4

Structures algébriques

I Groupes et sous-groupes

1 Structure de groupe (MP2I)

Définition 1 : Groupe

On appelle **groupe** tout couple $(G,\star)$ où G est un ensemble tel que

(i) $\star$ est une loi de composition interne sur G

(ii) $\star$ est associative

(iii) G admet un élément neutre pour $\star$

(iv) Tout élément de G admet un symétrique dans G pour $\star$.

Si, de plus, $\star$ est commutative, on dit que $(G,\star)$ est un **groupe commutatif** ou **groupe abélien**.

2 Puissances ou itérées d'un élément (MP2I)

Définition 2 : Itérées d'un élément

Soir E un ensemble muni d'une loi de composition interne $\star$ (notée multiplicativement) **associative** et possédant un élément neutre e.

Pour tout $x\in E$ et tout $n\in\mathbb{N}$, on définit récursivement

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

Propriété 1 : des exposants

Soient $x,y\in E$ et $n,m\in\mathbb{N}$.

(i) $x^{n+m}=x^n\star x^m=x^m\star x^n$.

(ii) $(x^n)^m=x^{nm}=(x^m)^n$.

(iii) *Si* $x\star y=y\star x$, $(x\star y)^n=x^n\star y^n$.

(iv) *Si x est inversible, x^n est inversible et* $(x^n)^{-1}=(x^{-1})^n$.

Notation 1 : Exposant négatif

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

3 Régularité

Soit [1] E un ensemble muni d'une loi de composition interne associative $\star$ et possédant un élément neutre e.

Définition 3 : Régularité

Soit $x\in E$. On dit que x est **régulier** (ou **simplifiable**)

- **à gauche** lorsque
$$\forall\, a,b\in E,\quad x\star a=x\star b\Longrightarrow a=b$$
- **à droite** lorsque
$$\forall\, a,b\in E,\quad a\star x=b\star x\Longrightarrow a=b$$

On dit que x est **régulier** lorsqu'il l'est à gauche et à droite.

Propriété 2 : Régularité d'un inversible

Tout élément inversible de $(E,\star)$ est régulier.

Corollaire 1 : Régularité dans un groupe

Si $(G,\star)$ est un groupe, alors tout élément de G est régulier.

Corollaire 2 : Bijectivité des translations

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

Les applications $\varphi_a:\left|\begin{array}{ccc}G&\longrightarrow&G\\ x&\longmapsto&a\star x\end{array}\right.$ *et* $\psi_a:\left|\begin{array}{ccc}G&\longrightarrow&G\\ x&\longmapsto&x\star a\end{array}\right.$ *(appelées translations à gauche et à droite) sont bijectives.*

Corollaire 3

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

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

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

4 Groupe produit (MP2I)

Propriété 3 : Groupe produit

Soit $(G,\star)$ et (H,Δ) des groupes.
Pour tout (g,h) et (g',h') dans $G\times H$, on pose

$$(g,h)\top(g',h') = (g\star g', h\Delta h').$$

Alors $(G\times H,\top)$ a une structure de groupe.
Si, de plus, les lois $\star$ et Δ sont commutatives, alors $\top$ l'est.

5 Sous-groupes

a Définition et caractérisation (MP2I)

Définition 4 : Sous-groupe

Soit $(G,\star)$ groupe. On note $\star|_{H^2}$ la restriction à H^2 de la loi $\star$.
On dit que H est un **sous-groupe** de $(G,\star)$ si $H\subset G$ et $(H,\star|_{H^2})$ est un groupe.

Propriété 4 : Sous-groupes triviaux

*Soit $(G,\star)$ groupe. G et $\{e_G\}$ sont des sous-groupes de $(G,\star)$ appelés **sous-groupes triviaux**.*

Propriété 5

Soit H un sous-groupe de $(G,\star)$.

(i) $(H,\star)$ possède le même élément neutre que $(G,\star)$.

(ii) Si $x\in H$, alors x a même inverse dans $(H,\star)$ et dans $(G,\star)$.

