9 Structures d'anneau, de corps, d'algèbre

Extrait du programme officiel :

Contenus	Capacités & commentaires
Compléments sur les anneaux	
Produit fini d'anneaux.	
Idéal d'un anneau commutatif.	Noyau d'un morphisme d'anneaux commutatifs.
Idéal engendré par un élément.	Notation xA.
Divisibilité dans un anneau commutatif intègre.	Interprétation en termes d'idéaux.
Idéaux de $\mathbb{Z}$	
Idéaux de $\mathbb{Z}$.	
Définition du PGCD de $n \geqslant 2$ entiers relatifs en termes d'idéaux, relation de Bézout.	Lien avec le programme de première année.
Anneaux $\mathbb{Z}/n\mathbb{Z}$	
Anneau $\mathbb{Z}/n\mathbb{Z}$.	
Inversibles de $\mathbb{Z}/n\mathbb{Z}$. Condition nécessaire et suffisante pour que $\mathbb{Z}/n\mathbb{Z}$ soit un corps.	Notation $\mathbb{F}_p$ lorsque p est premier.
Théorème chinois : isomorphisme naturel de $\mathbb{Z}/mn\mathbb{Z}$ sur $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ si $m \wedge n = 1$; extension à plus de deux facteurs.	Application aux systèmes de congruences et à la résolution de systèmes d'équations dans $\mathbb{Z}/n\mathbb{Z}$.
Indicatrice d'Euler φ. Calcul à l'aide de la décomposition en produits de facteurs premiers.	Relation $\varphi(mn) = \varphi(m)\varphi(n)$ si m et n sont premiers entre eux ; expression de $\varphi(p^k)$ pour p premier.
Théorème d'Euler.	Lien avec le petit théorème de Fermat.
Algèbres	
Algèbre.	Les algèbres sont unitaires. Exemples : $\mathbb{K}[X]$, $\mathcal{L}(E)$, $\mathcal{M}_n(\mathbb{K})$, $\mathcal{F}(X, \mathbb{K})$.
Sous-algèbre.	
Morphisme d'algèbres.	

Table des matières

9 Structures d'anneau, de corps, d'algèbre 1

I Anneaux et Corps 2
1 Anneaux (MP2I) . . . 2
2 Groupe des inversibles (MP2I) . . . 3
3 Calculs dans un anneau (MP2I) . . . 4
4 Corps (MP2I) . . . 5
5 Intégrité (MP2I) . . . 6
6 Anneau produit (MPI) . . . 6
7 Sous-anneau et sous-corps (MP2I) . . . 8
8 Morphismes d'anneaux (MP2I) . . . 9

II Idéal d'un anneau commutatif (MPI) 10
1 Généralités . . . 10
2 Somme et intersection d'idéaux . . . 12
3 Idéal principal . . . 13
4 Divisibilité dans un anneau intègre . . . 13

III Arithmétique sur $\mathbb{Z}$ 14
1 PGCD . . . 14
2 PPCM . . . 16
3 Nombres premiers . . . 16
4 Congruences . . . 18

IV Anneau $\mathbb{Z}/n\mathbb{Z}$ (MPI) 20
1 Structure . . . 20
2 Théorème Chinois . . . 21
3 Indicatrice d'Euler . . . 22

V Caractéristique d'un corps (HP) 26

VI Structure d'algèbre (MPI) 27
1 Algèbre et sous-algèbre . . . 27
2 Morphismes d'algèbres . . . 28
3 Norme d'algèbre . . . 29

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.**

Exemple

E 1 – $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$, $(\mathbb{C}^D,+,\times)$ et $(\mathbb{R}^D,+,\times)$ (avec $D\neq\varnothing$), $(\mathbb{C}^{\mathbb{N}},+,\times)$ et $(\mathbb{R}^{\mathbb{N}},+,\times)$ sont des anneaux commutatifs.

E 2 – $(\mathcal{M}_n(\mathbb{R}),+,\times)$ et $(\mathcal{M}_n(\mathbb{C}),+,\times)$ sont des anneaux non commutatifs si $n\geqslant 2$.

Remarque

R 1 – 0_A est **absorbant** :

$$\forall\, a\in A,\quad a\times 0_A=0_A\times a=0_A.$$

En effet, $0_A=a\times(0_A+0_A)=a\times 0_A+a\times 0_A$ donc $a\times 0_A=0_A$. Idem à droite.

R 2 – Si $1_A=0_A$, alors pour tout $a\in A$, $a=a\times 1_A=a\times 0_A=0_A$, donc $A=\{0_A\}$.

R 3 – Si $A\neq\{0_A\}$, alors 0_A n'est pas inversible (pour $\times$).

R 4 – Pour tout $a,b\in A$, $-ab=(-a)\times b=a\times(-b)$.

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.

Remarque

R 5 – On parle parfois d'unités de A, d'où la notation...

Exemple

E 3 – $\mathbb{R}^\times=\mathbb{R}^*$

E 4 – $\mathbb{Z}^\times=\{-1,1\}\neq\mathbb{Z}^*$

E 5 – $\left(\mathbb{C}^{\mathbb{N}}\right)^\times=\{\text{suites jamais nulles}\}$

E6 – $(\mathbb{C}^D)^\times = \{\text{fonctions jamais nulles}\}$

E7 – $(\mathcal{M}_n(\mathbb{K}))^\times = \mathrm{GL}_n(\mathbb{K})$

Propriété 1 : Groupe des inversibles

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

Démonstration

On a déjà l'associativité, l'élément neutre car A est un anneau. Comme de plus, tout élément inversible est lui même inversible et comme le produit de deux éléments inversibles l'est encore, on a bien une structure de groupe.

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

Remarque

R6 – Si a et b ne commutent pas,
$$\begin{aligned}(ab)^n&=abab\cdots ab\\(a+b)^2&=a^2+ab+ba+b^2\\(a+b)^3&=a^3+a^2b+aba+ba^2+ab^2+bab+b^2a+b^3\end{aligned}$$
etc.

Démonstration

- Par récurrence sur n.
- **Formule du binôme** :
  - ⋆ **Preuve par dénombrement** :

$$(a+b)^n = \underbrace{(a+b)(a+b)\cdots(a+b)}_{n \text{ fois}}$$

En développant, on obtient des termes de la forme $x_1x_2\cdots x_n$ avec $x_i = a$ ou b. Si on veut k termes a, on $\binom{n}{k}$ choix, et le terme vaut a^kb^{n-k} car a et b commutent.

