbb{Z}$.
- Si G est fini de cardinal n, $G \simeq \mathbb{Z}/n\mathbb{Z}$.

Exercice 5

Soit $n \in \mathbb{N}^*$. Montrer que l'ensemble $\mathbb{U}_n$ des racines n-ièmes de l'unité est un groupe cyclique, isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Remarques :

- $\mathbb{U}_n$ est le noyau du morphisme : $z \to z^n$.
- $\mathbb{U}_n$ est aussi un sous-groupe de $\mathbb{U}$, lui-même sous-groupe de $(\mathbb{C}^*, \times)$.

2.3. Ordre d'un élément d'un groupe

2.3. Ordre d'un élément d'un groupe

Definition 15

Soit $a \in G$. Si le sous-groupe $\langle a \rangle$ est fini, on appelle *ordre* de a le cardinal de $\langle a \rangle$. On dit sinon que a est d'ordre infini.

Remarque :

L'ordre de a est le plus petit entier n tel que $a^n = e$.

Proposition 15

Si a est d'ordre fini d alors pour tout $n \in \mathbb{Z}$, $a^n = e \Leftrightarrow d|n$.

Proposition 16

Si G est un groupe fini, alors tout élément de G est d'ordre fini, et son ordre divise $\mathrm{card}(G)$.

Exercice 6

a) Déterminer l'ordre de $(\overline{1}, \overline{1})$ dans le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, et en déduire qu'il s'agit d'un groupe cyclique.

b) Montrer que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (appelé groupe de Klein) n'est pas cyclique.

c) montrer que $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est cyclique **ssi** m et n sont premiers entre eux.

Table des matières

3. Complément sur les anneaux

3.1. Idéal d'un anneau commutatif

Definition 16

Une partie I de A est appelé un *idéal* lorsque :

- $(I, +)$ est un sous-groupe de $(A, +)$
- Pour tout $a \in I$ et tout $x \in A$, $ax \in I$.

Exercice 7

Soit I un idéal de A. Montrer que $I = A$ **ssi** $I \cap A^\times \neq \emptyset$.

Proposition 17

Le noyau d'un morphisme $f : A \to B$ d'anneaux est un idéal de A.

3.2. Idéal engendré par un élément

3.2. Idéal engendré par un élément

Proposition 18

Soit $a \in A$. L'ensemble $aA = \{ax,\ x \in A\}$ est un idéal de A. On dit que c'est l'*idéal engendré* par a.
Un idéal engendré ainsi par un seul élément est appelé un idéal *principal*.

Definition 17

On dit qu'un idéal I est *principal* lorqu'il est engendré par un seul élément, *i.e* lorsqu'il existe $a \in A$ tel que $I = aA$.

3.2. Idéal engendré par un élément

Proposition 19

Si I est un idéal de $\mathbb{Z}$, il existe un unique $n \in \mathbb{N}$ tel que $I = n\mathbb{Z}$.

Remarques :

- on dit que $\mathbb{Z}$ est un anneau *principal*.
- n et $-n$ sont les deux générateurs de $n\mathbb{Z}$

3.2. Idéal engendré par un élément

Proposition 20

Si I est un idéal de $\mathbb{K}[X]$, il existe un unique $P \in \mathbb{K}[X]$ unitaire tel que $I = P\mathbb{K}[X]$.

Remarques :

- $\mathbb{K}[X]$ est un anneau principal.
- Les générateurs de $P\mathbb{K}[X]$ sont les λP, avec $\lambda \in \mathbb{K}^*$.

3.3. Compléments sur $\mathbb{Z}/n\mathbb{Z}$

Proposition 21

Soit $n \in \mathbb{N}^*$ et $k \in \mathbb{Z}$.

- $\overline{k}$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ **ssi** k est premier avec n.
- $\overline{k}$ est inversible dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ **ssi** k est premier avec n.

Corollaire 1

$\mathbb{Z}/p\mathbb{Z}$ est un corps **ssi** p est premier. On note alors ce corps $\mathbb{F}_p$.

Exercice 8

Déterminer les inverses des éléments non nuls du corps $\mathbb{F}_{17}$.

3.4. Divisibilité dans un anneau intègre

3.4. Divisibilité dans un anneau intègre

Definition 18

Étant donnés a et b non nuls dans A, on dit que a *divise* b et on note $a \mid b$ lorsqu'il existe $c \in A$ tel que $b = ac$.

