
Anneaux, corps et algèbres

EL AMDAOUI Mustapha,

Lycée IBN TIMIYA,
site web: www.elamdaoui.com,
email: elamdaoui@gmail.com

Niveau: MP

Table des matières

I Anneaux	2
I.1 Anneaux	2
I.2 Anneau produit	4
I.3 Sous-anneaux	4
I.4 Morphisme d'anneaux	5
I.5 Anneau intègre. Corps	6
II Idéaux d'un anneau commutatif	7
II.1 Idéaux	7
II.2 Divisibilité	8
II.3 Idéaux de $\mathbb{Z}$	9
III L'anneau $\mathbb{Z}/n\mathbb{Z}$	10
III.1 Congruence dans $\mathbb{Z}$	10
III.2 Théorème chinois	12
III.3 Indicateur d'Euler	13
IV Arithmétique de $\mathbb{K}[X]$	15
IV.1 Idéaux de $\mathbb{K}[X]$	15
IV.2 Polynômes irréductibles	16
V Algèbre	19
V.1 Algèbre	19
V.2 Sous-algèbre	20
V.3 Morphisme d'algèbres	20
V.4 Idéal annulateur et polynôme minimal	21

I Anneaux

I.1 Anneaux

Définition 1

Soit $\mathbb{A}$ muni de deux lois de composition interne notées $+$ et $\times$. On dit que $(\mathbb{A}, +, \times)$ est un anneau si

1. $(A, +)$ est un groupe abélien, d'élément neutre noté 0_A .
2. La loi $\times$ est associative, c'est-à-dire

$$\forall (x, y, z) \in A^3, x \times (y \times z) = (x \times y) \times z$$

3. La loi possède un élément neutre 1_A , c'est-à-dire

$$\forall x \in A, x \times 1_A = 1_A \times x = x$$

4. La loi $\times$ est distributive par rapport à l'addition ;

$$\forall (x, y, z) \in A^3 : \begin{cases} x \times (y + z) &= x \times y + x \times z \\ (y + z) \times x &= y \times x + z \times x \end{cases}$$

Cet anneau est dit commutatif quand la loi $\times$ est commutative.

Exemples 1

$\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$

1. $\mathbb{Z}, \mathbb{R}, \mathbb{Q}$ et $\mathbb{C}$ sont des anneaux commutatifs pour l'addition et la multiplication usuelles.
2. Soit X un ensemble non vide. Alors $(\mathbb{K}^X, +, \times)$ est un anneau commutatif
 - ▶ d'élément unité : $1_{\mathbb{K}^X} : X \rightarrow \mathbb{K}, x \mapsto 1$
 - ▶ d'élément neutre : $0_{\mathbb{K}^X} : X \rightarrow \mathbb{K}, x \mapsto 0$
3. $(\mathbb{K}[X], +, \times)$ est un anneau commutatif
4. $(M_n(\mathbb{K}), +, \times)$ est un anneau non commutatif pour $n \geq 2$
5. Soit E est un $\mathbb{K}$ -espace vectoriel.
 $(\mathcal{L}(E), +, \circ)$ est un anneau non commutatif si $\dim E \geq 2$

Exemple: Anneau nul

Si $A = \{0\}$ alors $(A, +, \times)$ est un anneau appelé anneau nul.

Théorème 1: Règles de calcul dans un anneau

Soit $(A, +, \times)$ un anneau d'élément neutre 0 et d'unité 1. Alors

1. Pour tout $x \in A$: $x \times 0 = 0 \times x = 0$
2. Pour tout $x, y \in A$: $(-x) \times y = x \times (-y) = -(x \times y)$

Preuve:

1. Soit x un élément quelconque de A .

On a : $x = x \times 1 = x \times (0 + 1) = (x \times 0) + (x \times 1) = (x \times 0) + x$, d'où : $x - x = (x \times 0) + x - x$ et $0 = (x \times 0) + 0 = (x \times 0)$

On a aussi : $x = 1 \times x = (0 + 1) \times x = (0 \times x) + (1 \times x) = (0 \times x) + x$, d'où : $x - x = (0 \times x) + x - x$ et $0 = (0 \times x) + 0 = (0 \times x)$

2. Soient x et y deux éléments quelconques de A .

On a : $(x \times y) + ((-x) \times y) = (x + (-x)) \times y = 0 \times y = 0$. D'où : $(-x) \times y = -(x \times y)$

Et : $(x \times y) + (x \times (-y)) = x \times (y + (-y)) = x \times 0 = 0$. D'où : $x \times (-y) = -(x \times y)$

Il vient : $(-x) \times (-y) = -(x \times (-y)) = -(-(x \times y)) = x \times y$

Théorème 2: Deux formules importantes

Soit $(A, +, \times)$ un anneau et a, b deux éléments de A tels que $ab = ba$. Alors

1. **Formule du binôme de Newton** : Pour tout $n \in \mathbb{N}$

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

2. **Formule de factorisation** : Pour tout $n \in \mathbb{N}$

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

Preuve:

1. Par récurrence sur n
2. Somme télescopique

Définition 2

Soit $(A, +, \times)$ un anneau et $x \in A$. On dit que x est inversible s'il possède un symétrique pour la loi $\times$, c'est-à-dire si

$$\exists y \in A : y \times x = x \times y = 1$$

L'ensemble des inversibles dans A est noté $\mathbb{U}(A)$

Propriété 1

Soit $(A, +, \times)$ un anneau, alors $(\mathbb{U}(A), \times)$ est un groupe, appelé groupe des unités de A .

Preuve:

Soit a et b des éléments inversibles de A , d'inverses a^{-1} et b^{-1} , alors $a \times b$ est inversible d'inverse $b^{-1} \times a^{-1}$. Donc $\mathbb{U}(A)$ est stable pour la multiplication.

L'associativité de la multiplication est garantie par les propriétés de l'anneau et l'existence d'un élément neutre par le fait que $1_A \in \mathbb{U}(A)$

Exemple

1. $\mathbb{U}(\mathbb{Z}) = \{-1; 1\}$;
2. $\mathbb{U}(\mathbb{K}[X]) = \mathbb{K}^*$.
3. Soit $n \in \mathbb{N}^*$. Le groupe $\mathbb{U}(M_n(\mathbb{K})) = \text{GL}_n(\mathbb{K})$

Exemple

Soit x un élément nilpotent d'un anneau A . Montrer que $1_A - x$ est inversible.

Soit $n \in \mathbb{N}$ tel que $x^n = 0$. L'idée est d'utiliser l'identité remarquable (toujours valable dans un anneau)

$$\forall p \in \mathbb{N}^*, \quad 1_A - x^p = (1_A - x) \times \sum_{k=0}^{p-1} x^k$$

Si on l'applique pour $p = n$, alors on obtient

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

ce qui implique que $1_A - x$ est inversible d'inverse $\sum_{k=0}^{n-1} x^k$.

I.2 Anneau produit

Propriété 2: Produit fini d'anneaux

Soit $(A_1, +_1, \times_1), \dots, (A_n, +_n, \times_n)$ des anneaux et $A = A_1 \times \dots \times A_n$.

On définit des lois $+$ et $\times$ sur A en posant

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) := (x_1 +_1 y_1, \dots, x_n +_n y_n)$$

et

$$(x_1, \dots, x_n) \times (y_1, \dots, y_n) := (x_1 \times_1 y_1, \dots, x_n \times_n y_n)$$

L'ensemble A muni des lois $+$ et $\times$ définies ci-dessus est un anneau de neutres

$$0_A = (0_{A_1}, \dots, 0_{A_n}) \text{ et } 1_A = (1_{A_1}, \dots, 1_{A_n})$$

De plus, la loi $\times$ est commutative si, et seulement si, les lois $\times_1, \dots, \times_n$ sont commutatives

Corollaire 1

Si $\mathbb{A}$ est l'anneau produit $\prod_{i=1}^n \mathbb{A}_i$, alors

$$\mathbb{U}(\mathbb{A}) = \mathbb{U}(\mathbb{A}_1) \times \dots \times \mathbb{U}(\mathbb{A}_n)$$

Exemple: L'anneau produit $\mathbb{Z}^2$

$(\mathbb{Z}^2, +, \times)$ est un anneau commutatif. On a

$$\mathbb{U}(\mathbb{Z}^2) = \{(1, 1), (1, -1), (-1, 1), (-1, -1)\}$$

I.3 Sous-anneaux

Définition 3

Soit $(A, +, \times)$ un anneau et B une partie de A . On dit que B est un sous-anneau de $(A, +, \times)$ si, et seulement, si

