

MAT 205 – Introduction à la Théorie des Anneaux et des Corps

Notes de cours

Gönenç Onay
Université Galatasaray

Printemps 2026

0 Rappels d'arithmétique dans \mathbb{Z}

0.1 Rappels sur $(\mathbb{Z}, +)$

L'ensemble $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ muni de l'addition est un **groupe abélien** : l'addition est associative, commutative, admet 0 comme élément neutre, et tout élément a possède un opposé $-a$. Ce groupe est, de plus, **cyclique**, engendré par 1 (ou par -1) : tout entier s'écrit comme somme de copies de 1 ou de -1 .

0.2 Classification des sous-groupes de \mathbb{Z}

Un sous-ensemble $H \subseteq \mathbb{Z}$ est un **sous-groupe** de $(\mathbb{Z}, +)$ si $0 \in H$ et si $a - b \in H$ pour tous $a, b \in H$.

Théorème 0.1 (Sous-groupes de \mathbb{Z}). *Tout sous-groupe de $(\mathbb{Z}, +)$ est de la forme $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ pour un unique $n \in \mathbb{N}$.*

Démonstration. Soit H un sous-groupe de \mathbb{Z} . Si $H = \{0\}$, c'est $0\mathbb{Z}$. Sinon, H contient un élément non nul, donc aussi son opposé ; ainsi $H \cap \mathbb{N}^*$ est non vide. Par le bon ordre de \mathbb{N} , cet ensemble admet un plus petit élément n . Montrons que $H = n\mathbb{Z}$.

L'inclusion $n\mathbb{Z} \subseteq H$ est claire : $n \in H$ et H est stable par addition et passage à l'opposé.

Réiproquement, soit $a \in H$. La division euclidienne (théorème 0.2 ci-dessous) donne $a = qn + r$ avec $0 \leq r < n$. Alors $r = a - qn \in H$. Comme n est le plus petit élément strictement positif de H , on a nécessairement $r = 0$, d'où $a \in n\mathbb{Z}$. \square

Remarque 0.1. Notons que ce théorème utilise fondamentalement la division euclidienne (théorème 0.2), donc *au-delà* de l'addition, pour établir un résultat portant sur la structure additive $(\mathbb{Z}, +)$.

0.3 Somme de sous-groupes et pgcd

Soient $a, b \in \mathbb{Z}$. Les sous-groupes $a\mathbb{Z}$ et $b\mathbb{Z}$ engendrent un sous-groupe :

$$a\mathbb{Z} + b\mathbb{Z} = \{au + bv : u, v \in \mathbb{Z}\}.$$

Par le théorème 0.1, il existe un unique $d \in \mathbb{N}$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

Définition 0.1 (PGCD). L'entier $d \geq 0$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ est le **plus grand commun diviseur** de a et b , noté $\text{pgcd}(a, b)$ ou $a \wedge b$.

Justifions ce nom. Puisque $a \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, on a $d \mid a$; de même $d \mid b$. Réiproquement, si $c \mid a$ et $c \mid b$, alors $a\mathbb{Z} \subseteq c\mathbb{Z}$ et $b\mathbb{Z} \subseteq c\mathbb{Z}$, d'où $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \subseteq c\mathbb{Z}$, ce qui donne $c \mid d$. Ainsi d est bien le *plus grand* (au sens de la divisibilité) des diviseurs communs à a et b .

Remarque 0.2. On écrit $\text{pgcd}(a, b)$ pour la clarté, et $a \wedge b$ quand la concision l'exige. Les deux notations sont standard et seront utilisées librement.

0.4 Divisibilité et théorèmes fondamentaux

0.4.1 Divisibilité

Définition 0.2. Soient $a, b \in \mathbb{Z}$. On dit que a **divise** b , et on écrit $a | b$, s'il existe $k \in \mathbb{Z}$ tel que $b = ka$. Autrement dit, $b \in a\mathbb{Z}$.

La relation $a | b$ se lit aussi « b est un multiple de a » ou « a est un diviseur de b ». On a les propriétés immédiates :

- (i) $a | 0$ pour tout $a \in \mathbb{Z}$;
- (ii) $1 | a$ pour tout $a \in \mathbb{Z}$;
- (iii) si $a | b$ et $b | c$, alors $a | c$ (transitivité) ;
- (iv) si $a | b$ et $a | c$, alors $a | (bu + cv)$ pour tous $u, v \in \mathbb{Z}$ (les multiples de a forment un sous-groupe, à savoir $a\mathbb{Z}$).

0.4.2 Division euclidienne

Théorème 0.2 (Division euclidienne). *Pour tous $a \in \mathbb{Z}$ et $b \in \mathbb{Z} \setminus \{0\}$, il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que*

$$a = bq + r \quad \text{et} \quad 0 \leq r < |b|.$$

Démonstration. On peut supposer $b > 0$ (sinon remplacer b par $-b$ et q par $-q$).

Existence. L'ensemble $\{a - kb : k \in \mathbb{Z}\} \cap \mathbb{N}$ est non vide (il contient $a - kb$ pour k assez négatif). Par le bon ordre de \mathbb{N} , il admet un plus petit élément $r = a - qb \geq 0$. Si l'on avait $r \geq b$, alors $r' = r - b = a - (q+1)b$ appartiendrait aussi à cet ensemble et serait strictement plus petit que r : contradiction. Donc $0 \leq r < b$.

Unicité. Si $a = bq + r = bq' + r'$ avec $0 \leq r, r' < b$, alors $b(q - q') = r' - r$. Comme $|r' - r| < b$, on a $q = q'$, d'où $r = r'$. \square

L'entier q est le **quotient** et r le **reste**. On a $b | a$ si et seulement si $r = 0$.

