Structures d'anneau, de corps, d'algèbre

I Anneaux et Corps

1 Anneaux (MP2I)

Définition 1 : 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 2 : 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 3 : 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 1 : Groupe des inversibles

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

3 Calculs dans un anneau (MP2I)

Propriété 2 : Calculs dans un anneau

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

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

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

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

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

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

$$\begin{aligned}a^n-b^n&=(a-b)\left(a^{n-1}+a^{n-2}b+\ldots+ab^{n-2}+b^{n-1}\right)\\&=(a-b)\sum_{k=0}^{n-1}a^kb^{n-1-k}.\end{aligned}$$

- ***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 4 : 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 5 : 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

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

Propriété 3 : 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 4 : Régularité dans un anneau intègre

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

Propriété 5 : Intégrité d'un corps

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

6 Anneau produit (MPI)

Propriété 6 : 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

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

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 7 : Inversion dans un anneau produit

Si $(A,+,\times)$ et $(B,+,\times)$ sont deux anneaux, alors $(A\times B)^\times = A^\times \times B^\times$.
De plus, si $(a,b) \in (A\times B)^\times$, alors

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

7 Sous-anneau et sous-corps (MP2I)

Définition 6 : 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 8 : Caractérisation des sous-anneaux

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

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

ou, de manière équivalente,

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

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 7 : 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 9 : 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 8 : 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 10 : des morphismes d'anneaux

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

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

(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 9 : 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.

II Idéal d'un anneau commutatif (MPI)

1 Généralités

Définition 10 : 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 11 : 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 12 : 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 13 : 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 tous les idéaux I_j pour $j\in J$.

3 Idéal principal

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

Propriété 14 : 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 11 : 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 12 : 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 15 : 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 16 : 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 $u\in A^\times$ tel que $b=ua$.*

III Arithmétique sur $\mathbb{Z}$

1 PGCD

Définition 13 : 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 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 17 : Relation de Bézout

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

Propriété 18 : Caractérisation

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

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

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 19 : Propriété d'Euclide

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

Définition 14 : 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 1

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 $a|bc$ et $a \wedge b = 1$, alors $a|c$.

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 $\boxed{d = a \wedge b | c.}$

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 :

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

2 PPCM

Définition 15 : 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 20 : 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 16 : Nombre premier

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

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

Propriété 21 : d'Euclide

L'ensemble des nombres premiers est infini.

Propriété 22 : Diviseur premier ou non

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

Corollaire 2 : Nombre premier divisant un produit

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

$p|(a_1 \times \cdots \times a_n)$ 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 17 : Valuation p-adique

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

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

Propriété 23 : des valuations p-adiques

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

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

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

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

(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 18 : 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 24 : Relation d'équivalence

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

Propriété 25 : 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 26 : 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 27 : Rappel : critères de divisibilité

Si $a_0, \dots, a_k$ sont les chiffres de n en base 10,

$n = a_0 + a_1 \times 10 + \cdots + a_k \times 10^k$, *avec* $\forall i,\ a_i \in [\![0, 9]\!]$.

Divisibilité par 2 : $2|n \iff 2|a_0 \iff a_0 \in \{0, 2, 4, 6, 8\}$

Divisibilité par 3 : $3|n \iff 3 \left| \sum_{i=0}^{k} a_i \right.$

Divisibilité par 4 : $4|n \iff 4|\overline{a_1 a_0}^{10}$

Divisibilité par 5 : $5|n \iff 5|a_0 \iff a_0 \in \{0, 5\}$

Divisibilité par 8 : $8|n \iff 8|\overline{a_2 a_1 a_0}^{10}$

Divisibilité par 9 : $9|n \iff 9 \left| \sum_{i=0}^{k} a_i \right.$

Divisibilité par 11 : $11|n \iff 11|(a_0 - a_1 + a_2 - a_3 + \cdots)$

Propriété 28 : 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 $\mathbb{N}_*^3$.

IV Anneau $\mathbb{Z}/n\mathbb{Z}$ (MPI)

1 Structure

Lemme 1 : Compatibilité avec $\times$

Soient $a, b, c, d \in \mathbb{Z}$ tels que $\overline{a} = \overline{c}$ et $\overline{b} = \overline{d}$. Alors $\overline{ab} = \overline{cd}$.