1. B est un sous-groupe de $(A, +)$
2. B est stable pour la multiplication de A
3. $1_A \in B$

Propriété 3: Condition nécessaire et suffisante du sous-anneau

Soit $(A, +, \times)$ un anneau et B une partie de A . Pour que B soit un sous-anneau de A , il faut et il suffit que :

1. $1_A \in B$
2. $\forall (x, y) \in B^2, x - y \in B$
3. $\forall (x, y) \in B^2, x \times y \in B$

Propriété 4

Un sous-anneau d'un anneau est un anneau

I.4 Morphisme d'anneaux

Définition 4

Soient A, A' deux anneaux d'unités respectives 1_A et $1_{A'}$ et soit $f : A \rightarrow A'$ une application. On dit que f est un morphisme d'anneaux si et seulement si :

1. $f(1_A) = 1_{A'}$;
2. $\forall (x, y) \in A^2 : \begin{cases} f(x+y) = f(x) + f(y) \\ f(xy) = f(x)f(y) \end{cases}$

Remarque :

Un morphisme d'anneaux est un morphisme de groupes

Vocabulaire :

- un endomorphisme d'anneaux A est un morphisme de A dans A .
- un isomorphisme d'anneaux est un morphisme d'anneaux bijectif.
- un automorphisme d'un anneaux A est un endomorphisme d'anneaux A bijectif.
- Deux anneaux sont dits isomorphes s'il existe un isomorphisme de l'un vers l'autre

Propriété 5

Soit $f : A \rightarrow A'$ un morphisme d'anneaux. Alors

1. $f(0) = 0$
2. $\forall a \in A, f(-a) = -f(a)$
3. $\forall a \in A, \forall n \in \mathbb{Z}, f(na) = nf(a)$
4. $\forall a \in A, \forall n \in \mathbb{N}, f(a^n) = f(a)^n$
5. $\forall a \in \mathcal{U}(A), on a f(a) \in \mathcal{U}(A') et f(a)^{-1} = f(a^{-1})$

Preuve:

Les assertions 1, 2 et 3 sont vérifiées car f est un morphisme de groupes additifs.

4. Par récurrence sur $n \in \mathbb{N}$;

5. Soit $a \in \mathcal{U}(A)$, alors

$$f(a) \times f(a^{-1}) = f(a \times a^{-1}) = f(1_A) = 1_{A'}$$

et

$$f(a^{-1}) \times f(a) = 1_{A'}$$

Donc, par unicité de l'inverse, $f(a)$ est inversible dans A' d'inverse $f(a^{-1})$

Propriété 6

1. La composée de deux morphismes d'anneaux et un morphisme d'anneaux.
2. L'application réciproque d'un isomorphisme d'anneaux est un isomorphisme d'anneaux

Définition 5

Soit $f : A \rightarrow A'$ un morphisme d'anneaux.

On appelle image et noyau du morphisme f les ensembles

$$\text{Im}(f) = f(A) \quad \text{et} \quad \text{Ker}(f) = f^{-1}(\{0_{A'}\})$$

Remarque :

Ce sont en fait les images et noyaux de f en tant que morphisme de groupes additifs.

Propriété 7

$f : A \rightarrow A'$ un morphisme d'anneaux. Alors

1. f est injective si, et seulement si, $\text{Ker}f = \{0_A\}$.

2. f est surjective si, et seulement si, $\text{Im} f = A'$.

Preuve:

Car f est en particulier un morphisme de groupes additifs.

Propriété 8

1. L'image d'un sous-anneau par un morphisme d'anneaux est un sous-anneau.
2. L'image réciproque d'un sous-anneau par un morphisme d'anneaux est un sous-anneau.

I.5 Anneau intègre. Corps

Définition 6: Anneau intègre

Un anneau $(A, +, \times)$ est dit intègre quand il est commutatif, non nul et vérifie

$$\forall a, b \in A, \quad ab = 0 \Rightarrow (a = 0 \quad \text{ou} \quad b = 0)$$

Définition 7: Corps

Un ensemble $\mathbb{K}$ muni de deux lois $+$ et $\times$ est appelé corps si :

1. $(\mathbb{K}, +, \times)$ est un anneau commutatif non nul.
2. $\mathbb{U}(\mathbb{K}) = \mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

Remarque :

- Dans un corps $0_{\mathbb{K}} \neq 1_{\mathbb{K}}$;
- Les règles de calculs dans un corps sont les mêmes que dans un anneau.

Exemple

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps commutatifs.

Propriété 9

Tout corps est un anneau intègre

Preuve:

Soit $(\mathbb{K}, +, \times)$ un corps, $x, y \in \mathbb{K}$ avec $x \times y = 0_{\mathbb{K}}$.

Si $x \neq 0_{\mathbb{K}}$, alors x est inversible donc $x^{-1} \times x \times y = 0_{\mathbb{K}} \Rightarrow y = 0_{\mathbb{K}}$.

Définition 8: Sous-corps

Soient $(\mathbb{K}, +, \times)$ un corps et $\mathbb{L}$ une partie de $\mathbb{K}$. On dit que $\mathbb{L}$ est un sous-corps de $\mathbb{K}$ si et seulement si :

1. $\mathbb{L}$ est un sous-anneau de $\mathbb{K}$
2. $\forall x \in \mathbb{L} \setminus \{0\}, x^{-1} \in \mathbb{L}$

Propriété 10: Condition nécessaire et suffisante du sous-anneau

Soit $(\mathbb{K}, +, \times)$ un corps et $\mathbb{L}$ une partie de $\mathbb{K}$. Pour que $\mathbb{L}$ soit un sous-corps de $\mathbb{K}$, il faut et il suffit que :

1. $1_{\mathbb{K}} \in \mathbb{L}$
2. $\forall (x, y) \in \mathbb{L}^2, x - y \in \mathbb{L}$
3. $\forall x \in \mathbb{L} \text{ et } y \in \mathbb{L} \setminus \{0\}, x \times y^{-1} \in \mathbb{L}$

Propriété 11

Un sous-corps d'un corps est un corps

II Idéaux d'un anneau commutatif

Dans cette section $\mathbb{A}$ désigne un anneau commutatif d'unité 1_A

II.1 Idéaux

Définition 9

Une partie I de $\mathbb{A}$ est dit idéal si :

1. I est un sous-groupe de $(\mathbb{A}, +)$;
2. **Propriété d'absorption** : $\forall (a, b) \in \mathbb{A} \times I, \quad ab \in I$

Exemple

Les sous-ensembles $\{0\}$ et $\mathbb{A}$ sont des idéaux de $\mathbb{A}$, dits triviaux

Propriété 12: Idéal principal

Soit $a \in \mathbb{A}$. L'ensemble $\{ax, x \in \mathbb{A}\}$ est un idéal de $\mathbb{A}$, appelé l'idéal engendré par a et noté (a) ou $a\mathbb{A}$.
Un tel idéal est dit principal

Preuve:

Soit $a \in A$.

- ▶ $aA \subset A$;
- ▶ $aA \neq \emptyset$ car $0_A = a \times 0_A \in aA$;
- ▶ soit $x, y \in aA$, alors il existe $b, c \in A$ tels que $x = a \times b$ et $y = a \times c$, alors

$$x - y = a \times (b - c) \in aA$$

En outre pour $d \in A$, alors par associativité et commutativité de la loi $\times$, on a

$$d \times x = d \times (a \times b) = a \times (b \times d) \in aA$$

Remarque :

$\mathbb{A}$ est un idéal principal, car $\mathbb{A} = (1)$

Exemple

1. Soit $n \in \mathbb{Z}$, alors $(n) = n\mathbb{Z}$ est un idéal de $\mathbb{Z}$
2. Soit $P \in \mathbb{K}[X]$, alors $(P) = P\mathbb{K}[X]$ est un idéal de $\mathbb{K}[X]$

Propriété 13

Soit I et J deux idéaux de $(A, +, \times)$, alors

1. $I + J := \{x + y \mid x \in I \text{ et } y \in J\}$ est un idéal de $(A, +, \times)$.
2. $I \cap J$ est un idéal de $(A, +, \times)$.

Preuve:

Facile à vérifier

Propriété: Caractéristique

Une partie I de A est un idéal de $(A, +, \times)$ si, et seulement si,

1. $I \neq \emptyset$;
2. $\forall (u, v) \in A^2; \forall (a, b) \in I^2, au + bv \in I$

Propriété 14

Soit I un idéal de A

1. Si I contient 1_A , alors $I = A$.

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

Preuve:

1. Pour tout $a \in A$, on a $a = a \times 1_A \in I$, par la propriété d'absorption.
2. Si I contient un inversible d'inverse u^{-1} , il contient $u^{-1}u = 1$ par la première assertion, donc $a = a \cdot 1 \in I$.

