Chapitre 2

Structures algébriques

Contents

2.1 Structure de groupe . . . 37
2.1.1 Groupes, sous-groupes . . . 37
2.1.1.1 Définitions et caractérisations . . . 37
2.1.1.2 Groupe engendré par une partie . . . 38
2.1.2 Morphismes de groupes . . . 40
2.1.2.1 Définition et propriétés . . . 40
2.1.2.2 Image d'un morphisme de groupes . . . 40
2.1.2.3 Noyau d'un morphisme de groupes . . . 41
2.1.3 Les groupes $\mathbb{Z}/n\mathbb{Z}$ . . . 41
2.1.3.1 Congruences arithmétiques . . . 41
2.1.3.2 Les groupes $(\mathbb{Z}/n\mathbb{Z}, +)$ . . . 42
2.1.3.3 Représentation des groupes monogènes . . . 43
2.1.4 Ordre d'un élément dans un groupe . . . 43
2.1.4.1 Définitions . . . 43
2.1.4.2 Propriétés . . . 43
2.2 Anneaux et corps . . . 45
2.2.1 Anneaux, sous-anneaux, morphismes d'anneaux . . . 45
2.2.1.1 Structure d'anneau . . . 45
2.2.1.2 Morphismes d'anneaux . . . 46
2.2.1.3 Eléments inversibles, diviseurs de zéro . . . 46
2.2.1.4 Corps, sous-corps . . . 47
2.2.1.5 Rappels de calculs dans les anneaux . . . 47
2.2.1.6 Exemples . . . 47
2.2.2 Idéaux d'un anneau commutatif . . . 48
2.2.2.1 Définition . . . 48
2.2.2.2 Propriétés . . . 48
2.2.2.3 Relation de divisibilité dans un anneau intègre . . . 49
2.2.3 Exemples . . . 50
2.2.3.1 L'anneau $(\mathbb{Z}, +, \times)$ . . . 50
2.2.3.2 L'anneau $(\mathbb{K}[X], +, \times)$ . . . 52
2.2.3.3 L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ . . . 55
2.3 Algèbres . . . 58
2.3.1 Définitions, propriétés . . . 58
2.3.1.1 Structure d'algèbre sur le corps $\mathbb{K}$ . . . 58
2.3.1.2 Morphismes d'algèbres . . . 59

2.3.2 Sous-algèbre de $\mathcal{L}(E)$ engendrée par un élément 59
2.3.2.1 L'algèbre $\mathbb{K}[u]$ 59
2.3.2.2 Lemme de décomposition des noyaux 60
2.3.2.3 Idéal annulateur de u, polynôme minimal 61
2.3.3 Sous-algèbre de $\mathcal{M}_n(\mathbb{K})$ engendrée par un élément 62
2.3.3.1 L'algèbre $\mathbb{K}[A]$ 62
2.3.3.2 Idéal annulateur de A, polynôme minimal de A 62
2.3.3.3 Lien avec les endomorphismes 63

2.1 Structure de groupe

2.1.1 Groupes, sous-groupes

2.1.1.1 Définitions et caractérisations

- **DEFINITION**

Un **groupe** est un couple $(E, \odot)$ formé d'un ensemble E non non videet d'une loi de composition interne $\odot$ sur E vérifiant les axiomes suivants :

* La loi $\odot$ est associative : $\forall (a,b,c) \in E^3$, $a \odot (b \odot c) = (a \odot b) \odot c$.
* Un élément de E est neutre pour $\odot$: $\exists e \in E$, $\forall x \in E$, $e \odot x = x \odot e = x$
* Dans E tout élément est inversible : $\forall a \in E$, $\exists b \in E$, $a \odot b = b \odot a = e$.
  b est alors unique et sera noté a^{-1} (ou $-a$ si la ldci est $+$).

- **DEFINITION**

Si $(E, \odot)$ est un groupe, un sous-ensemble F de E est un **sous-groupe** de E si et seulement si : F est non vide, stable par $\odot$ et $(F, \odot)$ est un groupe.

- **THEOREME Caractérisations des sous-groupes**

F est un sous-groupe du groupe $(E, \odot)$ si et seulement si : F est non vide, inclus dans E, stable par $\odot$ et les inverses des éléments de F sont dans F.
On a également les caractérisations suivantes :

1) **F est non vide, inclus dans E, stable par $\odot$ et les inverses des éléments de F sont dans F.**

2) **$F \subset E$, $F \neq \emptyset$, et $\forall (a,b) \in F^2$, $a \odot b \in F$ et $\forall a \in F$, $a^{-1} \in F$.**

3) **$F \subset E$, $F \neq \emptyset$ et $\forall (a,b) \in F^2$, $a \odot b^{-1} \in F$**

Dem.

- **THEOREME**

L'intersection d'une famille de sous-groupes de $(E, \odot)$ est un sous-groupe de $(E, \odot)$

Dem.

- **PROPRIETE - DEFINITION**

Si $(G_1, \star)$ et $(G_2, \odot)$ sont deux groupes, on munit le produit cartésien $G_1 \times G_2$ d'une loi de composition interne \$ en posant :
$\forall((x_1, x_2), (y_1, y_2)) \in (G_1 \times G_2)^2$, $(x_1, x_2)\$(y_1, y_2) = (x_1 \star y_1, x_2 \odot y_2)$.
$(G_1 \times G_2, \$)$ est alors un groupe appelé groupe produit de G_1 et G_2.

Dem.

- **Cela se généralise au produit cartésien d'un nombre fini de groupes.**
- **Exemples de groupes** :
  - Groupes pour la loi + : $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}^{\mathbb{N}}$, $\mathbb{R}^I$, $\mathbb{K}[X]$, $\mathbb{K}(X)$, $\mathcal{L}(E, F)$, $\mathcal{M}_n(\mathbb{K})$ ...
  - Groupes pour la loi $\times$: $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$, U_n, $GL_n(\mathbb{K})$, $O(n)$, $SO(n)$...
  - Groupes pour la loi $\circ$: $GL(E)$, $O(E)$, ...
- **PROPRIETE Sous-groupes de $(\mathbb{Z}, +)$**

Si G est un sous-groupe de $(\mathbb{Z}, +)$, non réduit à $\{0\}$, alors $G = n\mathbb{Z}$ où $n = \min G \cap \mathbb{N}^*$, en notant : $n\mathbb{Z} = \left\{x \in \mathbb{Z} \middle| \exists p \in \mathbb{Z}, x = np\right\}$

Dem.

✏ **THEOREME Sous-groupes de $(\mathbb{Z}, +)$**

Les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$ avec $n \in \mathbb{N}$

Dem.

- **Notations** : dans la suite, sauf lorsqu'on travaillera avec un groupe bien défini, le groupe sera noté $(G, .)$, son neutre e_G. On posera $x^0 = e_G$, x^{-1} le symétrique de x et, pour $n \in \mathbb{N}^*$, $x^n = x.x.....x$ (n facteurs x) et, pour $n \in \mathbb{Z} \setminus \mathbb{N}$, $x^n = x^{-1}.x^{-1}.....x^{-1}$ ($|n|$ facteurs x^{-1}).

2.1.1.2 Groupe engendré par une partie

- **PROPRIETE**

L'intersection d'une famille de sous-groupes est un sous-groupe.

- **DEFINITION**

Etant donné une partie A d'un groupe G, il existe un plus petit sous-groupe de G qui contient A, c'est l'intersection de tous les sous-groupes de G qui contiennent A. Par définition, ce groupe est **le sous-groupe engendré par A, noté $Gr(A)$** ou $\langle A \rangle$.

