L'arithmétique ailleurs que sur $\mathbb{Z}$

[STA] Structures Algébriques

9 octobre 2025

EPITA

Introduction

Objectifs de la vidéo

- Comprendre la **motivation** qui conduit à formaliser la notion d'anneau.
- Identifier le rôle des **axiomes** dans la généralisation des opérations arithmétiques.
- Distinguer les principaux **types d'anneaux** : commutatifs, intègres, factoriels, euclidiens et corps.

Pourquoi formaliser les opérations arithmétiques ?

- En arithmétique, on manipule des opérations familières : addition, soustraction, multiplication, division.
- L'objectif est de **repérer quelles propriétés** sont indispensables pour que ces opérations soient valides et généralisables.
- Cette démarche conduit à la **notion d'anneau**, qui capture le comportement commun des opérations arithmétiques dans des contextes très différents.

Qu'est-ce que faire de l'arithmétique ?

Qu'est-ce que faire de l'arithmétique ?

Réponse à chaud

Faire de l'arithmétique c'est étudier les relations de divisibilité entre entiers.

C'est quoi la division déjà ?

Définition (Division sur $\mathbb{Z}$)

Un élément $b \in \mathbb{Z}^*$ divise un entier $a \in \mathbb{Z}$ s'il existe un entier $q \in \mathbb{Z}$ tel que $a = bq$. On note alors $q = \frac{a}{b}$.

C'est quoi la division déjà ?

Définition (Division sur $\mathbb{Z}$)

Un élément $b \in \mathbb{Z}^*$ divise un entier $a \in \mathbb{Z}$ s'il existe un entier $q \in \mathbb{Z}$ tel que $a = bq$. On note alors $q = \frac{a}{b}$.

Donc b ***ne divise pas*** a si $\forall q \in \mathbb{Z},\ a \neq bq$.

C'est quoi la division déjà ?

Définition (Division sur $\mathbb{Z}$)

Un élément $b \in \mathbb{Z}^*$ divise un entier $a \in \mathbb{Z}$ s'il existe un entier $q \in \mathbb{Z}$ tel que $a = bq$. On note alors $q = \frac{a}{b}$.

Donc b ***ne divise pas*** a si $\forall q \in \mathbb{Z},\ a \neq aq$.

En ce cas, on indroduit la notion de ***reste*** et on dit que $a = bq + r$.

%

$0 \leq r < b$

C'est quoi la division déjà ?

Définition (Division sur $\mathbb{Z}$)

Un élément $b \in \mathbb{Z}^*$ divise un entier $a \in \mathbb{Z}$ s'il existe un entier $q \in \mathbb{Z}$ tel que $a = bq$. On note alors $q = \frac{a}{b}$.

Donc b ***ne divise pas*** a si $\forall q \in \mathbb{Z}$, $a \neq aq$.

En ce cas, on indroduit la notion de ***reste*** et on dit que $a = bq + r$.

L'intérêt (notamment en cryptographie) c'est d'avoir des éléments divisibles et d'autres non.

De quoi a-t-on besoin pour parler de divisibilité ?

Étant donné un ensemble A, pour espérer faire de l'arithmétique sur A, il va nous falloir :

De quoi a-t-on besoin pour parler de divisibilité ?

Étant donné un ensemble A, pour espérer faire de l'arithmétique sur A, il va nous falloir :

- Une opération $+$ (addition)

De quoi a-t-on besoin pour parler de divisibilité ?

Étant donné un ensemble A, pour espérer faire de l'arithmétique sur A, il va nous falloir :

- Une opération $+$ (addition)
- Une opération $\cdot$ (multiplication)

De quoi a-t-on besoin pour parler de divisibilité ?

Étant donné un ensemble A, pour espérer faire de l'arithmétique sur A, il va nous falloir :

- Une opération $+$ (addition)
- Une opération $\cdot$ (multiplication)
- Que ces opérations soient ***compatibles***, c'est à dire : $\forall a, b, c \in A$,

$$a \cdot (b + c) = a \cdot b + a \cdot c\,.$$

De quoi a-t-on besoin pour parler de divisibilité ?