Conséquence 1

Les idéaux d'un corps sont exactement ses idéaux triviaux

Preuve:

Soit I un idéal non nul d'un corps $(\mathbb{K}, +, \times)$, alors I contient un élément de $\mathbb{K} \setminus \{0\}$ qui est inversible, donc $I = \mathbb{K}$

Propriété 15

Soit $(A, +, \times)$ et $(B, +, \times)$ deux anneaux commutatifs et $f : A \rightarrow B$ un morphisme d'anneaux.

1. $\text{Ker}(f)$ est un idéal de $(A, +, \times)$
2. Si J est un idéal de B alors $f^{-1}(J)$ est un idéal de $(A, +, \times)$.
3. l'image directe d'un idéal de A est un idéal de $(f(A), +, \times)$.

Preuve:

1. Découle de 2, car $\text{Ker}(f) = f^{-1}(\{0\})$
2. Soit $x, y \in f^{-1}(J)$ et $a \in A$. Comme J est non vide donc $f^{-1}(J)$ est également non vide. f est un morphisme d'anneaux, donc $f(x - y) = f(x) - f(y)$. J étant un idéal, $f(x) - f(y) \in J$, donc $x - y \in f^{-1}(J)$. Également, $f(ax) = f(a)f(x)$, et J étant un idéal, $f(a)f(x) \in J$, donc $ax \in f^{-1}(J)$.
3. Soit I un idéal de A .
 - $f(I)$ est un sous-groupe de $f(A)$;
 - Soit $a' \in f(I)$ et $x' \in f(A)$, alors il existe $a \in I$ et $x \in A$ tels que $a' = f(a)$ et $x' = f(x)$. Comme f est un endomorphisme d'anneaux

$$a' \cdot x' = f(a) \cdot f(x) = f(ax) \in f(I)$$

Attention

L'image directe d'un idéal par un morphisme d'anneaux n'est pas forcément un idéal. En effet,

$$f : \begin{cases} \mathbb{Z} & \longrightarrow & \mathbb{R} \\ n & \longmapsto & n \end{cases}$$

est un morphisme d'anneaux, $\mathbb{Z}$ est un idéal de $\mathbb{Z}$ mais $\text{Im}(f) = \mathbb{Z}$ n'est pas un idéal de $\mathbb{R}$.

Conséquence 2

Tout morphisme de corps est injectif

Preuve:

Le noyau d'un morphisme de corps est un idéal non nul

II.2 Divisibilité

On suppose dans cette section que A est intègre.

Définition 10

Soit $a, b \in A$. On dit que a divise b , ce que l'on note $a \mid b$, s'il existe $c \in A$ tel que $b = ac$.

Vocabulaire :

Lorsque a divise b , on dit que a est un diviseur de b et que b est un multiple de a .

Propriété 16

La relation de divisibilité | est réflexive et transitive.

Propriété 17

Soit $a, b, c \in A$.

1. Si c divise a et b , alors c divise l'expression $au + bv$ pour tout $u, v \in A$
2. $a \mid b \iff bA \subset aA$

Preuve:

L'idéal principal aA est l'ensemble des multiples de a . Supposons $a \mid b$.

Soit $x \in bA$, on a $b \mid x$, soit par transitivité $a \mid x$, par conséquent $x \in aA$.

Réciproquement, $bA \subset aA$, entraîne $b \in aA$, soit $a \mid b$.

Propriété 18

Soit $a, b \in A$, alors

$$\begin{cases} x \mid y \\ y \mid x \end{cases} \iff xA = yA \iff \begin{cases} \exists \varepsilon \in \mathcal{U}(A) \\ y = \varepsilon x \end{cases}$$

On dit alors que x et y sont associés, ce que l'on note $x \sim y$

Exemple: Dans $\mathbb{Z}$

Deux entiers a et b sont associés si et seulement si $b = \varepsilon a$ où $\varepsilon \in \mathcal{U}(\mathbb{Z}) = \{-1, 1\}$

Exemple: Dans $\mathbb{K}[X]$

Deux entiers P et Q sont associés si et seulement si $Q = \varepsilon P$ où $\varepsilon \in \mathcal{U}(\mathbb{K}[X]) = \mathbb{K}^*$

II.3 Idéaux de $\mathbb{Z}$ **Propriété 19**

Soit I un idéal de $\mathbb{Z}$, alors il existe un unique $n \in \mathbb{N}$ tel que $I = n\mathbb{Z}$

Preuve:

Un idéal de $(\mathbb{Z}, +, \times)$ est un sous-groupe de $(\mathbb{Z}, +)$

Propriété 20: ppcm et pgcd

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

1. Il existe un unique $\delta \in \mathbb{N}$ tel que $a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z}$.
En outre δ est l'unique entier naturel vérifiant :
 - δ divise a et b ;
 - Si d est un diviseur commun de a et b , alors d divise δ . δ est appelé le plus grand diviseur commun de a et b , noté **pgcd**(a, b) ou $a \wedge b$.
2. Il existe un unique $m \in \mathbb{N}$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.
En outre m est l'unique entier naturel vérifiant :
 - m est un multiple commun de a et b ;
 - Si M est un multiple commun de a et b , alors m divise M . m est appelé le plus petit multiple commun de a et b , noté **ppcm**(a, b) ou $a \vee b$.

Preuve:

1. Soit d le générateur positif ou nul de l'idéal $a\mathbb{Z} + b\mathbb{Z}$. Les inclusions :

$$a\mathbb{Z} \subset d\mathbb{Z} \quad \text{et} \quad b\mathbb{Z} \subset d\mathbb{Z}$$

montrent que d est un diviseur commun de a et b . Comme d appartient à $a\mathbb{Z} + b\mathbb{Z}$, il existe un couple $(u, v) \in \mathbb{Z}^2$ tel que : $d = ua + bv$.

Tout diviseur commun de a et b est alors un diviseur de d . Cet élément est donc le PGCD de a et b .

2. Soit m le générateur positif ou nul de l'idéal $a\mathbb{Z} \cap b\mathbb{Z}$. Un entier c est un multiple commun de a et b si, et seulement si, $c\mathbb{Z} \subset a\mathbb{Z}$ et $c\mathbb{Z} \subset b\mathbb{Z}$, c'est-à-dire $c\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z}$; cela équivaut à $m \mid c$. L'entier naturel m est donc le PPCM de a et b .

III L'anneau $\mathbb{Z}/n\mathbb{Z}$

III.1 Congruence dans $\mathbb{Z}$

Définition 11

Soient $n \in \mathbb{N}^*$ et $a, b \in \mathbb{Z}$. On dit que a est congru à b modulo n si $n \mid (b - a)$; cette relation entre a et b se note $a \equiv b \pmod{n}$

$$a \equiv b \pmod{n} \iff \exists k \in \mathbb{Z}, \quad a - b = kn$$

Propriété 21

Soit $n \in \mathbb{N}^*$. La relation $\equiv \pmod{n}$ est une relation d'équivalence compatible avec la somme et le produit

Preuve:

- La réflexivité et la symétrie de $\equiv \pmod{n}$ sont immédiates. Montrons seulement la transitivité. Trois entiers $a, b, c \in \mathbb{Z}$ étant donnés, supposons qu'on ait $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$. Alors $n \mid (a - b)$ et $n \mid (b - c)$, donc par somme $n \mid (a - c)$, c'est-à-dire $a \equiv c \pmod{n}$
- Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors $n \mid (a - b)$ et $n \mid (c - d)$, donc par somme $n \mid [(a + c) - (b + d)]$, c'est-à-dire $a + c \equiv b + d \pmod{n}$
- Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors $n \mid (a - b)$ et $n \mid (c - d)$, donc $n \mid [(a - b)c + b(c - d)]$, c'est-à-dire $n \mid (ac - bd)$, ou encore $ac \equiv bd \pmod{n}$

Définition 12

$\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des classes d'équivalence pour la congruence modulo n .