- **DEFINITION**

Une partie A d'un groupe G est dite **génératrice de G** lorsque $Gr(A) = G$.

- **Exemples** :
  - ✔ $Gr(e_G) = Gr(\emptyset) = \{e_G\}$, $Gr(G) = G$

✔ Si G est le groupe $(\mathbb{Z},+)$ et si $p \in \mathbb{Z}$, $Gr(p) = |p|\mathbb{Z}$

- **THEOREME**

Si $A \subset G$, $Gr(A) = A \Leftrightarrow A$ est un sous-groupe de G.

Dem.

- **DEFINITION**

Un groupe G est dit **monogène** lorsqu'il admet une partie génératrice A réduite à un singleton $\{a\}$, on le note alors $G = Gr(a)$ ou $\langle a \rangle$.

- **DEFINITION**

G est dit **cyclique** lorsqu'il est monogène et fini.

- **Exemples**
  - $(\mathbb{Z},+)$ est monogène, engendré par 1 (ou par -1)
  - Le groupe $(U_n,\times)$ des racines n-ièmes de l'unité est cyclique, engendré par $e^{\frac{2i\pi}{n}}$
  - Le groupe $(S_n,\circ)$ des permutations de $[\![1,n]\!]$ a pour parties génératrices : l'ensemble T des transpositions et l'ensemble C des cycles.

2.1.2 Morphismes de groupes

2.1.2.1 Définition et propriétés

- **DEFINITION**

$(G, \odot)$ et $(H, \$)$ étant deux groupes, on nomme **morphisme de groupes** de G dans H toute application α de G dans H vérifiant : $\forall (x, y) \in G^2$, $\alpha(x \odot y) = \alpha(x)\$\alpha(y)$

- **PROPRIETE**

Si $\alpha : (G, .) \to (H, .)$ est un morphisme de groupes, alors :

* $\alpha(e_G) = e_H$
* $\forall x \in G$, $\alpha(x^{-1}) = (\alpha(x))^{-1}$
* $\forall x \in G$, $\forall n \in \mathbb{N}^*$, $\alpha(x^n) = (\alpha(x))^n$
* **En résumé :** $\forall x \in G$, $\forall k \in \mathbb{Z}$, $\alpha(x^k) = (\alpha(x))^k$

Dem.

- **PROPRIETE**

La composée de deux morphismes de groupes est un morphisme de groupes.

Dem.

- **PROPRIETE - DEFINITION**

Si $\alpha : (G, \top) \to (H, \odot)$ est un morphisme de groupes bijectif, α^{-1} est un morphisme de groupes. α est dans ce cas nommé isomorphisme de groupes.

Dem.

- **DEFINITION**

Un **automorphisme** de groupes est un isomorphisme d'un groupe dans lui même .

- Les applications suivantes sont des morphismes de groupes :
  * $\ln : (\mathbb{R}_+^*, \times) \to (\mathbb{R}, +)$ (**Logarithme néperien**)
  * $\varepsilon : (S_n, \circ) \to (\{-1, 1\}, \times)$ (**Signature d'une permutation**)
  * $\text{Det} : (GL_n(\mathbb{R}), \times) \to (\mathbb{R}^*, \times)$ (**Déterminant d'une matrice inversible**)
  * Δ, opérateur de dérivation, de $(\mathbb{R}[X], +)$ vers $(\mathbb{R}[X], +)$ (**dérivation des polynômes**) ou de $(\mathcal{C}^{p+1}(I, F), +)$ vers $(\mathcal{C}^p(I, F), +)$ (**dérivation des fonctions de variable réelle**)

2.1.2.2 Image d'un morphisme de groupes

α désigne un morphisme d'un groupe $(G, .)$ dans un groupe $(H, .)$

- **THEOREME**

Si G_1 est un sous-groupe de G, alors l'image directe $\alpha(G_1)$ est un sous groupe de H.

Dem.

- **DEFINITION**

L'image de α est $\mathrm{Im}(\alpha) = \alpha(G) = \{\alpha(x),\ \ x \in G\}$. C'est un sous-groupe de H.

- **PROPRIETE**

Si a est un élément d'un groupe G, $\varphi_a : \begin{pmatrix} (\mathbb{Z},+) & \longrightarrow & (G,.) \\ k & \longmapsto & a^k \end{pmatrix}$ est un morphisme de groupes, son image est le sous-groupe de G engendré par a. On pourra donc écrire $Gr(a) = \{a^k,\ \ k \in \mathbb{Z}\}$.

Dem.

2.1.2.3 Noyau d'un morphisme de groupes

α désigne un morphisme d'un groupe $(G,.)$ dans un groupe $(H,.)$

- **THEOREME**

Si H_1 est un sous-groupe de H, alors l'image réciproque $\alpha^{-1}(H_1)$ est un sous groupe de G.

Dem.

- **DEFINITION**

Le noyau de α est $\mathrm{Ker}(\alpha) = \{x \in G,\ \ \alpha(x) = e_H\}$. C'est un sous-groupe de G.

- **THEOREME**

α est injectif si et seulement si $\mathrm{Ker}(\alpha) = \{e_G\}$.

Dem.

2.1.3 Les groupes $\mathbb{Z}/n\mathbb{Z}$

2.1.3.1 Congruences arithmétiques

- **DEFINITION**

n étant un entier naturel non nul, on appelle **congruence arithmétique modulo n** la relation définie sur $\mathbb{Z}$ par : $\forall (a,b) \in \mathbb{Z}^2,\ \ a \equiv b \bmod (n)$ si et seulement si $b - a \in n\mathbb{Z}$.

- Si $n = 0$, chaque entier est en relation uniquement avec lui même, cette relation (relation d'égalité) ne présente aucun intérêt nouveau.
- Si $n = 1$, tous les entiers sont en relation entre-eux, cette relation (dite triviale) ne présente aucun intérêt.

Désormais, on supposera $n \geqslant 2$.

- **PROPRIETE**

La congruence modulo n est une relation d'équivalence qui définit exactement n classes d'équivalence distinctes : les classes des entiers $k \in [\![0, n-1]\!]$ notées $\mathring{0}, \mathring{1}, \ldots \overset{\circ}{\overline{n-1}}$.

Dem.

- Soit $k \in [\![0, n-1]\!]$ et $p \in \mathbb{Z}$: $p \in \mathring{k} \Leftrightarrow$ le reste de la division euclidienne de p par n vaut k.
- **PROPRIETE**

La relation de congruence modulo n est compatible avec l'addition et la multiplication des entiers :

$$\forall (a,b,c,d) \in \mathbb{Z}^4, \quad \begin{cases} a \equiv b \bmod (n) \\ c \equiv d \bmod (n) \end{cases} \implies \begin{cases} (a+c) \equiv (b+d) \bmod (n) \\ (a \times c) \equiv (b \times d) \bmod (n) \end{cases}$$

Dem.

2.1.3.2 Les groupes $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$

- **DEFINITION**

On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence dans la relation de congruence modulo n. Cet ensemble est fini et son cardinal vaut n

.

- On obtient une loi de composition interne $+$ dans l'ensemble $\mathbb{Z}/n\mathbb{Z}$ en posant :
$\forall (\mathring{a}, \mathring{b}) \in \left(\mathbb{Z}/n\mathbb{Z}\right)^2, \ \mathring{a} + \mathring{b} = \overset{\circ}{\overline{a+b}}$.
Remarquons que par compatibilité de la relation de congruence modulo n avec l'addition, le résultat de l'opération $\mathring{a} + \mathring{b}$ ne dépend pas des représentants choisis dans les calsses de a et de b
- **PROPRIETE**

$\left(\mathbb{Z}/n\mathbb{Z}, +\right)$ est un groupe commutatif, son élément neutre est $\mathring{0}$, le symétrique de $\mathring{k}$ est $\overset{\circ}{\overline{n-k}} = \overset{\circ}{\overline{-k}}$.

