

Anneaux, idéaux et $\mathbb{Z}/n\mathbb{Z}$

I. Anneaux : rappels et produit fini d'anneaux

Ce chapitre reprend l'arithmétique de première année avec un langage plus puissant. En effet, les notions d'idéal et d'anneau quotient $\mathbb{Z}/n\mathbb{Z}$ unifient l'étude de $\mathbb{Z}$ et celle de $\mathbb{K}[X]$. Dans tout le chapitre, les anneaux sont unitaires. Sauf mention contraire, ils sont aussi commutatifs.

Définition :

Un anneau $(A, +, \times)$ est un groupe commutatif $(A, +)$ muni d'une loi $\times$ associative, distributive par rapport à $+$ et possédant un élément neutre 1_A . Un morphisme d'anneaux $f : A \rightarrow B$ vérifie $f(a + b) = f(a) + f(b)$, $f(ab) = f(a)f(b)$ et $f(1_A) = 1_B$.

L'anneau A est intègre s'il est commutatif, non nul et sans diviseur de zéro :

$ab = 0 \Rightarrow a = 0$ ou $b = 0$. Un corps est un anneau commutatif non nul dont tout élément non nul est inversible.

On note $A^\times$ le groupe des inversibles de A . Ce groupe multiplicatif jouera un rôle central pour $\mathbb{Z}/n\mathbb{Z}$. Construisons maintenant de nouveaux anneaux à partir d'anneaux connus.

Définition :

Soit $A_1, \dots, A_r$ des anneaux. Le produit $A_1 \times \dots \times A_r$ est muni des lois composante par composante :

$$(a_1, \dots, a_r) + (b_1, \dots, b_r) = (a_1 + b_1, \dots, a_r + b_r), (a_1, \dots, a_r)(b_1, \dots, b_r) = (a_1 b_1, \dots, a_r b_r).$$

C'est un anneau de neutre multiplicatif $(1_{A_1}, \dots, 1_{A_r})$.

Propriété :

Les inversibles du produit sont les r -uplets d'inversibles :

$$(A_1 \times \dots \times A_r)^\times = A_1^\times \times \dots \times A_r^\times.$$

Démonstration :

Le produit $(a_i)(b_i)$ vaut $(1, \dots, 1)$ si et seulement si $a_i b_i = 1$ pour tout i . Autrement dit, (a_i) est inversible si et seulement si chaque a_i l'est, et l'inverse est (a_i^{-1}) .

Attention :

Un produit de deux anneaux non nuls n'est jamais intègre. Par exemple, dans $\mathbb{Z} \times \mathbb{Z}$, on a $(1, 0) \times (0, 1) = (0, 0)$ alors que les deux facteurs sont non nuls.

II. Idéaux d'un anneau commutatif

1. Définition et premiers exemples

Un idéal est une partie stable par addition et « absorbante » pour la multiplication. C'est la bonne notion pour parler de multiples et de noyaux.

Définition :

Soit A un anneau commutatif. Une partie I de A est un idéal de A si :

- I est un sous-groupe de $(A, +)$;
- pour tout $a \in A$ et tout $x \in I$, on a $ax \in I$ (propriété d'absorption).

Exemple :

Pour $a \in A$, l'ensemble $aA = \{ax, x \in A\}$ des multiples de a est un idéal. On l'appelle l'idéal engendré par a . C'est le plus petit idéal contenant a . Par exemple, $6\mathbb{Z}$ est l'idéal de $\mathbb{Z}$ engendré par 6. De même, $(X - 1)\mathbb{R}[X]$ est l'ensemble des polynômes réels qui s'annulent en 1.

Remarque :

Si un idéal I contient un inversible u , alors $1 = u^{-1}u \in I$, donc $I = A$. Par conséquent, les seuls idéaux d'un corps $\mathbb{K}$ sont $\{0\}$ et $\mathbb{K}$.

Proposition :

Le noyau d'un morphisme d'anneaux $f : A \rightarrow B$, avec A commutatif, est un idéal de A .

Démonstration :

D'abord, $\ker f$ est un sous-groupe de $(A, +)$, car f est un morphisme de groupes additifs. Ensuite, si $x \in \ker f$ et $a \in A$, alors $f(ax) = f(a)f(x) = f(a) \times 0 = 0$. Donc $ax \in \ker f$.

En revanche, l'image d'un morphisme n'est pas un idéal en général. C'est un sous-anneau. Ainsi, l'injection $\mathbb{Z} \rightarrow \mathbb{Q}$ a pour image $\mathbb{Z}$, qui n'est pas un idéal de $\mathbb{Q}$.

Proposition :

Si I et J sont des idéaux de A , alors $I \cap J$ et $I + J = \left\{ \begin{matrix} x \\ y, \\ x \in I, \\ y \in J \end{matrix} \right\}$ sont des idéaux de A . De plus, $I + J$ est le plus petit idéal contenant $I \cup J$.

Méthode :

Pour montrer qu'une partie I est un idéal, on dispose de deux voies.