Étant donné un ensemble A, pour espérer faire de l'arithmétique sur A, il va nous falloir :

- Une opération $+$ (addition)
- Une opération $\cdot$ (multiplication) $\times$
- Que ces opérations soient ***compatibles***, c'est à dire : $\forall a, b, c \in A$,

$$a \cdot (b + c) = a \cdot b + a \cdot c\,.$$

Question

Est-ce tout ce qu'il faudrait ?

La notion d’anneau

Définition d'un anneau

Définition (Anneau)

Un **anneau** [a] est un triplet $(A, +, \cdot)$ où A est un ensemble et $+$ et $\cdot$ sont deux opérations binaires internes, c'est à dire deux fonctions

$$+ : A \times A \to A \qquad \cdot : A \times A \to A$$

qui vérifient les propriétés suivantes :
Pour l'addition :

- $\forall a, b, c \in A,\ (a + b) + c = a + (b + c)$ (associativité de $+$)
- $\exists 0 \in A,\ \forall a \in A,\ a + 0 = a = 0 + a$ (existence d'élément neutre pour $+$)
- $\forall a \in A,\ \exists (-a) \in A,\ a + (-a) = 0$ (existence d'élément opposé pour $+$)
- $\forall a, b \in A,\ a + b = b + a$ (commutativité)

a. On utilisera anneau pour ***anneau unitaire***.

Définition d'un anneau

Définition (Anneau)

Un **anneau** [a] est un triplet $(A, +, \cdot)$ où A est un ensemble et $+$ et $\cdot$ sont deux opérations binaires internes, c'est à dire deux fonctions

$$+ : A \times A \to A \qquad \cdot : A \times A \to A$$

qui vérifient les propriétés suivantes :
Pour la multiplication :

- $\forall a, b, c \in A,\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (associativité de $\cdot$)
- $\exists 1 \in A,\ \forall a \in A,\ a \cdot 1 = a = 1 \cdot a$ (existence d'élément neutre pour $\cdot$)

a. On utilisera anneau pour ***anneau unitaire***.

Définition d'un anneau

Définition (Anneau)

Un **anneau** [a] est un triplet $(A, +, \cdot)$ où A est un ensemble et $+$ et $\cdot$ sont deux opérations binaires internes, c'est à dire deux fonctions

$$+ : A \times A \to A \qquad \cdot : A \times A \to A$$

qui vérifient les propriétés suivantes :
Pour la compatibilité :

- $\forall a, b, c \in A,\ a \cdot (b + c) = a \cdot b + a \cdot c$ (distributivité à droite)
- $\forall a, b, c \in A,\ (a + b) \cdot c = a \cdot c + b \cdot c$ (distributivité à gauche)

Il est **commutatif** si $\forall a, b \in A,\ a \cdot b = b \cdot a$.

a. On utilisera anneau pour ***anneau unitaire***.

Exemples !

Exemples et contre-exemples

Premiers exemples d'anneaux

$+, \times$

$a+ib$

$\frac{a-ib}{a^2+b^2}$

$(a+ib)(a-ib) = a^2 - (ib)^2 = a^2 - (-1)b^2 = a^2 + b^2$

1. Les ensembles usuels $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$.
2. Les suites et fonctions numériques, les polynômes,
3. Les ensembles de matrices $\mathcal{M}_n(\mathbb{R})$.

$u_n + v_n$ $\quad u_n v_n$

$f + g$ $\quad f \times g$

$A \times B$

$A + B$

Exemples et contre-exemples

Premiers exemples d'anneaux

1. Les ensembles usuels $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$.
2. Les suites et fonctions numériques, les polynômes,
3. Les ensembles de matrices $\mathcal{M}_n(\mathbb{R})$.

Des choses qui n'en sont pas (**pourquoi ?**)

1. L'ensemble des entiers naturels $\mathbb{N}$. → pas d'opposé pour $+$
2. Les fonctions intégrables sur $]0, 1]$.
3. L'ensemble des matrices inversibles. →

$f(x) = \frac{1}{x^{3/4}}$

$\int_0^1 \frac{dx}{x^{3/4}} = \left[4x^{1/4}\right]_0^1 = 4 < \infty$

$\int_0^1 f^2 = \int_0^1 \frac{dx}{x^{3/2}} = \left[-2x^{-1/2}\right]_0^1 = \infty$

A inv $\Rightarrow -A$ inv

$A + (-A) = 0$ pas inv.