Dem.

- **THEOREME**

Le groupe $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$ est cyclique, $\mathring{1}$ en est un générateur, les autres générateurs sont les $\mathring{k}$ où k est un quelconque entier premier avec n.

Dem.

- **DEFINITION**

Si $n \geqslant 2$ on note $\varphi(n)$ le nombre de générateurs du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$. φ **est la fonction indicatrice d'Euler**

2.1.3.3 Représentation des groupes monogènes

- **PROPRIETE**

Si $(G, .)$ **est un groupe et** $a \in G$, φ_a **:** $\begin{pmatrix} (\mathbb{Z}, +) & \longrightarrow & (Gr(a), .) \\ k & \longmapsto & a^k \end{pmatrix}$ **est un morphisme de groupes surjectif.**

Dem.

- Le noyau de φ_a est un sous groupe de $\mathbb{Z}$, c'est un ensemble $n\mathbb{Z}$ où $n \in \mathbb{N}$.
  - Si $n = 1$, $Gr(a)$ est réduit au seul élément neutre de $Gr(a)$, ce qui équivaut à $a = e_G$, et dans ce cas $Gr(a)$ est cyclique.
  - Si $n = 0$, φ_a est injectif et $Gr(a)$ est isomorphe à $\mathbb{Z}$
  - Si $n \geqslant 2$, $Gr(a)$ est cyclique, isomorphe à $\mathbb{Z}/n\mathbb{Z}$. L'entier n est le cardinal de $Gr(a)$ et se nomme ordre de a.

  On regroupe ces cas dans la propriété suivante :

  PROPRIETE

  Tout groupe monogène infini est isomorphe à $(\mathbb{Z}, +)$
  Tout groupe monogène fini (dont le cardinal est noté n**) est isomorphe à** $(\mathbb{Z}/n\mathbb{Z}, +)$

- **Exemple** : le groupe $(U_n, \times)$ des racines $n-$ièmes de l'unité est isomorphe à $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$. On en déduit que tout groupe monogène fini est isomorphe à un groupe $(U_n, \times)$.

2.1.4 Ordre d'un élément dans un groupe

2.1.4.1 Définitions

- **DEFINITION**

x, élément d'un groupe $(G, .)$ **est dit d'ordre fini** lorsque $Gr(x)$ est fini (et donc cyclique)

- **DEFINITION**

Si $x \in G$ est d'ordre fini, **l'ordre de** x est le cardinal de l'ensemble fini $Gr(x)$.

- e_G est d'ordre 1, c'est le seul élément de G ayant cet ordre.
- **Exemple** : dans $(\mathbb{C}^*, \times)$, $x = i$ est d'ordre fini égal à 4, $y = 2$ n'est pas d'ordre fini.

2.1.4.2 Propriétés

- **PROPRIETE**

Si $a \in G$ **est d'ordre fini** $d(a)$**, on a** $d(a) = \min\{k \in \mathbb{N}^* \mid a^k = e_G\}$

Dem.

- **PROPRIETE**

  Si $x \in G$ est d'ordre fini $d(x) \geqslant 2$ (et donc $x \neq e_G$) : $\forall n \in \mathbb{Z}, \quad x^n = e_G \Leftrightarrow d(x)|n$.

  Dem.

- **PROPRIETE**

  Si G est un groupe fini, de cardinal N, tout élément x de G a un ordre fini $d(x)$ et $d(x)|N$.

  Dem.

2.2 Anneaux et corps

2.2.1 Anneaux, sous-anneaux, morphismes d'anneaux

2.2.1.1 Structure d'anneau

- **DEFINITION**

Un anneau est un triplet $(A, +, \times)$ où A est un ensemble non vide, $+$ et $\times$ deux lois de composition internes vérifiant les axiomes suivants :

* $(A, +)$ est un groupe commutatif (le neutre est noté 0_A) .
* $\times$ est associative et distributive par rapport à $+$
* Un élément de A (noté 1_A), distinct de 0_A, est neutre pour $\times$.

- Un anneau $(A, +, \times)$ est dit **commutatif** lorsque la loi $\times$ est commutative.

- **DEFINITION**

Une partie B d'un anneau $(A, +, \times)$ est un **sous-anneau** de A lorsque $(B, +, \times)$ est un anneau. Il faut et il suffit pour cela que $(B, +)$ soit un sous-groupe de $(A, +)$, que B soit stable par $\times$. et contienne 1_A

Remarquons que la distributivité de $\times$ par rapport à l'addition et l'associativité de $\times$ sont obtenues directement dès que l'on a la stabilité par produit et somme.

- **PROPRIETE**

Caractérisation des sous-anneaux B est un sous-anneau de A si et seulement si :

* $B \neq \emptyset$ **et** $B \subset A$
* $\forall (x, y) \in B^2$, $x - y \in B$ **et** $x \times y \in B$
* $1_A \in B$

Dem.

- **PROPRIETE - DEFINITION**

Si $(A, +, \times)$ et $(B, +, \times)$ sont des anneaux, on munit leur produit cartésien $A \times B$ des lois suivantes :

* $+ : \begin{pmatrix} (A \times B)^2 & \longrightarrow & A \times B \\ ((a, b), (a', b')) & \longmapsto & (a + a', b + b') \end{pmatrix}$
* $\times : \begin{pmatrix} (A \times B)^2 & \longrightarrow & A \times B \\ ((a, b), (a', b')) & \longmapsto & (a \times a', b \times b') \end{pmatrix}$

Muni de ces lois, $A \times B$ est un anneau (nommé anneau produit), son neutre additif est $(0_A, 0_B)$, son neutre multiplicatif $(1_A, 1_B)$.

Dem.

Remarque On généralise au produit fini d'anneaux $\prod_{i \in I} A_i$ est un anneau

2.2.1.2 Morphismes d'anneaux

- **DEFINITION**

Si $(A,+,\times)$ et $(B,+,\times)$ sont des anneaux, si $\varphi : A \to B$ est une application, φ est un **morphisme d'anneaux** si et seulement si :

* $\forall (a,b) \in A^2,\ \varphi(a+b) = \varphi(a) + \varphi(b)$
* $\forall (a,b) \in A^2,\ \varphi(a \times b) = \varphi(a) \times \varphi(b)$
* $\varphi(1_A) = 1_B$

- **PROPRIETE**

La composée de deux morphismes d'anneaux est un morphisme d'anneaux.

Dem.

- **PROPRIETE - DEFINITION**

La bijection réciproque d'un morphisme d'anneaux bijectif est un morphisme d'anneaux. On parle alors d'isomorphisme d'anneaux.

Dem.

- **PROPRIETE**

Si A et B sont des anneaux, si $\varphi : A \to B$ est un morphisme d'anneaux, alors :

* **L'image directe par φ d'un sous-anneau de A est un sous-anneau de B.**
* **En particulier, $\mathrm{Im}(\varphi) = \varphi(A)$ est un sous-anneau de B.**
* **L'image réciproque par φ d'un sous-anneau de B est un sous-anneau de A.**

Dem.

✏ **ATTENTION** : Si B est un anneau, $\{0_B\}$ n'est pas un sous-anneau de B et $\ker(\varphi) = \varphi^{-1}(\{0_B\})$ n'est pas un sous-anneau de A (mais seulement un sous-groupe du groupe $(B,+)$) .