Propriété 6 : caractérisation des sous-groupes

Soit $(G,\star)$ un groupe (multiplicatif). Les propositions suivantes sont équivalentes :

(i) H est un sous-groupe de $(G,\star)$

(ii)
$$\begin{cases} H\subset G \\ H\neq\varnothing \quad (e_G\in H) \\ H \text{ est stable par } \star \ : \ \forall x,y\in H,\ x\star y\in H \\ H \text{ est stable par inverse } \ : \ \forall x\in H,\ x^{-1}\in H \end{cases}$$

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

b Intersection et réunion (MPI)

Propriété 7 : Intersection de sous-groupes

Soit $(G,\star)$ un groupe et $(H_i)_{i\in I}$ une famille de sous-groupes de $(G,\star)$. Alors $\bigcap_{i\in I} H_i$ est un sous-groupe de $(G,\star)$.

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

Notation 2

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

Propriété 8 : Sous-groupes de $(\mathbb{Z},+)$

Les sous-groupes G de $(\mathbb{Z},+)$ sont exactement les $a\mathbb{Z}$ pour $a\in\mathbb{N}$.
De plus, si $G\neq\{0\}$, $a = \min(G\cap\mathbb{N}^*)$.

6 Morphismes (MP2I)

a Définition

Définition 5 : Morphisme de groupe

Soient $(G,\star)$ et $(G',\bullet)$ deux groupes.
$f : (G,\star)\to(G',\bullet)$ est un **morphisme de groupes** si et seulement si

$$\forall (x,y)\in G^2,\ f(x\star y) = f(x)\bullet f(y)$$

Lorsque $(G,\star) = (G',\bullet)$, on parle d'**endomorphisme** de groupes.
Lorsque f est bijective, on parle d'**isomorphisme**.
Lorsqu'il existe un isomorphisme entre G et G', on dit que G et G' sont **isomorphes.**
Lorsque f est bijective et $G = G'$, on parle d'**automorphisme**.

Propriété 9 : Image du neutre et du symétrique par un morphisme de groupes

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

Propriété 10 : Image d'une itérée

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

Propriété 11 : Composée de morphismes

Si $f : (G,\star) \to (G',\bullet)$ et $g : (G',\bullet) \to (G'',\Delta)$ sont des morphismes de groupes, alors $g \circ f$ en est encore un.

b Noyau et image

Définition 6 : Image et noyau d'un morphisme

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

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

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

Ainsi, $x \in \operatorname{Ker} f \iff f(x) = e_{G'}$.

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

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

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

Propriété 12 : Caractérisations de l'injectivité et de la surjectivité

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

- *f est injectif si et seulement si $\operatorname{Ker} f = \{e_G\}$.*
- *f est surjectif si et seulement si $\operatorname{Im} f = G'$.*

Propriété 13 : Images directe et réciproque d'un sous-groupe

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

(i) Si H est un sous-groupe de $(G,\star)$, alors $f(H)$ est un sous-groupe de $(G',\bullet)$

(ii) Si H' est un sous-groupe de $(G',\bullet)$, $f^{(-1)}(H')$ est un sous-groupe de $(G,\star)$.

Corollaire 4 : Cas particulier du noyau et de l'image

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

Alors $\operatorname{Ker} f$ est un sous-groupe de $(G,\star)$ et $\operatorname{Im} f$ est un sous-groupe de $(G',\bullet)$.

c Isomorphismes

Propriété 14 : Réciproque d'un isomorphisme

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

Alors f^{-1} est un isomorphisme du groupe $(G',\bullet)$ sur le groupe $(G,\star)$.

7 Groupes monogènes (MPI)

a Sous-groupes engendré par une partie

Définition 7 : Groupe engendré par une partie

Soit $(G,*)$ un groupe, A partie non vide de G.

On appelle **sous-groupe engendré par** A le plus petit (au sens de l'inclusion) sous-groupe de G contenant A, noté $\langle A\rangle$.

On dit alors que A est une **partie génératrice** de $\langle A\rangle$.