0.4.3 Algorithme d'Euclide

L'algorithme d'Euclide calcule $\text{pgcd}(a, b)$ par divisions successives. Le principe repose sur l'observation :

$$\text{pgcd}(a, b) = \text{pgcd}(b, r) \quad \text{où } r \text{ est le reste de la division de } a \text{ par } b.$$

En effet, $a = bq + r$ implique $a\mathbb{Z} + b\mathbb{Z} = b\mathbb{Z} + r\mathbb{Z}$ (tout élément de l'un est dans l'autre). On itère : $r_0 = a$, $r_1 = b$, et r_{i+1} est le reste de la division de r_{i-1} par r_i . La suite $(r_i)_{i \geq 1}$ est une suite d'entiers naturels vérifiant $r_{i+1} < r_i$, donc elle atteint 0 en un nombre fini d'étapes. Le dernier reste non nul est $\text{pgcd}(a, b)$.

Exemple 0.1. Calculons $\text{pgcd}(120, 44)$:

$$120 = 2 \times 44 + 32, \quad 44 = 1 \times 32 + 12, \quad 32 = 2 \times 12 + 8, \quad 12 = 1 \times 8 + 4, \quad 8 = 2 \times 4.$$

Donc $\text{pgcd}(120, 44) = 4$.

0.4.4 Théorème de Bézout

Théorème 0.3 (Bézout). *Soient $a, b \in \mathbb{Z}$. Il existe $u, v \in \mathbb{Z}$ tels que*

$$au + bv = \text{pgcd}(a, b).$$

Démonstration. C'est une reformulation immédiate de la définition 0.1 : $\text{pgcd}(a, b)$ est le générateur positif de $a\mathbb{Z} + b\mathbb{Z}$, donc il s'écrit $au + bv$ pour certains $u, v \in \mathbb{Z}$. \square

Remarque 0.3. On obtient les coefficients u, v en « remontant » l'algorithme d'Euclide.

Corollaire 0.1 (Lemme de Gauss). *Soient $a, b, c \in \mathbb{Z}$. Si $a \mid bc$ et $\text{pgcd}(a, b) = 1$, alors $a \mid c$.*

Démonstration. Par Bézout, il existe u, v tels que $au + bv = 1$. Alors $c = acu + bcv$. Or $a \mid acu$ et $a \mid bcv$ (car $a \mid bc$), d'où $a \mid c$. \square

0.4.5 Quotients $\mathbb{Z}/n\mathbb{Z}$

Pour $n \geq 1$, la relation de congruence modulo n , définie par $a \equiv b \pmod{n} \iff n \mid (a - b)$, est une relation d'équivalence compatible avec l'addition. L'ensemble quotient

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \bar{n-1}\}$$

hérite d'une structure de groupe abélien pour l'addition : $\bar{a} + \bar{b} = \overline{a+b}$.

0.4.6 Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$: correspondance

Rappelons un résultat général de théorie des groupes. Soit G un groupe et $H \trianglelefteq G$ un sous-groupe distingué. La projection canonique $\pi : G \rightarrow G/H$ induit une **bijection croissante** (i.e. qui préserve l'inclusion) entre les sous-groupes de G contenant H et les

$$\{\text{sous-groupes de } G \text{ contenant } H\} \xrightarrow{\sim} \{\text{sous-groupes de } G/H\}, \quad K \mapsto K/H = \pi(K).$$

La bijection réciproque est $\bar{K} \mapsto \pi^{-1}(\bar{K})$. Elle préserve l'inclusion, l'indice et la normalité.

Appliquons cela à $G = \mathbb{Z}$ et $H = n\mathbb{Z}$ (tout sous-groupe de \mathbb{Z} est distingué, le groupe étant abélien). Les sous-groupes de \mathbb{Z} contenant $n\mathbb{Z}$ sont exactement les $d\mathbb{Z}$ avec $d \mid n$ (car $n\mathbb{Z} \subseteq d\mathbb{Z}$ équivaut à $d \mid n$). La correspondance donne :

Proposition 0.1 (Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$). *Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les $d\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/(n/d)\mathbb{Z}$ pour d parcourant les diviseurs positifs de n . En particulier, $\mathbb{Z}/n\mathbb{Z}$ possède autant de sous-groupes que n a de diviseurs positifs, et chacun est cyclique.*

Exemple 0.2. Les sous-groupes de $\mathbb{Z}/12\mathbb{Z}$ correspondent aux diviseurs de 12 : ce sont $\mathbb{Z}/12\mathbb{Z}$, $2\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$, $3\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z}$, $4\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z}$, $6\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$ et $\{0\}$.

1 Anneaux

Les entiers ne vivent pas que par l'addition. L'addition et la multiplication cohabitent et interagissent via la distributivité. Avant de dégager la structure commune, observons d'autres objets munis de deux opérations.

1.1 Les matrices $M_n(\mathbb{R})$

Fixons $n \geq 1$. L'ensemble $M_n(\mathbb{R})$ des matrices carrées $n \times n$ à coefficients réels est muni de deux lois internes :

- l'**addition** : $(A + B)_{ij} = A_{ij} + B_{ij}$, pour laquelle $(M_n(\mathbb{R}), +)$ est un groupe abélien (l'élément neutre est la matrice nulle 0_n) ;
- la **multiplication** : $(AB)_{ij} = \sum_{k=1}^n A_{ik}B_{kj}$, qui est associative et admet la matrice identité I_n comme élément neutre.

Le pont entre les deux est la **distributivité** :

$$A(B + C) = AB + AC \quad \text{et} \quad (A + B)C = AC + BC.$$

Remarque 1.1. Deux différences majeures avec \mathbb{Z} :

- (a) la multiplication des matrices n'est **pas commutative** dès que $n \geq 2$;
- (b) il existe des **diviseurs de zéro** : des matrices $A \neq 0, B \neq 0$ telles que $AB = 0$ (pensez à deux projections sur des sous-espaces supplémentaires).

1.2 Les polynômes $\mathbb{R}[X]$

Rappelons qu'un **polynôme** à coefficients réels est une expression formelle

$$P = a_0 + a_1X + a_2X^2 + \cdots + a_dX^d, \quad a_i \in \mathbb{R},$$

où X est une **indéterminée** (un symbole formel, pas un nombre). Le **degré** de P est le plus grand indice i tel que $a_i \neq 0$ (par convention $\deg 0 = -\infty$). L'ensemble de tous ces polynômes est noté $\mathbb{R}[X]$.

