

Structures algébriques usuelles

Groupe

* Définition

Soit G un ensemble non vide muni d'une loi de composition interne (notée $*$).

On dit que $(G, *)$ est un groupe s'il vérifie les assertions suivantes :

- 1) $*$ est associative,
- 2) $*$ possède un élément neutre dans G
- 3) tout élément de G possède un élément symétrique dans G .

On dit que le groupe est abélien (commutatif) si $\forall x, y \in G, x y = y x$.

* Exemples

Des Groupes de référence.

- $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ sont des groupes commutatifs (abéliens).
- $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$, $(\mathbb{Q}^*, \times)$ sont des groupes commutatifs.
- $(K[X], +)$ est un groupe abélien.
- $(GL_n(K), \times)$ est un groupe.
- Soit $n \in \mathbb{N}^*$. On note S_n l'ensemble des bijections de $\{1, 2, 3, \dots, n\}$ vers $\{1, 2, 3, \dots, n\}$.
- $(S_n, \circ)$ est un groupe.

* Le groupe $\mathbb{Z}/n\mathbb{Z}$

Soient $n \in \mathbb{N}^*$, x et y deux éléments de $\mathbb{Z}$.

$$x \equiv y (n) \iff x - y \in n\mathbb{Z}.$$

La relation " $\equiv$ " est une relation d'équivalence dans $\mathbb{Z}$.

Pour $a \in \mathbb{Z}$, sa classe d'équivalence sera notée $\bar{a}$ et on a : $\bar{a} = \{a + kn \mid k \in \mathbb{Z}\}$. On note $\mathbb{Z}/n\mathbb{Z}$: l'ensemble des classes d'équivalences.

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

On définit dans $\mathbb{Z}/n\mathbb{Z}$ une addition et une multiplication par :

$$\bar{x} + \bar{y} = \overline{x + y} \quad \text{et} \quad \bar{x} \times \bar{y} = \overline{x \times y}.$$

* Théorème

Soient $n \in \mathbb{N}^*$, alors :

- 1) $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien de cardinal n .
- 2) $\forall k \in \mathbb{Z}$, et $\forall a \in \mathbb{Z}$, $k\bar{a} = \overline{ka}$.

* Produit cartésien de groupes

Soient $n \in \mathbb{N}^*$ et $(G_1, +_1), \dots, (G_n, +_n)$ n groupes. Sur le produit cartésien $G = G_1 \times \dots \times G_n$, on définit la loi suivante :

$$\forall ((x_1, \dots, x_n), (y_1, \dots, y_n)) \in (G_1, +_1), \dots, (G_n, +_n) \\ (x_1, \dots, x_n) +_G (y_1, \dots, y_n) = (x_1 +_1 y_1, \dots, x_n +_n y_n).$$

Alors

$(G = G_1 \times \dots \times G_n, +_G)$ est un groupe d'élément neutre $(e_{G_1}, e_{G_2}, \dots, e_{G_n})$.

Exemple

$(\mathbb{R}^*, \times)$ et $(\mathbb{R}, +)$ sont des groupes, alors $(\mathbb{R}^* \times \mathbb{R})$ est un groupe muni de la loi $*$ définie par : $\forall (x, y)$ et $\forall (x', y') \in \mathbb{R}^* \times \mathbb{R}$
 $(x, y) * (x', y') = (xx', y + y')$.
 L'élément neutre de $(\mathbb{R}^* \times \mathbb{R})$ est $(1, 0)$.

Sous-groupe

Soit $(G, *)$ un groupe et H une partie de G .

- H est un sous-groupe de G si et seulement si

$$\begin{cases} \cdot e_G \in H \\ \cdot \forall x, y \in H \quad x * y \in H \end{cases} \iff \begin{cases} \cdot e_G \in H \\ \cdot \forall x, y \in H \quad x * y^{-1} \in H \end{cases}$$

- Si H est un sous-groupe de G , alors $(H, *)$ est un groupe.