Propriété 15 : Éléments de $\langle A\rangle$

Les éléments de $\langle A\rangle$ sont exactement les produits (pour $*$) d'éléments de A ou de A^{-1}.

Autrement dit, $x \in \langle A\rangle$ si et seulement s'il existe $k \in \mathbb{N}$, $(a_1,\dots,a_k) \in A^k$ et $(\varepsilon_1,\dots,\varepsilon_k) \in \{-1,1\}^k$ tel que

$$x = a_1^{\varepsilon_1} * \cdots * a_k^{\varepsilon_k}.$$

b Groupes monogènes et cycliques

Propriété 16 : Sous-groupe engendré par un élément

*Soit $a \in G$. Le sous-groupe **engendré par** a noté $\langle a\rangle$ plutôt que $\langle\{a\}\rangle$ est*

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

*On dit que a en est un **générateur**.*

Définition 8 : Groupe monogène

Un groupe G est dit **monogène** s'il est engendré par un seul élément, c'est-à-dire s'il existe $a \in G$ tel que $G = \langle a \rangle$.

Un groupe G est dite **cyclique** si et seulement s'il est monogène et fini.

C Ordre d'un élément dans un groupe

$(G, *)$ est un groupe d'élément neutre e.

Définition 9 : Ordre d'un élément

On dit que $a \in G$ est **d'ordre fini** s'il existe $k \in \mathbb{N}^*$ tel que $a^k = e$.

Dans ce cas, on appelle **ordre de** a le plus petit $k \in \mathbb{N}^*$ tel que $a^k = e$.

Propriété 17 : de l'ordre d'un élément

Soit a un élément de G d'ordre fini m.

- *Si $k \in \mathbb{Z}$, $a^k = e$ si et seulement si $k \in m\mathbb{Z}$ ie m divise k.*
- *$\langle a \rangle = \{a^k, k \in [\![0, m-1]\!]\}$ et $|\langle a \rangle| = m$.*

Propriété 18 : Morphie des groupes monogènes

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

Tout groupe monogène fini (donc cyclique) de cardinal n est isomorphe à $(\mathbb{U}_n, +)$

Propriété 19 : de l'ordre

Soit $(G, *)$ un groupe fini de neutre e.

(i) Tout élément de G est d'ordre fini.

(ii) L'ordre de tout élément de G divise le cardinal de G.

(iii) Pour tout $a \in G$, $a^{|G|} = e$.

II Anneaux et Corps

1 Anneaux (MP2I)

Définition 10 : Distributivité

Soit E un ensemble et $\star$ et $\top$ deux lois de composition interne sur E, on dit que $\star$ est **distributive** sur $\top$ lorsque $\forall (x, y, z) \in E^3$,

$$x \star (y \top z) = (x \star y) \top (x \star z),$$

$$(y \top z) \star x = (y \star x) \top (z \star x).$$

Définition 11 : Anneau

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

(i) $(A, +)$ est un groupe abélien. L'élément neutre est noté 0_A.

(ii) $\times$ est une loi de composition interne associative admettant un élément neutre appelé unité de A, noté 1_A.

(iii) $\times$ est distributive sur $+$.

Lorsque, de plus, $\times$ est commutative, on dit que $(A, +, \times)$ est un **anneau commutatif.**

2 Groupe des inversibles (MP2I)

Définition 12 : Inversibles d'un anneau

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

$a \in A$ est dit **inversible** si et seulement s'il est symétrisable pour $\times$.

Son symétrique est appelé **inverse** de a, noté a^{-1}.

On note U_A ou $U(A)$ ou $A^\times$ l'ensemble des inversibles de A.