Définition 19 : Loi $\times$

Si $a, b \in \mathbb{Z}$, on pose $\overline{a} \times \overline{b} = \overline{ab}$, ce qui définit une loi de composition interne $\times$ sur $\mathbb{Z}/n\mathbb{Z}$.

Propriété 29 : Structure d'anneau

$\left(\mathbb{Z}/n\mathbb{Z}, +, \times\right)$ est un anneau commutatif.

Propriété 30 : Groupe des inversibles

Le groupe des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ noté $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ est l'ensemble des $\overline{k}$ pour $k \in \mathbb{Z}$ tel que $k \wedge n = 1$.

Méthode 2 : Calcul de l'inverse d'un élément inversible

Si $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ (donc si $k \wedge n = 1$), on trouve l'inverse de $\overline{k}$ soit « de tête », soit en utilisant l'algorithme d'Euclide étendu pour trouver une relation de Bézout entre k et n.

Corollaire 3 : CNS pour avoir un corps

$(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps si et seulement si p est premier.
On note alors $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

2 Théorème Chinois

Théorème 6 : chinois (ou des restes chinois)

Soient $n, m \in \mathbb{N}^*$ tels que $n \wedge m = 1$.

1re formulation *Si $a, b \in \mathbb{Z}$, alors*

$$\begin{cases} k \equiv a \ [n] \\ k \equiv b \ [m] \end{cases} \iff k \equiv c \ [nm]$$

où c est une solution particulière, qui existe bien.

2e formulation *Pour tout $k \in \mathbb{Z}$, note $(k \bmod n)$, $(k \bmod m)$ et $(k \bmod nm)$ les classes de k dans $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/nm\mathbb{Z}$ respectivement. On a alors*

(i) Si $k, \ell \in \mathbb{Z}$, et si

$$(k \bmod nm) = (\ell \bmod nm),$$

alors

$$(k \bmod n) = (\ell \bmod n)$$

et

$$(k \bmod m) = (\ell \bmod m).$$

(ii) L'application bien définie

$$f : \left| \begin{array}{ccc} \mathbb{Z}/nm\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ (k \bmod nm) & \longmapsto & (k \bmod n, k \bmod m) \end{array} \right.$$

est un isomorphisme d'anneaux.

Le résultat s'étend à un nombre fini d'entiers premiers entre eux deux à deux.

Méthode 3 : Résolution de système de congruences

Trouver une solution particulière au système de congruence se fait soit en testant les valeurs, soit en trouvant des entiers de Bézout : on a $u, v \in \mathbb{Z}$ tels que $n \cdot u + m \cdot v = 1$. Alors

$$c = nub + mva$$

est une solution particulière car $nu \equiv 1 \ [m]$ et $mv \equiv 1 \ [n]$.

On peut aussi résoudre directement le système en remarquant qu'il est équivalent à $k = a + n \cdot u = b + m \cdot v$ avec $u, v \in \mathbb{Z}$ et en résolvant l'équation diophantienne $n \cdot u - m \cdot v = b - a$ par la méthode habituelle.

3 Indicatrice d'Euler

Définition 20 : Indicatrice d'Euler

L'**indicatrice d'Euler** est l'application définie sur $\mathbb{N}^*$ par

$$\varphi(n) = |\{k \in [\![1, n]\!], \ n \wedge k = 1\}|.$$

Propriété 31 : Indicatrice d'Euler et nombres premiers

Si p est premier, alors

$$\varphi(p) = p - 1.$$

Et si, plus généralement, $k \in \mathbb{N}^*$,

$$\varphi\left(p^k\right) = p^{k-1}(p-1).$$

Propriété 32 : Théorème chinois avec les inversibles

Soient $n, m \in \mathbb{N}^*$ tels que $n \wedge m = 1$.

(i) Si $k \in \mathbb{Z}$, et si $(k \bmod nm) \in \left(\mathbb{Z}/nm\mathbb{Z}\right)^\times$ alors $(k \bmod n) \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ et $(k \bmod m) \in \left(\mathbb{Z}/m\mathbb{Z}\right)^\times$.