Exemple

- 1) Soit $S_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}), \text{telque } {}^t A = A\}$.
 $S_n(\mathbb{R})$ est un sous-groupe de $(M_n(\mathbb{R}), +)$.
- 2) On pose $O_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}), \text{telque } {}^t A A = I_n\}$.
 $O_n(\mathbb{R}, \times)$ est un sous-groupe de $(GL_n(\mathbb{R}), \times)$.
- 3) Soit $O_n^+(\mathbb{R}) = \{A \in O_n(\mathbb{R}), \text{telque } \det(A) = 1\}$.
 $(O_n^+(\mathbb{R}), \times)$ est un sous-groupe de $(O_n(\mathbb{R}), \times)$.
- 4) $U = \{z \in \mathbb{C}; |z| = 1\}$ et $U_n = \{z \in \mathbb{C}; z^n = 1\}$, alors
 $(U, \times)$ est un sous-groupe du groupe $(\mathbb{C}^*, \times)$.
 $(U_n, \times)$ est un sous-groupe du groupe $(U, \times)$ et par suite sous-groupe du groupe $(\mathbb{C}^*, \times)$.

Théorème

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

Proposition

- Soit H et K deux sous-groupes de $(G, *)$, alors
 $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$.
- Soit $(H_i)_{i \in I}$ une famille de sous-groupes de $(G, *)$, alors
 $\bigcap_{i \in I} H_i$ est un sous-groupe de $(G, *)$.

Sous-groupe engendré par un élément

- Soit $(G, *)$ un groupe et $a \in G$. le sous-groupe engendré par a est :

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

- Si le groupe est noté additivement $(G, +)$, alors

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

Exemple

- 1) Dans $\mathbb{C}^*$, pour $n \in \mathbb{N}^*$

$$\langle e^{\frac{2\pi i}{n}} \rangle = U_n = \{z \in \mathbb{C}; z^n = 1\}$$

- 2) $\mathbb{Z} = \langle 1 \rangle$.

Sous-groupe engendré par une partie

Soient $(G, *)$ un groupe et A une partie quelconque de G . Le sous-groupe engendré par la partie A est le plus petit sous-groupe de G qui contient la partie A et c'est :

$$gr(A) = \bigcap_{A \subset H, (H \text{ sous-groupe})} H.$$

$$gr(A) = \{x_1 * \dots * x_n \text{ avec } x_i \in A \text{ ou } x_i^{-1} \in A\}.$$

* Groupes monogènes et cyclique.

- On dit que $(G, *)$ est un groupe monogène si il existe un élément $a \in G$ tel que $G = \langle a \rangle$.
- Si $(G, *)$ est un groupe monogène, alors il est commutatif.
- On dit que $(G, *)$ est un groupe cyclique s'il est monogène et fini.

* Exemple

- 1) On a $\mathbb{Z} = \langle 1 \rangle \iff \mathbb{Z}$ est un groupe monogène et 1 est un générateur de $\mathbb{Z}$.
- 2) $\forall n \in \mathbb{N}^*, n\mathbb{Z} = \langle n \rangle \iff n\mathbb{Z}$ est un groupe monogène et n est un générateur de $n\mathbb{Z}$.
- 3) $U_n = \{z \in \mathbb{C}; z^n = 1\} = \langle e^{\frac{2i\pi}{n}} \rangle = \{e^{\frac{2i\pi k}{n}}, k \in \{0, 1, \dots, n\}\} \iff U_n$ est un groupe cyclique de générateur $e^{\frac{2i\pi}{n}}$.
- 4) $(\mathbb{Q}, +)$ n'est pas monogène.

* Générateur de $\mathbb{Z}/n\mathbb{Z}$

Les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont de la forme $\bar{a}$ avec $\gcd(a, n) = 1$
 $\mathbb{Z}/n\mathbb{Z} = \langle \bar{a} \rangle$ avec $a \wedge n = 1$.

* Exemple

- 1) $\mathbb{Z}/4\mathbb{Z} = \langle \bar{1} \rangle = \langle \bar{3} \rangle$.
- 2) Soit p un nombre premier, alors $\mathbb{Z}/p\mathbb{Z} = \langle \bar{k} \rangle \forall 1 \leq k \leq p-1$.