$(\mathbb{N}, \max, +)$ ✓ $(\max(a,b), c) = \max(a, \max(b,c))$

élt neutre 0 pour max , 0

$a + \max(b,c) = \max(a+b, a+c)$

Les anneaux intègres

$ab = 0 \rightarrow a = 0 \quad b = 0$

Anneaux intègres

Définition (Anneau intègre)

Un anneau $(A, +, \cdot)$ est dit ***intègre*** s'il est commutatif et si

$$\forall a, b \in A,\ a \cdot b = 0 \Rightarrow a = 0 \text{ ou } b = 0\,.$$

$x+y$

$x = \{x + nq : q \in \mathbb{Z}\}$ $x+y = \{x+y+kn : k \in \mathbb{Z}\}$

$y = \{y + np : p \in \mathbb{Z}\}$

Définition (Anneau intègre)

Un anneau $(A, +, \cdot)$ est dit ***intègre*** s'il est commutatif et si

$x \times y = \{xy + kn . n \in \mathbb{Z}\}$ $(x+nq)(y+np) = xy + nqy + npx + n^2pq$

$$\forall a, b \in A,\ a \cdot b = 0 \Rightarrow a = 0 \text{ ou } b = 0\,.$$

Dans un anneau A les éléments $a \neq 0$ pour lesquels il existe $b \neq 0$ tels que $a \cdot b = 0$ sont dits être des ***diviseurs de*** 0. Un anneau est donc intègre s'il est commutatif et sans diviseurs de 0.

Question

À quelles conditions sur n est-ce que $\mathbb{Z}/n\mathbb{Z}$ est intègre ?

0 n 1er

$2 \times 3 = 0 \bmod 6$

$ab = 0 \Rightarrow a = 0$ ou $b = 0$ si n n'est pas 1er

si n est 1er : ~~Soit~~ $0 < a < n$ mod n $0 = n = a.b$ où $0 < a < n$, $0 < b < n$

a et n sont 1ers entre eux ~~~~ Bezout $\Rightarrow \exists u, v$ tq $au + nv = 1$

$au = 1 - nv$

$= 1 \bmod n$

$5^{-1} \bmod 7$? $5^{-1} = 3$

$5 \cdot 3 + 7 \cdot (-2) = 1$

$u = a^{-1}$

Proposition

Dans un anneau intègre $(A, +, \cdot)$ on a la ***propriété de simplification***, c'est à dire : $\forall a, b \in A, \forall c \in A^* = A \setminus \{0\}$

$$a \cdot c = bc \Rightarrow a = b\,.$$

Anneaux intègres

Démonstration.

Soient $a, b \in A$, $c \in A^* = A \setminus \{0\}$. On veut prouver $a \cdot c = bc \Rightarrow a = b$.

$$
\begin{aligned}
a \cdot c = b \cdot c &\overset{+(-(b\cdot c))}{\Longrightarrow} a \cdot c + (-(b \cdot c)) = b \cdot c + (-(b \cdot c)) \\
&\overset{\text{Neutre } +}{\Longrightarrow} a \cdot c + (-(b \cdot c)) = 0 \\
&\overset{?}{\Longrightarrow} a \cdot c + (-b) \cdot c = 0 \\
&\overset{\text{Distr.}}{\Longrightarrow} (a + (-b)) \cdot c = 0 \\
&\overset{\text{Intègrité}}{\Longrightarrow} c = 0 \text{ ou } a + (-b) = 0
\end{aligned}
$$

Or, $c \neq 0$ donc $a + (-b) = 0$.

+b   +b

Lemme : $\forall x, y, z \quad x = y + z \iff x - z = y$

Démonstration.

On sait que $a + (-b) = 0$. On a alors :

$$
\begin{aligned}
(a + (-b)) = 0 &\overset{+b}{\Rightarrow} (a + (-b)) + b = 0 + b \\
&\overset{\text{Asso. } +}{\Rightarrow} a + ((-b) + b) = 0 + b \\
&\overset{\text{Opp. } +}{\Rightarrow} a + 0 = 0 + b \\
&\overset{\text{Neutre } +}{\Rightarrow} a = 0 + b \\
&\overset{\text{Neutre } +}{\Rightarrow} a = b
\end{aligned}
$$

$\square$

$x = y + z$

$-z \qquad -z$

$x - z = (y + z) + (-z)$

$= y + \underbrace{(z + (-z))}_{=0}$

$= y + 0$

$= y$

Où sont les nombres premiers ?