Notation :

On note $\bar{x}$ la classe d'équivalence de x dans $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire

$$\bar{x} = \{y \in \mathbb{Z} \mid y \equiv x \pmod{n}\}.$$

Propriété 22

1. Pour tout $x \in \mathbb{Z}$, il existe un unique $r \in \bar{x}$ tel que $0 \leq r < n$
2. $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$
3. $\text{card}\left(\mathbb{Z}/n\mathbb{Z}\right) = n$

Preuve:

1. On effectue la division euclidienne de x par n : il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que $x = qn + r$ et $0 \leq r < n$, donc $r \equiv x \pmod{n} \iff r \in \bar{x}$ et $0 \leq r < n$.
2. Par l'assertion précédente, $r \in \bar{x}$ est unique. Donc, par transitivité, tous les éléments congrus à r modulo n le sont aussi à x modulo n , ce qui nous amène à écrire que $\bar{r} = \bar{x}$. Mais $\bar{r} \in \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$, d'où le résultat.
3. L'application $\psi : \begin{cases} \llbracket 0, n-1 \rrbracket & \longrightarrow \mathbb{Z}/n\mathbb{Z} \\ k & \longmapsto \bar{k} \end{cases}$ est bijective

Remarque :

D'après la compatibilité de la congruence modulo n avec la somme et le produit, on peut définir deux lois internes dans $\mathbb{Z}/n\mathbb{Z}$ de la manière suivante :

$$\forall \bar{x}, \bar{y} \in \mathbb{Z}/n\mathbb{Z}, \quad \bar{x} + \bar{y} := \overline{x + y} \quad \text{et} \quad \bar{x} \times \bar{y} := \overline{x \times y}$$

cette définition est indépendante du choix des représentants, ce qui la rend pertinente.

Propriété 23

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

Preuve:

Découle directement du fait que $\mathbb{Z}$ soit un anneau commutatif.

Propriété 24: Les unités de $\mathbb{Z}/n\mathbb{Z}$

Soit $n \geq 2$. Alors $\mathbb{U}(\mathbb{Z}/n\mathbb{Z}) = \{\bar{x}, x \in \llbracket 0, n-1 \rrbracket \text{ et } x \wedge n = 1\}$

Preuve:

Soit $x \in \llbracket 0, n-1 \rrbracket$, alors

$$\begin{aligned} \bar{x} \in \mathbb{U}(\mathbb{Z}/n\mathbb{Z}) &\iff \exists u \in \mathbb{Z}, \bar{x} \cdot \bar{u} = \bar{1} \\ &\iff \exists u \in \mathbb{Z}, x \cdot u \equiv 1 \pmod{n} \\ &\iff \exists u, v \in \mathbb{Z}, xu + vn = 1 \\ &\iff x \wedge n = 1 \end{aligned}$$

Remarque :

Les éléments de $\mathbb{U}(\mathbb{Z}/n\mathbb{Z})$ sont les générateurs de groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$

Propriété 25

Soit $n \in \mathbb{N}^*$. Les assertions suivantes sont équivalentes :

1. n est premier,
2. l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps,
3. l'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre

Preuve:

1. $\Rightarrow$ 2.) Supposons que n est premier, alors tous les nombres de $\llbracket 1, n-1 \rrbracket$ sont premiers avec n , donc $\mathbb{U}(\mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z} \setminus \{\bar{0}\}$, et par suite, $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps
2. $\Rightarrow$ 3.) Tout corps est un anneau intègre
3. $\Rightarrow$ 1.) Par contraposée. Si n n'est pas premier, alors $n = pq$ avec $p, q \in \llbracket 2, n-1 \rrbracket$ d'où :

$$\bar{0} = \bar{n} = \overline{pq} = \bar{p} \times \bar{q}$$

Or $\bar{p} \neq \bar{0}$ et $\bar{q} \neq \bar{0}$ donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.

Application 1: Théorème de Wilson

Soit $p \in \mathbb{N}, p \geq 2$. Montrons que p est premier si, et seulement si, $(p-1)! + 1 \equiv 0[p]$

$\Rightarrow$) Si $p \in \{2, 3\}$ le résultat est immédiat. Si $p \geq 5$, p étant premier, $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps :

$$x = x^{-1} \iff x^2 = \bar{1} \iff (x - \bar{1})(x + \bar{1}) = \bar{0} \iff x \in \{\bar{1}, \overline{p-1}\}$$

Dans l'ensemble $\{\bar{2}, \dots, \overline{p-2}\}$ chaque élément est l'inverse d'un autre élément du même ensemble, donc $\bar{2} \times \dots \times \overline{p-2} = \bar{1}$. D'où $\bar{1} \cdot \bar{2} \cdots \overline{p-2} \cdot \overline{p-1} = -\bar{1}$, donc $(p-1)! + 1 \equiv 0 \pmod{p}$

- Dans $\mathbb{Z}/p\mathbb{Z}$, on a $\bar{1} \cdot \bar{2} \cdots \overline{(p-1)} = -\bar{1}$. Donc $\bar{1}, \bar{2}, \dots, \overline{(p-1)}$ sont inversibles dans l'anneau $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ ie. $1, 2, \dots, (p-1)$ sont premiers avec p . Donc p est premier.

Notation :

Lorsque p est premier, le corps $\mathbb{Z}/p\mathbb{Z}$ se note $\mathbb{F}_p$

Exemple

Résoudre dans $\mathbb{Z}/13\mathbb{Z}$ l'équation $x^2 + x + \bar{7} = \bar{0}$.

On met le trinôme $x^2 + x + \bar{7}$ sous forme canonique. On peut remarquer pour cette question que $\bar{14} = \bar{1}$. Ainsi,

$$x^2 + x + \bar{7} = x^2 + \bar{14}x + \bar{7} = (x + \bar{7})^2 - \bar{42}$$

soit encore $x^2 + x + \bar{7} = \bar{0}$ équivaut à $(x + \bar{7})^2 = \bar{3}$. On remarque alors que $\bar{4}^2 = \bar{3}$. Ainsi, l'équation est équivalente à

$$(x + \bar{7})^2 - \bar{4}^2 = 0 \iff (x + \bar{11})(x + \bar{3}) = 0.$$

Puisque $\mathbb{Z}/13\mathbb{Z}$ est un corps, et donc en particulier est intègre, ceci est encore équivalent à $x + \bar{11} = \bar{0}$ ou $x + \bar{3} = \bar{0}$. L'ensemble des solutions est donc $\{\bar{2}, \bar{10}\}$.

Exemple

Résoudre dans $\mathbb{Z}/12\mathbb{Z}$ l'équation $x^2 - \bar{4}x + \bar{3} = \bar{0}$.

On procède de la même façon. L'équation est équivalente à

$$(x - \bar{2})^2 - \bar{1} = 0 \iff (x - \bar{3})(x - \bar{1}) = 0.$$

Mais $\mathbb{Z}/12\mathbb{Z}$ n'est pas un corps. On écrit $(x - \bar{2})^2 = \bar{1}$ et on cherche les racines carrées de $\bar{1}$ dans $\mathbb{Z}/12\mathbb{Z}$. Pour cela on utilise le tableau :

t	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
t^2	$\bar{0}$	$\bar{1}$	$\bar{4}$	$-\bar{3}$	$\bar{4}$	$\bar{1}$	$\bar{0}$

(on a bien sûr $(-t)^2 = t^2$). Ainsi, l'équation est équivalente $x - \bar{2} \in \{-\bar{5}, -\bar{1}, \bar{1}, \bar{5}\}$. L'ensemble des solutions est donc $\{-\bar{3}, \bar{1}, \bar{3}, \bar{7}\}$. Il y a en particulier plus de deux solutions à cette équation polynomiale de degré 2 !

III.2 Théorème chinois**Théorème 3: Chinois**

Soit $m, n \in \mathbb{N}^*$ premiers entre eux, alors l'application

$$\psi : \begin{cases} \mathbb{Z}/mn\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ [x]_{mn} & \longmapsto & ([x]_m, [x]_n) \end{cases}$$

est un isomorphisme d'anneaux.

Preuve:

L'application ψ est bien définie car

$$\begin{aligned} [x]_{mn} = [y]_{mn} &\Rightarrow mn \mid (y - x) \\ &\Rightarrow \begin{cases} m \mid (y - x) \\ n \mid (y - x) \end{cases} \\ &\Rightarrow \begin{cases} [x]_m = [y]_m \\ [x]_n = [y]_n \end{cases} \end{aligned}$$

On vérifie aisément que cette application est un morphisme d'anneaux.