2.2.1.3 Eléments inversibles, diviseurs de zéro

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

- **DEFINITION**

$a \in A$ est un **élément inversible** lorsque : $\exists b \in A \ / \ a \times b = b \times a = 1_A$

- **PROPRIETE**

L'ensemble $A^\times$ des éléments de A inversibles pour la loi $\times$ (aussi appelés unités de A) est un groupe muni de la loi $\times$.

Dem.

- **DEFINITION**

Si $(A,+,\times)$ est un anneau, un élément a est dit **diviseur de zéro dans A** si et seulement si : $a \neq 0_A$ et $\exists b \in A,\ b \neq 0_A \ / \ a \times b = 0_A$ (diviseur de zéro à gauche) et $\exists b' \in A,\ b' \neq 0_A \ / \ b' \times a = 0_A$ (diviseur de zéro à droite).

- $A^\times$, $\{0_A\}$, et l'ensemble des diviseurs de zéro sont trois ensembles disjoints.
- **DEFINITION**

A est dit **intègre** si c'est un anneau commutatif dans lequel aucun élément n'est diviseur de zéro. Dans un anneau intègre : $a \times b = 0_A \Leftrightarrow a = 0_A$ ou $b = 0_A$.

2.2.1.4 Corps, sous-corps

- **DEFINITION**

On appelle **corps** tout anneau commutatif $(K,+,\times)$ pour lequel $K^\times = K^* = K\backslash\{0\}$.

- Dans un corps K, l'inverse de $x \neq 0$ sera noté $\dfrac{1}{x}$.
- Si K est un corps, alors, K est un anneau intègre.

2.2.1.5 Rappels de calculs dans les anneaux

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

- **PROPRIETE**

Si $(x,y) \in A^2$ **et** $xy = yx$ **, si** $n \in \mathbb{N}^*$ **alors :** $(x+y)^n = \displaystyle\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$

Dem.

- **PROPRIETE**

Si $(x,y) \in A^2$ **et** $xy = yx$ **, si** $n \in \mathbb{N}^*$ **alors :** $x^n - y^n = (x-y)\left(\displaystyle\sum_{k=0}^{n-1} x^k y^{n-k-1}\right)$.

Dem.

- **PROPRIETE**

Si A **est un corps , si** $x \neq 1$ **et** $n \in \mathbb{N}^*$ **alors** $\displaystyle\sum_{k=0}^{n-1} x^k = \frac{1-x^n}{1-x}$.

Dem.

2.2.1.6 Exemples

- $(\mathbb{Z},+,\times)$ est un anneau intègre, son groupe des unités est $(\{-1,1\},\times)$.
- $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$ sont des corps. Dans la suite, $\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$.
- $(\mathcal{M}_n(\mathbb{K}),+,\times)$ est un anneau non commutatif et possédant des diviseurs de 0, son groupe des unités est $GL_n(\mathbb{K})$.
- $(\mathbb{K}[X],+,\times)$ est un anneau intègre, son groupe des unités est $\mathbb{K}\backslash\{0\} = \{P \ / \ deg(P) = 0\}$.
- $(\mathbb{K}^{\mathbb{N}},+,\times)$ est un anneau commutatif non intègre.
- Si I est un intervalle de $\mathbb{R}$ non vide et non réduit à un point, $(\mathcal{F}(I,\mathbb{K}),+,\times)$ est un anneau commutatif non intègre.

2.2.2 Idéaux d'un anneau commutatif

$(A, +, \times)$ est un anneau commutatif, $A^\times$ est le groupe des éléments inversibles de l'anneau A

2.2.2.1 Définition

- **DEFINITION**

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

* $(I, +)$ est un sous groupe de $(A, +)$
* $\forall (a, x) \in A \times I,\ a \times x \in I$

- **PROPRIETE**

$I \subset A$ est un idéal si et seulement si :

* $I \neq \emptyset$
* $\forall (a, x, y) \in A \times I \times I,\ x - y \in I$ **et** $a \times x \in I$

Dem.

- $\{0_A\}$ et A sont deux idéaux de A.
- **PROPRIETE**

Si $b \in A$, $bA = \{b \times a,\ a \in A\}$ est un idéal de A.

Dem.

2.2.2.2 Propriétés

- **PROPRIETE**

Soit I un idéal de A : $A = I \Leftrightarrow 1_A \in I \Leftrightarrow I \cap A^\times \neq \emptyset$.

Dem.

- **PROPRIETE**

Si A et B sont deux anneaux commutatifs, et si $\varphi : A \to B$ est un morphisme d'anneaux :

* **Pour tout idéal I de A, $\varphi(I)$ est un idéal de $\varphi(A)$ (mais pas en général un idéal de B).**
* **Pour tout idéal J de B, $\varphi^{-1}(J)$ est un idéal de A. En particulier, puisque $\{0_B\}$ est un idéal de B, $\ker(\varphi)$ est un idéal de A.**

Dem.

- **PROPRIETE**

L'intersection d'une famille quelconque d'idéaux de A est un idéal de A

Dem.

- **PROPRIETE - DEFINITION**

Si P est une partie de l'anneau A, il existe un plus petit idéal de A contenant P, on le nomme idéal engendré par P, on le note $Id(P)$, il s'agit de l'intersection de tous les idéaux de A contenant P.

Dem.

- **PROPRIETE - DEFINITION**

Lorsque P est un singleton $\{b\}$, l'idéal engendré par b est dit principal et $Id(b) = bA$.

Dem.

- **PROPRIETE**

Si I et J sont deux idéaux de A, $I + J$ est un idéal de A.

Dem.

2.2.2.3 Relation de divisibilité dans un anneau intègre

$(A, +, \times)$ est un anneau intègre (et donc commutatif).

- **DEFINITION**

La **relation de divisibilité** est définie dans $A\backslash\{0\}$ par :
$\forall (a, b) \in (A\backslash\{0\})^2$, $a|b \Leftrightarrow \quad \exists c \in A\backslash\{0\}$; $b = a \times c$.

- **PROPRIETE**

Caractérisation : $\forall (a, b) \in (A\backslash\{0\})^2$, $a \big| b \Leftrightarrow bA \subset aA$

Dem.

- La relation de divisibilité est réflexive et transitive.
- $\forall (a, b) \in (A\backslash\{0\})^2$, $a|b$ et $b|a \Leftrightarrow \exists u \in A^\times$; $b = a \times u$.
- **DEFINITION**

Deux éléments a et b de A sont dits **associés** lorsque : $\exists u \in A^\times$ / $b = a \times u$.

- **PROPRIETE**

On a donc, pour $(a,b) \in (A\backslash\{0\})^2$: $a|b$ et $b|a \Leftrightarrow aA = bA \Leftrightarrow a$ et b sont associés.

- **DEFINITION**

Un élément a de A, non inversible, est dit **irréductible** lorsque ses seuls diviseurs sont ses associés et les inversibles de A.

2.2.3 Exemples

2.2.3.1 L'anneau $(\mathbb{Z}, +, \times)$

- **PROPRIETE**

$(\mathbb{Z}, +, \times)$ est un anneau intègre. Le groupe des inversibles est $\{-1, 1\}$. Les associés d'un entier $k \neq 0$ sont donc k et $-k$.

Dem.

- **PROPRIETE Division euclidienne**

$$\forall (a,b) \in \mathbb{Z} \times \mathbb{N}^*, \quad \exists !(q,r) \in \mathbb{Z}^2 \;\Big|\; a = bq + r \quad \text{et} \quad 0 \leqslant r < b.$$

Dem.