Proposition 22

Soient $a, b \in A \backslash \{0\}$. Alors $a \mid b$ **ssi** $bA \subset aA$.

Proposition 23

Les trois assertions suivantes sont équivalentes :

(i) $a \mid b$ et $b \mid a$.

(ii) $aA = bA$

(iii) Il existe $u \in A^\times$ tel que $b = ua$

Dans ces conditions, on dit que a et b sont *associés*.

Exemples :

- dans l'anneau $\mathbb{Z}$, a et b sont associés **ssi** $a = \pm b$.
- dans l'anneau $\mathbb{K}[X]$, P et Q sont associés **ssi** il existe $\lambda \in \mathbb{K}^*$, tel que $P = \lambda Q$.

3.4. Divisibilité dans un anneau intègre

Definition 19

Un élément $p \in A$ non nul est dit *irréductible* lorsque :

- $p \notin A^{\times}$
- Pour tout $a, b \in A$, $p = ab \Rightarrow a \in A^{\times}$ ou $b \in A^{\times}$.

Autrement dit, un élément irréductible n'est pas inversible et ses seuls diviseurs sont ses associés ou les inversibles.

Exemples :

- Cas de $\mathbb{Z}$:
- Cas de $\mathbb{K}[X]$:

3.5. Décomposition en facteurs irréductibles

3.5. Décomposition en facteurs irréductibles

Theoreme 1

(de décomposition en facteurs premiers dans $\mathbb{Z}$)
Soit $n \in \mathbb{Z}$ avec $|n| \geqslant 2$. Il existe alors $k \in \mathbb{N}^*$, $p_1, \ldots, p_k \in \mathbb{N}$ premiers et deux à deux distincts, et $m_1, \ldots, m_k \in \mathbb{N}^*$ tels que

$$n = \pm p_1^{m_1} \cdots p_k^{m_k}$$

Cette décomposition est unique à l'ordre des facteurs près.

Remarque :

$\nu_{p_i}(n) = m_i$ est la *valuation* p_i-adique de n.

Exemple :

$-6600 =$

3.5. Décomposition en facteurs irréductibles

Theoreme 2

(de décomposition en facteurs irréductibles dans $\mathbb{K}[X]$)
Soit $P \in \mathbb{K}[X]$ avec $\deg(P) \geqslant 1$. Il existe alors $a \in \mathbb{K}^*$, $k \in \mathbb{N}^*$, $P_1, \ldots, P_k \in \mathbb{K}[X]$ unitaires irréductibles deux à deux distincts et $m_1, \ldots, m_k \in \mathbb{N}^*$ tels que

$$P = aP_1^{m_1} \cdots P_k^{m_k}$$

Cette décomposition est unique à l'ordre des facteurs près.

Remarques :

- ...

3.5. Décomposition en facteurs irréductibles

Theoreme 3

(de d'Alembert-Gauss)
Tout polynôme de $\mathbb{C}[X]$ non constant admet au moins une racine.

Corollaire 2

- Les éléments irrédutibles de $\mathbb{C}[X]$ sont les polynômes de degré 1 ;
- Tout polynôme $P \in \mathbb{C}[X]$ est scindé : il existe $a \in \mathbb{K}^*$, $k \in \mathbb{N}^*$, $\lambda_1, \dots, \lambda_k \in \mathbb{C}$ deux à deux distincts et $n_1, \dots, n_k \in \mathbb{N}^*$ tels que

$$P = a(X - \lambda_1)^{m_1} \cdots (X - \lambda_k)^{m_k}$$

Cette décomposition est unique à l'ordre des facteurs près.

Remarque :

m_i est la *multiplicité* de la racine λ_i

Exercice 9

a) Montrer que tout polynôme $P \in \mathbb{R}[X]$ de degré impair admet au moins une racine réelle.

b) En déduire que les polynômes irréductibles de $\mathbb{R}[X]$ sont ceux de degré 1 et ceux de degré 2 à discriminant strictement négatif.

c) Expliciter le théorème de decomposition en facteurs irréductibles dans $\mathbb{R}[X]$.

Exercice 10

Déterminer la décomposition de $X^4 - X^2 - 2$ en facteurs irréductibles dans $\mathbb{K}[X]$ suivant que $\mathbb{K}$ est le corps $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, et $\mathbb{Q}[i] = \mathbb{Q} + i\mathbb{Q}$.