$x = a \times b \times c \times c^{-1}$

Définition

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

- Un élément $a \in A$ est dit **inversible** s'il existe $b \in A$ tel que

$$\underline{a \cdot b = 1 = b \cdot a.}$$

On dit alors que b est l'***inverse*** de a, et on note $a^{-1} = b$. L'ensemble des éléments inversibles est noté $A^{\times}$. On l'appelle aussi l'ensemble des ***unités***.

Éléments inversibles et irréductibles

$0 = (1-x^3) = \underbrace{\overset{=0}{(1-x)}}\underbrace{(1+\overset{=0}{x}+x^2)}$

Définition

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

- Un élément $a \in A$ est dit **inversible** s'il existe $b \in A$ tel que

$$a \cdot b = 1 = b \cdot a.$$

  On dit alors que b est l'***inverse*** de a, et on note $a^{-1} = b$. L'ensemble des éléments inversibles est noté $A^\times$. On l'appelle aussi l'ensemble des ***unités***.

- Si A est **intègre**, un élément $p \in A \setminus A^\times$ est dit $\boxed{\textbf{irréductible}}$ si toute écriture de la forme

$$p = a \cdot b$$

$(p \times c) \times c^{-1} = p$

  implique que a est inversible ou b est inversible.

Exemples d'éléments inversibles

Exemple

- Dans $\mathbb{Z}$: les seuls inversibles sont ± 1.

$$\mathbb{Z}^\times = \{-1, 1\}$$

Exemples d'éléments inversibles

Exemple

- Dans $\mathbb{Z}$: les seuls inversibles sont ± 1.

$$\mathbb{Z}^\times = \{-1, 1\}$$

- Dans $\mathbb{Q}$: tous les éléments sont inversibles donc $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$.

Exemples d'éléments inversibles

Exemple

- Dans $\mathbb{Z}$: les seuls inversibles sont ± 1.

$$\mathbb{Z}^{\times} = \{-1, 1\}$$

- Dans $\mathbb{Q}$: tous les éléments sont inversibles donc $\mathbb{Q}^{\times} = \mathbb{Q} \setminus \{0\}$.
- Dans $\mathbb{R}[X]$: les inversibles sont les **polynômes constants non nuls**.

$$\mathbb{R}[X]^{\times} = \mathbb{R} \setminus \{0\}.$$

Exemples d'éléments inversibles

A, B $\exists Q, R$ $A = BQ + R$ $\deg R < \deg B$

Exemple

- Dans $\mathbb{Z}$: les seuls inversibles sont ± 1.

$$\mathbb{Z}^\times = \{-1, 1\}$$

$X^3 = X(X^2-1) + X$

$= X \bmod (X^2-1)$

- Dans $\mathbb{Q}$: tous les éléments sont inversibles donc $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$.

$X \cdot X = X^2$

- Dans $\mathbb{R}[X]$: les inversibles sont les **polynômes constants non nuls**.

$= 1.(X^2-1) + 1$

$= 1 \bmod (X^2-1)$

$$\mathbb{R}[X]^\times = \mathbb{R} \setminus \{0\}.$$

- Dans $\mathcal{M}_n(\mathbb{R})$: les inversibles sont les matrices de déterminant non nul.

$$\mathcal{M}_n(\mathbb{R})^\times = \mathrm{GL}_n(\mathbb{R}).$$

Les corps : quand tout est inversible

Définition (Corps)

Un **corps** est un anneau $(A, +, \cdot)$ dans lequel tout élément non nul est inversible :

$$\forall a \in A \setminus \{0\},\ \exists a^{-1} \in A,\ a \cdot a^{-1} = 1 = a^{-1} \cdot a.$$

$\underbrace{a}_{\neq 0} . b = 0$

$\underbrace{a^{-1} \times (a}\, b) = a^{-1} \times 0 = 0$

$\underbrace{(a^{-1} a)}_{=1} . b$

$\underbrace{\qquad}_{1 . b = b}$

Les corps : quand tout est inversible

Définition (Corps)

Un **corps** est un anneau $(A, +, \cdot)$ dans lequel tout élément non nul est inversible :

$$\forall a \in A \setminus \{0\},\ \exists a^{-1} \in A,\ a \cdot a^{-1} = 1 = a^{-1} \cdot a.$$

Observation

Dans un corps, il n'existe plus d'irréductibles ni de nombres premiers : tout élément non nul divise tout autre élément.