Étudions le noyau de ψ . Soit $[x]_{mn} \in \mathbb{Z}/mn\mathbb{Z}$ on a $\psi([x]_{mn}) = ([0]_m, [0]_n)$, alors $\begin{cases} [x]_m = [0]_m \\ [x]_n = [0]_n \end{cases}$. On a alors $n \mid x$ et $m \mid x$, puis $mn \mid x$, puisque $\text{ppcm}(m, n) = 1$. Ainsi $[x]_{mn} = [0]_{mn}$ ce qui permet d'affirmer $\text{Ker}(\psi) = \{[0]_{mn}\}$. Le morphisme ψ est injectif, et puisque les deux ensembles $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont de même cardinal on peut affirmer que ψ est bijectif

Propriété 26: Système de congruence

Soient $m, n \in \mathbb{N}^*$ premiers entre eux, alors

1. il existe une solution $k_1 \in \llbracket 0, mn - 1 \rrbracket$ au système de congruences :

$$\begin{cases} k \equiv a \pmod{n} \\ k \equiv b \pmod{m} \end{cases} \quad \text{ou } a, b \in \mathbb{Z}$$

2. un entier $k \in \mathbb{Z}$ vérifie le système précédent si, et seulement si : $k \equiv k_1 \pmod{mn}$

Méthode: C

Comment résoudre un système du type

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases} \quad \text{avec } \text{pgcd}(m, n) = 1$$

Par ce qui précède, ce système possède une unique solution modulo mn . Pour la déterminer, on part de la relation de Bézout $mu + nv = 1$, puis $x_0 = mub + nva$ est alors solution du système initial.

Exemple

Résoudre dans $\mathbb{Z}$ les systèmes suivants

$$\begin{cases} x \equiv 3 \pmod{17} \\ x \equiv 4 \pmod{11} \end{cases}$$

$11 \wedge 17 = 1$, le système admet une solution unique à 187 près. On a aussi $-3 \times 11 + 2 \times 17 = 1$, donc $x_0 = -3 \times 3 \times 11 + 4 \times 2 \times 17 = 37$ est une solution particulière. Ainsi les autres solutions sont $37 + 187k$ avec $k \in \mathbb{Z}$

III.3 Indicateur d'Euler**Définition 13: Indicateur d'Euler**

L'application

$$\varphi : \begin{cases} \mathbb{N}^* & \longrightarrow \mathbb{N} \\ n & \longmapsto \text{Card}\left(\bigcup \left(\mathbb{Z}/n\mathbb{Z}\right)\right) \end{cases}$$

est appelée l'indicateur d'Euler

Propriété 27

Pour tout $n \in \mathbb{N}^*$, on a : $\varphi(n) = \text{Card}(\{k \in \llbracket 0, n - 1 \rrbracket, \quad k \wedge n = 1\})$

Propriété 28

Soit p un nombre premier et $k \in \mathbb{N}^*$, alors :

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

Preuve:

Soit $n \in \llbracket 0, p^k - 1 \rrbracket$. Alors $\bar{n}$ n'est pas inversible dans $\mathbb{Z}/p^k\mathbb{Z}$ si, et seulement si $n \wedge p^k \neq 1$ si, et seulement, si p divise n .

Les multiples de p dans $\llbracket 0, p^k - 1 \rrbracket$ sont de la forme αp , avec $\alpha \in \llbracket 0, p^{k-1} - 1 \rrbracket$. Il y a donc p^{k-1} éléments non inversibles dans cet anneau.

On obtient donc :

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

Théorème 4: d'Euler

Soit n un entier ≥ 2 et a un entier premier avec n , alors

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

Preuve:

a est premier avec n , alors $\bar{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$. D'après le théorème de Lagrange $\bar{a}^{\varphi(n)} = \bar{1}$, soit $a^{\varphi(n)} \equiv 1 \pmod{n}$

Conséquence 3 (Théorèmes de Fermat)

Soit p un nombre premier. Alors

1. $a^{p-1} \equiv 1 \pmod{p}$ pour tout $a \wedge p = 1$
2. $a^p \equiv a \pmod{p}$ pour tout $a \in \mathbb{Z}$

Preuve:

1. Le groupe multiplicatif $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$, formé des éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ est d'ordre $p-1$. Tout élément $\bar{a} \in \left(\mathbb{Z}/p\mathbb{Z}\right)^*$ vérifie $\bar{a}^{p-1} = \bar{1}$
2. L'égalité $a^p \equiv a \pmod{p}$ est vraie lorsque a et p est évidente lorsque p divise a

Exemple

Trouvons le reste de la division euclidienne de $a = 10^{(9^8)}$ par 7

D'après le théorème de Fermat $10^6 \equiv 1 \pmod{7}$. Il suffit alors d'étudier 9^8 modulo 6. En utilisant $9 \equiv 3 \pmod{6}$, on obtient $9^8 \equiv 3 \pmod{6}$. Finalement : $10^{(9^8)} \equiv 6 \pmod{7}$

Conséquence 4

Si $m \wedge n = 1$, alors

1. $\mathbb{U}\left(\mathbb{Z}/mn\mathbb{Z}\right)$ et $\mathbb{U}\left(\mathbb{Z}/n\mathbb{Z}\right) \times \mathbb{U}\left(\mathbb{Z}/m\mathbb{Z}\right)$ sont isomorphes
2. $\varphi(mn) = \varphi(m)\varphi(n)$, c'est-à-dire φ est multiplicative

Preuve:

Supposons que n et m soient premiers entre eux. L'isomorphisme du lemme chinois montre que $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ ont même nombre d'éléments inversibles. De plus, un couple $(\bar{r}, \bar{s}) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est inversible si, et seulement si, $\bar{r}$ et $\bar{s}$ le sont respectivement dans $\mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$. On obtient donc :

$$\varphi(mn) = \varphi(m)\varphi(n)$$

Conséquence 5

Soit $n = \prod_{i=1}^r p_i^{k_i}$ est la décomposition en facteurs premiers de l'entier n . Alors

$$\varphi(n) = \prod_{i=1}^r \left(p_i^{k_i} - p_i^{k_i-1}\right) = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right)$$

Exemple

Calculons $\varphi(78)$

Exemple: Cryptage RSA

Soit $n \in \mathbb{N}^*$ sans facteur carré et $d, e \in \mathbb{N}^*$ tels que $de \equiv 1 \pmod{\varphi(n)}$. Alors les applications $x \mapsto x^d$ et $x \mapsto x^e$ sont deux permutations de $\mathbb{Z}/n\mathbb{Z}$ réciproques.

IV Arithmétique de $\mathbb{K}[X]$

Dans ce paragraphe et le suivant, $\mathbb{K}$ est un sous-corps de $\mathbb{C}$.

Rappel :

Soit $A \in \mathbb{K}[X]$, $B \in \mathbb{K}[X] \setminus \{0\}$, alors il existe un et un seul couple $(Q, R) \in \mathbb{K}[X]^2$ appelé division euclidienne de A par B dans $\mathbb{K}[X]$ tel que :

1. $A = BQ + R$
2. $\deg R < \deg B$

Q est le quotient et R le reste de cette division euclidienne.

IV.1 Idéaux de $\mathbb{K}[X]$

Définition 14

Un polynôme est dit normalisé s'il est nul ou s'il est unitaire

Propriété 29

Tout polynôme est associé à un unique polynôme normalisé.

Propriété 30

Tout idéal I de $\mathbb{K}[X]$ peut s'écrire de façon unique sous la forme : $P\mathbb{K}[X]$ avec $P \in \mathbb{K}[X]$ normalisé. Le polynôme P s'appelle le générateur normalisé de I .

Preuve:

► Existence :

- Si I est réduit à $\{0\}$, il s'écrit $0\mathbb{K}[X]$.
- Sinon, considérons $P \in I \setminus \{0\}$ de degré minimal. Quitte à le multiplier par une constante non nulle, on peut supposer que P est unitaire. On a évidemment $P\mathbb{K}[X] \subset I$.
Inversement. Soit $S \in I$, on effectue la division euclidienne de S par P il existe $Q, R \in \mathbb{K}[X]$ tel que

$$S = PQ + R, \quad \deg R < \deg P$$

Le polynôme R , égal à $S - PQ$, appartient à I . Son degré étant strictement inférieur à $\deg P$, minimum des degrés des polynômes non nuls de I , R est nul et $S = PQ$. Finalement $I = P\mathbb{K}[X]$.

- **Unicité :** Deux polynômes P et Q vérifiant $I = P\mathbb{K}[X] = Q\mathbb{K}[X]$ sont associés et, par la proposition précédente, égaux s'ils sont normalisés.

Propriété 31

Soit $P, Q \in \mathbb{K}[X]$

- $P.\mathbb{K}[X] + Q.\mathbb{K}[X] = \text{pgcd}(P, Q).\mathbb{K}[X]$;
- $P.\mathbb{K}[X] \cap Q.\mathbb{K}[X] = \text{ppcm}(P, Q).\mathbb{K}[X]$.

Preuve:

- Soit D le générateur unitaire de l'idéal $P\mathbb{K}[X] + Q\mathbb{K}[X]$. Les inclusions :

$$P\mathbb{K}[X] \subset D\mathbb{K}[X] \quad \text{et} \quad Q\mathbb{K}[X] \subset D\mathbb{K}[X]$$

montrent que D est un diviseur commun de P et Q . Comme D appartient à $P\mathbb{K}[X] \subset D\mathbb{K}[X]$, il existe un couple $(U, V) \in \mathbb{K}[X]^2$ tel que : $D = UP + VQ$.