Propriété 20 : Groupe des inversibles

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

3 Calculs dans un anneau (MP2I)

Propriété 21 : Calculs dans un anneau

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

- *Si $a \times b = b \times a$,*

$$(ab)^n = a^n b^n.$$

- ***Formule du binôme de Newton** : Si $a \times b = b \times a$,*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

- ***Factorisation**[a] **de** $a^n - b^n$: Si $a \times b = b \times a$*

$$a^n - b^n = (a-b)\left(a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1}\right)$$

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

- ***Somme géométrique** : En particulier, pour tout $x \in A$;*

$$1_A - x^n = (1_A - x) \times \sum_{k=0}^{n-1} x^k$$

a. parfois appelée formule de Bernoulli

4 Corps (MP2I)

Définition 13 : Corps

Soit $\mathbb{K}$ un ensemble, $+, \times$ deux lois de composition internes sur $\mathbb{K}$. On dit que $(\mathbb{K}, +, \times)$ est un **corps** lorsque

- $(\mathbb{K}, +, \times)$ est un anneau commutatif.
- $\mathbb{K} \setminus \{0_\mathbb{K}\}$ est non vide et tous ses éléments sont inversibles (c'est-à-dire $\mathbb{K} \neq \{0_\mathbb{K}\}$ et $U_\mathbb{K} = \mathbb{K}^\times = \mathbb{K} \setminus \{0_\mathbb{K}\}$.)

ou, de manière équivalente,

- $(\mathbb{K}, +)$ est un groupe abélien,
- $(\mathbb{K} \setminus \{0_\mathbb{K}\}, \times)$ est un groupe,
- $\times$ est commutative et distributive sur $+$.

5 Intégrité (MP2I)

Définition 14 : Anneau intègre

Un anneau $(A, +, \times)$ est dit **intègre** si

- A est commutatif,
- $A \neq \{0_A\}$ c'est-à-dire $1_A \neq 0_A$,
- A n'admet aucun diviseur de zéro, c'est-à-dire

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

Propriété 22 : Généralisation

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

Propriété 23 : Régularité dans un anneau intègre

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

Propriété 24 : Intégrité d'un corps

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

6 Anneau produit (MPI)

Propriété 25 : Anneau produit

Soit $(A, \dot{+}, \dot{\times})$ et $(B, \oplus, \otimes)$ des anneaux.
Pour tout (a, b) et (a', b') dans $A \times B$, on pose

$$(a, b) + (a', b') = (a \dot{+} a', b \oplus b')$$
$$(a, b) \times (a', b') = (a \dot{\times} a', b \otimes b')$$

Alors $(A \times B, +, \times)$ a une structure d'anneau.
Si, de plus, les lois $\dot{\times}$ et $\otimes$ sont commutatives, alors $\times$ l'est.

Propriété 26 : Inversion dans un anneau produit

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

$$(a, b)^{-1} = (a^{-1}, b^{-1}).$$

7 Sous-anneau et sous-corps (MP2I)

Définition 15 : Sous-anneau

Soit $(A, +, \times)$ un anneau. On dit que B est un **sous-anneau** de $(A, +, \times)$ lorsque

- $B \subset A$
- **Important :** $1_A \in B$
- $(B, +|_{B^2}, \times|_{B^2})$ est un anneau.

Propriété 27 : Caractérisation des sous-anneaux

B est un sous-anneau de $(A, +, \times)$ si et seulement si

$$\begin{cases} B \subset A \\ (B, +) \text{ est un sous-groupe de } (A, +) \\ B \text{ est stable par } \times : \forall\, x, y \in B,\quad x \times y \in B \\ 1_A \in B \end{cases}$$

ou, de manière équivalente,

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

ou encore

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

Définition 16 : Sous-corps

Soit $(\mathbb{K}, +, \times)$ un corps. On dit que $(\mathbb{L}, +, \times)$ est un **sous-corps** de $(\mathbb{K}, +, \times)$ lorsque $\mathbb{L} \subset \mathbb{K}$ et $(\mathbb{L}, +|_{\mathbb{L}^2}, \times|_{\mathbb{L}^2})$ est un corps.