  - ⋆ **Preuve par récurrence** sur n, c'est simple si $n = 0$ ou 1. Si c'est vrai pour $n-1$,

$$\begin{aligned}(a+b)^n = (a+b)(a+b)^{n-1} &= (a+b)\sum_{k=0}^{n-1}\binom{n-1}{k}a^kb^{n-1-k}\\ &= \sum_{k=0}^{n-1}\binom{n-1}{k}a^{k+1}b^{n-k-1} + \sum_{k=0}^{n-1}\binom{n-1}{k}a^kb^{n-k}\end{aligned}$$

(associativité, distributivité, a et b commutent, dans la seconde somme)

$$\begin{aligned}(a+b)^n &= \sum_{k=1}^{n}\binom{n-1}{k-1}a^kb^{n-k} + \sum_{k=0}^{n-1}\binom{n-1}{k}a^kb^{n-k}\\ &\text{(changement d'indice } k \mapsto k-1)\\ &= \sum_{k=0}^{n}\binom{n-1}{k-1}a^kb^{n-k} + \sum_{k=0}^{n}\binom{n-1}{k}a^kb^{n-k}\\ &\text{(les termes ajoutés sont nuls)}\\ &= \sum_{k=0}^{n}\left(\binom{n-1}{k-1} + \binom{n-1}{k}\right)a^kb^{n-k}\\ &\text{(associativité, distributivité,}\end{aligned}$$

Donc $(a+b)^n = \sum_{k=0}^{n}\binom{n}{k}a^kb^{n-k}$ d'après la formule de Pascal étendue au cœfficients avec $k < 0$.

- **Factorisation de $a^n - b^n$** :

$$\begin{aligned}(a-b)\sum_{k=0}^{n-1}a^kb^{n-1-k} &= \sum_{k=0}^{n-1}\left(a^{k+1}b^{n-(k+1)} - a^kb^{n-k}\right)\\ &\text{(a et b commutent, associativité, distributivité)}\\ &= a^nb^0 - a^0b^n = a^n - b^n\\ &\text{(somme télescopique)}\end{aligned}$$

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 $+$.

Exemple

E 8 – $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ munis des lois $+$ et $\times$ sont des corps, mais pas $\mathbb{Z}$.

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

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

Exemple

E 9 – $\mathbb{R}, \mathbb{Z}, \mathbb{C}, \mathbb{Q}$ sont des anneaux intègres. $\mathbb{R}^{\mathbb{N}}$ et plus généralement $\mathbb{R}^D$ avec D contenant au moins deux éléments ne le sont pas.

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 $a_1 \times \cdots \times a_n \neq 0_A$.

Démonstration

Par contraposée et récurrence. ■

Propriété 4 : Régularité dans un anneau intègre

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

Démonstration

Si $a, b, c \in A$ et $a \neq 0_A$ tels que $ab = ac$, alors $a(b - c) = 0_A$ et donc $b - c = 0_A$ soit $b = c$. ■

Propriété 5 : Intégrité d'un corps

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

Démonstration

Si $ab = 0_{\mathbb{K}}$ et si $a \neq 0_K$, alors a est inversible et $b = a^{-1}ab = a^{-1}0_{\mathbb{K}} = 0_{\mathbb{K}}$ car $0_{\mathbb{K}}$ est un élément absorbant.
Pour la réciproque, $(\mathbb{Z}, +, \times)$ est un anneau commutatif intègre qui n'est pas un corps. ■

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.

Démonstration

- On a bien $(A \times B, +)$ groupe (produit) abélien.
- $\times$ est bien une loi de composition interne sur $A \times B$.
  Un calcul facile mais pénible à écrire permet de vérifier que les associativités de $\dot{\times}$ et $\otimes$ donnent celle de $\times$.
  Un calcul facile mais pénible à écrire permet de vérifier que les distributivités de $\dot{\times}$ sur $\dot{+}$ et $\otimes$ sur $\oplus$ donnent celle de $\times$ sur $+$.
- Si 1_A et 1_B sont les unités de A et B, alors $(1_A, 1_B)$ est bien neutre sur $A \times B$.

■

Remarque

R 7 – Cela se généralise à un nombre d'anneaux quelconque $\left(A_1, \underset{(1)}{+}, \underset{(1)}{\times}\right), \ldots, \left(A_p, \underset{(p)}{+}, \underset{(p)}{\times}\right)$ avec pour tout $(x_1, \ldots, x_p)$ et $(y_1, \ldots, y_p)$ dans $A_1 \times \cdots \times A_p$,

$$(x_1, \ldots, x_p) + (y_1, \ldots, y_p) = \left(x_1 \underset{(1)}{+} y_1, \ldots, x_p \underset{(p)}{+} y_p\right)$$
$$(x_1, \ldots, x_p) + (y_1, \ldots, y_p) = \left(x_1 \underset{(1)}{\times} y_1, \ldots, x_p \underset{(p)}{\times} y_p\right)$$

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

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

Démonstration

$$\begin{aligned}(a, b) \in (A \times B)^\times &\iff \exists\, (c, d) \in A \times B,\ \ (a, b) \times (c, d) = (c, d) \times (a, b) = (1_A, 1_B) \\ &\iff \exists\, (c, d) \in A \times B,\ \ ac = ca = 1_A \text{ et } bd = db = 1_B \\ &\iff (a, b) \in A^\times \times B^\times\end{aligned}$$

et on a bien 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 :** $1_A \in B$
- $\left(B,+|_{B^2},\times|_{B^2}\right)$ est un anneau.

Remarque

R 8 – Une partie peut avoir une structure d'anneau pour les lois induites sans avoir la même unité (ce n'est pas un sous-anneau au sens de la définition précédente.) C'est le cas trivialement de $\{0_A\}$.

Exemple

E 10 – Soit, dans l'anneau des matrices 2×2, l'ensemble B des matrices $\left(\begin{smallmatrix} a & 0 \\ 0 & 0 \end{smallmatrix}\right)$ pour $a \in \mathbb{K}$. Alors $(B,+,\times)$ est un anneau d'unité $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \neq I_2$.

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

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

Démonstration

Même principe que pour les sous-groupes, la présence de 1_A n'étant automatique que si B possède un élément inversible, d'où la nécessité d'imposer $1_A \in B$. ■

Exemple

E 11 – **Anneau des entiers de Gauss**[a] : $\mathbb{Z}[\mathrm{i}] = \mathbb{Z}+\mathrm{i}\mathbb{Z}$ est un sous-anneau de $(\mathbb{C},+,\times)$.