On munit $\mathbb{R}[X]$ de deux opérations : l'**addition** (coefficient par coefficient) et la **multiplication** usuelle des polynômes. L'élément neutre pour l'addition est le polynôme nul 0, et celui pour la multiplication est le polynôme constant 1. La multiplication est commutative et distributive par rapport à l'addition.

L'analogie avec \mathbb{Z} est instructive :

- le **degré** joue le rôle de la **valeur absolue** : on a $\deg(PQ) = \deg P + \deg Q$ (en particulier, si $PQ = 0$ alors $P = 0$ ou $Q = 0$) ;
- on dispose d'une **division euclidienne** : pour $A, B \in \mathbb{R}[X]$ avec $B \neq 0$, il existe un unique couple (Q, R) tel que $A = BQ + R$ et $\deg R < \deg B$;
- on en déduit un pgcd, un algorithme d'Euclide, une identité de Bézout — toute l'arithmétique de la section 0.4 se transpose.

Nous étudierons $\mathbb{K}[X]$ en détail en semaine 5.

1.3 Tableau comparatif

Propriété	\mathbb{Z}	$\mathbb{Z}/n\mathbb{Z}$	$\mathbb{R}[X]$	$M_n(\mathbb{R})$
$(E, +)$ groupe abélien	oui	oui	oui	oui
\times associative, neutre 1	oui	oui	oui	oui
Distributivité	oui	oui	oui	oui
\times commutative	oui	oui	oui	non ($n \geq 2$)
Division euclidienne	oui	—	oui	—
Diviseurs de zéro	non	oui (n non premier)	non	oui ($n \geq 2$)

Quatre objets de natures différentes, une même architecture. Il est temps de nommer cette structure commune.

1.4 Définition

Définition 1.1 (Anneau). Un **anneau** est un triplet $(A, +, \times)$ où A est un ensemble muni de deux lois de composition interne vérifiant :

- (A1) $(A, +)$ est un **groupe abélien** (on note 0_A son élément neutre) ;
- (A2) la multiplication est **associative** : $a(bc) = (ab)c$ pour tous $a, b, c \in A$;
- (A3) il existe un élément $1_A \in A$ (**l'unité**) tel que $1_A \cdot a = a = a \cdot 1_A = a$ pour tout $a \in A$;
- (A4) la multiplication est **distributive** par rapport à l'addition :

$$a(b + c) = ab + ac \quad \text{et} \quad (a + b)c = ac + bc.$$

L'anneau est dit **commutatif** si, de plus, $ab = ba$ pour tous $a, b \in A$.

Remarque 1.2. Certains auteurs n'exigent pas l'existence de 1_A . Dans ce cours, *tous nos anneaux possèdent un élément unité*, sauf mention explicite du contraire. C'est la convention dominante en algèbre moderne.

Proposition 1.1 (Propriétés élémentaires). *Soit $(A, +, \times)$ un anneau. Pour tous $a, b \in A$:*

- (i) $0_A \cdot a = a \cdot 0_A = 0_A$;
- (ii) $(-a) \cdot b = a \cdot (-b) = -(ab)$;
- (iii) $(-a)(-b) = ab$;
- (iv) *l'unité 1_A est unique ; si $1_A = 0_A$, alors $A = \{0_A\}$ (l'**anneau nul**).*

Démonstration. (i) $0_A \cdot a = (0_A + 0_A)a = 0_A \cdot a + 0_A \cdot a$. En ajoutant $-(0_A \cdot a)$ des deux côtés, on obtient $0_A \cdot a = 0_A$.

(ii) $(-a)b + ab = (-a + a)b = 0_A \cdot b = 0_A$, donc $(-a)b = -(ab)$.

(iii) Découle de (ii) appliqué deux fois.

(iv) Si 1_A et $1'_A$ sont deux unités, $1_A = 1_A \cdot 1'_A = 1'_A$. Si $1_A = 0_A$, alors $a = 1_A \cdot a = 0_A \cdot a = 0_A$ pour tout a . \square

Le premier exemple non trivial est $\mathbb{Z}/n\mathbb{Z}$. On sait de la section 0 que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe ; la surjection canonique $\pi : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$ en est un morphisme de groupes.

Exercice 1. Montrer que l'on peut définir une loi, *multiplication*, sur $\mathbb{Z}/n\mathbb{Z}$, comme suivant : $\bar{a} \cdot \bar{b} = \overline{ab}$, et que avec cette loi $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau commutatif d'unité $\bar{1}$.

Exemple 1.1. Les exemples fondamentaux d'anneaux :

- (a) $(\mathbb{Z}, +, \times)$: anneau commutatif, intègre (cf. définition 1.6).
- (b) $(\mathbb{Z}/n\mathbb{Z}, +, \times)$: anneau commutatif à n éléments (exercice 1).
- (c) $(M_n(A), +, \times)$ pour un anneau A : anneau non commutatif si $n \geq 2$.
- (d) $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$: anneaux commutatifs (et même des corps, cf. définition 1.7).
- (e) L'anneau des polynômes $\mathbb{K}[X]$ (détaillé en semaine 5).
- (f) Pour tout ensemble E , l'ensemble $\mathcal{F}(E, \mathbb{R})$ des fonctions de E dans \mathbb{R} , muni de l'addition et la multiplication point par point, est un anneau commutatif. Son unité est la fonction constante 1.

Exercice 2. Soit $n \geq 2$. Montrer que $\mathbb{Z}/n\mathbb{Z}$ possède des diviseurs de zéro si et seulement si n n'est pas premier. *Indication* : utiliser le lemme de Gauss (corollaire 0.1).

1.5 Éléments d'un anneau : une taxonomie

La structure additive d'un anneau est celle d'un groupe abélien — elle est bien comprise. La question fondamentale de cette section est d'ordre *multiplicatif* : étant donné un élément a d'un anneau A , que peut-on dire de son comportement vis-à-vis de la multiplication ?

1.5.1 Inversibles (unités)

Définition 1.2 (Inversible, groupe des unités). Soit $(A, +, \times)$ un anneau. Un élément $a \in A$ est dit **inversible** (ou **unité**) s'il existe $b \in A$ tel que $ab = ba = 1_A$. Cet élément b , nécessairement unique, est noté a^{-1} . L'ensemble des éléments inversibles de A est noté A^\times .