Tout diviseur commun de P et Q est alors un diviseur de D . Cet élément est donc le PGCD de P et Q que (P, Q) soit égal à $(0, 0)$ ou non.

- Soit M le générateur unitaire de l'idéal $P\mathbb{K}[X] \cap Q\mathbb{K}[X]$. Un polynôme C est un multiple commun de P et Q si, et seulement si, $C\mathbb{K}[X] \subset P\mathbb{K}[X]$ et $C\mathbb{K}[X] \subset Q\mathbb{K}[X]$, c'est-à-dire $C\mathbb{K}[X] \subset P\mathbb{K}[X] \cap Q\mathbb{K}[X]$; cela équivaut à $M \mid C$. L'entier naturel M est donc le PPCM de (P, Q) que ce couple soit égal à $(0, 0)$ ou non.

Propriété 32

Soit $P_1, \dots, P_n \in \mathbb{K}[X]$

- $\sum_{i=1}^n P_i \mathbb{K}[X] = \mathbf{pgcd}(P_1, \dots, P_n) \mathbb{K}[X];$
- $\bigcap_{i=1}^n P_i \mathbb{K}[X] = \mathbf{ppcm}(P_1, \dots, P_n) \mathbb{K}[X].$

Corollaire 2

Soit $P_1, \dots, P_n \in \mathbb{K}[X]$. Alors il existe $(U_1, \dots, U_n) \in \mathbb{K}[X]^n$ tel que $\sum_{i=1}^n U_i P_i = \mathbf{pgcd}(P_1, \dots, P_n)$

Définition 15

Les polynômes $P_1, \dots, P_n \in \mathbb{K}[X]$ sont dits premiers entre eux dans leur ensemble, si

$$\mathbf{pgcd}(P_1, \dots, P_n) = 1$$

Corollaire 3 (Théorème de Bezout)

Les polynômes $P_1, \dots, P_n \in \mathbb{K}[X]$ sont dits premiers entre eux dans leur ensemble, si et seulement si

$$\exists (U_1, \dots, U_n) \in \mathbb{K}[X]^n, \quad \sum_{i=1}^n U_i P_i = 1$$

$U_1, \dots, U_n$ sont appelés les coefficients de Bezout

Corollaire 4 (Théorème de Bezout)

Les polynômes $P, Q \in \mathbb{K}[X]$ sont dits premiers entre eux si, et seulement si,

$$\exists (U, V) \in \mathbb{K}[X]^2, \quad UP + VQ = 1$$

Corollaire 5 (Lemme de Gauss)

Soient $P, Q, R \in \mathbb{K}[X]$.

$$\left\{ \begin{array}{l} P|QR \\ P \wedge Q = 1 \end{array} \right. \Rightarrow P|R.$$

Preuve:

Soit $S \in \mathbb{K}[X]$ tel que $QR = SP$, et soit $(U, V) \in \mathbb{K}[X]^2$ tel que $PU + QV = 1$. Multipliant les deux membres de cette égalité par R , on obtient $R = RPU + RQV$, puis remplaçant QR par SP , il vient

$$R = RPU + SPV = P(RU + SV)$$

$RU + SV \in \mathbb{K}[X]$, donc $P|R$

IV.2 Polynômes irréductibles**Définition 16**

Soit $P \in \mathbb{K}[X]$ un polynôme non constant.

1. On dit que P est irréductible dans $\mathbb{K}[X]$ si, et seulement si, ses seuls diviseurs sont les constantes et les polynômes qui lui sont associés.
2. P est dit composé ou réductible s'il n'est pas irréductible (dans $\mathbb{K}[X]$).

Propriété 33

1. Les polynômes irréductibles de $\mathbb{C}[X]$ sont exactement les polynômes de degré 1 ;
2. Les polynômes irréductibles de $\mathbb{R}[X]$ sont : les polynômes de degré 1, et les polynômes de degré 2 de discriminant < 0 (i.e. sans racines réelles).

Preuve:

1. Soit P un polynôme irréductible de $\mathbb{C}[X]$. Par le théorème de d'Alembert-Gauss, P possède au moins une racine α donc $X - \alpha$ divise P . Puisque P est irréductible et $X - \alpha$ est non constant, alors P et $X - \alpha$ sont associés.
2.
 - On sait déjà que les polynômes de degré 1 sont irréductibles.
 - Considérons maintenant un polynôme P de degré 2 sans racines réelles et soit D un diviseur de P . On a $\deg D \geq 2$ et $D \neq 0$.
 - Si $\deg D = 0$ ou 2 alors D est un diviseur trivial de P .
 - Si $\deg D = 1$ alors D possède une racine réelle qui sera racine de P . C'est exclu.
 Ainsi P est irréductible.
 - Inversement : Soit P un polynôme irréductible dans $\mathbb{R}[X]$. P est non constant donc P possède une racine complexe a .
 - Si $a \in \mathbb{R}$ alors $X - a \mid P$ et donc P est associé à $X - a$ puis c'est un polynôme de degré 1.
 - Si $a \in \mathbb{C} \setminus \mathbb{R}$ alors $a, \bar{a}$ sont racines distinctes de P puis $A = (X - a)(X - \bar{a})$ divise P dans le cadre des polynômes complexes. Ainsi il existe $B \in \mathbb{C}[X]$ tel que $P = AB$. Or $P \in \mathbb{R}[X]$ et $A = X^2 - 2\Re(a)X + |a|^2 \in \mathbb{R}[X]$ donc $\bar{P} = \bar{A}\bar{B}$ donne $P = A\bar{B}$. On en déduit $B = \bar{B}$ d'où $B \in \mathbb{R}[X]$. Ainsi A divise P dans le cadre des polynômes réels. Or P est irréductible, il est donc associé à A et apparaît comme étant un polynôme de degré 2 sans racines réelles.

Théorème 5

Soit $A \in \mathbb{K}[X]$ et P et Q deux polynômes irréductibles de $\mathbb{K}[X]$. Alors

1. $P \mid A$ ou $A \wedge P = 1$
2. P et Q sont associés ou $P \wedge Q = 1$

Théorème 6: Lemme d'Euclide

Soit $A, B \in \mathbb{K}[X]$. et P un polynôme irréductible de $\mathbb{K}[X]$. Alors

$$P \mid AB \Rightarrow P \mid A \text{ ou } P \mid B$$

Corollaire 6

Soient $A_1, \dots, A_n$ sont des polynômes et P un polynôme irréductible. Alors

$$P \mid \prod_{k=1}^n A_k \Rightarrow \exists i \in \llbracket 1, n \rrbracket, \quad P \mid A_i$$

Théorème 7

Soit A un polynôme non constant de $\mathbb{K}[X]$. $\exists \lambda \in \mathbb{K}^*, \exists n \in \mathbb{N}^*, \exists P_1, \dots, P_n$ polynômes irréductibles de $\mathbb{K}[X]$ unitaires et deux à deux distincts et $\exists \alpha_1, \dots, \alpha_n \in \mathbb{N}^*$. tels que :

$$A = \lambda \prod_{i=1}^n P_i^{\alpha_i}$$

De plus cette décomposition est unique à l'ordre près des facteurs, on l'appelle décomposition primaire de A .

Preuve:

On prouve d'abord l'existence puis l'unicité à l'ordre des facteurs près.

- **Existence:** Elle se fait par récurrence sur le degré de A .
 - Si $\deg A = 1$ alors P est irréductible. On pose $k = 1$, $\alpha_1 = 1$ et l'on prend pour P_1 le polynôme unitaire associé à P . Il est de degré 1 donc irréductible.
 - Soit $n \in \mathbb{N}^*$. Supposons maintenant que le théorème de décomposition soit valable pour tout polynôme de degré compris entre 1 et n . Soit A un polynôme de degré $n + 1$ et A_0 le polynôme unitaire associé à A . Le polynôme est unitaire et de degré $n + 1$. S'il est irréductible, alors $A = \lambda A_0$, où λ est le coefficient dominant de A , constitue une décomposition de A en facteurs premiers. Sinon, il existe un polynôme unitaire A_1 de degré compris entre 1 et n tel que $A_1 \mid A_0$. Soit $B_1 \in \mathbb{K}[X]$ tel que $A_0 = A_1 B_1$. B_1 est aussi unitaire de degré compris entre 1 et n . D'après l'hypothèse de récurrence A_1 et B_1 admettent chacun une décomposition en facteurs premiers :

$$A = \prod_{i=1}^r P_i^{\alpha_i} \text{ et } B_1 = \prod_{i=1}^{\ell} Q_i^{\beta_i}$$

Donc

$$A = \lambda \left(\prod_{i=1}^r P_i^{\alpha_i} \right) \left(\prod_{i=1}^{\ell} Q_i^{\beta_i} \right)$$

Il ne reste plus qu'à renuméroter les facteurs de la décomposition pour obtenir le résultat voulu.