Propriété 28 : Caractérisation des sous-corps

$(\mathbb{L}, +, \times)$ est un sous-corps de $(\mathbb{K}, +, \times)$ si et seulement si

$$\begin{cases} \mathbb{L} \subset \mathbb{K} \\ (\mathbb{L}, +) \text{ est un sous-groupe de } (\mathbb{K}, +) \\ (\mathbb{L} \setminus \{0_{\mathbb{K}}\}, \times) \text{ est un sous-groupe de } (\mathbb{K} \setminus \{0_{\mathbb{K}}\}, \times) \end{cases}$$

ou, de manière équivalente,

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

8 Morphismes d'anneaux (MP2I)

Définition 17 : Morphisme d'anneaux

Soient $(A, +, \times)$ et $(A', \oplus, \otimes)$ deux anneaux.
$f : (A, +, \times) \to (A', \oplus, \otimes)$ est un **morphisme d'anneaux** si et seulement si

(i) $\forall (a, b) \in A^2,\ \ f(a + b) = f(a) \oplus f(b)$
(ie $f : (A, +) \to (A', \oplus)$ morphisme de groupes)

(ii) $\forall (a, b) \in A^2,\ \ f(a \times b) = f(a) \otimes f(b)$

(iii) $f(1_A) = 1_{A'}$

On parle aussi, d'**endomorphisme**, d'**isomorphisme** et d'**automorphisme** d'anneaux.

$\operatorname{Ker} f = f^{(-1)}(\{0_{A'}\}) = \{a \in A \mid f(a) = 0_{A'}\}$ est le **noyau** de f.

$\operatorname{Im} f = f(A) = \{f(x),\ x \in A\}$ est l'**image** de f.

Propriété 29 : des morphismes d'anneaux

Soit $f : (A, +, \times) \to (B, \oplus, \otimes)$ est un morphisme d'anneaux.

(i) Si a est inversible dans A, alors $f(a)$ l'est dans B et $f(a^{-1}) = (f(a))^{-1}$.

(ii) Si f est un isomorphisme alors $f^{-1} : (B, \oplus, \otimes) \to (A, +, \times)$ est aussi un isomorphisme d'anneau.

(iii) Si $g : (B, \oplus, \otimes) \to (C, \dot{+}, \dot{\times})$ est aussi un morphisme d'anneau, alors $g \circ f : (A, +, \times) \to (C, \dot{+}, \dot{\times})$ l'est encore.

Définition 18 : Morphisme de corps

Soient $(\mathbb{K}, +, \times)$ et $(\mathbb{K}', \oplus, \otimes)$ deux corps.
$f : (\mathbb{K}, +, \times) \to (\mathbb{K}', \oplus, \otimes)$ est un **morphisme de corps** si et seulement s'il s'agit d'un morphisme d'anneaux.

III Idéal d'un anneau commutatif (MPI)

1 Généralités

Définition 19 : Idéal

Soit $(A, +, \times)$ un anneau **commutatif** et $I \subset A$. On dit que I est un **idéal** de $(A, +, \times)$ lorsque

(i) I est un sous-groupe de $(A, +)$

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

Propriété 30 : Idéaux triviaux

Soit $(A, +, \times)$ un anneau commutatif. $\{0_A\}$ et A sont des idéaux (triviaux) de $(A, +, \times)$.
Ce sont les seuls idéaux si de plus $(A, +, \times)$ est un corps.

Propriété 31 : Noyau d'un morphisme d'anneaux

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

2 Somme et intersection d'idéaux

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

Propriété 32 : Somme et intersection d'idéaux

(i) *Soient $I_1, \dots, I_n$ des idéaux de $(A,+,\times)$. On note*

$$I_1 + \cdots + I_n = \{x_1 + \cdots + x_n,\ \forall\, j \in [\![1,n]\!],\ \ x_j \in I_j\}$$

Il s'agit d'un idéal de $(A,+,\times)$.
Il s'agit plus précisément du plus petit idéal de $(A,+,\times)$ (au sens de l'inclusion) contenant tous les idéaux I_j pour $1 \leqslant j \leqslant n$.

(ii) *Soient $(I_j)_{j\in J}$ une famille d'idéaux de $(A,+,\times)$.*
Alors $\bigcap_{j\in J} I_j$ est un idéal de $(A,+,\times)$.
Il s'agit du plus grand idéal de $(A,+,\times)$ (au sens de l'inclusion) contenu dans les idéaux I et J.