- Vérifier directement : $0 \in I$, stabilité par différence, puis absorption par un élément quelconque de A .
- Reconnaître I comme le noyau d'un morphisme d'anneaux, par exemple d'un morphisme d'évaluation $P \rightarrow P(a)$.

Pour montrer qu'une partie n'est pas un idéal, un seul contre-exemple suffit. Souvent, on montre qu'elle contient 1 sans être égale à A .

2. Divisibilité dans un anneau intègre

Dans un anneau intègre A , on dit que a divise b s'il existe $c \in A$ tel que $b = ac$. Le lien avec les idéaux est immédiat.

Propriété :

Soit A intègre et $a, b \in A$. Alors a divise b si et seulement si $bA \subset aA$. De plus, $aA = bA$ si et seulement si a et b sont associés, c'est-à-dire s'il existe $u \in A^\times$ tel que $b = ua$.

Démonstration :

La première équivalence découle de la définition, car $bA \subset aA$ équivaut à $b \in aA$. Pour la seconde, supposons $aA = bA$. Il existe alors u, v tels que $b = ua$ et $a = vb$. Donc $a = vua$, soit $a(1 - vu) = 0$. Si $a = 0$, alors $b = 0$ et tout convient. Sinon, l'intégrité donne $vu = 1$, donc u est inversible. La réciproque est claire.

Ainsi, en passant aux idéaux, on oublie les inversibles. C'est pourquoi, dans $\mathbb{Z}$, on raisonne sur les entiers positifs, et dans $\mathbb{K}[X]$, sur les polynômes unitaires.

III. Idéaux de $\mathbb{Z}$ et PGCD

La division euclidienne permet de décrire tous les idéaux de $\mathbb{Z}$. C'est le premier exemple d'anneau principal.

Théorème :

Les idéaux de $\mathbb{Z}$ sont exactement les $n\mathbb{Z}$, avec $n \in \mathbb{N}$. L'entier n est unique.

Démonstration :

Soit I un idéal de $\mathbb{Z}$. Si $I = \{0\}$, alors $I = 0\mathbb{Z}$. Sinon, I contient un entier strictement positif, car il est stable par passage à l'opposé. Soit n le plus petit d'entre eux. D'abord, $n\mathbb{Z} \subset I$ par absorption. Ensuite, pour $a \in I$, on écrit $a = nq + r$ avec $0 \leq r < n$. Alors $r = a - nq \in I$, et la minimalité de n impose $r = 0$. Donc $I = n\mathbb{Z}$.

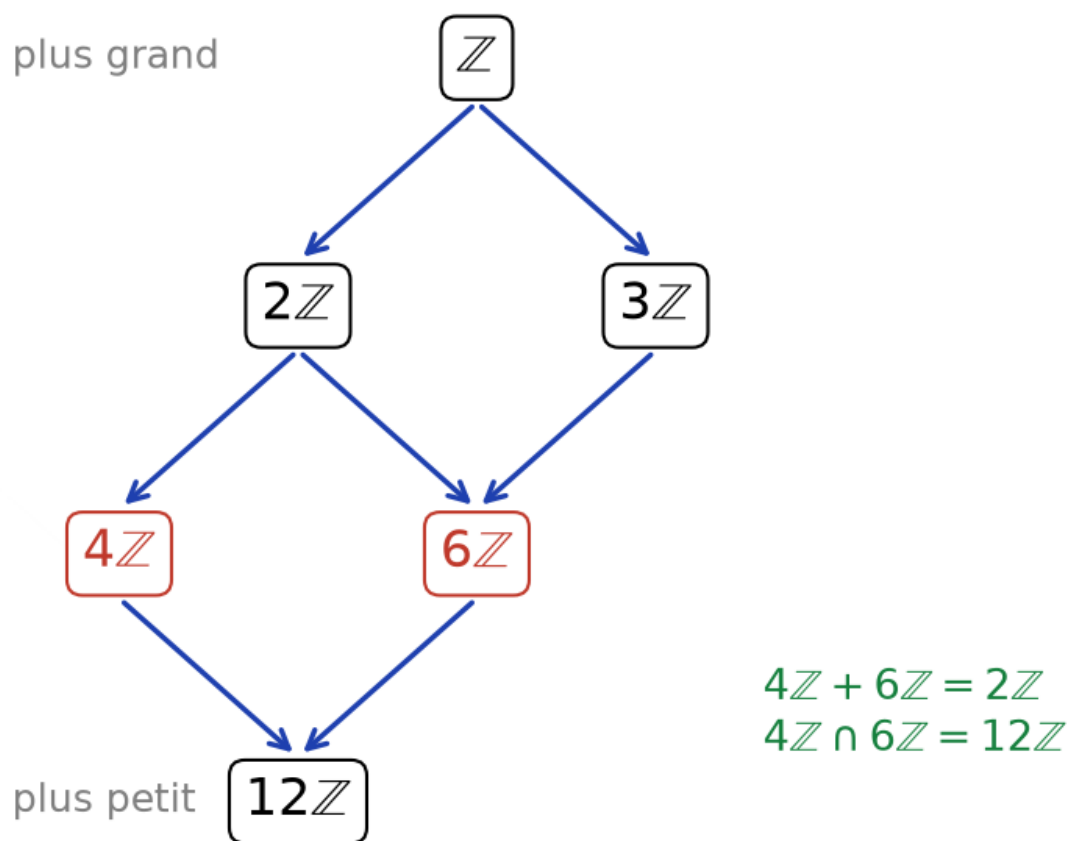
Ce théorème donne une définition élégante du PGCD et du PPCM. En effet, $a\mathbb{Z} + b\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z}$ sont des idéaux. Ils s'écrivent donc $d\mathbb{Z}$ et $m\mathbb{Z}$.