E 12 – $\mathcal{T}_n^+(\mathbb{K})$ est un sous-anneau de $(\mathcal{M}_n(\mathbb{K}),+,\times)$

E 13 – L'ensemble $\mathcal{B}(\mathbb{R})$ des fonctions bornées est un sous-anneau de $\left(\mathbb{R}^{\mathbb{R}},+,\times\right)$.

a. 

Carl Friedrich Gauss (Brunswick 1777 - Göttingen 1855) est un mathématicien, astronome et physicien allemand. Surnommé *le prince des mathématiciens*, il est considéré comme l'un des plus grands mathématiciens de tous les temps. Gauss était un génie particulièrement précoce : à 7 ans (ou 10 selon les sources), il donne la formule calculant $1+2+\cdots+100$. À 19 ans, il fut le premier à démontrer la loi de réciprocité quadratique. Parmi ses autres prouesses, on peut citer la démonstration du théorème fondamental de l'algèbre, dans sa thèse en 1799, l'invention de la théorie des congruences, la résolution de problèmes de construction à la règle et au compas...Il est considéré comme le fondateur de la géométrie différentielle.

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 $\left(\mathbb{L},+|_{\mathbb{L}^2},\times|_{\mathbb{L}^2}\right)$ 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,

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

Démonstration

Le sens $\Longrightarrow$ ne pose pas de problème. Pour le sens $\Longleftarrow$, on a bien un sous-anneau dont tous les éléments non nuls sont inversibles car $1_{\mathbb{K}}=xx^{-1}\in\mathbb{L}$. ■

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.

Remarque

R 9 – Comme on a en particulier un morphisme de groupes additifs, on peut utiliser les propriétés de ceux-ci :
- $f(0_A) = 0_{A'}$,
- Pour tout $a \in A$, $f(-a) = -f(a)$,
- f est injective si et seulement si $\operatorname{Ker} f = \{0_A\}$.

R 10 – En général, $\operatorname{Ker} f$ n'est pas un sous-anneau de A. C'est un sous-groupe additif stable par multiplication... Nous les étudions juste après !

Exemple

E 14 – $f : \left| \begin{array}{ccc} \mathbb{R}[X] & \longrightarrow & \mathbb{C} \\ P & \longmapsto & \widetilde{P}(\mathrm{i}) \end{array} \right.$; $\operatorname{Ker} f = \left(X^2+1\right)\mathbb{R}[X]$ n'est pas un sous-anneau de $\mathbb{R}[X]$.

Propriété 10 : 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 $f\left(a^{-1}\right) = (f(a))^{-1}$.

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

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

Démonstration

(i) $f(a)f\left(a^{-1}\right) = f\left(aa^{-1}\right) = f(1_A) = 1_{A'}$ et de même $f\left(a^{-1}\right)f(A) = 1_{A'}$.

(ii) Même principe que pour les morphismes de groupes.

(iii) Simple vérification. ■

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.

Remarque

R 11 – Avec (i) et (ii), $f(1_{\mathbb{K}}) = (f(1_{\mathbb{K}}))^2$ et comme $\mathbb{K}'$ est intègre, $f(1_{\mathbb{K}})$ vaut $1_{\mathbb{K}'}$ ou $0_{\mathbb{K}'}$. S'il vaut $0_{\mathbb{K}'}$ et si (ii) est vérifiée, alors $f \equiv 0_{\mathbb{K}'}$.

Exemple

E 15 – $\mathrm{id}_{\mathbb{C}}$, $z \mapsto \overline{z}$ sont des automorphismes (involutifs) du corps $\mathbb{C}$.

E 16 – Tout morphisme de corps est injectif, car si $x \neq 0_{\mathbb{K}}$, x est inversible donc $f(x)$ est inversible, donc $f(x) \neq 0_{\mathbb{K}'}$ donc $x \notin \operatorname{Ker} f$, donc $\operatorname{Ker} f = \{0_{\mathbb{K}}\}$.

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

Remarque

R 12 – Finalement, I est un **idéal** de $(A,+,\times)$ lorsque

- $I \subset A$
- $I \neq \varnothing$
- $\forall\, x,y \in I,\ x-y \in I$
- $\forall\, a \in A,\ \forall\, x \in I,\ ax \in I$.

Comme $-1_A \in A$, on peut se contenter de

- $I \subset A$
- $I \neq \varnothing$
- $\forall\, x,y \in I,\ x+y \in I$
- $\forall\, a \in A,\ \forall\, x \in I,\ ax \in I$.

Exemple

E 17 – $2\mathbb{Z}$ est un idéal de $(\mathbb{Z},+,\times)$.

E 18 – L'ensemble des suites convergeant vers 0 est un idéal de l'anneau des suites bornées.

Remarque

R 13 – Si un idéal contient l'unité 1_A ou plus généralement un élément inversible, il est égal à A tout entier.

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.

Démonstration

Simple vérification. Dans le cas d'un corps, comme tous les éléments non nuls sont inversibles, s'il y en a un dans I, en le multipliant par son inverse on obtient $1_A \in I$ puis $I = A$. ■

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 $(A,+,\times)$.

Démonstration

- $0_A \in \operatorname{Ker} f \neq \varnothing$
- Si $x,y \in \operatorname{Ker} f$, $f(x-y) = f(x) - f(y) = 0_{A'}$ donc $x-y \in \operatorname{Ker} f$.
- Si $x \in \operatorname{Ker} f$ et $a \in A$, $f(ax) = f(a)f(x) = 0_{A'}$ donc $ax \in \operatorname{Ker} f$.

■

Remarque

R 14 – $\operatorname{Im} f$ est un sous-anneau de $(A', \oplus, \otimes)$.
En général, $\operatorname{Ker} A$ n'est pas un sous-anneau de $(A, +, \times)$.

Exercice 1

Montrer que si $f : (A, +, \times) \to (A', \oplus, \otimes)$ est un morphisme d'anneaux :

- **L'image réciproque d'un sous-anneau de $(A', \oplus, \otimes)$ est un sous-anneau de $(A, +, \times)$.**
- **L'image directe d'un sous-anneau de $(A, +, \times)$ est un sous-anneau de $(A', \oplus, \otimes)$.**
- **L'image réciproque d'un idéal de $(A', \oplus, \otimes)$ par f est un idéal de $(A, +, \times)$.**
- **L'image directe d'un idéal de $(A, +, \times)$ par f est un idéal de $(f(A) = \operatorname{Im} f, \oplus, \otimes)$.**

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 $j \in J$.