On vérifie immédiatement que (A^\times, \times) est un **groupe** : le produit de deux inversibles est inversible ($(ab)^{-1} = b^{-1}a^{-1}$), $1_A \in A^\times$, et l'inverse d'un inversible est inversible.

Exemple 1.2. (a) $\mathbb{Z}^\times = \{1, -1\}$.

- (b) $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} : \text{pgcd}(a, n) = 1\}$. En effet, \bar{a} est inversible si et seulement si $au \equiv 1 \pmod{n}$ pour un certain u , ce qui, par Bézout (0.3), équivaut à $\text{pgcd}(a, n) = 1$.
- (c) $M_n(\mathbb{K})^\times = GL_n(\mathbb{K})$.
- (d) Si \mathbb{K} est un corps, $\mathbb{K}[X]^\times = \mathbb{K} \setminus \{0\}$ (car $\deg(PQ) = \deg P + \deg Q$).

1.5.2 Diviseurs de zéro

Définition 1.3 (Diviseur de zéro). Un élément $a \in A \setminus \{0\}$ est un **diviseur de zéro** s'il existe $b \in A \setminus \{0\}$ tel que $ab = 0$ ou $ba = 0$. Dans un anneau commutatif, on parle simplement de **diviseur de zéro**.

Exemple 1.3. (a) Dans $\mathbb{Z}/6\mathbb{Z}$: $\bar{2} \cdot \bar{3} = \bar{0}$.

- (b) Dans $M_2(\mathbb{R})$: $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = 0$.
- (c) Dans $C(\mathbb{R}, \mathbb{R})$: $f = \max(\cdot, 0)$ et $g = \min(\cdot, 0)$ vérifient $fg = 0$, $f \neq 0$, $g \neq 0$.

Proposition 1.2. Un élément inversible n'est jamais diviseur de zéro.

Démonstration. Si $a \in A^\times$ et $ab = 0$, alors $b = a^{-1}(ab) = 0$. □

1.5.3 Nilpotents et idempotents

Définition 1.4 (Nilpotent). Un élément $a \in A$ est **nilpotent** s'il existe $n \geq 1$ tel que $a^n = 0$. Le plus petit tel n est l'**indice de nilpotence**.

Définition 1.5 (Idempotent). Un élément $e \in A$ est **idempotent** si $e^2 = e$.

Proposition 1.3. (i) Tout nilpotent non nul est diviseur de zéro.

(ii) Tout idempotent $e \neq 0, 1$ d'un anneau commutatif est diviseur de zéro.

Démonstration. (i) Si $a^n = 0$ avec n minimal, alors $a \cdot a^{n-1} = 0$ et $a^{n-1} \neq 0$. (ii) $e(1 - e) = e - e^2 = 0$, avec $e \neq 0$ et $1 - e \neq 0$. □

Exemple 1.4. (a) $\bar{2} \in \mathbb{Z}/8\mathbb{Z}$ est nilpotent d'indice 3 : $\bar{2}^3 = \bar{0}$.

(b) $\bar{3} \in \mathbb{Z}/6\mathbb{Z}$ est idempotent : $\bar{3}^2 = \bar{3}$.

(c) Dans $M_n(\mathbb{K})$, les projecteurs ($P^2 = P$) sont idempotents ; les matrices strictement triangulaires sont nilpotentes.

Exercice 3. Soit $n \geq 2$. Montrer qu'un élément $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ est nilpotent si et seulement si tout facteur premier de n divise a . *Indication* : pour le sens direct, raisonner par contraposée en utilisant un facteur premier de n ne divisant pas a .

Le résultat suivant relie nilpotence et inversibilité : la série géométrique $(1 - a)^{-1} = \sum a^k$, qui en analyse requiert $|a| < 1$, devient une somme *finie* grâce à la nilpotence.

Proposition 1.4 (1+ nilpotent est inversible). *Soit $a \in A$ nilpotent d'indice n . Alors $1_A - a$ est inversible, d'inverse $\sum_{k=0}^{n-1} a^k$.*

Démonstration. Posons $s = 1_A + a + \cdots + a^{n-1}$. Par télescopage :

$$(1_A - a) \cdot s = (1_A + a + \cdots + a^{n-1}) - (a + \cdots + a^n) = 1_A - a^n = 1_A. \quad \square$$

1.5.4 Bilan

Type	Comportement
Inversible ($a \in A^\times$)	$\exists a^{-1}$; jamais div. de zéro
Diviseur de zéro	$\exists b \neq 0$, $ab = 0$; jamais inversible
Nilpotent	$a^n = 0$; cas particulier de div. de zéro
Idempotent $\neq 0, 1$	$a^2 = a$; cas particulier de div. de zéro
Régulier non inversible	ni inversible, ni div. de zéro

1.6 Anneaux intègres et corps

1.6.1 Intégrité

Définition 1.6 (Anneau intègre). Un anneau A est dit **intègre** s'il est commutatif, $1_A \neq 0_A$, et A n'a pas de diviseurs de zéro : $ab = 0 \implies a = 0$ ou $b = 0$.

Exercice 4. Montrer que dans un anneau intègre, la **loi de simplification** est vérifiée : si $a \neq 0$ et $ab = ac$, alors $b = c$.

Exemple 1.5. (a) $\mathbb{Z}, \mathbb{K}[X], \mathbb{Z}[i]$ sont intègres.

(b) $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre ; $M_n(\mathbb{K})$ non plus pour $n \geq 2$.

1.6.2 Corps

Définition 1.7 (Corps). Un **corps** est un anneau commutatif $(\mathbb{K}, +, \times)$ tel que $1_{\mathbb{K}} \neq 0_{\mathbb{K}}$ et $\mathbb{K}^\times = \mathbb{K} \setminus \{0\}$.

Proposition 1.5. *Tout corps est intègre.*

Démonstration. Dans un corps, tout élément non nul est inversible, donc n'est pas diviseur de zéro (proposition 1.2). \square

La réciproque est fausse en général (\mathbb{Z} est intègre mais pas un corps). Cependant, pour les anneaux finis, les deux notions coïncident.