Théorème :

Pour $a, b \in \mathbb{Z}$, on a $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$. En particulier, il existe $u, v \in \mathbb{Z}$ tels que $au + bv = a \wedge b$ (relation de Bézout).

Plus généralement, $a_1\mathbb{Z} + \dots + a_r\mathbb{Z} = (a_1 \wedge \dots \wedge a_r)\mathbb{Z}$.

Ainsi, l'inclusion des idéaux renverse la divisibilité : plus l'entier est grand pour la divisibilité, plus son idéal est petit. La figure ci-dessous montre les idéaux de $\mathbb{Z}$ qui contiennent $12\mathbb{Z}$. Une flèche descend de $d\mathbb{Z}$ vers $m\mathbb{Z}$ quand $m\mathbb{Z} \subset d\mathbb{Z}$.



Exemple :

On a $4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$ et $4\mathbb{Z} \cap 6\mathbb{Z} = 12\mathbb{Z}$. Sur la figure, $2\mathbb{Z}$ est le plus petit idéal au-dessus de $4\mathbb{Z}$ et $6\mathbb{Z}$. De même, $12\mathbb{Z}$ est le plus grand en dessous des deux.

IV. L'anneau $\mathbb{Z}/n\mathbb{Z}$

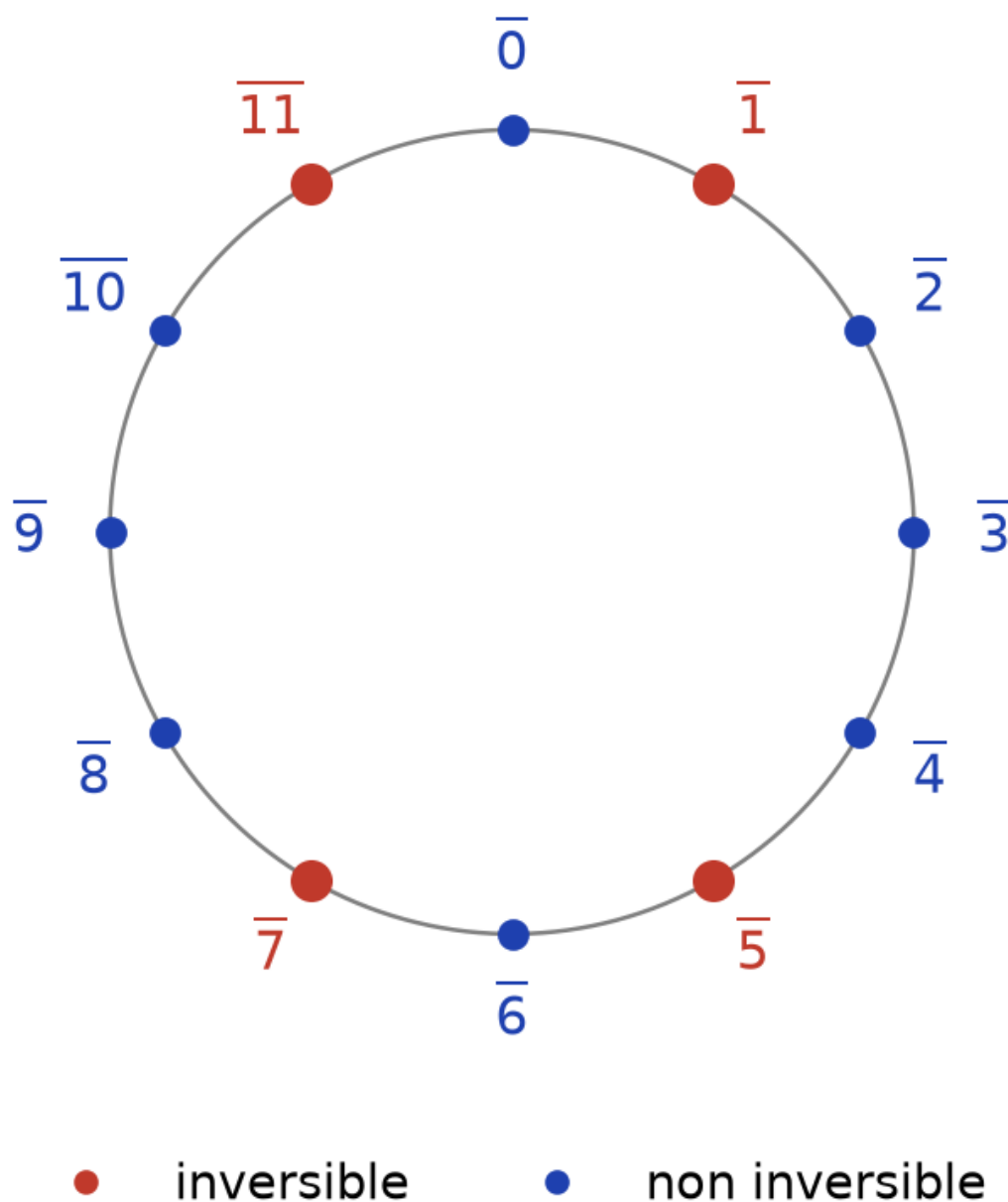
1. Structure d'anneau

Soit $n \geq 1$. La congruence modulo n est compatible avec l'addition et la multiplication. Par conséquent, les lois de $\mathbb{Z}$ passent aux classes.

Définition :

On note $\bar{k}$ la classe de k modulo n . L'ensemble $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$, muni de $\bar{a} + \bar{b} = \overline{a+b}$ et $\bar{a} \times \bar{b} = \overline{ab}$, est un anneau commutatif à n éléments. La surjection canonique $k \rightarrow \bar{k}$ est un morphisme d'anneaux de noyau $n\mathbb{Z}$.

On visualise $\mathbb{Z}/n\mathbb{Z}$ comme une horloge à n graduations. La figure ci-dessous représente $\mathbb{Z}/12\mathbb{Z}$; les classes inversibles y sont marquées en rouge.



2. Éléments inversibles

Théorème :

La classe $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $k \wedge n = 1$. Dans le cas contraire, $\overline{k}$ est nul ou diviseur de zéro.

Démonstration :

D'abord, $\bar{k}$ est inversible si et seulement s'il existe u tel que $ku \equiv 1 \pmod{n}$. Autrement dit, il existe u, v tels que $ku + nv = 1$. D'après le théorème de Bézout, cela équivaut à $k \wedge n = 1$. Ensuite, si $d = k \wedge n > 1$, on pose $m = n/d$. Alors $0 < m < n$, donc $\bar{m} \neq \bar{0}$, et $km = (k/d)n$, donc $\bar{k}\bar{m} = \bar{0}$.