Morphisme de Groupes

* Définition

- Soient $(G, *)$ et (G', T') deux groupes.
- Un **morphisme** du groupe $(G, *)$ vers le groupe (G', T') est une application $f : G \longrightarrow G'$ vérifiant :

$$\forall (x, y) \in G^2, f(x * y) = f(x) T' f(y).$$

* Exemples

- $f : G \longrightarrow G'$ est un isomorphisme si c'est un morphisme bijective.
- Dans ce cas on dit que G et G' sont isomorphes.
- Un endomorphisme de groupe $f : G \longrightarrow G$ est un morphisme du groupe $(G, *)$ vers le groupe $(G, *)$.
- Un automorphisme de G est un endomorphisme bijectif.
- Si f est un isomorphisme de groupes, alors f^{-1} est un morphisme (et par suite isomorphisme)

* Exemples

- 1) L'application $\exp : (\mathbb{R}, +) \longrightarrow (\mathbb{R}^*, \times)$
 $x \longmapsto e^x$ est un morphisme de groupes.

- 2) L'application $\psi : (\mathbb{R}, +) \longrightarrow (\mathbb{C}^*, \times)$
 $\theta \longmapsto e^{i\theta}$ est un morphisme de groupes.

* Propriétés

- 1) Soient $f : G \longrightarrow G'$ un morphisme de groupes et $c_G, c_{G'}$ les éléments neutres respectivement des groupes G et G' , alors

$$f(c_G) = c_{G'}.$$

- $\forall x \in G, f(x^{-1}) = f(x)^{-1}$.
 - $\forall x \in G, \text{ et } \forall n \in \mathbb{Z}, f(x^n) = (f(x))^n$.
- 2) Soit $f : G \longrightarrow G'$ et $g : G' \longrightarrow G''$ deux morphismes de groupes, alors $g \circ f : G \longrightarrow G''$ est un morphisme de groupes.

✿ Proposition

Soient $f : G \rightarrow G'$ un morphisme de groupes.

- Si H est un sous groupe de G , alors $f(H)$ est un sous groupe de G' .
- Si K est un sous groupe de G' , alors $f^{-1}(K)$ est un sous groupe de G .

✿ Noyau et image

Soit $f : (G, *) \rightarrow (G', T)$ un morphisme de groupes.

- Le noyau de f , noté $\text{Ker}(f)$, est défini par :

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

- $\text{Ker}(f)$ est un sous-groupe de G .

- L'image de f , notée $\text{Im}(f)$, est :

$$\text{Im}(f) = \{f(x), x \in G\} = f(G) \subset G'.$$

- $\text{Im}(f)$ est un sous-groupe de G' .

Application

- L'application $f = \det : (\text{GL}_n(K), \times) \rightarrow (K^*, \times)$ est un morphisme de groupes.

$$A \mapsto \det A$$

- Le noyau de f est $\text{SL}_n(K) = \{A \in \text{GL}_n(K), \det(A) = 1\}$: Le groupe spécial linéaire est un sous groupe de $\text{GL}_n(K)$.

✿ Théorème

Soit $f : (G, *) \rightarrow (G', T)$ un morphisme de groupes.

- f est injective si et seulement si $\text{Ker}(f) = \{e_{G'}\}$.
- f est surjective si et seulement si $\text{Im}(f) = G'$

✿ Description des groupes monogènes

- Si $(G, *)$ est un groupe monogène et infini ($G = \langle a \rangle$), alors $(G, *)$ est isomorphe à $(\mathbb{Z}, +)$ via l'isomorphisme de groupes

$$\varphi : (\mathbb{Z}, +) \rightarrow G \\ k \mapsto a^k$$

- Si $(G, *)$ est un groupe monogène et fini (cyclique) avec $\text{card}(G) = n$ ($G = \langle a \rangle$), alors $(G, *)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$ via l'isomorphisme de groupes

$$\varphi : (\mathbb{Z}/n\mathbb{Z}, +) \rightarrow G \\ k \mapsto a^k$$

✿ Ordre d'un élément

Soient $(G, *)$ un groupe d'élément neutre e_G et $x \in G$. Pour $n \in \mathbb{N}^*$, on note $x^n = \underbrace{x * x * \dots * x}_n$.