3 Idéal principal

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

Propriété 33 : Idéal engendré par un élément

Soit $x \in A$. On note

$$(x) = xA = \{xa, a \in A\}.$$

*C'est un idéal de A, appelé **idéal engendré** par x.*

Définition 20 : Idéal et anneau principal (HP)

- Tout idéal de la forme xA (donc engendré par un seul élément) est dit **principal**.
- Un anneau commutatif est dit **principal** lorsque
  (i) C'est un anneau intègre.
  (ii) Tous ses idéaux sont principaux.

Théorème 1 : Principalité de $\mathbb{Z}$

L'anneau $\mathbb{Z}$ est principal.

4 Divisibilité dans un anneau intègre

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

Définition 21 : Divisibilité

Soient $a, b \in A$.
On dit que b **divise** a ou que a est multiple de b lorsqu'il existe $q \in A$ tel que $a = bq$. On note $b|a$.
a et b sont dit associés lorsque $a|b$ et $b|a$.

Propriété 34 : Caractérisation avec les idéaux

Soient $a, b \in A$.
b divise a si et seulement si $a \in bA$ si et seulement si $aA \subset bA$.

Propriété 35 : Éléments associés

*On rappelle que $(A,+,\times)$ est un anneau commutatif **intègre**. Soient $a, b \in A$.*
a et b sont associés si et seulement si $aA = bA$ si et seulement s'il existe $u \in U_A$ tel que $b = ua$.

IV ARITHMÉTIQUE SUR $\mathbb{Z}$ (MP2I)

1 PGCD

Définition 22 : PGCD

Soient $a, b \in \mathbb{Z}$.
$I = (a) + (b) = a\mathbb{Z} + b\mathbb{Z} = \{au + bv,\ u, v \in \mathbb{Z}\}$ est un idéal non réduit à $\{0\}$ de $(\mathbb{Z},+,\times)$ qui est un anneau principal.
Son unique générateur positif est appelé **pgcd de a et b**, noté $a \wedge b$.
On a donc, par définition, $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$.

Propriété 36 : Relation de Bézout

Si $a, b \in \mathbb{Z}$, on peut trouver $a, b \in \mathbb{Z}$ tels que $au + bv = a \wedge b$.

Propriété 37 : Caractérisation

Soit $(a,b) \in \mathbb{Z}^2$.

$$d = a \wedge b \iff \begin{cases} d \in \mathbb{N} \\ d|a \text{ et } d|b \\ \forall\, c \in \mathbb{Z},\ \ (c|a \text{ et } c|b) \Longrightarrow c|d \end{cases}$$

Il s'agit donc du plus grand diviseur positif au sens de la division.
Par conséquent, les diviseurs de $a \wedge b$ sont exactement les diviseurs communs de a et de b.

Propriété 38 : Propriété d'Euclide

Si $a, b, q \in \mathbb{Z}$, $a \wedge b = (a - bq) \wedge b$ (pas nécessairement une division euclidienne).

Définition 23 : Nombre entiers premiers entre eux

$a, b \in \mathbb{Z}$ sont dits **premiers entre eux** lorsque $a \wedge b = 1$, c'est-à-dire lorsque les seuls diviseurs communs ± 1.

Théorème 2 : de Bézout

Soit $a, b \in \mathbb{Z}$.

$$a \wedge b = 1 \iff \exists\, u, v \in \mathbb{Z},\ \ au + bv = 1$$

Corollaire 5

Soient $a, b, c \in \mathbb{Z}$.

(i) $a \wedge bc = 1 \iff a \wedge b = a \wedge c = 1$

(ii) Si $d = a \wedge b$, on a $a', b' \in \mathbb{Z}$ tels que $a = da'$, $b = db'$ et $a' \wedge b' = 1$.

Théorème 3 : Lemme de Gauß

Soient $a, b, c \in \mathbb{Z}$. Si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$.