- **PROPRIETE**

Les idéaux de l'anneau $(\mathbb{Z}, +, \times)$ sont les $n\mathbb{Z}$ où $n \in \mathbb{N}$.

Dem.

- **PROPRIETE PGCD, PPCM de deux entiers**

Si a et b sont des entiers non nuls :

* **L'idéal $a\mathbb{Z} \bigcap b\mathbb{Z}$ est $m\mathbb{Z}$ où m est le ppcm positif de a et b.**
* **Relation de Bézout : si $d = \text{pgcd}(a,b)$, $\exists (u,v) \in \mathbb{Z}^2 \;\Big|\; au + bv = d$**
* **L'idéal $a\mathbb{Z} + b\mathbb{Z}$ est $d\mathbb{Z}$ où d est le pgcd positif de a et b.**
* **Théorème de Bézout : si $(a,b) \in (\mathbb{Z}^*)^2$,**
  $\text{pgcd}(a,b) = 1 \Leftrightarrow a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z} \Leftrightarrow \exists (u,v) \in \mathbb{Z}^2 \;\Big|\; au + bv = 1.$
* **Lemme de Gauss : si $(a,b,c) \in (\mathbb{Z}^*)^3$, $a|bc$ et $\text{pgcd}(a,b) = 1 \Longrightarrow a|c$.**

Dem.

- **DEFINITION PGCD de $n \geqslant 2$ entiers**

Soit $n \in \mathbb{N}, n \geqslant 2$. Soit $a_1, a_2, \ldots, a_n$ n entiers relatifs non tous nuls. On appelle **pgcd** de la famille $(a_1, a_2, \ldots, a_n)$ l'unique entier naturel d tel que l'idéal $a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z}$ soit $d\mathbb{Z}$

- **PROPRIETE Caractérisation du PGCD**

Soit $a_1, a_2, \ldots, a_n$ n entiers relatifs non tous nuls et d le PGCD de cette famille. Alors $d = \max\left\{k \in \mathbb{N}^* \middle| k \text{ divise tous les } a_i\right\}$

Dem.

- **PROPRIETE Relation de Bézout**

Soit $a_1, a_2, \ldots, a_n$ n entiers relatifs non tous nuls et d leur PGCD. Alors il existe $(u_1, u_2, \ldots, u_n) \in \mathbb{Z}^n$ tels que $d = a_1u_1 + a_2u_2 + \cdots + a_nu_n$

Dem.

- **DEFINITION Nombres premiers entre eux**

Soit $a_1, a_2, \ldots, a_n$ n entiers relatifs non tous nuls. On dit que ces entiers sont **premiers entre eux (dans leur ensemble)** si leur PGCD est 1

- **THEOREME Théorème de Bézout**

Soit $a_1, a_2, \ldots, a_n$ n entiers relatifs non tous nuls.
Alors $a_1, a_2, \ldots, a_n$ sont premiers entre eux si et seulement si il existe n entiers relatifs $(u_1, u_2, \ldots, u_n)$ tels que $1 = a_1u_1 + a_2u_2 + \cdots + a_nu_n$

Dem.

- **PROPRIETE Irréductibles de $\mathbb{Z}$**

Les irréductibles de $\mathbb{Z}$ sont les nombres premiers et leurs opposés.

Dem.

- **PROPRIETE**

Tout entier naturel $n \geqslant 2$ admet une décomposition en facteurs premiers de la forme $n = p_1^{k_1} \ldots p_r^{k_r}$ où les p_i sont des nombres premiers deux à deux distincts et les k_i des entiers naturels non nuls.

Dem.

DEFINITION Valuation $p-$adique

Si $n \in \mathbb{Z} \setminus \{0\}$ et p est un nombre premier, on appelle **valuation $p-$adique de n** , le plus grand entier k tel que p^k divise n. On la note $v_p(n)$ et, pour $|n| \geqslant 2$, il s'agit de la puissance de p dans la décomposition de $|n|$ en facteur premier.

- **PROPRIETE**

Si $n = \prod_{i=1}^{r} p_i^{k_i}$ **et** $q = \prod_{i=1}^{r} p_i^{l_i}$ **avec** $\forall i, \quad k_i \in \mathbb{N}$ **et** $l_i \in \mathbb{N}$**,**

$$\textbf{pgcd}(n,q) = \prod_{i=1}^{r} p_i^{\min(k_i,l_i)} \textbf{ et } \textbf{ppcm}(n,q) = \prod_{i=1}^{r} p_i^{\max(k_i,l_i)}$$

Dem.

2.2.3.2 L'anneau $(\mathbb{K}[X], +, \times)$

$\mathbb{K}$ est un sous-corps de $\mathbb{C}$.
On rappelle les propriétés de $\mathbb{K}[X]$ vues en MPSI :

- **PROPRIETE**

$(\mathbb{K}[X], +, \times)$ **est un anneau intègre. Le groupe des inversibles est** $\mathbb{K}\backslash\{0\}$**. Les associés d'un polynôme** $P \neq 0$ **sont donc les polynômes** μP **où** μ **est un scalaire non nul.**

- **PROPRIETE Division euclidienne**

$\forall (A,B) \in \mathbb{K}[X] \times (\mathbb{K}[X]\backslash\{0\})$, $\exists ! (Q,R) \in \mathbb{K}[X]^2 \mid A = BQ + R$ **et** $\deg(R) < \deg(B)$

- **PROPRIETE Idéaux de l'anneau des polynomes**

Tout idéal I **de** $\mathbb{K}[X]$ **est principal, c'est à dire :** $\exists P \in \mathbb{K}[X] \ / \ I = P\,\mathbb{K}[X]$
Plus précisément, si I **est un idéal de** $\mathbb{K}[X]$ **non réduit à** $\{0\}$ **:**

* **Il existe un unique polynôme** P **unitaire tel que** $I = P\mathbb{K}[X]$,
  P **est caractérisé par :** $P \in I$, P **unitaire,** $\deg(P) = \min_{Q \in I\backslash\{0\})} \{\deg(Q)\}$
* **Les générateurs de** I **sont les polynômes** αP **où** $\alpha \in \mathbb{K}$ **et** $\alpha \neq 0$**.**

Dem.

- **PROPRIETE PGCD, PPCM de deux polynomes**

Si A et B sont deux polynômes non nuls :

- **Le *ppcm* (unitaire) de A et B est l'unique polynôme M unitaire tel que $A\mathbb{K}[X] \cap B\mathbb{K}[X] = M\mathbb{K}[X]$.**
- **<u>Relation de Bézout</u> : si $D = pgcd(A, B)$, $\exists (U, V) \in K[X]^2 \ \big| AU + BV = D$**
- **Le *pgcd* (unitaire) de A et B est l'unique polynôme D unitaire tel que $A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X]$.**
- **Le *pgcd* (unitaire) de A_1, A_2, ...et A_n est l'unique polynôme D unitaire tel que $A_1\mathbb{K}[X] + A_2\mathbb{K}[X] + \dots A_n\mathbb{K}[X] = D\mathbb{K}[X]$.**
- **<u>Théorème de Bézout</u> : A et B sont premiers entre eux si et seulement si $A\mathbb{K}[X] + B\mathbb{K}[X] = \mathbb{K}[X]$ si et seulement si $\exists (U, V) \in \mathbb{K}[X]^2 \, | AU + BV = 1$**
- **<u>Théorème de Gauss</u> : si A et B sont premiers entre eux et A divise BC, A divise C.**
- **Deux polynomes A et B sont premiers entre eux si et seulement si A et B n'ont pas de racine commune dans $\mathbb{C}$.**

- **<u>DEFINITION PGCD de $n \geqslant 2$ polynômes</u>**

Soit $n \in \mathbb{N}, n \geqslant 2$. Soit $P_1, P_2, \dots, P_n$ n polynomes non tous nuls.
On appelle **<u>PGCD</u>** de la famille $(P_1, P_2, \dots, P_n)$ l'unique polynome unitaire engendrant l'idéal $P_1\mathbb{K}[X] + P_2\mathbb{K}[X] + \dots + P_n\mathbb{K}[X]$

- **<u>PROPRIETE Caractérisation du PGCD</u>**

Soit $P_1, P_2, \dots, P_n$ n polynomes non tous nuls et D le PGCD de cette famille. Alors D est le polynome unitaire de plus grand degré divisant tous les P_i.
Plus précisément, si Q est un polynome divisant tous les P_i alors Q divise également D

Dem.