- On dit que x est d'ordre fini si il existe $p \in \mathbb{N}^*$ tel que $x^p = e_G$. Dans ce cas l'ordre de x est :

$$o(x) = \min\{p \in \mathbb{N}^* \text{ tel que } x^p = e_G\}.$$

💡 Remarque

Si le groupe est noté additivement $(G, +)$, alors x^p sera remplacé par $\underbrace{px = x + x + \dots + x}_p$.

* Théorème

Soient $(G, *)$ un groupe, x un élément de G et $k, p \in \mathbb{Z}$.

- Si x est d'ordre fini, alors

$$x^k = e \iff o(x) \mid k$$

- Si x est d'ordre fini, alors

$$x^k = x^p \iff k \equiv p \pmod{o(x)}.$$

* Théorème

Soient $(G, *)$ un groupe et x un élément de G d'ordre fini $(o(x) = n)$. Alors

- 1) $\langle x \rangle = \{x^k, 0 \leq k \leq n-1\}$.
- 2) $\text{card}(\langle x \rangle) = n = o(x)$.

* Théorème

Soient $(G, *)$ un groupe.

- Si G est un groupe fini avec $\text{card}(G) = n$, alors
- * $\forall x \in G, x^n = e \implies x$ est d'ordre fini.
- * Si l'ordre de x est d , alors $d \mid n \iff o(x) \mid \text{card}(G)$.

Anneau

* Définition

Soient A un ensemble, " $+$ " et " $\times$ " deux lois de composition interne.

On dit que $(A, +, \times)$ est un anneau si

- $(A, +)$ est un groupe commutatif.
- " $\times$ " a un élément neutre
- " $\times$ " est associative
- " $\times$ " est distributive par rapport à la loi " $+$ "

L'anneau $(A, +, \times)$ est commutatif si la loi $\times$ est commutative.

* Exemples

- $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$, $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$ sont des Anneaux commutatifs.
- $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un Anneau commutatif.
- $(IK[X], +, \times)$ est un Anneau commutatif.
- $(M_n(K), +, \times)$ est un Anneau non commutatif.
- Soit E un IK -espace vectoriel, alors $(\mathcal{L}(E), +, \times)$ est un Anneau non commutatif.

* Produit fini d'anneaux

Soient $(A_1, +_1, \times_1), \dots, (A_n, +_n, \times_n)$ anneaux. Sur le produit cartésien $A_1 \times \dots \times A_n$, on définit les lois suivantes :

$$\forall ((x_1, \dots, x_n), (y_1, \dots, y_n)) \in (A_1 \times \dots \times A_n), \quad (x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 +_1 y_1, \dots, x_n +_n y_n).$$

$$\forall ((x_1, \dots, x_n), (y_1, \dots, y_n)) \in (A_1 \times \dots \times A_n), \quad (x_1, \dots, x_n) \times (y_1, \dots, y_n) = (x_1 \times_1 y_1, \dots, x_n \times_n y_n).$$

Alors

$(A_1 \times \dots \times A_n, +, \times)$ est un anneau.

* Sous-anneau

- Soient $(A, +, \times)$ un anneau d'élément neutre 1_A pour la loi $\times$ et B une partie de A .

On dit que B est un sous-anneau de l'anneau $(A, +, \times)$ si :

$$\begin{cases} \cdot 1_A \in B \\ \cdot \forall (x, y) \in B^2, x - y \in B \text{ et } x \times y \in B \end{cases}$$

- Si B est un sous-anneau de l'anneau $(A, +, \times)$, alors $(B, +, \times)$ est un anneau.

✿ Proposition

Soit $(A, +, \times)$ un anneau.
On pose $\text{Inv}(A)$ l'ensemble des éléments de A inversibles pour la loi $\times$, alors

$(\text{Inv}(A), \times)$ est un groupe

✿ Théorème

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

$$\text{Inv}(\mathbb{Z}/n\mathbb{Z}) = \{\bar{k} \text{ tel que } k \wedge n = 1\}.$$

✿ Proposition

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

Soient a et $b \in A$ tel que $ab = ba$ (a et b commutent), alors

$$(a+b)^n = \sum_{k=0}^n C_n^k a^k b^{n-k}. \text{ "Formule de binôme"}$$

$$a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^k b^{n-1-k} = (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \dots + b^{n-1}).$$

$$1 - b^n = (1-b) \sum_{k=0}^{n-1} b^k = (1-b)(1 + b + b^2 + \dots + b^{n-1}).$$

✿ Anneau intègre

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

On dit que A est un **anneau intègre** si $\forall x$ et y dans A , si $xy = 0$, alors $x = 0$ ou $y = 0$.