Démonstration

(i)
- $I_1 + \cdots + I_n$ est un idéal :
  - $0_A = 0_A + \cdots + 0_A \in I_1 + \cdots + I_n$
  - Si $x, y \in I_1 + \cdots + I_n$, on a $(x_1, \dots, x_n), (y_1, \dots, y_n) \in \prod_{j=1}^{n} I_j$ tels que $x = x_1 + \cdots + x_n$ et $y = y_1 + \cdots + y_n$.
    Alors $x + y = (x_1 + y_1) + \cdots + (x_n + y_n) \in I_1 + \cdots + I_n$.
  - Si $x = x_1 + \cdots + x_n \in I_1 + \cdots + I_n$ et $a \in A$ alors $ax = ax_1 + \cdots + ax_n \in I_1 + \cdots + I_n$.
- $I_1 + \cdots + I_n$ contient tous les I_j car ceux-ci contiennent 0_A.
- Si K est un idéal de A contenant tous les I_j, alors par stabilité par $+$, $I_1 + \cdots + I_n \subset K$.

(ii)
- $\bigcap_{j \in J} I_j$ est un idéal :
  - $0_A \in \bigcap_{j \in J} I_j$
  - Si $x, y \in \bigcap_{j \in J} I_j$, $x + y \in \bigcap_{j \in J} I_j$.
  - Si $x \in \bigcap_{j \in J} I_j$ et $a \in A$ alors $ax \in \bigcap_{j \in J} I_j$.
- $\bigcap_{j \in J} I_j$ est contenu dans tous les I_j.
- Si K est un idéal de A contenu dans tous les I_j, alors $K \subset \bigcap_{j \in J} I_j$.

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.*

Remarque

R 15 – C'est aussi le plus petit idéal contenant x, et donc l'intersection de tous les idéaux contenant x par unicité du plus petit élément.
Cette notion se généralise à plus d'un élément, un peu comme avec les Vect en algèbre linéaire.
Ainsi, l'idéal engendré par un nombre quelconque d'élément est l'ensemble des combinaisons linéaires (finies) de ces éléments, à cœfficients dans A.

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.

Démonstration

C'est un anneau intègre et ses idéaux qui sont aussi ses sous-groupes sont tous principaux. ■

Remarque

R 16 – Les idéaux de $\mathbb{Z}$ sont donc principaux, c'est-à-dire engendré par un élément. Tous les générateurs sont associés.
Donc, quitte à choisir un générateur positif (ou nul), on a de plus unicité de celui-ci.

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 $aA \subset bA$.

Remarque

R 17 – Soit encore ssi tous les multiples de a sont des multiples de b.

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 $b = ua$.*

Exemple

E 19 – Dans $\mathbb{Z}$, a, b sont associés si et seulement si $a = \pm b$.

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 $au + bv = a \wedge b$.

Démonstration

Immédiat avec la nouvelle définition. ■

Propriété 18 : Caractérisation

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

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

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.

Démonstration

Soit $d = a \wedge b$. Alors, par définition, $d \in \mathbb{N}$ et $a \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, $b \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.
Soit $c \in \mathbb{Z}$ tel que $c|a$ et $c|b$ alors, avec une relation de Bézout, $c|d = au + bv$.
Réciproquement, soit d tel que $\begin{cases} d \in \mathbb{N} \\ d|a \text{ et } d|b \\ \forall\, c \in \mathbb{Z},\ \ (c|a \text{ et } c|b) \implies c|d \end{cases}$
Alors, avec le premier sens, $a \wedge b | d$ et $d | a \wedge b$ et donc, par positivité, $d = a \wedge b$. ■

Propriété 19 : Propriété d'Euclide

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

Démonstration

Les diviseurs communs sont les mêmes. ■

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

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

Démonstration

Le sens direct a déjà été vu.
Réciproquement, si $au + bv = 1$, alors $1 \in a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$ donc $1 | a \wedge b$ donc $a \wedge b = 1$ par positivité. ■

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 $a' \wedge b' = 1$.

Démonstration

(i) Sens direct immédiat par Bézout. Sens réciproque : il suffit de multiplier les relations de Bézout. Voir CCINP 86.

(ii) Si $d \neq 0$, comme $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$, on obtient $\mathbb{Z} = a'\mathbb{Z} + b'\mathbb{Z}$ donc $a' \wedge b' = 1$. Sinon, tout couples (a', b') convient, donc... ■

Théorème 3 : Lemme de Gauß

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

Démonstration

On a $u, v \in \mathbb{Z}$ tels que $au + bv = 1$ donc $c = acu + bcv$ est divisible par b. ■

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 :

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

Exercice 2 : Résoudre $199x + 54y = 4$ dans $\mathbb{Z}^2$.

Ici, par l'algorithme d'Euclide, on a

$$(1)\ 199 = 54 \times 3 + 37 \quad (2)\ 54 = 37 \times 1 + 17 \quad (3)\ 37 = 17 \times 2 + 3 \quad (4)\ 17 = 3 \times 5 + 2 \quad (5)\ 3 = 2 \times 1 + \mathbf{1}$$

Donc $199 \wedge 54 = 1$ et $(5) - (4) + 6(3) - 13(2) + 19(1)$ donne $199 \times 19 - 54 \times 70 = 1$.
On a donc comme solution particulière $x_0 = 76$ et $y_0 = -280$.
Comme ci-dessus, on a ensuite (x, y) est solution de (E) si et seulement si $199(x - x_0) + 54(y - y_0) = 0$ si et seulement si $199(x - x_0) = 54(y_0 - y)$. Comme $199 \wedge 54 = 1$ et $199 | 54(y_0 - y)$, le théorème de Gauß donne alors $k \in \mathbb{Z}$ tel que $y_0 - y = 199k$ soit $y = -280 - 199k$. Puis, en remplaçant dans l'équation, $x = x_0 + 54k = 76 + 54k$. On vérifie aisément que la réciproque est vraie.
L'ensemble des solutions est donc $\boxed{\{(76 + 54k, -280 - 199k) \mid k \in \mathbb{Z}\}.}$

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

Remarque

R 18 – Cette fois, il s'agit clairement de la même définition qu'en première année : le plus petit multiple commun positif.

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.

Remarque

R 19 – 1 n'est pas premier.

R 20 – 2 est le seul nombre premier pair.

R 21 – Un nombre premier possède exactement 4 diviseurs : ± 1 et $\pm p$.

R 22 – Pour qu'un nombre entier n soit premier, il faut et il suffit qu'il n'ait pas de diviseur entre 2 et $\sqrt{n}$.