► **Unicité:** Supposons que A admette deux décompositions en facteurs irréductibles :

$$A = \lambda \prod_{i=1}^r P_i^{\alpha_i} = \mu \prod_{i=1}^{\ell} Q_i^{\alpha_i}$$

Comme tous les facteurs irréductibles sont unitaires, λ et μ sont égaux au coefficient du terme dominant de A . Donc $\lambda = \mu$. De ce fait, on a

$$\prod_{i=1}^r P_i^{\alpha_i} = \prod_{i=1}^{\ell} Q_i^{\alpha_i}$$

Par ailleurs, P_1 divise le produit de droite, on déduit que P_1 divise au moins un des Q_j : il existe j_1 tel que Q_{j_1} et P_1 ne soient pas premiers entre eux. Comme par ailleurs Q_{j_1} et P_1 sont irréductibles et unitaires, cela signifie que $P_1 = Q_{j_1}$. En vertu du caractère intègre de $\mathbb{K}[X]$, on peut donc simplifier par P_1 .

On itère ce procédé et en $\alpha_1 + \dots + \alpha_k$ étapes, on parvient à une expression du type $1 = \prod_{j=1}^{\ell} Q_j^{\beta'_j}$ avec $\beta'_j = \beta_j - \alpha_j$. Cela permet de conclure que tous les β_j sont nuls. Donc les deux décompositions sont identiques à ordre près des facteurs.

Conséquence 6

Tout polynôme non constant de $\mathbb{C}[X]$ est scindé sur $\mathbb{C}$.

Preuve:

Sa décomposition en facteurs irréductibles est une décomposition en produit de facteurs du premier degré.

Remarque :

Ce résultat est faux dans $\mathbb{R}[X]$, exemple du polynôme $X^2 + 1$ à l'appui.

Conséquence 7

Tout polynôme P non constant de $\mathbb{R}[X]$ possède une unique décomposition, à l'ordre près, de la forme :

$$P = A \prod_{i=1}^r (X - \lambda_i)^{\alpha_i} \times \prod_{j=1}^s (X^2 + b_j X + c_j)^{\beta_j}$$

dans laquelle :

- A est le coefficient dominant de P ;
- $\lambda_1, \dots, \lambda_r$ est la suite des racines réelles distinctes de P et $\alpha_1, \dots, \alpha_r$ la suite des multiplicités associées
- les polynômes $X^2 + b_j X + c_j$ sont deux à deux distincts et irréductibles dans $\mathbb{R}[X]$ pour tout $j \in \llbracket 1, s \rrbracket$.

Exemple

Factorisons dans $\mathbb{R}[X]$ le polynôme $X^5 - 1$

Les racines complexe de $X^5 - 1$ sont $\omega_0, \omega_1, \dots, \omega_4$ avec $\omega_k = e^{i \frac{2k\pi}{5}}$.
 $\omega_0 = 1$ est réel, $\omega_4 = \overline{\omega_1}$ et $\omega_3 = \overline{\omega_2}$. Par suite

$$X^5 - 1 = (X - 1)[(X - \omega_1)(X - \overline{\omega_1})] \cdot [(X - \omega_2)(X - \overline{\omega_2})]$$

ce qui donne

$$X^5 - 1 = (X - 1) \left(X^2 - 2 \cos \frac{2\pi}{5} X + 1 \right) \left(X^2 - 2 \cos \frac{4\pi}{5} X + 1 \right).$$

Exemple

La décomposition de $X^4 + 16$ en produit de polynômes irréductibles dans $\mathbb{C}[X]$ est :

$$X^4 + 16 = \left(X - 2e^{-i \frac{\pi}{4}} \right) \left(X - 2e^{i \frac{\pi}{4}} \right) \left(X - 2e^{-i \frac{3\pi}{4}} \right) \left(X - 2e^{i \frac{3\pi}{4}} \right)$$

Pour la décomposition dans $\mathbb{R}[X]$: $X^4 + 16 = (X^2 - 2\sqrt{2}X + 4)(X^2 + 2\sqrt{2}X + 4)$

Propriété 34

Soient $A, B \in \mathbb{K}[X] \setminus \{0\}$. A et B peuvent s'écrire $A = a \prod_{i=1}^r P_i^{\alpha_i}$ et $B = b \prod_{i=1}^r P_i^{\beta_i}$ avec $r \in \mathbb{N}^*$, $\alpha_1, \dots, \alpha_r \in \mathbb{N}$, $\beta_1, \dots, \beta_r \in \mathbb{N}$ et $P_1, \dots, P_r$ sont irréductibles unitaires. Alors

1. Alors $A = B \Leftrightarrow a = b$ et $\forall i \in \llbracket 1, r \rrbracket : \alpha_i = \beta_i$.
2. $A \mid B$ si et seulement si $\forall i \in \llbracket 1, r \rrbracket, \alpha_i \leq \beta_i$.
3. $\text{pgcd}(A, B) = \prod_{i=1}^r P_i^{\min(\alpha_i, \beta_i)}$.
4. $\text{ppcm}(A, B) = \prod_{i=1}^r P_i^{\max(\alpha_i, \beta_i)}$.

Preuve:

$$2. \Leftarrow B = \frac{b}{a} \prod_{i=1}^r P_i^{\beta_i - \alpha_i} a \cdot \prod_{i=1}^r P_i^{\alpha_i} \text{ donc } B = AC \text{ avec } C \in \mathbb{K}[X].$$

$\Rightarrow$ Si $B = AC$ avec $C \in \mathbb{K}[X]$, alors $B = a \prod_{i=1}^r P_i^{\alpha_i} \times c \prod_{i=1}^r P_i^{\gamma_i} \times \text{autres polynômes irréductibles unitaires}$. Par unicité de l'écriture en produit d'irréductibles, $\beta_i = \alpha_i + \gamma_i \geq \alpha_i$.

$$3. \text{ En effet, soient } D = A \wedge B \text{ et } \Delta = \prod_{i=1}^r P_i^{\min(\alpha_i, \beta_i)}.$$

► Il est clair que $\Delta \mid A$ et $\Delta \mid B$ donc $\Delta \mid D$.

► Réciproquement, si P irréductible divise D , alors P divise $A = a \prod_{i=1}^r P_i^{\alpha_i}$ donc P divise l'un des P_i donc D va s'écrire

$$D = \prod_{i=1}^r P_i^{\delta_i} \text{ avec } \delta_1, \dots, \delta_r \in \mathbb{N}^*. \text{ Il n'y a pas d'autres irréductibles qui divisent } D \text{ que } P_1, \dots, P_r, D \mid A \text{ et } D \mid B \text{ donc } \delta_i \leq \min(\alpha_i, \beta_i) \text{ d'après la propriété précédente donc } D \mid \Delta.$$

V Algèbre**V.1 Algèbre****Définition 17: Algèbre**

Soit $\mathbb{K}$ un corps. On appelle $\mathbb{K}$ -algèbre tout ensemble A muni de deux lois de composition interne $+$, $\times$ et d'une loi de composition externe $\cdot$ sur $\mathbb{K} \times A$ à valeurs dans A , telles que

1. $(A, +, \cdot)$ est un $\mathbb{K}$ -espace vectoriel ;
2. $(A, +, \times)$ est un anneau ;
3. $\forall x, y \in A, \forall \alpha \in \mathbb{K}, \alpha.(x \times y) = (\alpha.x) \times y = x \times (\alpha.y)$

Une telle algèbre se note $(A, +, \times, \cdot)$.

Lorsque $\times$ est commutative, on parle d'algèbre commutative.