- Pour montrer qu'un anneau $(A, +, \times)$ n'est pas intègre il suffit de trouver deux éléments x et y de A tels que $x \neq 0$, $y \neq 0$ et vérifient $x \times y = 0$.

✿ Exemple

$(\mathbb{R}, +, \times)$ est un anneau intègre.

$(M_n(\mathbb{R}), +, \times)$ n'est pas intègre.

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ n'est pas intègre en général

✿ Corps

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

- $(A, +, \times)$ est un corps si tout élément non nul de A admet un inverse dans A pour la loi " $\times$ ".
- Le corps est commutatif si la loi " $\times$ " est commutative.

✿ Remarque

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

$$(A, +, \times) \text{ est un corps } \iff \text{Inv}(A) = A \setminus \{0\}.$$

✿ Proposition

Si $(A, +, \times)$ est un corps, alors $(A, +, \times)$ est un anneau intègre.

✿ Théorème

Soit $p \in \mathbb{N}$ avec $p \geq 2$. Alors les assertions suivantes sont équivalentes :

- $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps.
- L'anneau $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est intègre
- p est un nombre premier.

* Sous-corps

- Soit $(K, +, \times)$ un corps d'élément neutre 1 pour la loi $\times$. Soit L une partie de K . K est un sous-corps du corps $(K, +, \times)$ si :

$$\begin{cases} 1 \in L \\ \forall (x, y) \in L^2, x - y \in L \\ \forall (x, y) \in L^2, x \times y \in L \\ \forall x \in L \setminus \{0\}, x^{-1} \in L \end{cases}$$

* Morphisme d'anneaux

Soient $(A, +_A, \times_A)$ et $(B, +_B, \times_B)$ deux anneaux.

- $f : (A, +_A, \times_A) \rightarrow (B, +_B, \times_B)$ est un morphisme de l'anneaux si :

$$\begin{cases} f(1_A) = 1_B \\ f(x +_A y) = f(x) +_B f(y) \\ f(x \times_A y) = f(x) \times_B f(y) \end{cases}$$

- $\text{Ker}(f) = \{x \in A, f(x) = 0_B\} = f^{-1}(\{0_B\}) \subset A$.
- $\text{Im}(f) = \{f(x), x \in A\} \subset B$.
- f est injectif si et seulement si $\text{Ker}(f) = \{0_A\}$.
- f est surjectif si et seulement si $\text{Im}(f) = B$.

* Propriétés

Soient $(A, +_A, \times_A)$ et $(B, +_B, \times_B)$ deux anneaux et $f : (A, +, \times) \rightarrow (B, +_B, \times_B)$ est un morphisme de l'anneaux. Alors :

- 1) $f(0_A) = 0_B$
- 2) $\forall x \in A, f(-x) = -f(x)$ 3) $\forall x \in A, \forall k \in \mathbb{Z}, f(kx) = kf(x)$.
- 4) $\forall x \in A, \forall k \in \mathbb{N}, f(x^k) = (f(x))^k$
- 5) Si x est inversible dans A , alors $f(x)$ est inversible dans B et on a $f(x^{-1}) = (f(x))^{-1}$.
- 6) $\text{Im}(f)$ est un sous-anneau de B .

* Proposition

Soient $(A, +_A, \times_A)$ et $(B, +_B, \times_B)$ deux anneaux et $f : (A, +, \times) \rightarrow (B, +_B, \times_B)$ est un morphisme de l'anneaux.

- Si f est bijective, on dit que f est un isomorphisme d'anneaux.
- Si f est bijective de A dans A , on dit que f est un automorphisme d'anneaux.

* Définition

Soient $(A, +_A, \times_A)$ et $(B, +_B, \times_B)$ deux anneaux et $f : (A, +, \times) \rightarrow (B, +_B, \times_B)$ est un morphisme de l'anneaux.

- 1) f est injectif $\iff \text{Ker}(f) = \{0_A\}$.
- 2) f est surjective $\iff \text{Im}(f) = B$.