Propriété 21 : d'Euclide

L'ensemble des nombres premiers est infini.

Démonstration : tellement classique...

Sinon, soient $p_1, \dots, p_n$ les nombres premiers.
Alors $N = p_1 \cdots p_n + 1$ n'aurait pas de diviseur premier... (Alors qu'il doit en avoir un, le plus petit $\geqslant 2$, par exemple.) ■

Propriété 22 : Diviseur premier ou non

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

Démonstration

Si $p \wedge n$ divise p donc vaut soit 1 soit p... ■

Corollaire 2 : Nombre premier divisant un produit

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

$$p|(a_1 \times \cdots \times a_n) \text{ si et seulement si } p \text{ divise l'un des } a_k.$$

Théorème 4 : fondamental de l'arithmétique – Décomposition primaire

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

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

Remarque

R 23 – La décomposition primaire se réécrit $n = \pm \prod_{p \in \mathcal{P},\ p|n} p^{v_p(n)} = \pm \prod_{p \in \mathcal{P}} p^{v_p(n)}$.

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

Remarque

R 24 – Si $a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ et $b = \pm p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ avec des exposants éventuellement nuls, alors

$$a \wedge b = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_k^{\min(\alpha_k,\beta_k)}$$

$$a \vee b = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \cdots p_k^{\max(\alpha_k,\beta_k)}$$

Exercice 3 : Montrer que $\sqrt{n} \in \mathbb{Q}$ si et seulement si n est un carré parfait.

Si $\sqrt{n} = \dfrac{a}{b}$, alors $a^2 = n \times b^2$, $\forall\, p \in \mathcal{P},\ \ 2v_p(a) = v_p(n) + 2v_p(b)$ donc $\forall\, p \in \mathcal{P},\ \ v_p(n) \in 2\mathbb{N}$, donc n est un carré parfait.

Ou encore : si $\sqrt{n} = \dfrac{a}{b}$ sous forme irréductible, alors $a^2 = n \times b^2$ donc $b^2|a^2$. Or $a \wedge b = 1$ donc $b^2 = a^2 \wedge b^2 = 1$ donc $n = a^2$.

Exercice 4 : Exprimer le nombre de diviseurs positifs de n à l'aide de ses valuations p-adiques.

Il s'agit de $\displaystyle\prod_{p \in \mathcal{P}, p|n} (v_p(n) + 1)$ vu la propriété (iii).

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 $n = \overline{a_k \cdots a_1 a_0}^{10}$ en base 10,

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

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 : $11|n \iff 11|(a_0 - a_1 + a_2 - a_3 + \cdots) = \sum_{i=0}^{k} (-1)^i a_i$

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),

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

Exercice 5 : CCINP 86

Remarque

R 25 – Nous verrons dans la prochaine partie un théorème d'Euler qui rendra triviale la démonstration du petit théorème de Fermat.

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 $\mathbb{N}_*^3$.

Démonstration : Non exigible[1]

■

[1] J'ai découvert une démonstration véritablement merveilleuse que ce cadre est trop étroit pour contenir...

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 $\overline{ab} = \overline{cd}$.

Démonstration

Comme pour la somme : $a \equiv c\ [n]$ et $b \equiv d\ [n]$ implique $ab \equiv cd\ [n]$. ■

Ce lemme rend licite la définition suivante, car le produit de deux entiers modulo n ne dépend pas du choix de leurs représentants.

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

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

Démonstration

On a déjà que $(\mathbb{Z}/n\mathbb{Z}, +)$ a une structure de groupe abélien.
Reste à voir que $\times$ est associative, distributive sur $+$, commutative et admet un neutre $\overline{1}$ de façon similaire à ce qui a été vu pour $+$. ■

Propriété 30 : Groupe des inversibles

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

Démonstration

$\overline{k}$ est inversible si et seulement s'il existe $\ell \in \mathbb{Z}$ tel que $\overline{k\ell} = \overline{k\ell} = \overline{1}$ si et seulement si $k\ell \equiv 1\ [n]$ si et seulement s'il existe $u \in \mathbb{Z}$ tel que $1 = k\ell + un$, ce qui permet de conclure par théorème de Bézout. ■

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.

Exemple

E 20 – Inversibles et leurs inverses dans $\mathbb{Z}/12\mathbb{Z}$.

E 21 – Inverse de $\overline{23}$ dans $\mathbb{Z}/120\mathbb{Z}$.

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 $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

Démonstration

On élimine le cas $n = 1$ car $\mathbb{Z}/1\mathbb{Z} = \{\overline{0}\}$. On a alors que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps si et seulement si pour tout $k \in [\![1, n-1]\!]$, $\overline{k}$ est inversible si et seulement si pour tout $k \in [\![1, n-1]\!]$, k est premier avec n si et seulement si les seuls diviseurs positifs de n sont 1 et n si et seulement si $n \geqslant 2$ premier. ■

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.

Démonstration

1re formulation La méthode ci-dessus donne l'existence d'une solution particulière c. Puis

$$\begin{cases} k \equiv a \ [n] \\ k \equiv b \ [m] \end{cases} \iff \begin{cases} k \equiv c \ [n] \\ k \equiv c \ [m] \end{cases}$$
$$\iff k - c \text{ est divisible par } n \text{ et } m$$
$$\underset{n\wedge m=1}{\iff} nm \mid (k-c) \iff k \equiv c \ [nm].$$

2e formulation

(i) $k \equiv \ell \ [nm]$ donc $nm \mid (k-\ell)$ donc $n \mid (k-\ell)$ et $m \mid (k-\ell)$ donc $k \equiv \ell \ [n]$ et $k \equiv \ell \ [m]$.