Théorème 1.1 (Anneau intègre fini \Rightarrow corps). *Tout anneau intègre fini est un corps.*

Démonstration. Soit A intègre fini et $a \in A \setminus \{0\}$. L'application $\varphi_a : x \mapsto ax$ est **injective** : $ax = ay$ implique $a(x - y) = 0$, donc $x = y$ par intégrité. Une injection d'un ensemble fini dans lui-même étant surjective, il existe b tel que $ab = 1_A$. \square

Exercice 5. Soit p premier. Montrer que $\mathbb{Z}/p\mathbb{Z}$ est intègre. *Indication* : si $\bar{a} \cdot \bar{b} = \bar{0}$, alors $p \mid ab$; conclure par le lemme de Gauss (0.1).

Corollaire 1.1. $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est premier.

Démonstration. Le sens direct résulte de l'exercice 5 et du théorème 1.1. La réciproque est claire : si p n'est pas premier, $\mathbb{Z}/p\mathbb{Z}$ a des diviseurs de zéro. \square

Remarque 1.3. Le corollaire boucle la boucle avec la semaine 1 : la primalité, caractérisée par le lemme de Gauss, se traduit en intégrité de $\mathbb{Z}/p\mathbb{Z}$, qui par finitude équivaut à la structure de corps.

1.7 Sous-anneaux

Nous savons ce qu'est un anneau. La première question structurelle est : quand une partie d'un anneau est-elle *elle-même* un anneau, pour les mêmes lois ?

Définition 1.8 (Sous-anneau). Soit $(A, +, \times)$ un anneau. Une partie $B \subseteq A$ est un **sous-anneau** de A si :

- (i) $(B, +)$ est un **sous-groupe** de $(A, +)$;
- (ii) B est **stable par multiplication** : $b, b' \in B \implies bb' \in B$;
- (iii) $1_A \in B$.

Remarque 1.4. La condition $1_A \in B$ est essentielle. Sans elle, B peut hériter d'une structure d'anneau avec une unité *different*e de 1_A , ce qui brise le lien avec A . Par exemple, dans $M_2(\mathbb{R})$, l'ensemble $\left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R} \right\}$ est un anneau pour les lois induites, d'unité $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq I_2$. On ne le considère pas comme sous-anneau de $M_2(\mathbb{R})$.

- Exemple 1.6.**
- (a) $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$: chaque inclusion est celle d'un sous-anneau.
 - (b) L'anneau des **entiers de Gauss** $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ est un sous-anneau de \mathbb{C} .
 - (c) $2\mathbb{Z} \subset \mathbb{Z}$ n'est **pas** un sous-anneau : $1 \notin 2\mathbb{Z}$. C'est un sous-groupe additif, stable par multiplication, mais il manque l'unité.

Exercice 6. Montrer que l'intersection d'une famille quelconque de sous-anneaux de A est un sous-anneau de A (et que cette intersection est non vide car 1_A appartient à tous).

1.8 Anneaux produits

Le sous-anneau est une construction *interne*. Il existe aussi une construction *externe* : à partir de deux anneaux donnés, on en fabrique un troisième.

Définition 1.9 (Anneau produit). Soient $(A, +, \times)$ et $(B, +, \times)$ deux anneaux. L'**anneau produit** $A \times B$ est l'ensemble des couples (a, b) muni des lois *composante par composante* :

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2), \quad (a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2).$$

L'élément neutre additif est $(0_A, 0_B)$ et l'unité est $(1_A, 1_B)$.

- Remarque 1.5.**
- (a) Si A et B sont commutatifs, $A \times B$ l'est aussi.
 - (b) Les éléments $(1_A, 0_B)$ et $(0_A, 1_B)$ sont des **idempotents** non triviaux de $A \times B$; ce sont donc des diviseurs de zéro (proposition 1.3). En particulier, le **produit de deux anneaux intègres n'est jamais intègre**.

1.9 Morphismes d'anneaux

Pour comparer des anneaux — et pour donner un sens précis au symbole \cong utilisé ci-dessus — on a besoin d'applications qui *respectent* les deux lois.

Définition 1.10 (Morphisme d'anneaux). Soient $(A, +, \times)$ et $(B, +, \times)$ deux anneaux. Une application $f : A \rightarrow B$ est un **morphisme d'anneaux** si c'est un morphisme de groupes $(A, +) \rightarrow (B, +)$ qui, de plus, préserve la multiplication et l'unité :

$$f(aa') = f(a)f(a') \quad \text{pour tous } a, a' \in A, \quad f(1_A) = 1_B.$$

Un morphisme bijectif est un **isomorphisme** ; on écrit alors $A \cong B$.

Remarque 1.6. La condition $f(1_A) = 1_B$ ne découle pas de la multiplicativité en général : $f : \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ définie par $f(a) = (a, 0)$ préserve $+$ et \times mais $f(1) = (1, 0) \neq (1, 1)$.

Exemple 1.7. (a) La **surjection canonique** $\pi : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$, $a \mapsto \bar{a}$, est un morphisme d'anneaux (exercice 1).

- (b) Les **projections** $p_1 : A \times B \rightarrow A$ et $p_2 : A \times B \rightarrow B$ sont des morphismes surjectifs.
- (c) L'inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$ est un morphisme injectif.
- (d) Pour tout anneau A , il existe un *unique* morphisme $\mathbb{Z} \rightarrow A$, donné par $n \mapsto n \cdot 1_A$. Cela fait de \mathbb{Z} l'**objet initial** de la catégorie des anneaux.
- (e) Le **morphisme d'évaluation** $\text{ev}_\alpha : \mathbb{K}[X] \rightarrow \mathbb{K}$, $P \mapsto P(\alpha)$, est un morphisme d'anneaux pour tout α dans un anneau commutatif \mathbb{K} .

Exercice 7. Soit $f : A \rightarrow B$ un morphisme d'anneaux.