Méthode :

Pour calculer l'inverse de $\bar{k}$ modulo n , on applique l'algorithme d'Euclide étendu à k et n . On obtient $ku + nv = 1$, et l'inverse est $\bar{u}$. Pour de petites valeurs, un essai direct des multiples de k suffit souvent.

Exemple :

Cherchons l'inverse de 11 modulo 26. Les divisions successives donnent $26 = 2 \times 11 + 4$, puis $11 = 2 \times 4 + 3$, puis $4 = 1 \times 3 + 1$. En remontant :

$$1 = 4 - 3 = 4 - (11 - 2 \times 4) = 3 \times 4 - 11 = 3 \times 26 - 7 \times 11.$$

Donc l'inverse de $\bar{11}$ est $\overline{-7} = \bar{19}$. On vérifie : $11 \times 19 = 209 = 8 \times 26 + 1$.

3. Le corps F_p

Théorème :

Pour $n \geq 2$, les assertions suivantes sont équivalentes : $\mathbb{Z}/n\mathbb{Z}$ est un corps ; $\mathbb{Z}/n\mathbb{Z}$ est intègre ; n est premier. Lorsque p est premier, on note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Démonstration :

Un corps est intègre. Si $n = ab$ avec $1 < a, b < n$, alors $\bar{a}\bar{b} = \bar{0}$ avec $\bar{a}, \bar{b}$ non nuls : l'anneau n'est pas intègre. Enfin, si n est premier, tout k non multiple de n est premier avec n , donc $\bar{k}$ est inversible.

Dans le corps $\mathbb{F}_p$, on peut diviser et utiliser toute l'algèbre linéaire. De plus, un polynôme de degré d à coefficients dans $\mathbb{F}_p$ a au plus d racines. Par exemple, l'équation $x^2 = \bar{1}$ n'a que les solutions $\pm \bar{1}$ dans $\mathbb{F}_p$.

V. Théorème chinois et indicatrice d'Euler

1. Le théorème chinois

Théorème :

Soit $m, n \geq 1$ premiers entre eux. L'application

$$\psi : \mathbb{Z}/mn\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, k \bmod mn \rightarrow (k \bmod m, k \bmod n)$$

est bien définie, et c'est un isomorphisme d'anneaux.

Démonstration :

Si $k \equiv k' \pmod{mn}$, alors $k \equiv k'$ modulo m et modulo n : ψ est bien définie. C'est clairement un morphisme d'anneaux. Ensuite, si $\psi(\bar{k}) = 0$, alors m et n divisent k . Comme $m \wedge n = 1$, leur produit mn divise k . Donc ψ est injective. Enfin, les deux ensembles ont mn éléments, donc ψ est bijective.