(ii) f est bien définie d'après (i).
Puis, pour $k, \ell \in \mathbb{Z}$, par définition des additions sur $\mathbb{Z}/nm\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$,

$$\begin{aligned} f\Big((k \bmod nm) + (\ell \bmod nm)\Big) &= f\Big((k+\ell) \bmod nm\Big) \\ &= \Big((k+\ell) \bmod n, (k+\ell) \bmod m\Big) \\ &= (k \bmod n, k \bmod m) + (\ell \bmod n, \ell \bmod m) \\ &= f\Big(k \bmod nm\Big) + f\Big(\ell \bmod nm\Big) \end{aligned}$$

On montre exactement de la même manière que

$$f\Big((k \bmod nm) \times (\ell \bmod nm)\Big) = f\Big(k \bmod nm\Big) \times f\Big(\ell \bmod nm\Big)$$

On a enfin que

$$f(1 \bmod nm) = (1 \bmod n, 1 \bmod m) = 1_{\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}}.$$

Donc f est un morphisme d'anneaux.
La bijectivité correspond à la 1re méthode. Mais elle peut se retrouver plus facilement : comme le cardinal est le même au départ et à l'arrivée, on se contente de montrer l'injectivité (qui équivaut alors à la bijectivité) : si $f(k \bmod nm) = 0_{\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}}$, alors $\begin{cases} k \equiv 0 \ [n] \\ k \equiv 0 \ [m] \end{cases}$ donc $k \equiv 0 \ [nm]$ soit en utilisant la première formulation, soit en remarquant que $n \mid k$, $m \mid k$ et $n \wedge m = 1$ donc $nm \mid k$.
Finalement, $\operatorname{Ker} f = \{0_{\mathbb{Z}/n\mathbb{Z}}\}$ et f est un isomorphisme.

Exercice 6 : CCINP 94

3 Indicatrice d'Euler

Définition 20 : Indicatrice d'Euler

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

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

Remarque

R 26 – $\varphi(1) = 1$.

R 27 – Si $n \geqslant 2$, $\varphi(n)$ est la cardinal du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ des inversibles de $\mathbb{Z}/n\mathbb{Z}$ (donc le nombre d'éléments inversibles).

R 28 – Il s'agit aussi du nombre de générateurs du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$.

Propriété 31 : Indicatrice d'Euler et nombres premiers

Si p est premier, alors

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

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

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

Démonstration

En effet, tous les entiers entre 1 et $p-1$ sont non divisibles par p donc premier avec lui.
Puis les entiers premiers avec p^k sont les entiers n'admettant pas p comme diviseur premier.
Combien y a-t-il de multiple de p entre 1 et p^k ?
Autant que de $\ell \in \mathbb{N}$ tel que $1 \leqslant \ell p \leqslant p^k$, c'est-à-dire, ℓ étant entier, $1 \leqslant \ell p \leqslant p^{k-1}$ soit exactement p^{k-1}.
D'où, finalement, $\varphi(p) = p^k - p^{k-1}$.

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).

Démonstration

(i) Si $(k \bmod nm) \in \left(\mathbb{Z}/nm\mathbb{Z}\right)^\times$ alors $k \wedge (nm) = 1$ donc

$$k \wedge n = k \wedge m = 1$$

(pas de diviseur commun non trivial) donc $(k \bmod n) \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ et $(k \bmod m) \in \left(\mathbb{Z}/m\mathbb{Z}\right)^\times$.

(ii) Par (i), (et le (i) du théorème chinois), g est bien définie et comme f (du théorème chinois) était un morphisme d'anneaux, g est bien un morphisme de groupes multiplicatifs.
Comme restriction de f, g est injectif, reste à montrer la surjectivité (pas d'égalité des cardinaux cette fois : elle va servir au corollaire suivant) : soit $a, b \in \mathbb{Z}$ tel que $(a \bmod n, b \bmod m) \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/m\mathbb{Z}\right)^\times$.
Par surjectivité de f, on a $k \in \mathbb{Z}$ tel que

$$(a \bmod n, b \bmod m) = f(k \bmod nm).$$

Reste à voir si $(k \bmod nm) \in \left(\mathbb{Z}/nm\mathbb{Z}\right)^\times$. Or

$$(a \bmod n) = (k \bmod n) \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$$

et

$$(b \bmod m) = (k \bmod m) \in \left(\mathbb{Z}/m\mathbb{Z}\right)^\times$$

donc $k \wedge n = k \wedge m = 1$, donc $k \wedge (mn) = 1$ d'où $(k \bmod nm) \in \left(\mathbb{Z}/nm\mathbb{Z}\right)^\times$ puis

$$(a \bmod n, b \bmod m) = f(k \bmod nm) = g(k \bmod nm)$$

donc g est surjective.

Corollaire 4 : Multiplicativité de φ

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

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

Démonstration

En effet, avec l'isomorphisme de la question précédente,

$$\left|\left(\mathbb{Z}/_{nm\mathbb{Z}}\right)^\times\right| = \left|\left(\mathbb{Z}/_{n\mathbb{Z}}\right)^\times \times \left(\mathbb{Z}/_{m\mathbb{Z}}\right)^\times\right| = \left|\left(\mathbb{Z}/_{n\mathbb{Z}}\right)^\times\right| \times \left|\left(\mathbb{Z}/_{m\mathbb{Z}}\right)^\times\right|.$$

■

Corollaire 5 : Produit de plus de deux termes

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

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

Démonstration

Récurrence. ■

Corollaire 6 : Expression à l'aide des diviseurs premiers

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

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

Exercice 7 : La même formule, avec des probabilités

Soit $\Omega = [\![1, n]\!]$ où n est un entier non premier supérieur ou égal à 2, muni de la probabilité uniforme. Si $d|n$, on note $A_d = \{kd,\ k \in \Omega \text{ et } kd \in \Omega\}$.

1. **Quelle est la probabilité de A_d ?**
2. **Soit P l'ensemble des diviseurs premiers de n.**
   (a) **Démontrer que $(A_p)_{p\in P}$ est une famille d'événements indépendants.**
   (b) **En déduire que $\varphi(n) = n \prod_{p\in P} \left(1 - \frac{1}{p}\right)$.**

---

1. $\mathbb{P}(A_d) = \dfrac{|A_d|}{|\Omega|} = \dfrac{\frac{n}{d}}{n} = \dfrac{1}{d}$.
2. (a) Si $p_1, \dots, p_\ell$ sont des diviseurs premiers deux à deux distincts de n, comme ils sont premiers, $\bigcap_{j=1}^{\ell} A_{p_j} = A_{p_1 \cdots p_\ell}$.

$$\mathbb{P}\left(\bigcap_{j=1}^{\ell} A_{p_j}\right) = \mathbb{P}(A_{p_1\cdots p_\ell}) = \frac{1}{p_1 \cdots p_\ell} = \prod_{j=1}^{\ell} \mathbb{P}(A_{p_j}).$$

   (b) Les $\overline{A}_p$ sont aussi indépendant, $A = \bigcap_{p\in P} \overline{A}_p$ est l'ensemble des entiers de $[\![1, n]\!]$ premiers avec n, donc

$$\mathbb{P}(A) = \frac{\varphi(n)}{n} = \prod_{p\in P} \left(1 - \frac{1}{p}\right).$$