L'arithmétique y est donc ***triviale*** : aucun phénomène de factorisation non banal.

Les corps : quand tout est inversible

Définition (Corps)

Un **corps** est un anneau $(A, +, \cdot)$ dans lequel tout élément non nul est inversible :

$$\forall a \in A \setminus \{0\},\ \exists a^{-1} \in A,\ a \cdot a^{-1} = 1 = a^{-1} \cdot a.$$

Observation

Dans un corps, il n'existe plus d'irréductibles ni de nombres premiers : tout élément non nul divise tout autre élément.

L'arithmétique y est donc ***triviale*** : aucun phénomène de factorisation non banal.

Exemple

Des exemples de corps

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$
- $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ pour un nombre premier p (***pourquoi ?***) (Bezout $\Rightarrow \forall a \in [\![1, p-1]\!]$ a est inversible

car $\exists u, v$ $au + vp = 1$

$au = 1 - vp \Rightarrow u = a^{-1}$

$= 1 \bmod p$

Définition (Anneau factoriel)

Un **anneau factoriel** est un anneau intègre $(A, +, \cdot)$ tel que :

- tout élément non nul et non inversible de A se décompose en produit fini d'irréductibles :
$$a = p_1 \cdot p_2 \cdots p_n;$$
- et cette décomposition est **unique** à permutation des facteurs et multiplication par des unités près.

C'est l'analogue du ***Théorème fondamental de l'arithmétique***.

Les anneaux factoriels

Exemple

L'anneau $(\mathbb{Z}, +, \cdot)$ est factoriel : en effet, tout entier se factorise comme produit de premiers (irréductibles).

Par exemple, $12 = 2 \cdot 2 \cdot 3$. Cette décomposition est unique à permutation des facteurs près ($12 = 2 \cdot 3 \cdot 2$) et à multiplication par des unités près ($12 = \underbrace{(-1) \cdot (-1)}_{(1)} \cdot 1 \cdot 2 \cdot 2 \cdot 3$).

$\sqrt{-1} = i$

$x^2 + 5 = 0$

$\sqrt{-5} \times \sqrt{-5} = -5$

Exemple

L'anneau $(\mathbb{Z}, +, \cdot)$ est factoriel : en effet, tout entier se factorise comme produit de premiers (irréductibles).

Par exemple, $12 = 2 \cdot 2 \cdot 3$. Cette décomposition est unique à permutation des facteurs près ($12 = 2 \cdot 3 \cdot 2$) et à multiplication par des unités près ($12 = (-1) \cdot (-1) \cdot 1 \cdot 2 \cdot 2 \cdot 3$).

$(a^2 - b^2) = (a+b)(a-b)$

Exemple

L'anneau [a] $(\mathbb{Z}[\sqrt{-5}], +, \cdot)$ n'est pas factoriel : en effet, l'élément 6 a deux décompositions différentes [b] : $6 = 2 \times 3$ et $6 = (1+\sqrt{-5}) \cdot (1-\sqrt{-5}) = 1 - \sqrt{-5}^2 = 1 - (-5) = 6$.

a. Pour rappel, $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$

b. On peut prouver que 2, 3, $(1 + \sqrt{-5})$ et $(1 - \sqrt{-5})$ dont irréductibles.

$(a+b\sqrt{-5})(c+d\sqrt{-5}) = ac - 5bd + \sqrt{-5}(bc+ad)$

On s'y prend comment en machine ?