La figure ci-dessous illustre le cas $m = 3$, $n = 5$. Chaque entier k de 0 à 14 est placé dans la case $(k \bmod 3, k \bmod 5)$. Chaque case reçoit exactement un entier : c'est la bijectivité de ψ .

		reste modulo 5				
		0	1	2	3	4
reste modulo 3	0	0	6	12	3	9
	1	10	1	7	13	4
	2	5	11	2	8	14

Méthode :

Pour résoudre $x \equiv a \pmod{m}$ et $x \equiv b \pmod{n}$ avec $m \wedge n = 1$:

- on écrit une relation de Bézout $mu + nv = 1$;
- on pose $x_0 = a nv + b mu$; en effet, $nv \equiv 1 \pmod{m}$ et $mu \equiv 1 \pmod{n}$;
- les solutions sont exactement les $x_0 + kmn$, $k \in \mathbb{Z}$.

Pour trois congruences ou plus, on combine les deux premières, puis on recommence.

Exemple :

Réolvons $x \equiv 1 \pmod{4}$ et $x \equiv 3 \pmod{5}$. On a $4 \times (-1) + 5 \times 1 = 1$. Ainsi, $x_0 = 1 \times 5 + 3 \times (-4) = -7$. Les solutions sont donc les $x \equiv 13 \pmod{20}$. Vérification : $13 = 3 \times 4 + 1$ et $13 = 2 \times 5 + 3$.

Attention :

Si m et n ne sont pas premiers entre eux, le système peut n'avoir aucune solution. Il en a si et seulement si $a \equiv b \pmod{\gcd(m, n)}$. Dans ce cas, les solutions forment une classe modulo $m \vee n$.

2. Indicatrice d'Euler

Définition :

Pour $n \geq 1$, on note $\varphi(n)$ le nombre d'entiers $k \in \llbracket 1, n \rrbracket$ premiers avec n . D'après la partie IV, $\varphi(n)$ est le cardinal du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$.

Théorème :

- Si p est premier et $k \geq 1$, alors $\varphi(p^k) = p^k - p^{k-1}$.
- Si $m \wedge n = 1$, alors $\varphi(mn) = \varphi(m) \varphi(n)$.
- Par conséquent, si $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, alors $\varphi(n) = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right)$.

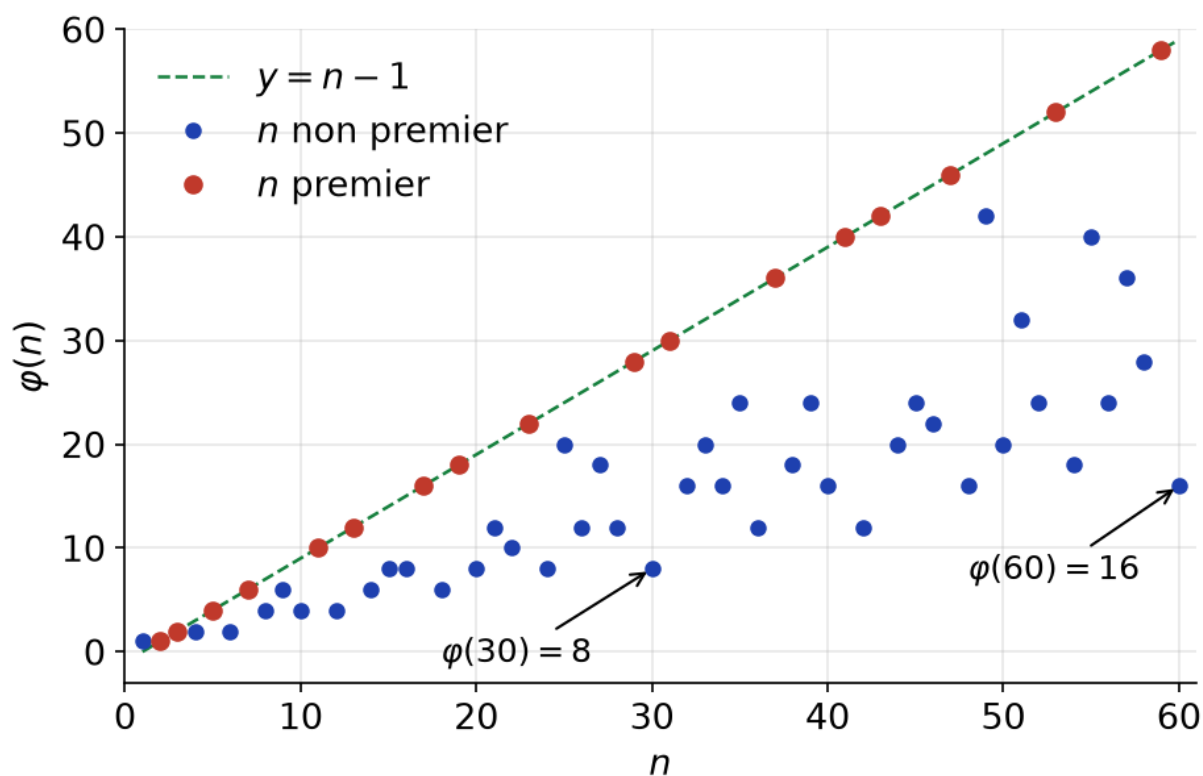
Démonstration :

D'abord, un entier est premier avec p^k si et seulement s'il n'est pas multiple de p . Or il y a $p^k - 1$ multiples de p dans $[[1, p^k]]$. Ensuite, l'isomorphisme chinois ψ envoie les inversibles sur les inversibles. Avec la propriété du produit d'anneaux, $(\mathbb{Z}/mn\mathbb{Z})^\times$ est en bijection avec $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. Enfin, la formule générale s'obtient par récurrence sur r .