* Idéaux d'un anneau commutatif

* Idéal

Soient $(A, +, \times)$ un anneau commutatif et I une partie de A . I est un idéal de l'anneau $(A, +, \times)$ si

$$\begin{cases} (I, +) \text{ est un sous groupe de } (A, +) \\ \forall x \in I, \forall a \in A, a \times x \in I. \end{cases} \iff$$

$$\begin{cases} 0_A \in I \\ \forall (x, y) \in I^2, x - y \in I \\ \forall x \in I, \forall a \in A, a \times x \in I. \end{cases}$$

* Exemples

- 1) $\forall n \in \mathbb{Z}, n\mathbb{Z}$ est un idéal de $\mathbb{Z}$.
- 2) $\forall P \in IK[X], PIK[X]$ est un idéal de $IK[X]$.

Remarque

Soient $(A, +, \times)$ un anneau commutatif et I un idéal de A .

• Si $1_A \in I$, alors $I = A$.

• Si I contient un élément inversible de A , alors $I = A$.

$$\text{car } u \in I \text{ et } u \text{ inversible} \Rightarrow \exists x, y \in A, xy = 1 \Rightarrow x \in I, y \in I \Rightarrow 1 \in I \Rightarrow A = I$$

Proposition

Soit $(A, +, \cdot)$ un anneau commutatif

1) Pour tout $x \in A$, l'ensemble

$$xA = \{ax, a \in A\} \text{ est un idéal de } A.$$

Soit I et J deux idéaux de A , alors.

1) $I \cap J$ est un idéal de A .

2) $I + J$ est un idéal de A .

Théorème

Soit $(A, +, \cdot)$ un anneau commutatif. Alors,

• Soit $f : (A, +, \cdot) \rightarrow (B, +, \cdot)$ un morphisme de l'anneaux, alors $\ker(f)$ est un idéal de $(A, +, \cdot)$.

Théorème

I est un idéal de l'anneau $(\mathbb{Z}, +, \cdot)$ si et seulement si il existe $n \in \mathbb{Z}$ tel que $I = n\mathbb{Z}$.

Divisibilité dans un anneau commutatif intègre

Soit $(A, +, \times)$ un anneau commutatif intègre, a et b deux éléments de A .

• On dit que a divise b s'il existe $q \in A$ tel que $b = qa$.

• a divise $b \iff bA \subset aA$

Théorème chinois

Soient m et n deux entiers naturels non nuls et premiers entre eux et $x \in \mathbb{Z}$. on note $\bar{x}$, $\hat{x}$ et $\tilde{x}$ les classes de x respectivement dans $\mathbb{Z}/m\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ et $(\mathbb{Z}/m\mathbb{Z}, +, \times) \times (\mathbb{Z}/n\mathbb{Z}, +, \times)$ Alors l'application

$$\begin{cases} f : (\mathbb{Z}/m\mathbb{Z}, +, \times) \rightarrow (\mathbb{Z}/m\mathbb{Z}, +, \times) \times (\mathbb{Z}/n\mathbb{Z}, +, \times) \\ \bar{x} \mapsto (\bar{x}, \hat{x}) \end{cases}$$

est un isomorphisme.

Indicatrice d'Euler

On définit, la fonction indicatrice d'Euler φ par : $\forall n \in \mathbb{N}$ avec $n \geq 2$,

$$\varphi(n) = \text{card}\{k \in \{0, \dots, n\} \text{ tel que } \text{pgcd}(k, n) = 1\}.$$

• Soient p et n deux entiers supérieurs ou égale à deux tels que p et n sont premiers entre eux. Alors

$$\varphi(np) = \varphi(n)\varphi(p).$$

Remarque

$\varphi(n) = \text{card}\{k \in \mathbb{Z}, \text{ tel que } \bar{k} \text{ est inversible dans } \mathbb{Z}/n\mathbb{Z}\}.$

Théorème

1) Pour tout nombre premier p , $\varphi(p) = p - 1$

2) Pour tout nombre premier p et tout entier naturel non nul k , $\varphi(p^k) = p^k - p^{k-1}$.