- (a) Montrer que f préserve les idempotents ($a^2 = a \implies f(a)^2 = f(a)$), les nilpotents ($a^n = 0 \implies f(a)^n = 0$) et les inversibles ($a \in A^\times \implies f(a) \in B^\times$).
- (b) Soit $P \in \mathbb{Z}[X]$. Montrer que si $P(a) = 0$ dans A , alors $P(f(a)) = 0$ dans B . Si de plus f est injectif, montrer la réciproque.
- (c) Montrer que même si f est injectif et $f(a)$ est inversible, on ne peut *pas* conclure que a est inversible. *Indication* : $\mathbb{Z} \hookrightarrow \mathbb{Q}$.

Les morphismes transportent les sous-structures :

Proposition 1.6. Soit $f : A \rightarrow B$ un morphisme d'anneaux.

- (i) Si A' est un sous-anneau de A , alors $f(A')$ est un sous-anneau de B .
- (ii) Si B' est un sous-anneau de B , alors $f^{-1}(B')$ est un sous-anneau de A .

Démonstration. Pour (i) : $f(A')$ est un sous-groupe additif de B (image d'un sous-groupe par un morphisme de groupes), il est stable par multiplication ($f(a)f(a') = f(aa') \in f(A')$), et $1_B = f(1_A) \in f(A')$. Pour (ii) : $f^{-1}(B')$ est un sous-groupe de $(A, +)$, il est stable par multiplication ($f(aa') = f(a)f(a') \in B'$ si $f(a), f(a') \in B'$), et $f(1_A) = 1_B \in B'$ donc $1_A \in f^{-1}(B')$. \square

Définition 1.11 (Noyau). Soit $f : A \rightarrow B$ un morphisme d'anneaux. Le **noyau** de f est

$$\text{Ker } f \stackrel{\text{déf}}{=} f^{-1}(\{0_B\}) = \{a \in A : f(a) = 0_B\}.$$

Remarque 1.7. Le noyau est un sous-groupe additif de A , mais ce n'est **pas** un sous-anneau en général ($1_A \notin \text{Ker } f$ dès que $B \neq 0$). Le noyau possède une propriété différente, et plus forte : c'est un *idéal* — notion **définie ci-dessous** (définition 1.12).

1.10 Idéaux et anneaux quotients

En théorie des groupes, on sait quoter : si H est un sous-groupe distingué d'un groupe G , le quotient G/H hérite d'une structure de groupe. Peut-on quoter un anneau par un sous-anneau ?

Soit A un anneau et $B \subseteq A$ un sous-anneau. Le quotient *additif* A/B est bien défini comme groupe. La question est : peut-on définir une multiplication sur A/B qui en fasse un anneau, avec la surjection canonique $\pi : A \rightarrow A/B$ comme morphisme d'anneaux ? Si oui, on est *forcé* de poser $\pi(a) \cdot \pi(b) = \pi(ab)$, ce qui exige que le produit soit **bien défini**. Or, si $a' = a + s$, $b' = b + t$ avec $s, t \in B$:

$$a'b' - ab = at + sb + st.$$

Le terme $st \in B$ (stabilité). Mais at et sb exigent que B *absorbe* la multiplication par tout élément de A : il faut $aB \subseteq B$ et $Ba \subseteq B$ pour **tout** $a \in A$. Cette condition est **strictement plus forte** que la stabilité interne ; par exemple, \mathbb{Z} est un sous-anneau de \mathbb{Q} , mais $\mathbb{Q} \cdot \mathbb{Z} \not\subseteq \mathbb{Z}$. On ne peut pas quoter \mathbb{Q} par \mathbb{Z} comme anneau.

Ce raisonnement mène à la bonne définition.

Définition 1.12 (Idéal). Soit A un anneau. Un sous-ensemble $I \subseteq A$ est un **idéal (bilatère)** de A , noté $I \trianglelefteq A$, si :

- (i) $(I, +)$ est un **sous-groupe** de $(A, +)$;
- (ii) pour tout $a \in A$ et tout $x \in I$, on a $ax \in I$ et $xa \in I$.

Si A est commutatif, la condition (ii) se simplifie en : pour tout $a \in A$ et tout $x \in I$, $ax \in I$.

On parle d'**idéal à gauche** si seule $ax \in I$ est exigée, et d'**idéal à droite** si seule $xa \in I$ l'est.

Remarque 1.8. Observons les différences entre sous-anneau et idéal :

Propriété	Sous-anneau	Idéal
Sous-groupe de $(A, +)$	oui	oui
Contient 1_A	oui	non (sauf si $I = A$)
Stable par \times interne	oui	oui
Absorbe \times par A	non requis	oui
Est un anneau en soi	oui	non (pas d'unité)
Permet de quoter	non	oui

En fait, si un idéal I contient 1_A , alors pour tout $a \in A$, $a = a \cdot 1_A \in I$, donc $I = A$. Ainsi les seuls idéaux qui sont des sous-anneaux sont les **idéaux triviaux** : $\{0\}$ et A .

Exemple 1.8. (a) **Idéaux de \mathbb{Z} .** Pour tout $n \in \mathbb{Z}$, l'ensemble $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ est un idéal de \mathbb{Z} . Ce sont les *seuls* (car \mathbb{Z} est principal ; cf. §1.12). En fait, on le savait déjà : les sous-groupes de \mathbb{Z} sont les $n\mathbb{Z}$ (théorème 0.1), et chacun est stable par multiplication externe.

(b) **Idéaux principaux.** Dans un anneau commutatif A , pour $a \in A$, l'ensemble

$$(a) \stackrel{\text{déf}}{=} aA = \{ax : x \in A\}$$

est un idéal, appelé l'**idéal engendré par a** ou **idéal principal**.

- (c) **Le noyau.** Si $f : A \rightarrow B$ est un morphisme d'anneaux, alors $\text{Ker } f$ est un idéal de A : c'est un sous-groupe additif, et si $f(x) = 0$ et $a \in A$, alors $f(ax) = f(a)f(x) = 0$.
- (d) **Idéaux de $\mathbb{K}[X]$.** Pour $P \in \mathbb{K}[X]$, $(P) = P \cdot \mathbb{K}[X]$ est un idéal. En semaine 5, on montrera que ce sont les seuls.