Exemple :

Comme $84 = 2^2 \times 3 \times 7$, on obtient $\varphi(84) = 2 \times 2 \times 6 = 24$. De même, $\varphi(100) = 100 \times \frac{1}{2} \times \frac{4}{5} = 40$.

La figure ci-dessous représente $\varphi(n)$ pour n de 1 à 60. Les points des nombres premiers sont sur la droite $y = n - 1$, qui est le maximum possible. En revanche, les nombres très composés, comme 30 ou 60, ont une indicatrice nettement plus faible.



3. Théorème d'Euler

Théorème :

Soit $n \geq 2$ et a un entier premier avec n . Alors $a^{\varphi(n)} \equiv 1 \pmod{n}$. En particulier, si p est premier et ne divise pas a , alors $a^{p-1} \equiv 1 \pmod{p}$ (petit théorème de Fermat).

Démonstration :

Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est commutatif et de cardinal $\varphi(n)$. D'après le théorème de Lagrange, l'ordre de $\bar{a}$ divise $\varphi(n)$. Donc $\bar{a}^{\varphi(n)} = \bar{1}$.

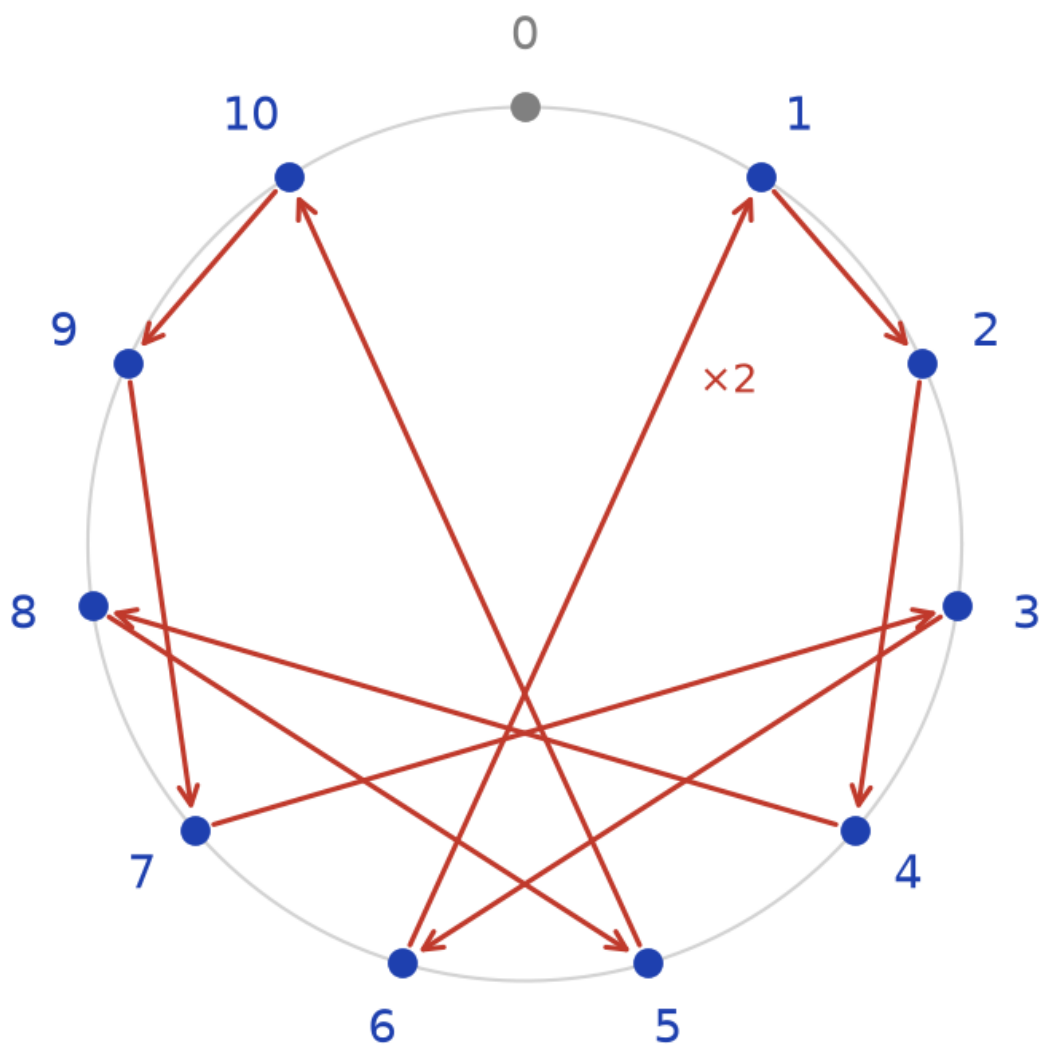
Méthode :

Pour calculer $a^N \bmod n$ avec $a \wedge n = 1$, on divise N par $\varphi(n)$: $N = q\varphi(n) + r$. Alors $a^N \equiv a^r \pmod{n}$. Mieux encore, si l'on connaît l'ordre ω de $\bar{a}$, il suffit de réduire N modulo ω .