(ii) L'application bien définie

$$g : \left| \begin{array}{ccc} \left(\mathbb{Z}/nm\mathbb{Z}\right)^\times & \longrightarrow & \left(\mathbb{Z}/n\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/m\mathbb{Z}\right)^\times \\ (k \bmod nm) & \longmapsto & (k \bmod n, k \bmod m) \end{array} \right.$$

est un isomorphisme de groupes (multiplicatifs).

Corollaire 4 : Multiplicativité de φ

φ est multiplicative, c'est-à-dire que si $n \wedge m = 1$, alors

$$\varphi(nm) = \varphi(n)\varphi(m).$$

Corollaire 5 : Produit de plus de deux termes

Plus généralement, si $n_1, \ldots, n_r$ sont deux à deux premiers entre eux,

$$\varphi(n_1 \cdots n_r) = \varphi(n_1) \cdots \varphi(n_r).$$

Corollaire 6 : Expression à l'aide des diviseurs premiers

Si $p_1, \dots, p_r$ sont les diviseurs premiers distincts de n,

$$\varphi(n) = n \prod_{k=1}^{r} \left(1 - \frac{1}{p_k}\right).$$

Théorème 7 : d'Euler

Si $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$ tel que $a \wedge n = 1$, alors

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

Corollaire 7 : 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),

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

V Caractéristique d'un corps (HP)

Définition 21 : Caractéristique d'un corps

Soit $(\mathbb{K}, +, \times)$ un corps.

S'il existe $n \in \mathbb{N}^*$ tel que $n \cdot 1_{\mathbb{K}} = \underbrace{1_{\mathbb{K}} + \cdots + 1_{\mathbb{K}}}_{n \text{ fois}} = 0_{\mathbb{K}}$, on appelle **caractéristique** de $\mathbb{K}$ le plus petit entier ayant cette propriété.

Si un tel entier n'existe pas, on dit que $\mathbb{K}$ est de **caractéristique nulle**.

Propriété 33

Soit $(\mathbb{K}, +, \times)$ un corps.

(i) Si $\mathbb{K}$ n'est pas de caractéristique nulle, sa caractéristique est un nombre premier.

(ii) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont de caractéristique nulle.
Pour tout p premier, $\mathbb{Z}/p\mathbb{Z}$ est de caractéristique p.

VI Structure d'algèbre (MPI)

1 Algèbre et sous-algèbre

Définition 22 : Structure d'algèbre

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

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

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

Propriété 34 : Caractérisation des sous-algèbres

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

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

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

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

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

Définition 23 : Polynôme en un élément d'une algèbre

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

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

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

2 Morphismes d'algèbres

Définition 24 : Morphisme d'algèbre

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

(i) f est linéaire ie

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

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

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

Propriété 35 : Morphisme d'évaluation polynomiale

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

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

3 Norme d'algèbre

Définition 25 : Norme d'algèbre

Une norme N sur une $\mathbb{K}$-algèbre $(\mathcal{A}, +, \times, \cdot)$ est dite **sous-multiplicative** si pour tout $(a, b) \in \mathcal{A}^2$, $N(ab) \leqslant N(a)N(b)$.On parle aussi de **norme d'algèbre**.

Propriété 36 : Norme d'algèbre et puissance

On a alors, pour tout $a \in \mathcal{A}$ et $k \in \mathbb{N}^*$,

$$N\left(a^k\right) \leqslant N(a)^k.$$

Corollaire 8 : Convergence de séries vectorielles exponentielles et géométriques

Soit $(\mathcal{A}, +, \times, \cdot)$ une $\mathbb{K}$-algèbre munie de N norme d'algèbre, et $a \in \mathcal{A}$.

(i) La série $\displaystyle\sum_{k\geqslant 0} \frac{a^k}{k!}$ est absolument convergente.

(ii) Si $N(a) < 1$, alors la série $\displaystyle\sum_{k\geqslant 0} a^k$ est absolument convergente.
Si $1_{\mathcal{A}}$ est l'unité de $\mathcal{A}$, et $\mathcal{A}$ de dimension finie, on a alors $1_{\mathcal{A}} - a$ inversible, d'inverse $\displaystyle\sum_{n=0}^{+\infty} a^k$.