Exercice 8 : Une identité remarquable (et classique)

1. **Soient $n \in \mathbb{N}^*$ et $k \in \mathbb{N}$ un diviseur de n. Parmi tous les nombres rationnels de la forme $\frac{q}{n}$ où $1 \leqslant q \leqslant n$, combien y en a-t-il qui s'écrivent sous forme irréductible avec k au dénominateur ?**
   Formulation équivalente : combien y a-t-il dans $\mathbb{U}_n$ de complexes d'ordre exactement k ?
   Formulation équivalente : combien y a-t-il dans $\mathbb{Z}/_{n\mathbb{Z}}$ d'éléments d'ordre exactement k ?
2. **Montrer que, si $n \in \mathbb{N}^*$, $n = \sum_{k|n} \varphi(k)$.**

1. Notons F_k l'ensemble des nombres rationnels de la forme $\frac{q}{m}$ où $1 \leqslant q \leqslant m$ qui s'écrivent sous forme irréductible avec k au dénominateur et $E_k = \{\ell \in [\![1,k]\!],\ \ell \wedge k = 1\}$.

   L'application $f : \left| \begin{array}{ccc} E_k & \longrightarrow & F_k \\ \ell & \longmapsto & \frac{\ell}{k} \end{array} \right.$ est *bijective*[a]. En effet,

   - si $k = 1$, f est l'identité de $F_1 = E_1 = \{1\}$;
   - sinon,
     - ⋆ elle est *bien définie* car si $\ell \in E_k$, $\frac{\ell}{k}$ est un nombre rationnel de la forme $\frac{q}{m}$ car $k|m$ avec $1 \leqslant q \leqslant m$ car $\frac{\ell}{k} \in]0,1]$, qui s'écrit sous forme irréductible avec k au dénominateur car $\ell \wedge k = 1$ et donc $f(\ell) \in F_k$;
     - ⋆ elle est *injective* car si $\ell, \ell' \in E_k$ tels que $f(\ell) = f(\ell')$, alors $\frac{\ell}{k} = \frac{\ell'}{k}$ donc $\ell = \ell'$;
     - ⋆ elle est *surjective* car si $r \in F_k$, $r \in \mathbb{Q} \cap]0,1]$ et r s'écrit forme irréductible avec k au dénominateur, donc on a $l \in [\![1,k]\!]$ avec $k \wedge \ell = 1$ tel que $r = \frac{\ell}{k}$. Comme $k \neq 1$, $\ell \neq k$ donc $\ell \in [\![1, k-1]\!]$, $\ell \in E_k$ et donc $r = f(\ell)$.

   Ainsi, le nombre de rationnels de la forme $\frac{q}{m}$ où $1 \leqslant q \leqslant m$ qui s'écrivent sous forme irréductible avec k au dénominateur est le nombre d'entiers l tels que $0 \leqslant l \leqslant k-1$ et $k \wedge l = 1$ si $k \neq 1$, 1 sinon : il y en a donc $\varphi(k)$.
2. Si on note $F = \left\{\frac{q}{m}\ ;\ 1 \leqslant q \leqslant m\right\}$, alors $F = \bigsqcup_{k|m} F_k$ car tout rationnel de F s'écrit de manière unique sous forme irréductible avec un diviseur de m au dénominateur.

   Donc $|F| = \sum_{k|m} |F_k|$, et comme $|F| = |[\![1,m]\!]| = m$, $\boxed{m = \sum_{k|m} \varphi(k)}$ d'après la question précédente.

a. On peut aller un peu plus vite oralement en invoquant simplement l'existence et l'unicité de la forme irréductible des fractions.

Théorème 7 : d'Euler

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

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

Démonstration

$\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ qui est un groupe multiplicatif **fini**, donc $\overline{a}^{|\mathbb{Z}/n\mathbb{Z}|} = \overline{a}^{\varphi(n)} = \overline{1}$. ■

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),

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

Démonstration

Théorème d'Euler avec $\varphi(p) = p - 1$. ■

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**.

Remarque

R 29 – L'application $f : \left|\begin{array}{ccc} (\mathbb{Z},+) & \longrightarrow & (\mathbb{K},+) \\ k & \longmapsto & k \cdot 1_\mathbb{K} \end{array}\right.$ est un morphisme de groupe.
Son noyau est un sous-groupe de $(\mathbb{Z}, +)$ donc de la forme $p\mathbb{Z}$ où $p \in \mathbb{N}$.
Si $p = 0$, $\mathbb{K}$ est de caractéristique nulle.
Sinon, $\mathbb{K}$ est de caractéristique p.

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.

Démonstration

(i) Si $\mathbb{K}$ est de caractéristique $p = dk \neq 0$, alors par intégrité, $d \cdot 1_\mathbb{K} = 0_\mathbb{K}$ ou $k \cdot 1_\mathbb{K} = 0_\mathbb{K}$ donc, par minimalité $d = p$ ou $k = p$. Ainsi, p est un nombre premier.

(ii) Immédiat. ■

Remarque

R 30 – On peut montrer que les corps finis de caractéristique un nombre premier p sont de cardinal une puissance de p et que pour tout $n \in \mathbb{N}^*$, il existe, à isomorphisme près, un unique corps de cardinal p^n, noté $\mathbb{F}_{p^n}$. Attention, pour $n \geqslant 2$, il n'est pas isomorphe à l'anneau $\mathbb{Z}/p^n\mathbb{Z}$, qui n'est même pas intègre.
Pour le démontrer, il suffit d'interpréter un tel corps comme un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel, nécessairement de dimension finie.
À isomorphisme près, le seul corps de cardinal p est $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

R 31 – Un théorème, dit de Wedderburn, affirme que pour tout corps fini, la commutativité (qui fait partie de la définition dans notre programme) est en fait automatique.

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* : $\forall\, \lambda \in \mathbb{K},\ \ \forall\, x, y \in \mathcal{A},$

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

Exemple

E 22 – $(\mathbb{C}, +, \times, \cdot)$ est une $\mathbb{R}$-algèbre et une $\mathbb{C}$-algèbre.
E 23 – $\left(\mathbb{K}^X, +, \times, \cdot\right)$ est une $\mathbb{K}$-algèbre.
E 24 – $\left(\mathbb{K}^{\mathbb{N}}, +, \times, \cdot\right)$ est une $\mathbb{K}$-algèbre.
E 25 – $(\mathbb{K}[X], +, \times, \cdot)$ est une $\mathbb{K}$-algèbre.
E 26 – $(\mathbb{K}(X), +, \times, \cdot)$ est une $\mathbb{K}$-algèbre.
E 27 – Si E est un $\mathbb{K}$-espace vectoriel, $(\mathcal{L}(E), +, \circ, \cdot)$ est une $\mathbb{K}$-algèbre.
E 28 – Si $n \in \mathbb{N}^*$, $(\mathcal{M}_n(\mathbb{K}), +, \times, \cdot)$ est une $\mathbb{K}$-algèbre.