Exemple :

Calculons $2^{2026} \bmod 11$. Comme 11 est premier, $2^{10} \equiv 1 \pmod{11}$. Or $2026 = 202 \times 10 + 6$. Donc $2^{2026} \equiv 2^6 = 64 \equiv 9 \pmod{11}$.

La figure ci-dessous suit les puissances successives de 2 modulo 11. Elles parcourent les dix classes non nulles avant de revenir à 1 : la classe de 2 est d'ordre 10, qui est bien $\varphi(11)$.



$$1 \rightarrow 2 \rightarrow 4 \rightarrow 8 \rightarrow 5 \rightarrow 10 \rightarrow 9 \rightarrow 7 \rightarrow 3 \rightarrow 6 \rightarrow 1$$

VI. Idéaux de $K[X]$ et décomposition en irréductibles

Dans cette partie, $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$, ou plus généralement un corps. La division euclidienne des polynômes joue le rôle de celle des entiers.

Théorème :

Tout idéal non nul I de $\mathbb{K}[X]$ s'écrit $I = P \mathbb{K}[X]$ pour un unique polynôme unitaire P .

Démonstration :

Soit P un polynôme non nul de I de degré minimal, qu'on peut rendre unitaire en le multipliant par une constante. Par absorption, $P \mathbb{K}[X] \subset I$. Soit $A \in I$; on écrit $A = PQ + R$ avec $\deg R < \deg P$. Alors $R = A - PQ \in I$, donc $R = 0$ par minimalité. Pour l'unicité, deux générateurs unitaires sont associés, donc égaux, car les inversibles de $\mathbb{K}[X]$ sont les constantes non nulles.

Théorème :

Soit $A, B \in \mathbb{K}[X]$ non tous deux nuls. Le PGCD $D = A \wedge B$ est l'unique polynôme unitaire tel que $A \mathbb{K}[X] + B \mathbb{K}[X] = D \mathbb{K}[X]$. En particulier, il existe U, V tels que $AU + BV = D$.

De plus, tout polynôme non constant se décompose en produit d'une constante et de polynômes irréductibles unitaires, de façon unique à l'ordre près. Sur $\mathbb{C}$, les irréductibles sont les polynômes de degré 1. Sur $\mathbb{R}$, ce sont ceux de degré 1 et ceux de degré 2 à discriminant strictement négatif.

Exemple :

On a $X^4 - 1 = (X - 1)(X + 1)(X^2 + 1)$ dans $\mathbb{R}[X]$, et $X^4 - 1 = (X - 1)(X + 1)(X - i)(X + i)$ dans $\mathbb{C}[X]$. Par ailleurs, $X^4 - 1 = X(X^3 - 1) + (X - 1)$ et $X - 1$ divise $X^3 - 1$. Donc $(X^4 - 1) \wedge (X^3 - 1) = X - 1$.

Méthode :

L'ensemble $I_a = \left\{ P \in \mathbb{K}[X], P(a) = 0 \right\}$ est le noyau du morphisme d'évaluation $P \rightarrow P(a)$.

C'est donc un idéal, et ici $I_a = (X - a) \mathbb{K}[X]$. Pour déterminer un idéal de $\mathbb{K}[X]$, on cherche un polynôme de degré minimal qu'il contient, puis on vérifie qu'il divise tous les autres.

VII. Algèbres, sous-algèbres et morphismes d'algèbres

Beaucoup d'anneaux étudiés en spé sont aussi des espaces vectoriels. La notion d'algèbre combine ces deux structures.

Définition :

Une $\mathbb{K}$ -algèbre est un ensemble A muni de deux lois internes $+$ et $\times$ et d'une loi externe $\cdot$ telles que $(A, +, \times)$ est un anneau, $(A, +, \cdot)$ est un $\mathbb{K}$ -espace vectoriel, et, pour tous $\lambda \in \mathbb{K}$ et $a, b \in A$:

$$(\lambda \cdot a) \times b = a \times (\lambda \cdot b) = \lambda \cdot (a \times b).$$

Exemple :

Les ensembles $\mathbb{K}[X]$, $\mathcal{M}_n(\mathbb{K})$, $\mathcal{L}(E)$ et $\mathcal{F}(X, \mathbb{K})$ sont des $\mathbb{K}$ -algèbres. Seules $\mathcal{M}_n(\mathbb{K})$ et $\mathcal{L}(E)$, pour $n \geq 2$ ou $\dim E \geq 2$, ne sont pas commutatives.