Table des matières

4. Algèbres

4.1. Définition

4.1. Définition

Definition 20

On appelle $\mathbb{K}$-*algèbre*, ou *algèbre* sur $\mathbb{K}$, tout quadruplet $(A, +, \times, \cdot)$ tel que :

(i) $(A, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel.

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

(iii) $\forall \lambda \in \mathbb{K},\ \forall (a, b) \in A^2,\ (\lambda \cdot a) \times b = a \times (\lambda \cdot b) = \lambda \cdot (a \times b)$

On dit de plus que l'algèbre $(A, +, \times, \cdot)$, ou plus simplement A, est

- commutative si l'anneau sous-jacent $(A, +, \times)$ est commutatif
- intègre si l'anneau sous-jacent $(A, +, \times)$ est intègre.
- de dimension finie si l'espace vectoriel sous-jacent $(A, +, \cdot)$ est de dimension finie. La dimension de A est alors la dimension de cet espace vectoriel.

4.1. Définition

Exemples :

- $\mathbb{K}[X]$ est une algèbre intègre.
- Si E est un $\mathbb{K}$-espace vectoriel, $\big(\mathcal{L}(E), +, \circ, \cdot\big)$ est une $\mathbb{K}$-algèbre non intègre en général.
- $\mathcal{M}_n(\mathbb{K})$ est une $\mathbb{K}$-algèbre non intègre si $n \geqslant 2$.
- Si $\mathbb{K}$ est un sous-corps de $\mathbb{K}'$, $\mathbb{K}'$ est une $\mathbb{K}$-algèbre.
- Si X est un ensemble quelconque, $\mathcal{F}(X, \mathbb{K})$ est une $\mathbb{K}$-algèbre commutative mais non intègre pour les lois usuelles $+$ et $\times$ déduites de celles de $\mathbb{K}$. La loi externe $(\lambda, f) \mapsto \lambda f$ se confond avec la loi interne $\times$ en interprétant λ comme une fonction constante.

4.2. Sous-algèbre et morphisme d'algèbre

4.2. Sous-algèbre et morphisme d'algèbre

Definition 21

Soit A une $\mathbb{K}$-algèbre. On appelle sous-algèbre de A toute partie de A qui est à la fois un sous-espace vectoriel et un sous-anneau de A.

Definition 22

Soient A et B deux algèbres sur le même corps $\mathbb{K}$. On dit que $f : A \to B$ est un morphisme d'algèbres lorsque f est à la fois un morphisme d'anneaux et une application linéaire :

- $\forall (x, y) \in A^2,\ \forall \lambda \in \mathbb{K},\ f(x + \lambda y) = f(x) + \lambda f(y)$
- $\forall (x, y) \in A^2\ f(xy) = f(x)f(y)$
- $f(1_A) = 1_B$.

Proposition 24

Si $f : A \to B$ est un morphisme d'algèbres, alors :

- $\mathrm{Im}(f)$ est une sous-algèbre de B
- $\mathrm{Ker}(f)$ est à la fois un idéal et un sous-espace vectoriel de A.

Exemple :

$u \mapsto \underset{\mathcal{B}}{\mathrm{Mat}}(u)$ isomorphisme d'algèbre de $\mathcal{L}(E)$ sur $\mathcal{M}_n(\mathbb{K})$.

Avec $\mathcal{B}$ base canonique de $\mathbb{K}^n$, identification $\mathcal{L}(\mathbb{K}^n) = \mathcal{M}_n(\mathbb{K})$.

4.2. Sous-algèbre et morphisme d'algèbre

Proposition 25

Soit $n \in \mathbb{N}^*$ et $A \in \mathcal{M}_n(\mathbb{K})$. Il existe un unique morphisme d'algèbres $\Phi : \mathbb{K}[X] \to \mathcal{L}(E)$ vérifiant $\Phi(X) = u$.

Remarques :

- $\mathrm{Ker}(\Phi)$ idéal de $\mathbb{K}[X]$ appelé *idéal annulateur* de u. Engendré par le *polynôme minimal* de A.
- $\mathrm{Im}(\Phi)$ sous-algèbre commutative de $\mathcal{M}_n(\mathbb{K})$ notée $\mathbb{K}[A]$.