Méthode 1 : résolution des équations diophantiennes $ax + by = c$

où $a, b, c \in \mathbb{Z}^*$ sont fixés, on cherche les solutions entières.

On a facilement qu'il y a des solutions si et seulement si $\boxed{d = a \wedge b \mid c.}$

Lorsque c'est le cas, on peut trouver une solution particulière (x_0, y_0) avec l'algorithme d'Euclide par exemple.

Alors, si (x, y) solution , $ax + by = ax_0 + by_0$ puis $a(x - x_0) = b(y_0 - y)$ donc $a'(x - x_0) = b'(y_0 - y)$ avec $a' \wedge b' = 1$ en divisant par d.

Par lemme de Gauß, on a $k \in \mathbb{Z}$ tel que $x = x_0 + b'k$ puis en réinjectant $y = y_0 - a'k$.

On vérifie enfin que la réciproque étant vraie. Ensemble des solutions :

$$\{(x_0 + b'k, y_0 - a'k),\ k \in \mathbb{Z}\}.$$

2 PPCM

Définition 24 : PPCM

Le PPCM de deux entiers a, b est l'unique générateur positif $a \vee b$ de l'idéal $a\mathbb{Z} \cap b\mathbb{Z}$ des multiples communs à a et à b.

On a donc $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$.

Propriété 39 : du PPCM

(i) Il s'agit du plus petit multiple positif commun à a et à b au sens de la division.

(ii) On a toujours que $|ab| = (a \wedge b)(a \vee b)$.

3 Nombres premiers

Définition 25 : Nombre premier

Un **nombre premier** est un entier naturel $p \geqslant 2$ dont les seuls diviseurs positifs sont 1 et p.

On notera $\mathscr{P}$ l'ensemble des nombres premiers.

Propriété 40 : d'Euclide

L'ensemble des nombres premiers est infini.

Propriété 41 : Diviseur premier ou non

Si $p \in \mathscr{P}$ et $n \in \mathbb{Z}$, alors $p \mid n$ ou (exclusif) $p \wedge n = 1$.

Corollaire 6 : Nombre premier divisant un produit

Soient $p \in \mathscr{P}$ et $a_1, \ldots, a_n \in \mathbb{Z}$.

$p \mid (a_1 \times \cdots \times a_n)$ si et seulement si p divise l'un des a_k.

Théorème 4 : fondamental de l'arithmétique – Décomposition primaire

Soit $n \in \mathbb{Z}^*$. On peut trouver $k \in \mathbb{N}$, $p_1, \ldots, p_k$ premiers deux à deux distincts, $\alpha_1, \ldots, \alpha_k \in \mathbb{N}^*$ tels que

$$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

appelée décomposition primaire de n.

De plus, cette écriture est unique à l'ordre des facteurs près.

$p_1, \ldots, p_k$ sont les diviseurs premiers de n.

Définition 26 : Valuation p-adique

Soit $p \in \mathscr{P}$ et $n \in \mathbb{Z}^*$. On appelle **valuation p-adique** de n l'entier

$$v_p(n) = \max\{i \in \mathbb{N} \mid p^i \text{ divise } n\}.$$

Propriété 42 : des valuations p-adiques

Soient $n, m \in \mathbb{Z}^*$, $p \in \mathscr{P}$.

(i) $v_p(n) \neq 0 \iff p|n$

(ii) $v_p(n \times m) = v_p(n) + v_p(m)$

(iii) $n|m \iff \forall\, p \in \mathscr{P},\ \ v_p(n) \leqslant v_p(m)$

(iv) $v_p(n \wedge m) = \min(v_p(n), v_p(m))$
$v_p(n \vee m) = \max(v_p(n), v_p(m))$

4 Congruences

Définition 27 : Congruence

Soit $n \in \mathbb{N}^*$. On dit que $a, b \in \mathbb{Z}$ sont **congrus modulo** n et on note $a \equiv b\ [n]$ lorsque $n|(a-b)$ ie lorsqu'il existe $k \in \mathbb{Z}$ tel que $a = b + kn$.