- **<u>PROPRIETE Relation de Bézout</u>**

Soit Soit $P_1, P_2, \dots, P_n$ n polynomes non tous nuls et D leur PGCD. Alors il existe $(U_1, U_2, \dots, U_n) \in (\mathbb{K}[X])^n$ tels que $D = P_1U_1 + P_2U_2 + \dots + P_nU_n$

Dem.

- **<u>DEFINITION Polynomes premiers entre eux</u>**

Soit $P_1, P_2, \dots, P_n$ n polynomes non tous nuls. On dit que ces polynomes sont **<u>premiers entre eux (dans leur ensemble)</u>** si leur PGCD est 1

- **<u>THEOREME Théorème de Bézout</u>**

Soit $P_1, P_2, \dots, P_n$ n polynomes non tous nuls.
Alors $P_1, P_2, \dots, P_n$ sont premiers entre eux si et seulement si il existe n polynomes $(U_1, U_2, \dots, U_n) \in (\mathbb{K}[X])^n$ tels que $1 = P_1U_1 + P_2U_2 + \dots + P_nU_n$

Dem.

- **<u>DEFINITION Polynomes irréductibles</u>**

Soit $\mathbb{K}$ un sous-corps de $\mathbb{C}$. Soit $P \in \mathbb{K}[X]$. On dit que P est **irréductible** dans $\mathbb{K}[X]$ s'il est non constant et que ses seuls diviseurs sont les polynomes qui lui sont associés et les polynomes constants non nuls

Remarque On retrouve la définition d'un élément irréductible dans un anneau intègre.

- **PROPRIETE Caractérisation des polynomes irréductibles**

Soit $P \in \mathbb{K}[X]$ non constant. Alors P est irréductible si et seulement pour tout couple $(A, B) \in (\mathbb{K}[X])^2$ si $A \times B = P$ alors A ou B est un polynome constant

Dem.

- **Exemple** : tout polynome de degré 1 est irréductible : en prenant la caractérisation, si $A \times B$ est un polynome de degré 1, entre A et B, il y en a un de degré 1 et l'autre de degré 0.
- **PROPRIETE**

Deux polynomes irréductibles unitaires distincts sont premiers entre eux

Dem.

- **PROPRIETE**

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

Dem.

- **PROPRIETE**

Les irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 sans racines réelles (i.e. dont le discriminant est strictement négatif).

Dem.

- Par contre les irréductibles de $\mathbb{Q}[X]$ sont plus difficiles à obtenir. Par exemple on peut montrer que $X^3 - X + 1$ est irréductible dans $\mathbb{Q}[X]$. Il existe d'ailleurs des polynomes irréductibles dans $\mathbb{Q}[X]$ de degré aussi grand que souhaiter.
- **PROPRIETE**

Tout polynôme P de $\mathbb{K}[X]$, non constant admet une décomposition en facteurs irréductibles de la forme $P = \mu P_1^{k_1} \dots P_r^{k_r}$ où μ est un scalaire, les P_i des polynômes unitaires irréductibles deux à deux distincts et les k_i des entiers naturels non nuls. Cette décomposition est unique à l'ordre près des facteurs.

Dem.

2.2.3.3 L'anneau $\left(\mathbb{Z}/n\mathbb{Z}, +, \times\right)$

Dans ce qui suit, n est un entier, $n \geqslant 2$

- **PROPRIETE**

La relation de congruence modulo n est compatible avec la multiplication des entiers : $\forall (a,b,c,d) \in \mathbb{Z}^4,\ \ a \equiv b \bmod n$ **et** $c \equiv d \bmod n \Rightarrow (a \times c) \equiv (b \times d) \bmod n$

Dem.

- **DEFINITION**

On définit une loi de composition interne $\times$ dans l'ensemble $\mathbb{Z}/n\mathbb{Z}$ en posant : $\forall (\mathring{a}, \mathring{b}) \in (\mathbb{Z}/n\mathbb{Z})^2,\ \ \mathring{a} \times \mathring{b} = \overline{a \times b}^{\circ}$

- **PROPRIETE**

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif, son élément neutre multiplicatif est $\mathring{1}$.

Dem.

- **PROPRIETE Théorème chinois**

Si m et n sont des entiers premiers entre-eux, si, pour tout $k \in \mathbb{Z}$, on note $\mathring{k}$, $\breve{k}$ et $\hat{k}$ les classes de k modulo respectivement n, m et nm. alors, $\phi : \begin{pmatrix} \mathbb{Z}/mn\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \hat{k} & \longmapsto & \left(\breve{k}, \mathring{k}\right) \end{pmatrix}$ **est un isomorphisme d'anneaux.**

Dem.

PROPRIETE

Généralisation **Si m_1, m_2, ..., m_p sont p entiers premiers entre-eux 2 à 2, si, pour tout $k \in \mathbb{Z}$, on note $\overline{k}^{(m_j)}$ la classe de k modulo m_j et $\hat{k}$ la classe de k modulo $m_1 m_2 \dots m_p$**
Alors, $\phi : \begin{pmatrix} \mathbb{Z}/m_1 m_2 \cdots m_p\mathbb{Z} & \longrightarrow & \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_p\mathbb{Z} \\ \hat{k} & \longmapsto & \left(\overline{k}^{(m_1)}, \overline{k}^{(m_2)}, \cdots, \overline{k}^{(m_p)}\right) \end{pmatrix}$ **est un isomorphisme d'anneaux.**

- **Corollaire**

Si m et n sont des entiers premiers entre-eux, si a et b sont des entiers, le système de congruences $\begin{cases} x \equiv a \bmod m \\ x \equiv b \bmod n \end{cases}$ **a des solutions. Si x_0 est l'une d'elles, les autres solutions sont les entiers $x_0 + kmn$ où $k \in \mathbb{Z}$**

- **PROPRIETE**

Les éléments inversibles (ou unités) de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ sont les $\mathring{k}$ où k est un entier premier avec n (ce sont aussi les générateurs du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$).

Dem.

- **PROPRIETE**

Pour n entier $n \geqslant 2$,
$\mathbb{Z}/n\mathbb{Z}$ est intègre $\iff$ $\mathbb{Z}/n\mathbb{Z}$ est un corps $\iff$ n est un nombre premier.
Dans le cas où p est un nombre premier, on note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$

Dem.