Exemple

- $(\mathbb{C}, +, \times, \cdot)$ est une $\mathbb{K}$ -algèbre commutative, avec $\mathbb{K}$ sous-corps de $\mathbb{C}$
- $(M_n(\mathbb{K}), +, \times, \cdot)$ est une $\mathbb{K}$ -algèbre
- $(\mathcal{F}(X, \mathbb{K}), +, \times, \cdot)$ est une $\mathbb{K}$ -algèbre. En particulier $(\mathbb{R}^{\mathbb{N}}, +, \times, \cdot)$ est une $\mathbb{R}$ -algèbre
- $(\mathcal{L}(E), +, \circ, \cdot)$ est une $\mathbb{K}$ -algèbre, où E est un $\mathbb{K}$ -espace vectoriel
- $\mathbb{K}^n$ est une $\mathbb{K}$ -algèbre si l'on définit la multiplication par :

$$(x_1, \dots, x_n) \times (y_1, \dots, y_n) = (x_1 y_1, \dots, x_n y_n)$$

V.2 Sous-algèbre

Définition 18: Sous-algèbre

Soit $(\mathbb{A}, +, \times, .)$ une $\mathbb{K}$ -algèbre et $\mathbb{B} \subset \mathbb{A}$. On dit $\mathbb{B}$ est une sous-algèbre de $(\mathbb{A}, +, \times, .)$ si :

1. $1_{\mathbb{A}} \in \mathbb{B}$
2. $\forall x, y \in \mathbb{B}, \forall \alpha, \beta \in \mathbb{K} \quad \alpha x + \beta y \in \mathbb{B}$
3. $\forall x, y \in \mathbb{B}, \quad x \times y \in \mathbb{B}$

Propriété 35

Une sous-algèbre d'une $\mathbb{K}$ -algèbre est une $\mathbb{K}$ -algèbre

Exemple: Commutants d'une matrice

Soit $n \geq 2$ et $A \in M_n(\mathbb{K})$ où $\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$. Montrons que

$$C_A = \{M \in M_n(\mathbb{K}) \mid AM = MA\}$$

muni de la somme, le produit et la multiplication par un scalaire usuels est $\mathbb{K}$ -algèbre.

- $I_n \in C_A$;
- Soit $M, N \in C_A$, $\alpha, \beta \in \mathbb{K}$, on a

$$A(\alpha M + \beta N) = \alpha AM + \beta AN = \alpha MA + \beta NA = (\alpha M + \beta N)A.$$

En outre

$$AMN = MAN = MNA.$$

Donc $\alpha M + \beta N$ et MN sont dans C_A . On en déduit que C_A est une sous-algèbre de $(M_n(\mathbb{K}), +, \times, .)$

V.3 Morphisme d'algèbres

Définition 19: Morphisme d'algèbres

Soit $(A, +, \times, .)$ et $(A', +, \times, .)$ deux $\mathbb{K}$ -algèbres. On dit $f : A \rightarrow A'$ est un morphisme d'algèbres si :

1. $f(1_A) = 1_{A'}$
2. $\forall x, y \in A, \forall \alpha, \beta \in \mathbb{K} \quad f(\alpha x + \beta y) = \alpha f(x) + \beta f(y)$
3. $\forall x, y \in A, \quad f(x \times y) = f(x) \times f(y)$

Remarque :

Un morphisme d'algèbres est à la fois une application linéaire et un morphisme d'anneaux

Vocabulaire :

1. Un isomorphisme d'algèbres est un morphisme d'algèbres bijectif.
2. Un automorphisme d'algèbres est un endomorphisme d'algèbres bijectif.
3. Deux $\mathbb{K}$ -algèbres sont dites isomorphes si, et seulement si, il existe un isomorphisme de l'une vers l'autre.

Exemple

Soit E un $\mathbb{K}$ -espace de dimension finie $n \geq 1$ et $\mathcal{B}$ une base de E . Alors l'application

$$\text{Mat}_{\mathcal{B}} : \begin{cases} \mathcal{L}(E) & \longrightarrow M_n(\mathbb{K}) \\ f & \longmapsto \text{Mat}_{\mathcal{B}}(f) \end{cases}$$

est un isomorphisme d'algèbres

- $\text{Mat}(\text{Id}_E) = I_n$;
- Pour tous $f, g \in \mathcal{L}(E)$, $\alpha, \beta \in \mathbb{K}$, on a :

$$\text{Mat}_{\mathcal{B}}(\alpha f + \beta g) = \alpha \text{Mat}_{\mathcal{B}}(f) + \beta \text{Mat}_{\mathcal{B}}(g) \quad \text{et} \quad \text{Mat}_{\mathcal{B}}(f \circ g) = \text{Mat}_{\mathcal{B}}(f) \times \text{Mat}_{\mathcal{B}}(g)$$

V.4 Idéal annulateur et polynôme minimal

Dans ce qui suit $\mathbb{A}$ désigne une $\mathbb{K}$ -algèbre (non nécessairement commutative) et $a \in \mathbb{A}$

Définition 20

Pour tout polynôme $P = \sum_{k=0}^n \alpha_k X^k \in \mathbb{K}[X]$, on pose $P(a) = \sum_{k=0}^n \alpha_k a^k \in \mathbb{A}$

Propriété 36

1. L'application

$$\varphi_a : \begin{cases} \mathbb{K}[X] & \longrightarrow \mathbb{A} \\ P & \longmapsto P(a) \end{cases}$$

est un morphisme de $\mathbb{K}$ -algèbres , appelé morphisme d'évaluation en a .

2. $\text{Im}(\varphi_a) = \{P(a) \mid P \in \mathbb{K}[X]\}$ est une sous-algèbre commutative de $\mathbb{A}$ contenant a notée $\mathbb{K}[a]$
3. $\mathbb{K}[a]$ est la plus petite sous-algèbre de $\mathbb{A}$ contenant a ; appelée la sous-algèbre engendrée par a .

Preuve:

Comme image de l'algèbre commutative $\mathbb{K}[X]$ par un morphisme d'algèbres, $\mathbb{K}[a]$ est une sous-algèbre commutative de $\mathbb{A}$. Elle contient évidemment a .

Toute sous-algèbre $\mathbb{B}$ de $\mathbb{A}$ contenant a , contiendra les combinaisons linéaires des puissances de a , c'est-à-dire les éléments $P(a)$ lorsque P appartient à $\mathbb{K}[X]$.

Définition 21

On appelle sous-algèbre monogène de $\mathbb{A}$ toute sous-algèbre de $\mathbb{A}$ de la forme $\mathbb{K}[a]$ avec $a \in \mathbb{A}$.

Définition 22

1. On appelle polynôme annulateur de a tout polynôme $P \in \mathbb{K}[X]$ tel que $P(a) = 0$.
2. On appelle idéal annulateur de a l'ensemble

$$I_a := \{P \in \mathbb{K}[X] , P(a) = 0\}$$

3. Si $I_a \neq \{0\}$, on appelle polynôme minimal de a le polynôme normalisé générateur I_a et on le note π_a

Remarque :

Si $I_a \neq \{0\}$, le polynôme minimal π_a de a est caractérisé par :

$$\forall P \in \mathbb{K}[X], P(a) = 0 \iff \pi_a \mid P$$

Exemple

Soit p un projecteur non trivial d'un espace vectoriel E , c'est-à-dire que l'on considère un endomorphisme p de E tel que

$$p^2 = p \quad \text{avec} \quad p \neq 0 \text{ et } p \neq \text{Id}_E$$

Alors le polynome minimal de p est $X^2 - X$

Propriété 37

Si $\mathbb{A}$ est de dimension finie, alors tout élément $a \in \mathbb{A}$ admet un polynôme minimal

Preuve:

φ_a n'est pas injectif

Propriété 38: Structure d'une sous-algèbre monogène

1. Si $I_a = \{0\}$, alors la sous-algèbre $\mathbb{K}[a]$ est de dimension infinie et φ_a réalise un isomorphisme d'algèbres de $\mathbb{K}[X]$ sur $\mathbb{K}[a]$.
2. Si $I_a \neq \{0\}$. On note p le degré de π_a . Alors la sous-algèbre $\mathbb{K}[a]$ est de dimension finie égale à $p = \deg \pi_a$ et la famille $(1, a, \dots, a^{p-1})$ une base de $\mathbb{K}[a]$.

Preuve:

1. Si $I_a = \{0\}$, l'application φ_a est un morphisme d'algèbres injectif de $\mathbb{K}[X]$ vers $\mathbb{A}$. Son image $\mathbb{K}[a]$ est donc de dimension infinie. La deuxième affirmation est évidente.
2. La division euclidienne nous fournit la somme directe :

$$\mathbb{K}[x] = \pi_a \mathbb{K}[x] \oplus \mathbb{K}_{p-1}[x].$$

L'application linéaire φ_a de noyau $\pi_a \mathbb{K}[X]$ induit alors un isomorphisme d'espaces vectoriels de $\mathbb{K}_{p-1}[X]$ sur $\mathbb{K}[a]$. Cet espace est donc de dimension p et l'image $(1, a, \dots, a^{p-1})$ de la base $(1, X, \dots, X^{p-1})$ de $\mathbb{K}_{p-1}[X]$ est une base de $\mathbb{K}[a]$.