3) Pour tout nombre entier $n \geq 2$,

$$\varphi(n) = n \prod_{p \text{ premier} \atop p|n} \left(1 - \frac{1}{p}\right)$$

* Théorème d'Euler

Soient $n \geq 2$ et $a \in \mathbb{Z}$ tels que $\text{pgcd}(a, n) = 1$, alors

$$a^{\varphi(n)} \equiv 1(n).$$

En particulier, si n est un nombre premier tels que $\text{pgcd}(a, n) = 1$, alors $a^{n-1} \equiv 1(n)$.

* Algèbres

Soient A un ensemble, "+" et "×" deux lois de composition interne et "." une loi de composition externe sur le corps $IK = \mathbb{R}$ ou $\mathbb{C}$.

On dit que $(A, +, \times, \cdot)$ est une IK -algèbre si

- $(A, +, \cdot)$ est un IK -espace vectoriel
 - $(A, +, \times)$ est un anneau
 - $\forall (x, y) \in A^2, \lambda(x \times y) = (\lambda \cdot x) \times y = x \times (\lambda \cdot y)$
- L'algèbre $(A, +, \times, \cdot)$ est commutatif si la loi $\times$ est commutative.

* Exemple fondamentaux

- $(\mathbb{C}, +, \times, \cdot)$ est une $\mathbb{R}$ -algèbre commutative
- $(IK[X], +, \times, \cdot)$ est une IK -algèbre commutative.
- $(M_n(IK), +, \cdot, \times)$ est une algèbre non commutative.
- $(\mathcal{L}(E), +, \cdot, \circ)$ est une algèbre non commutative.

* Sous-algèbre.

Soit $(A, +, \cdot, \times)$ une IK -algèbre et B une partie de A .

B est une sous-algèbre de l'algèbre $(A, +, \cdot, \times)$ si

- $1_A \in B$
- $\forall (x, y) \in B^2, \forall \lambda \in IK, \lambda \cdot x + y \in B$
- $\forall (x, y) \in B^2, x \times y \in B$

* Morphisme d'algèbres.

Soient $(A, +, \cdot, \times)$, $(B, +, \cdot, \times)$ deux IK -algèbres et $f : A \rightarrow B$.

On dit que f est un morphisme d'algèbres si

- $f(1_A) = 1_B$
- $\forall (x, y) \in A^2, f(x + y) = f(x) + f(y)$
- $\forall (x, y) \in A^2, f(x \times y) = f(x) \times f(y)$
- $\forall x \in A \text{ et } \lambda \in IK, f(\lambda \cdot x) = \lambda f(x)$

Exemple.

L'application $z \mapsto \bar{z}$ est un morphisme la $\mathbb{R}$ -algèbre $(\mathbb{C}, +, \times, \cdot)$ sur elle-même.

Anneaux de polynômes

Dans notre partie IK est un sous-corps de $\mathbb{C}$.

* Les idéaux

Les idéaux de l'anneau $(IK[X], +, \times)$ sont de la forme

$$P \times IK[X] = \{P \times Q, Q \in IK[X]\} \text{ où } P \in IK[X].$$

* PGCD de deux polynômes non nuls

Soient A et B deux polynômes non nuls.

- Le $\text{PGCD}(A, B)$ est le polynôme unitaire, diviseur commun à A et à B de degré maximum.

- A et B sont premiers entre eux si $\text{PGCD}(A, B) = 1$.

* Propriétés

- 1) Si D est un diviseur commun à deux polynômes non nuls, alors D divise leur PGCD.
- 2) Pour tous polynômes A et $B \in IK[X]$, et tous λ et $\mu \in IK$, $\text{PGCD}(\lambda A, \mu B) = \text{PGCD}(A, B)$.
- 3) $\text{PGCD}(A, B) = \text{PGCD}(B, A)$.
- 4) $\text{PGCD}(\text{PGCD}(A, B), C) = \text{PGCD}(A, \text{PGCD}(B, C))$.
- 5) Soient C un polynôme unitaire, alors $\text{PGCD}(CA, CB) = C \text{PGCD}(A, B)$.
- 6)

* Théorème

Soient $A, B \in IK[X]$ et $D = PGCD(A, B)$, alors il existe $A_1, B_1 \in IK[X]$ tels que $A = DA_1$ et $B = DB_1$ avec $PGCD(A_1, B_1) = 1$.