- **DEFINITION**

La **fonction indicatrice d'Euler** est φ définie sur $\mathbb{N}^*$ par $\varphi(1) = 1$ et, pour $n \geqslant 2$, $\varphi(n)$ est le cardinal du groupe des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$:
$\varphi(n) = \text{Card}\{k \in [\![1, n]\!],\ k \wedge n = 1\}$

- Si p est un nombre premier, $\varphi(p) = p - 1$.
- Si p est un nombre premier et $k \in \mathbb{N}^*$, $\varphi(p^k) = (p-1)p^{k-1}$.
- **THEOREME**

Si m et n sont des entiers premiers entre-eux, alors $\varphi(mn) = \varphi(m)\varphi(n)$. (on dit que φ est multiplicative)

Dem.

- **THEOREME**

Si $n \in \mathbb{N}$, $n \geqslant 2$, a pour décomposition en facteurs premiers $n = p_1^{k_1} \dots p_r^{k_r}$,
$$\varphi(n) = \prod_{i=1}^{r}(p_i - 1)p_i^{k_i - 1} = n\prod_{i=1}^{r}(1 - \frac{1}{p_i})$$

Dem.

- **THEOREME Théorème d'Euler**

Si $n \in \mathbb{N}$, $n \geqslant 2$, si a est un entier premier avec n, alors $a^{\varphi(n)} \equiv 1 \bmod n$.

Dem.

- **Corollaire Cas particulier : le petit théorème de Fermat**

si p est un nombre premier, si a n'est pas multiple de p, alors $a^{p-1} \equiv 1 \bmod p$.

Dem.

2.3 Algèbres

2.3.1 Définitions, propriétés

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

2.3.1.1 Structure d'algèbre sur le corps $\mathbb{K}$

- **DEFINITION**

Une **$\mathbb{K}$-algèbre** est un quadruplet $(A, +, \times, .)$ constitué d'un ensemble A, de deux lois internes sur A ($+$ et $\times$) et d'une loi externe $(.)$ dont les scalaires sont les éléments de $\mathbb{K}$ vérifiant les axiomes suivants :

* $(A, +, \times)$ est un anneau.
* $(A, +, .)$ est un $\mathbb{K}$-espace vectoriel.
* $\forall \mu \in \mathbb{K},\ \forall (a, b) \in A^2,\ (\mu.a) \times b = \mu.(a \times b) = a \times (\mu.b)$

- **DEFINITION**

Une partie B d'une $\mathbb{K}$-algèbre $(A, +, \times, .)$ en est une **sous-algèbre** lorsque $(B, +, \times)$ est un sous-anneau de $(A, +, \times)$ et $(B, +, .)$ un sous-espace vectoriel de $(A, +, .)$ c'est à dire :

* $\forall (x, y) \in B^2$, $x + y \in B$ et $x \times y \in B$
* $\forall x \in B$, $\forall \mu \in \mathbb{K}$, $\mu.x \in B$
* $1_A \in B$

- **PROPRIETE**

L'intersection d'une famille de sous-algèbres d'une $\mathbb{K}$-algèbre A est une sous-algèbre de A.

Dem.

- **DEFINITION**

Si $(A, +, \times, .)$ est une $\mathbb{K}$-algèbre, si B est une partie de A, on appelle **sous-algèbre de A engendré par B** la plus petite sous-algèbre de A contenant B, c'est l'intersection de la famille des sous-algèbres de A contenant B.

- **Exemples :**

* $(\mathbb{K}[X], +, \times, .)$ est une $\mathbb{K}$-algèbre commutative et intègre.
* Si E est un $\mathbb{K}$-espace vectoriel, $(\mathcal{L}(E), +, \circ, .)$ est une $\mathbb{K}$-algèbre.
* $(\mathcal{M}_n(\mathbb{K}), +, \times, .)$ est une $\mathbb{K}$-algèbre.
* Si I est un intervalle de $\mathbb{R}$, $(\mathscr{C}(I, \mathbb{R}), +, \times, .)$ est une $\mathbb{R}$ algèbre.
* Si X est un ensemble non vide, l'ensemble $\mathcal{F}(X, \mathbb{K})$ des applications de X vers le corps $\mathbb{K}$ est une $\mathbb{K}-$algèbre

2.3.1.2 Morphismes d'algèbres

- **DEFINITION**

Si $(A,+,\times,.)$ et $(B,+,\times,.)$ sont des $\mathbb{K}$-algèbres, si $\varphi : A \to B$ est une application, φ est un **morphisme d'algèbres** si et seulement si c'est à la fois une application linéaire et un morphisme d'anneaux i.e.

* $\forall (a,b) \in A^2$, $\varphi(a+b) = \varphi(a) + \varphi(b)$ et $\varphi(a \times b) = \varphi(a) \times \varphi(b)$
* $\forall a \in A$, $\forall \mu \in \mathbb{K}$, $\varphi(\mu.a) = \mu.\varphi(a)$
* $\varphi(1_A) = 1_B$

- **PROPRIETE**

La composée de morphismes d'algèbres, la réciproque d'un morphisme d'algèbres bijectif sont des morphismes d'algèbres.

- **Exemple :** si E est un $\mathbb{K}$ espace-vectoriel de dimension finie n et si $\mathcal{B}$ est une base de E, l'application $\varphi : \begin{pmatrix} \mathcal{L}(E) & \longrightarrow & \mathcal{M}_n(\mathbb{K}) \\ u & \longmapsto & Mat_{\mathcal{B}}(u) \end{pmatrix}$ est un isomorphisme d'algèbres.

- **PROPRIETE**

Si A et B sont des $\mathbb{K}$-algèbres, si $\varphi : A \to B$ est un morphisme d'algèbres :

* **L'image directe par φ d'une sous-algèbre de A est une sous-algèbre de B.**
* **L'image réciproque par φ d'une sous-algèbre de B est une sous-algèbre de A.**

- **Attention** : $\{0_B\}$ n'est pas une sous-algèbre de B et si $\varphi : A \to B$ est un morphisme d'algèbres, $\mathrm{Ker}(\varphi)$ n'est pas une sous-algèbre de A, mais seulement un sous-espace vectoriel de l'espace vectoriel A et un idéal de l'anneau A.

2.3.2 Sous-algèbre de $\mathcal{L}(E)$ engendrée par un élément

E est un $\mathbb{K}$-espace vectoriel et u un endomorphisme de E.

2.3.2.1 L'algèbre $\mathbb{K}[u]$

- **DEFINITION**

Si $P = a_0 + a_1 X + \ldots + a_d X^d$ est un polynôme de $\mathbb{K}[X]$, on définit **l'endomorphisme $P(u)$** par : $P(u) = a_0 Id_E + a_1 u + \ldots + a_d u^d$ où u^k est l'itéré de u pour la loi $\circ$ avec la convention $u^0 = I_d$.

- **PROPRIETE**

$\varphi_u : \begin{pmatrix} \mathbb{K}[X] & \longrightarrow & \mathcal{L}(E) \\ P & \longmapsto & P(u) \end{pmatrix}$ est un morphisme d'algèbres.

Dem.

- **PROPRIETE**

$\mathrm{Im}(\varphi_u)$ est une sous algèbre de $\mathcal{L}(E)$, c'est la sous algèbre de $\mathcal{L}(E)$ engendrée par u et on la note $\mathbb{K}[u]$, cette algèbre est commutative.

Dem.

- **PROPRIETE**

$\forall P \in \mathbb{K}[X]$, $\ker(P(u))$ et $\mathrm{Im}(P(u))$ sont stables par u.

Dem.