Anneaux euclidiens : la division revient

Définition (Anneau euclidien)

Un anneau $(A, +, \cdot)$ est dit **euclidien** s'il est intègre et s'il existe une application

$$v : A^* \to \mathbb{N}$$

$|a|$

deg

appelée ***stathme euclidien***, telle que :

1. $\forall a, b \in A^*, \ \ v(a) \leq v(ab)$
2. $\forall a \in A, \ \forall b \in A^*, \ \exists q, r \in A$ tels que

$$a = bq + r, \text{ avec } r = 0 \text{ ou } v(r) < v(b).$$

Anneaux euclidiens : la division revient

Définition (Anneau euclidien)

Un anneau $(A, +, \cdot)$ est dit **euclidien** s'il est intègre et s'il existe une application

$$v : A^* \to \mathbb{N}$$

appelée ***stathme euclidien***, telle que :

1. $\forall a, b \in A^*,\ \ v(a) \leq v(ab)$
2. $\forall a \in A,\ \forall b \in A^*,\ \exists q, r \in A$ tels que

$$a = bq + r, \quad \text{avec } r = 0 \text{ ou } v(r) < v(b).$$

Idée intuitive

Le stathme v joue le rôle d'une ***taille*** : on peut effectuer une division avec reste, comme dans $\mathbb{Z}$, et ainsi retrouver une arithmétique **algorithmique**.

Exemples d'anneaux euclidiens

aX

Exemple

- $\mathbb{Z}$ avec $v(a) = |a|$: c'est l'exemple canonique.
- $\mathbb{K}[X]$ avec $v(P) = \deg(P)$: division euclidienne des polynômes.
- $\mathbb{Z}[i]$ (entiers de Gauss) avec $v(a + ib) = a^2 + b^2$: on divise par approximation complexe.

Exemples d'anneaux euclidiens

$(X-1)$ $\quad 7X$ $\quad 7^{-1}$

$X-1 = \frac{1}{7}(7X) \ldots$

Exemple

- $\mathbb{Z}$ avec $v(a) = |a|$: c'est l'exemple canonique.
- $\mathbb{K}[X]$ avec $v(P) = \deg(P)$: division euclidienne des polynômes.
- $\mathbb{Z}[i]$ (entiers de Gauss) avec $\boxed{v(a+ib) = a^2 + b^2}$: on divise par approximation complexe.

Théorème fondamental

Tout anneau euclidien est **factoriel**.

Exemple

- $\mathbb{Z}$ avec $v(a) = |a|$: c'est l'exemple canonique.
- $\mathbb{K}[X]$ avec $v(P) = \deg(P)$: division euclidienne des polynômes.
- $\mathbb{Z}[i]$ (entiers de Gauss) avec $v(a + ib) = a^2 + b^2$: on divise par approximation complexe.

Théorème fondamental

Tout anneau euclidien est **factoriel**.

Question

- Pourquoi $\mathbb{Z}[X]$ n'est-il pas euclidien avec $\boxed{v(P) = \deg(P)}$? $\mathbb{Z}$ n'est pas un corps ($\exists^{-1}$ $\nexists$)
- Que change la présence ou non d'un ***stathme*** ?

↳ si $\exists$ stathme $\exists$ algo

Pour résumer

À retenir

Faire de l'arithmétique, c'est étudier des ensembles où la **divisibilité** et la **factorisation** ont un sens.

À retenir

Faire de l'arithmétique, c'est étudier des ensembles où la **divisibilité** et la **factorisation** ont un sens.

- Un **anneau** permet d'additionner et de multiplier de manière cohérente.
- Un **anneau intègre** élimine les diviseurs de zéro : la divisibilité devient fiable.
- Un **anneau factoriel** rétablit l'unicité de la factorisation.
- Un **anneau euclidien** rend la division ***effective*** : on peut calculer le pgcd et appliquer Bézout.
- Un **corps** simplifie tout : tout élément non nul est inversible, mais l'arithmétique y devient triviale.

À retenir

Faire de l'arithmétique, c'est étudier des ensembles où la **divisibilité** et la **factorisation** ont un sens.

- Un **anneau** permet d'additionner et de multiplier de manière cohérente.
- Un **anneau intègre** élimine les diviseurs de zéro : la divisibilité devient fiable.
- Un **anneau factoriel** rétablit l'unicité de la factorisation.
- Un **anneau euclidien** rend la division ***effective*** : on peut calculer le pgcd et appliquer Bézout.
- Un **corps** simplifie tout : tout élément non nul est inversible, mais l'arithmétique y devient triviale.

Hiérarchie

corps $\overset{\text{Pourquoi ?}}{\Rightarrow}$ euclidien $\Rightarrow$ factoriel $\Rightarrow$ intègre

That's All Folks!