* Théorème de Bézout

A et B sont premiers entre eux si et seulement si il existe deux polynômes U et V tels que $AU + BV = 1$.

* Théorème de Gauss

Soient A, B et C trois polynômes non nuls.

Si A divise BC et A et B sont premiers entre eux, alors A divise C .

* PGCD de plusieurs polynômes

Soient $n \geq 2$, et $A_1, \dots, A_n$, n polynômes non nuls.

Le $PGCD(A_1, \dots, A_n)$ est l'unique polynôme unitaire D qui divise $A_1, \dots, A_n$ et de degré maximum.

Si D est un diviseur commun à $A_1, \dots, A_n$, alors D divise leur PGCD.

On dit que $(A_1, \dots, A_n)$ sont premiers entre eux si $PGCD(A_1, \dots, A_n) = 1$.

On dit que $(A_1, \dots, A_n)$ sont deux à deux premiers entre eux si $PGCD(A_i, A_j) = 1, \forall i \neq j$.

* Théorème

Si $D = PGCD(A_1, \dots, A_n)$, alors il existe n des polynômes $U_1, \dots, U_n$ tels que $A_1U_1 + \dots + A_nU_n = D$.

Si $(A_1, \dots, A_n)$ sont deux à deux premiers entre eux, alors ils sont premiers entre eux.

* PPCM de deux polynômes

Le $PPCM(A, B)$ est le polynôme unitaire degré minimum, multiple commun à A et B .

* Propriétés

- 1) $PPCM(A, B) = PPCM(B, A)$.
- 2) Soient C un polynôme unitaire, alors $PPCM(CA, CB) = CPPCM(A, B)$.

* Théorème

Soient A et B deux polynômes non nuls et unitaires. Alors

$$PGCD(A, B) \cdot PPCM(A, B) = AB$$

En particulier, si $PGCD(A, B) = 1$ (et A et B unitaires), alors $PPCM(A, B) = AB$.

* Irréductibilité

* Théorème de d'Alembert-Gauss

Soit P un élément de $\mathbb{C}[X]$ de degré supérieur ou égal à 1. Alors P admet au moins une racine dans $\mathbb{C}$.

* Polynôme irréductible

Soit P un élément de $IK[X]$.

- On dit que P est irréductible sur IK s'il n'existe pas de polynômes A et B , tous deux de degré supérieur ou égal à 1, tel que $P = AB$.
- Les polynômes irréductibles sur $\mathbb{C}$ sont les polynômes de degré 1.
- Les polynômes de $\mathbb{R}[X]$ irréductibles sur $\mathbb{R}$ sont les polynômes de degré 1 et les polynômes de degré 2 à discriminant strictement négatif.

* Théorème

- Soit $P \in \mathbb{R}[X]$ de degré supérieur ou égal à 1 et $z \in \mathbb{C}$. z est racine de P si et seulement si $\bar{z}$ est racine de P et dans ce cas, z et $\bar{z}$ ont même ordre de multiplicité.

✿ Décomposition en facteurs irréductibles dans $\mathbb{C}[X]$.

Soit P un élément de $\mathbb{C}[X]$ de degré supérieur ou égal à 1. P s'écrit, de manière unique sous la forme

$$P = \lambda \prod_{k=1}^p (X - z_k)^{\alpha_k}$$

où $z_1, \dots, z_p$, sont des nombres complexes deux à deux distincts et $\alpha_1, \dots, \alpha_p$ sont des entiers naturels non nuls.

✿ Décomposition en facteurs irréductibles dans $\mathbb{R}[X]$.

Tout polynôme de $\mathbb{R}[X]$, de degré supérieur ou égal à 1, s'écrit de manière unique à l'ordre près des facteurs, sous la forme :

$$P = \lambda \prod_{k=1}^p (X - z_k)^{\alpha_k} \prod_{k=1}^q (X^2 + b_k X + c_k)^{\beta_k}$$

$\lambda = \text{dom}(P)$, les a_k sont des réels deux à deux distincts, les (b_k, c_k) sont des couples de réels tels que $b_k^2 - 4c_k < 0$.