Exercice 8. Soit A un anneau commutatif et $a_1, \dots, a_n \in A$. Montrer que

$$(a_1, \dots, a_n) \stackrel{\text{déf}}{=} a_1A + \dots + a_nA = \left\{ \sum_{i=1}^n a_i x_i : x_i \in A \right\}$$

est un idéal de A , le plus petit contenant a_1, \dots, a_n .

Théorème 1.2 (Anneau quotient). *Soit A un anneau et $I \trianglelefteq A$ un idéal. L'ensemble quotient $A/I = \{a + I : a \in A\}$, muni des lois*

$$(a + I) + (b + I) = (a + b) + I, \quad (a + I) \cdot (b + I) = ab + I,$$

est un anneau, d'unité $1_A + I$. De plus, la surjection canonique $\pi : A \rightarrow A/I$, $a \mapsto a + I$, est un morphisme d'anneaux surjectif, de noyau I .

Démonstration. On sait déjà que $(A/I, +)$ est un groupe abélien et que l'addition est bien définie. Il reste à vérifier que la **multiplication** est bien définie. Soient $a' = a + s$ et $b' = b + t$ avec $s, t \in I$. Alors

$$a'b' = ab + at + sb + st.$$

Or $at \in I$ (car $t \in I$ et I absorbe la multiplication à gauche), $sb \in I$ (car $s \in I$ et I absorbe à droite), et $st \in I$ (car I est stable par produit interne). Donc $a'b' - ab \in I$, et la multiplication est bien définie.

Les axiomes d'anneau (associativité, distributivité) pour A/I se vérifient en passant aux représentants. L'unité est $1_A + I$. Enfin, $\pi(a + b) = \pi(a) + \pi(b)$, $\pi(ab) = \pi(a)\pi(b)$, et $\pi(1_A) = 1_A + I$, donc π est bien un morphisme d'anneaux. Son noyau est $\{a \in A : a + I = 0 + I\} = I$. \square

Exemple 1.9. (a) $\mathbb{Z}/n\mathbb{Z}$ est le quotient de \mathbb{Z} par l'idéal $n\mathbb{Z}$. C'est *exactement* la construction de la section 0.

- (b) $\mathbb{K}[X]/(X^2 + 1)$: dans ce quotient, la classe de X satisfait $\bar{X}^2 = -\bar{1}$. Si $\mathbb{K} = \mathbb{R}$, on obtient un anneau isomorphe à \mathbb{C} (via $\bar{X} \mapsto i$).
- (c) $\mathbb{K}[X]/(X^2)$: ici $\bar{X}^2 = 0$, donc \bar{X} est nilpotent. On obtient l'anneau des **nombres duaux** $\mathbb{K}[\varepsilon]/(\varepsilon^2)$, utilisé en géométrie algébrique pour formaliser les tangentes.

Le lien entre morphismes et idéaux est scellé par le théorème suivant, qui généralise le premier théorème d'isomorphisme des groupes.

Théorème 1.3 (Factorisation / Premier théorème d'isomorphisme). *Soit $f : A \rightarrow B$ un morphisme d'anneaux. Alors :*

- (i) $\text{Ker } f$ est un idéal de A ;
- (ii) $\text{Im } f$ est un sous-anneau de B ;
- (iii) f induit un **isomorphisme** d'anneaux

$$\bar{f} : A/\text{Ker } f \xrightarrow{\sim} \text{Im } f, \quad a + \text{Ker } f \mapsto f(a).$$

En d'autres termes, tout morphisme se factorise en

$$A \xrightarrow{\pi} A/\text{Ker } f \xrightarrow{\bar{f}} \text{Im } f \hookrightarrow B,$$

où π est surjectif, \bar{f} est un isomorphisme, et l'inclusion est injective.

Démonstration. Les points (i) et (ii) ont été établis (exemple 1.8(c) et proposition 1.6). Pour (iii) : on sait du théorème d'isomorphisme des groupes que \bar{f} est un isomorphisme de groupes abéliens. Il reste à vérifier la multiplicativité : $\bar{f}((a + \text{Ker } f)(a' + \text{Ker } f)) = \bar{f}(aa' + \text{Ker } f) = f(aa') = f(a)f(a') = \bar{f}(a + \text{Ker } f) \cdot \bar{f}(a' + \text{Ker } f)$. Et $\bar{f}(1_A + \text{Ker } f) = f(1_A) = 1_B$. \square

Exemple 1.10. Le morphisme d'évaluation $\text{ev}_i : \mathbb{R}[X] \rightarrow \mathbb{C}$, $P \mapsto P(i)$, est surjectif (car $a + bi = \text{ev}_i(a + bX)$ pour $a, b \in \mathbb{R}$). Son noyau est l'idéal $(X^2 + 1)$ (tout polynôme annulé par i est multiple de $X^2 + 1$ dans $\mathbb{R}[X]$). Le théorème de factorisation donne

$$\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}.$$

Proposition 1.7. Soit $f : A \rightarrow B$ un morphisme d'anneaux.

- (i) Si $J \trianglelefteq B$, alors $f^{-1}(J) \trianglelefteq A$.
- (ii) Si f est surjectif et $I \trianglelefteq A$, alors $f(I) \trianglelefteq B$.

Démonstration. Pour (i) : $f^{-1}(J)$ est un sous-groupe additif de A . Si $a \in A$ et $x \in f^{-1}(J)$, alors $f(ax) = f(a)f(x) \in J$, donc $ax \in f^{-1}(J)$.

Pour (ii) : $f(I)$ est un sous-groupe additif de B . Si $b \in B$ et $y \in f(I)$, écrivons $b = f(a)$ (surjectivité) et $y = f(x)$ avec $x \in I$. Alors $by = f(a)f(x) = f(ax)$ et $ax \in I$, donc $by \in f(I)$. \square

Remarque 1.9. Sans la surjectivité dans (ii), l'image directe d'un idéal n'est en général qu'un sous-groupe additif. Par exemple, l'inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$ envoie l'idéal $2\mathbb{Z}$ sur $2\mathbb{Z} \subset \mathbb{Q}$, qui n'est pas un idéal de \mathbb{Q} (car $\frac{1}{2} \cdot 2 = 1 \notin 2\mathbb{Z}$, mais la condition est que $\mathbb{Q} \cdot 2\mathbb{Z} \subseteq 2\mathbb{Z}$).