On a aussi une notion de sous-algèbre : c'est simultanément un sous-espace vectoriel et un sous-anneau, donc stable par combinaisons linéaires et par produit et contenant l'unité.

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

Exemple

E 29 – $\mathbb{K}[X]$ est une sous-algèbre de $\mathbb{K}(X)$.
E 30 – $\mathcal{C}^k(I, \mathbb{K})$ est une sous-algèbre de $\mathbb{K}^I$.
E 31 – L'ensemble des suites convergentes est une sous-algèbre de $\mathbb{K}^{\mathbb{N}}$.
E 32 – L'ensemble $\mathbb{K}[x]$ des fonctions polynomiales est une sous-algèbre de $\mathbb{K}^{\mathbb{K}}$.

L'intérêt principal des algèbres est de pouvoir évaluer un polynôme à cœfficients dans $\mathbb{K}$ en un élément d'une $\mathbb{K}$-algèbre :

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

Exemple

E 33 – Si $X \neq \varnothing$, $\mathcal{A}$ une $\mathbb{K}$-algèbre, $a \in X$, $u_a : \left| \begin{array}{ccc} \mathcal{A}^X & \longrightarrow & \mathcal{A} \\ f & \longmapsto & f(a) \end{array} \right.$ est un morphisme de $\mathbb{K}$-algèbres. (morphisme d'évaluation).

E 34 – $f : \left| \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{K}[x] \\ P & \longmapsto & \widetilde{P} \end{array} \right.$ est un isomorphisme d'algèbre si $\mathbb{K}$ est infini, et $g : \left| \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{K}(X) \\ P & \longmapsto & \frac{P}{1} \end{array} \right.$ est un morphisme d'algèbres injectif.

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.

Démonstration

Soit $P = \sum_{k \geqslant 0} a_k X^k, Q = \sum_{k \geqslant 0} b_k X^k \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$. L'associativité et la distributivité des lois sur $\mathcal{A}$, toutes les sommes étant finies, permettent d'écrire :

- $(P + \lambda Q)(x) = \sum_{k \geqslant 0} (a_k + \lambda b_k) x^k = \sum_{k \geqslant 0} a_k x^k + \lambda \sum_{k \geqslant 0} b_k x^k = P(x) + \lambda Q(x).$
- $(PQ)(x) = \sum_{k,\ell \geqslant 0} a_k b_\ell x^k = \left(\sum_{k \geqslant 0} a_k x^k \right) \times \left(\sum_{\ell \geqslant 0} b_\ell x^\ell \right) = P(x) \times Q(x).$
- $f\left(1_{\mathbb{K}[X]}\right) = f\left(X^0\right) = x^0 = 1_{\mathcal{A}}.$ ■

Remarque

R 32 – En particulier, deux polynômes en $x \in \mathcal{A}$ commutent toujours.

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**.

Exemple

E 35 – $n\|\cdot\|_\infty$ est une norme d'algèbre sur $\mathcal{M}_n(\mathbb{K})$.
On verra plus tard une catégorie de normes d'algèbre sur $\mathcal{L}(E)$ et sur $\mathcal{M}_n(\mathbb{K})$ appelées normes subordonnées, ou normes d'opérateur.

Propriété 36 : Norme d'algèbre et puissance

On a alors, pour tout $a\in\mathcal{A}$ et $k\in\mathbb{N}^*$, $N\left(a^k\right)\leqslant N(a)^k$.

Démonstration

Récurrence immédiate. ■

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 $\sum_{k\geqslant 0}\frac{a^k}{k!}$ est absolument convergente.

(ii) Si $N(a)<1$, alors la série $\sum_{k\geqslant 0}a^k$ 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 $\sum_{n=0}^{+\infty}a^k$.

Démonstration

(i) Pour tout $k\in\mathbb{N}$, $0\leqslant N\left(\frac{a^k}{k!}\right)\leqslant\frac{N(a)^k}{k!}$ et $\sum_{k\geqslant 0}\frac{N(a)^k}{k!}$ converge comme série exponentielle réelle.

(ii) Pour tout $n\in\mathbb{N}$, $0\leqslant N\left(a^n\right)\leqslant N(a)^n$ qui est un terme général de série géométrique réelle convergente car $N(a)\in[0,1[$ donc, par comparaison de séries à termes généraux positifs, $\sum N\left(a^n\right)$ converge, donc $\sum a^n$ est absolument convergente.
Si, de plus, $\mathcal{A}$ est de dimension finie, on en déduit que $\sum a^n$ converge.
Puis on a, pour $n\in\mathbb{N}$,

$$(1_\mathcal{A}-a)\times\sum_{k=0}^{n}a^k=\sum_{k=0}^{n}(1_\mathcal{A}-a)\times a^n=\sum_{k=0}^{n}\left(a^k-a^{k+1}\right)=1_\mathcal{A}-a^{n+1}$$

par télescopage. Or $u^{N+1}\xrightarrow[N\to+\infty]{}0_A$ car $\sum u^n$ converge, ou car $\left\|u^{N+1}\right\|\leqslant\|u\|^{N+1}\to 0$, donc

$$(e-u)\times\sum_{n=0}^{N}u^n\xrightarrow[N\to\infty]{}e.$$

Par ailleurs, comme $x \mapsto (e-u)x$ est continue sur A car linéaire sur l'espace vectoriel A de dimension finie,

$$(e-u) \times \sum_{n=0}^{N} u^n \xrightarrow[N\to\infty]{} (e-u) \times \sum_{n=0}^{+\infty} u^n.$$

Par unicité de la limite, $(e-u) \times \sum_{n=0}^{+\infty} u^n = e$.

On montre de même que $\left(\sum_{n=0}^{+\infty} u^n\right) \times (e-u) = e$.

On a donc que $\boxed{e-u \text{ est inversible et que } (e-u)^{-1} = \sum_{n=0}^{+\infty} u^n.}$

Remarque

R 33 – Il faut être en **dimension finie** pour en déduire la convergence de ces séries.

Exercice 9 : CCINP 40 et 61