Définition :

Une sous-algèbre de A est une partie B qui contient 1_A et qui est stable par combinaison linéaire et par produit. Un morphisme d'algèbres $f : A \rightarrow A'$ est une application linéaire qui est aussi un morphisme d'anneaux : $f(ab) = f(a)f(b)$ et $f(1_A) = 1_{A'}$.

Méthode :

Pour montrer que B est une sous-algèbre de A , on vérifie trois points : $1_A \in B$, B est un sous-espace vectoriel, et $ab \in B$ pour tous $a, b \in B$. Une autre voie consiste à écrire B comme l'image d'un morphisme d'algèbres.

Proposition :

Soit A une $\mathbb{K}$ -algèbre et $a \in A$. L'application $\text{ev}_a : \mathbb{K}[X] \rightarrow A$, $P \rightarrow P(a)$, est un morphisme d'algèbres. Son image $\mathbb{K}[a]$ est une sous-algèbre commutative de A . Son noyau est un idéal de $\mathbb{K}[X]$, formé des polynômes annulateurs de a .

Exemple :

Soit $\mathcal{C} = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, a, b \in \mathbb{R} \right\}$. C'est l'image de $\text{ev}_J : \mathbb{R}[X] \rightarrow \mathcal{M}_2(\mathbb{R})$, avec $J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. En effet, $J^2 = -I_2$, donc $X^2 + 1$ annule J . Écrivons la division euclidienne $P = (X^2 + 1)Q + a + bX$. On obtient alors $P(J) = aI_2 + bJ$. Ainsi, $\mathcal{C}$ est une sous-algèbre de $\mathcal{M}_2(\mathbb{R})$. De plus, $a + ib \rightarrow aI_2 + bJ$ est un isomorphisme d'algèbres de $\mathbb{C}$ sur $\mathcal{C}$.

Ce qu'il faut retenir

- Un idéal est un sous-groupe additif absorbant ; le noyau d'un morphisme d'anneaux en est un.
- Dans un anneau intègre, a divise b si et seulement si $bA \subset aA$, et $aA = bA$ si et seulement si a et b sont associés.
- Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$; $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$.
- $\bar{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $k \wedge n = 1$; l'inverse se calcule par l'algorithme d'Euclide étendu.
- $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.
- Théorème chinois : si $m \wedge n = 1$, $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
- φ est multiplicative et $\varphi(n) = n \prod (1 - 1/p)$ sur les premiers p divisant n .
- Théorème d'Euler : $a^{\varphi(n)} \equiv 1 \pmod{n}$ si $a \wedge n = 1$.
- Tout idéal non nul de $\mathbb{K}[X]$ est engendré par un unique polynôme unitaire.
- Une sous-algèbre contient 1 et est stable par combinaison linéaire et produit ; $P \rightarrow P(a)$ est un morphisme d'algèbres.

Questions fréquentes sur anneaux, idéaux et $\mathbb{Z}/n\mathbb{Z}$

Quelle différence entre un idéal et un sous-anneau ?

Un sous-anneau contient 1 et est stable par produit de deux de ses éléments. Un idéal absorbe les produits par n'importe quel élément de l'anneau. Un idéal qui contient 1 est l'anneau entier : sauf ce cas, un idéal n'est jamais un sous-anneau. Le noyau d'un morphisme est un idéal, son image un sous-anneau.

Comment trouver rapidement l'inverse de k modulo n ?

Il faut d'abord vérifier que $k \wedge n = 1$, sinon l'inverse n'existe pas. On applique ensuite l'algorithme d'Euclide étendu pour obtenir $ku + nv = 1$; l'inverse est la classe de u . Pour de petites valeurs, tester les multiples de k suffit, et on vérifie toujours par une multiplication.

Quand peut-on appliquer le théorème chinois ?

La forme du cours exige des modules premiers entre eux deux à deux : $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ si $m \wedge n = 1$. Si les modules ne sont pas premiers entre eux, le système $x \equiv a \pmod{m}$, $x \equiv b \pmod{n}$ a des solutions seulement si $a \equiv b \pmod{m \wedge n}$. Les solutions forment alors une classe modulo le PPCM.

Le théorème d'Euler donne-t-il le plus petit exposant qui annule ?

Non. Il affirme que $a^{\varphi(n)} \equiv 1 \pmod{n}$ si $a \wedge n = 1$, mais l'ordre de a peut être un diviseur strict de $\varphi(n)$. Par exemple, $7^4 \equiv 1 \pmod{100}$ alors que $\varphi(100) = 40$. Dans les calculs, chercher d'abord une petite puissance égale à 1 fait gagner du temps.

Pour aller plus loin en maths spé

- Les énoncés : [exercices de maths spé sur anneaux, idéaux et \$\mathbb{Z}/n\mathbb{Z}\$](#)
- À maîtriser avant : [Compléments sur les groupes : groupes monogènes et ordre](#)
- Chapitre précédent : [Compléments sur les groupes : groupes monogènes et ordre](#)
- Chapitre suivant : [Éléments propres et polynôme caractéristique](#)
- Tester vos connaissances : [QCM de maths spé par chapitre](#)
- Le sommaire : [tous les chapitres de maths spé](#) et les [chapitres de maths sup](#)