Propriété 43 : Relation d'équivalence

C'est une relation d'équivalence sur $\mathbb{Z}$.

Propriété 44 : Nombre d'entiers modulo n

$\forall\, a \in \mathbb{Z},\ \ \exists!\, r \in [\![0, n-1]\!],\ \ a \equiv r\ [n]$. r est le reste de la division euclidienne de k par n.

Ainsi, la relation d'équivalence $\cdot \equiv \cdot\ [n]$ possède exactement n classes d'équivalences.

Propriété 45 : Compatibilité de $+$ et $\times$

Soient $n \in \mathbb{N}^*$ et $a, b, c, d \in \mathbb{Z}$ tels que $a \equiv b\ [n]$ et $c \equiv d\ [n]$. Alors $a + c \equiv b + d\ [n]$ et $a \times c \equiv b \times d\ [n]$.

Plus généralement, si $m \in \mathbb{N}$, $a^m \equiv b^m\ [n]$.

Propriété 46 : Petit théorème de Fermat

Si p est premier et $a \in \mathbb{Z}^*$ non divisible par p, alors

$$a^{p-1} \equiv 1\ [p].$$

Dans tous les cas (que a soit divisible ou non par p),

$$a^p \equiv a\ [p].$$

Théorème 5 : de Fermat-Wiles, ou grand théorème de Fermat

Si $n \in \mathbb{N}$ tel que $n \geqslant 3$, alors l'équation

$$x^n + y^n = z^n$$

n'admet aucune solution dans $\mathbb{N}_*^3$.

V STRUCTURE D'ALGÈBRE (MPI)

1 Algèbre et sous-algèbre

Définition 28 : Structure d'algèbre

On dit que $(\mathscr{A}, +, \times, \cdot)$ est une **$\mathbb{K}$-algèbre** lorsque

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

$$\lambda \cdot (x \times y) = (\lambda \cdot x) \times y = x \times (\lambda \cdot y).$$

Propriété 47 : Caractérisation des sous-algèbres

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

(i) $\mathscr{B} \subset \mathscr{A}$

(ii) $1_A \in \mathscr{B}$

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

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

Définition 29 : Polynôme en un élément d'une algèbre

Si $P = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{K}[X]$ et $x \in \mathscr{A}$, on pose

$$P(x) = \sum_{k=0}^{n} a_k x^k = a_0 1_{\mathscr{A}} + a_1 x + \cdots + a_n x^n.$$

Attention à ne pas oublier l'unité de $\mathscr{A}$!

2 Morphismes d'algèbres

Définition 30 : Morphisme d'algèbre

Soit $(\mathscr{A}, +, \times, \cdot)$, $(\mathscr{B}, +, \times, \cdot)$ et $f : \mathscr{A} \to \mathscr{B}$. On dit que f est un **morphisme d'algèbres** lorsque

(i) f est linéaire ie

$$\forall\, x, y \in \mathscr{A},\ \ \forall\, \lambda \in \mathbb{K},\ \ f(x + \lambda y) = f(x) + \lambda f(y)$$

(ii) $\forall\, x, y \in \mathscr{A},\ \ f(x \times y) = f(x) \times f(y)$

(iii) $f(1_{\mathscr{A}}) = 1_{\mathscr{B}}$.

Propriété 48 : Morphisme d'évaluation polynomiale

Soit $(\mathscr{A},+,\times,\cdot)$ une $\mathbb{K}$-algèbre et $x\in\mathscr{A}$.

Alors l'application $f : \left|\begin{array}{ccc}\mathbb{K}[X] & \longrightarrow & \mathscr{A} \\ P & \longmapsto & P(x)\end{array}\right.$ *est un morphisme de $\mathbb{K}$-algèbres.*

VI Complément (HP) : sous-groupes de $(\mathbb{R},+)$

Théorème 6 : Hors-Programme

Soit G est un sous-groupe de $(\mathbb{R},+)$.

Alors G est soit dense dans $\mathbb{R}$, soit discret (de la forme $\alpha\mathbb{Z}$).