1.11 Idéaux premiers et maximaux

Dans cette section, tous les anneaux sont supposés commutatifs.

La structure d'un anneau commutatif est largement déterminée par les propriétés de ses idéaux. Deux classes d'idéaux jouent un rôle central.

Définition 1.13 (Idéal premier). Soit A un anneau commutatif. Un idéal $\mathfrak{p} \subsetneq A$ est dit **premier** si :

$$\forall a, b \in A, \quad ab \in \mathfrak{p} \implies a \in \mathfrak{p} \text{ ou } b \in \mathfrak{p}.$$

Proposition 1.8. Un idéal $\mathfrak{p} \subsetneq A$ est premier si et seulement si A/\mathfrak{p} est intègre.

Démonstration. Par définition, A/\mathfrak{p} est intègre si et seulement si $(a + \mathfrak{p})(b + \mathfrak{p}) = \mathfrak{p}$ implique $a + \mathfrak{p} = \mathfrak{p}$ ou $b + \mathfrak{p} = \mathfrak{p}$, c'est-à-dire $ab \in \mathfrak{p} \implies a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$. \square

Exemple 1.11. (a) Dans \mathbb{Z} , les idéaux premiers sont (0) et (p) pour p premier. En effet, $\mathbb{Z}/p\mathbb{Z}$ est intègre si et seulement si p est premier (exercice 5).

(b) Dans $\mathbb{K}[X]$, l'idéal (P) est premier si et seulement si P est irréductible (ou $P = 0$).

Définition 1.14 (Idéal maximal). Un idéal $\mathfrak{m} \subsetneq A$ est dit **maximal** s'il n'existe aucun idéal J tel que $\mathfrak{m} \subsetneq J \subsetneq A$.

Proposition 1.9. Un idéal $\mathfrak{m} \subsetneq A$ est maximal si et seulement si A/\mathfrak{m} est un corps.

Démonstration. (\Rightarrow) Soit $a \notin \mathfrak{m}$. L'idéal $\mathfrak{m} + (a) = \mathfrak{m} + aA$ contient strictement \mathfrak{m} , donc par maximalité $\mathfrak{m} + (a) = A$. Il existe donc $m \in \mathfrak{m}$ et $x \in A$ tels que $m + ax = 1$. Ainsi $\bar{a} \cdot \bar{x} = \bar{1}$ dans A/\mathfrak{m} .

(\Leftarrow) Si A/\mathfrak{m} est un corps et $\mathfrak{m} \subsetneq J$, alors J/\mathfrak{m} est un idéal non nul de A/\mathfrak{m} , donc contient un inversible, donc $J/\mathfrak{m} = A/\mathfrak{m}$, d'où $J = A$. \square

Corollaire 1.2. Tout idéal maximal est premier.

Démonstration. Si \mathfrak{m} est maximal, alors A/\mathfrak{m} est un corps, donc intègre (proposition 1.5), donc \mathfrak{m} est premier. \square

Remarque 1.10. La réciproque est fausse : (0) est un idéal premier de \mathbb{Z} (car \mathbb{Z} est intègre), mais il n'est pas maximal ($\mathbb{Z}/0 \cong \mathbb{Z}$ n'est pas un corps).

1.12 Panorama : anneaux classifiés par leurs idéaux

En algèbre commutative et en théorie des nombres, les anneaux se distinguent par les propriétés de leur ensemble d'idéaux. Voici une vue d'ensemble des classes principales, que nous développerons dans les semaines suivantes.

Classe	Condition sur les idéaux	Exemples
Euclidien	admet une division euclidienne	$\mathbb{Z}, \mathbb{K}[X], \mathbb{Z}[i]$
Principal	tout idéal est principal	$\mathbb{Z}, \mathbb{K}[X], \mathbb{Z}[i]$
Factoriel	factorisation unique en irréductibles	$\mathbb{Z}, \mathbb{K}[X], \mathbb{Z}[X]$
De Dedekind	tout idéal est produit d'idéaux premiers	$\mathbb{Z}[\sqrt{-5}]$

Les implications sont :

$$\text{Euclidien} \implies \text{Principal} \implies \text{Factoriel} \implies \text{Intègre}.$$

Les anneaux de Dedekind forment une classe à part, cruciale en théorie algébrique des nombres : dans $\mathbb{Z}[\sqrt{-5}]$, on perd la factorisation unique en éléments irréductibles ($6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$), mais on la récupère au niveau des *idéaux*.

Exemple non commutatif : idéaux de $M_n(\mathbb{K})$.

L'anneau des matrices $M_n(\mathbb{K})$ offre un contraste saisissant avec le cas commutatif.

Théorème 1.4. Soit \mathbb{K} un corps et $n \geq 1$. Les seuls idéaux bilatères de $M_n(\mathbb{K})$ sont $\{0\}$ et $M_n(\mathbb{K})$.

Démonstration. Soit $I \neq \{0\}$ un idéal bilatère de $M_n(\mathbb{K})$, et soit $M \in I$, $M \neq 0$. Il existe des indices i_0, j_0 tels que $M_{i_0 j_0} \neq 0$. Désignons par E_{ij} la matrice élémentaire ayant 1 en position (i, j) et 0 ailleurs. Alors pour tous i, j :

$$E_{i,i_0} \cdot M \cdot E_{j_0,j} = M_{i_0 j_0} E_{ij}.$$

Comme $M_{i_0 j_0} \neq 0$ et I est bilatère, on a $M_{i_0 j_0} E_{ij} \in I$, donc $E_{ij} \in I$ (en divisant par le scalaire). Toute matrice étant combinaison linéaire des E_{ij} , on conclut $I = M_n(\mathbb{K})$. \square

Remarque 1.11. Un anneau dont les seuls idéaux bilatères sont $\{0\}$ et lui-même est dit **simple**. Le théorème affirme que $M_n(\mathbb{K})$ est simple. En conséquence, tout morphisme d'anneaux $f : M_n(\mathbb{K}) \rightarrow B$ est soit le morphisme nul (si B est nul), soit injectif (car $\text{Ker } f$ est un idéal bilatère).