2.3.2.2 Lemme de décomposition des noyaux

- **DEFINITION**

Deux sous-espaces vectoriels F et G de E sont dits

- ✎ **en somme directe** si pour tout $x \in F+G$, l'écriture de x sous la forme $x = y+z$ avec $(y,z) \in F \times G$ est unique.
- ✎ **supplémentaires** si la somme $F+G$ est directe et $F+G=E$. On note alors $E = F \oplus G$

- **PROPRIETE**

Deux sous-espaces vectoriels F et G sont en somme directe si et seulement si $F \cap G = \{0\}$

Dem.

- **PROPRIETE**

Soient F et G deux sous-espaces vectoriels de E. Alors :
$E = F \oplus G \iff \forall x \in E, \exists!(y,z) \in F \times G; x = y+z$

Dem.

- **DEFINITION**

Soient $F_1, \dots, F_n$ n sous-espaces vectoriels de E.
On dit que **la somme** $F = F_1 + \cdots + F_n = \sum_{i=1}^{n} F_i$ **est directe** si l'écriture de tout élément de cette somme sous la forme $x = x_1 + \cdots + x_n$ avec pour tout i, $x_i \in F_i$, est unique. On note alors $F = F_1 \oplus \cdots \oplus F_n = \bigoplus_{i=1}^{n} F_i$.

- **PROPRIETE**

Soient $F_1, \dots, F_n$ n sous-espaces vectoriels de E de somme $F = \sum_{i=1}^{n} F_i$. On a équivalence entre :

1. **la somme $F = \sum_{i=1}^{n} F_i$ est directe, i.e. $F = \bigoplus_{i=1}^{n} F_i$**
2. $\forall (x_1, \dots, x_n) \in F_1 \times \cdots \times F_n, x_1 + \cdots + x_n = 0 \Longrightarrow \forall i \in [\![1, n]\!], x_i = 0$
3. $\forall i \in [\![1, n]\!], F_i \bigcap \left(\sum_{j \neq i} F_j \right) = \{0\}$

Dem.

Remarque : Attention : la relation $\forall (i,j) \big| i \neq j,\ F_i \bigcap F_j = \{0\}$ ne caractérise pas les sommes directes. Par exemple $\mathbb{R}$, $i\mathbb{R}$ et $(1+i)\mathbb{R}$ vérifie la relation avec les intersections mais ne sont pas en somme directe dans $\mathbb{C}$

- **THEOREME Lemme de décomposition des noyaux**

Si P et Q sont deux polynômes premiers entre eux, alors :
$\ker((P \times Q)(u)) = \ker(P(u)) \oplus \ker(Q(u))$.

Dem.

- **Corollaire Lemme de décomposition des noyaux**

Si $r \geqslant 2$ et si $P_1, \dots P_r$ sont r polynômes deux à deux premiers entre eux, alors :
$\ker\left(\left(\prod_{k=1}^{r} P_k\right)(u)\right) = \bigoplus_{k=1}^{r} \ker(P_k(u))$.

Dem.

2.3.2.3 Idéal annulateur de u, polynôme minimal

- **DEFINITION**

$\ker(\varphi_u)$ est un idéal de l'anneau $\mathbb{K}[X]$, nommé **idéal annulateur de u** et noté $Ann(u)$: $Ann(u) = \{P \in \mathbb{K}[X],\ \ P(u) = 0_{\mathcal{L}(E)}\}$.

- **PROPRIETE**

Si $Ann(u) = \{0_{\mathbb{K}[X]}\}$, φ_u induit un isomorphisme de $\mathbb{K}[X]$ sur $\mathbb{K}[u]$, $\mathbb{K}[u]$ est donc de dimension infinie et a pour base $(u^n)_{n \in \mathbb{N}}$.

Dem.

- **PROPRIETE - DEFINITION**

Si $Ann(u) \neq \{0_{\mathbb{K}[X]}\}$, $Ann(u)$ admet un unique polynôme unitaire pour générateur : ce polynôme s'appelle polynôme minimal de u et sera noté π_u ou μ_u.

Dem.

- **PROPRIETE**

Si P est un polynôme unitaire :
$P = \pi_u \Leftrightarrow ($ $P(u) = 0$ **et** $\forall Q \in \mathbb{K}[X],\ Q(u) = 0 \Rightarrow P|Q$ $)$
$\Leftrightarrow P(u) = 0$ **et** $\forall Q \in \mathbb{K}[X]\backslash\{0\},\ \deg(Q) < \deg(P) \Rightarrow Q(u) \neq 0$.

Dem.

- **PROPRIETE**

π_u existe si et seulement si $\mathbb{K}[u]$ est de dimension finie.
Si $\deg(\pi_u) = d$, $\mathbb{K}[u]$ est de dimension d et $(Id_E, u, \ldots, u^{d-1})$ en est une base.

Dem.

- Si E est de dimension finie, π_u existe.

2.3.3 Sous-algèbre de $\mathcal{M}_n(\mathbb{K})$ engendrée par un élément

n est un entier naturel non nul et A une matrice de $\mathcal{M}_n(\mathbb{K})$.

2.3.3.1 L'algèbre $\mathbb{K}[A]$

- **DEFINITION**

Si $P = a_0 + a_1X + \ldots + a_dX^d$ est un polynôme de $\mathbb{K}[X]$, on définit la **matrice $P(A)$** par :
$P(A) = a_0I_n + a_1A + \ldots + a_dA^d$.

- **PROPRIETE**

$\varphi_A : \begin{pmatrix} \mathbb{K}[X] & \longrightarrow & \mathcal{M}_n(\mathbb{K}) \\ P & \longmapsto & P(A) \end{pmatrix}$ est un morphisme d'algèbres.

Dem.

- **PROPRIETE**

$\mathrm{Im}(\varphi_A)$ est une sous algèbre de $\mathcal{M}_n(\mathbb{K})$, c'est la sous algèbre de $\mathcal{M}_n(\mathbb{K})$ engendrée par A et on la note $\mathbb{K}[A]$. Cette algèbre est commutative.

Dem.

2.3.3.2 Idéal annulateur de A, polynôme minimal de A

- **DEFINITION**

$\ker(\varphi_A)$ est un idéal de l'anneau $\mathbb{K}[X]$, nommé **idéal annulateur de A** et noté $Ann(A)$:
$Ann(A) = \{P \in \mathbb{K}[X],\ P(A) = 0_{\mathcal{M}_n(\mathbb{K})}\}$

- **PROPRIETE - DEFINITION**

$Ann(A) \neq \{0_{\mathcal{M}_n(\mathbb{K})}\}$, $Ann(A)$ admet un unique polynôme unitaire pour générateur : ce polynôme s'appelle polynôme minimal de A et sera noté π_A ou μ_A

Dem.

- **PROPRIETE**

Une matrice et sa transposée ont le même polynôme minimal.

Dem.

- **PROPRIETE**

Si $\deg(\pi_A) = d$**,** $\mathbb{K}[A]$ **est de dimension** d **et** $(I_n, A, \ldots, A^{d-1})$ **en est une base.**

Dem.

2.3.3.3 Lien avec les endomorphismes

On suppose que E est un $\mathbb{K}$ espace vectoriel de dimension n muni d'une base $\mathcal{B}$ et que A est la matrice dans $\mathcal{B}$ d'un endomorphisme $u \in \mathcal{L}(E)$.

- **PROPRIETE**

Pour tout polynôme $P \in \mathbb{K}[X]$**,** $P(A)$ **est la matrice dans** $\mathcal{B}$ **de** $P(u)$**.**

Dem.

- **PROPRIETE**

$Ann(u) = Ann(A)$ **et donc** $\pi_u = \pi_A$

Dem.

- **PROPRIETE**

Deux matrices semblables ont le même polynôme minimal.

Dem.