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

Semaine 1 : Arithmétique dans $\mathbb{Z}$ et naissance des anneaux

Gönenç Onay
Université Galatasaray

Printemps 2026

1 Le groupe $(\mathbb{Z}, +)$ et ses sous-groupes

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

L'ensemble $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ 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.

1.2 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 1.1 (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.

Réciproquement, soit $a \in H$. La division euclidienne (théorème 2.1 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 $a \in n\mathbb{Z}$. □

Remarque 1.1. Notons que ce théorème utilise fondamentalement la division euclidienne (théorème 2.1), donc *au-delà* de l'addition, pour établir un résultat portant sur la structure additive $(\mathbb{Z}, +)$.

1.3 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 1.1, il existe un unique $d \in \mathbb{N}$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

Définition 1.1 (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 $d \mid b$. Réciproquement, 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 1.2. On écrit $\gcd(a,b)$ pour la clarté, et $a \wedge b$ quand la concision l'exige. Les deux notations sont standard et seront utilisées librement.

2 Divisibilité et théorèmes fondamentaux

2.1 Divisibilité

Définition 2.1. Soient $a, b \in \mathbb{Z}$. On dit que a **divise** b, et on écrit $a \mid b$, s'il existe $k \in \mathbb{Z}$ tel que $b = ka$. Autrement dit, $b \in a\mathbb{Z}$.

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

(i) $a \mid 0$ pour tout $a \in \mathbb{Z}$;

(ii) $1 \mid a$ pour tout $a \in \mathbb{Z}$;

(iii) si $a \mid b$ et $b \mid c$, alors $a \mid c$ (transitivité) ;

(iv) si $a \mid b$ et $a \mid c$, alors $a \mid (bu + cv)$ pour tous $u, v \in \mathbb{Z}$ (les multiples de a forment un sous-groupe, à savoir $a\mathbb{Z}$).

2.2 Division euclidienne

Théorème 2.1 (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 $r = r'$. □

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

2.3 Algorithme d'Euclide

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

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

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 $\gcd(a,b)$.

Exemple 2.1. Calculons $\gcd(120, 44)$:

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

Donc $\gcd(120, 44) = 4$.

2.4 Théorème de Bézout

Théorème 2.2 (Bézout)**.** *Soient $a, b \in \mathbb{Z}$. Il existe $u, v \in \mathbb{Z}$ tels que*

$$au + bv = \gcd(a, b).$$

Démonstration. C'est une reformulation immédiate de la définition 1.1 : $\gcd(a, b)$ est le générateur positif de $a\mathbb{Z} + b\mathbb{Z}$, donc il s'écrit $au + bv$ pour certains $u, v \in \mathbb{Z}$. □

Remarque 2.1. On obtient les coefficients u, v en « remontant » l'algorithme d'Euclide.

Corollaire 2.1 (Lemme de Gauss)**.** *Soient $a, b, c \in \mathbb{Z}$. Si $a \mid bc$ et $\gcd(a, b) = 1$, 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 $a \mid c$. □

2.5 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

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

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

Exercice 1. Montrer que la congruence est aussi compatible avec la multiplication : si $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$, alors $ab \equiv a'b' \pmod{n}$. En déduire que $\mathbb{Z}/n\mathbb{Z}$ est muni d'une multiplication bien définie.

2.6 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 $\pi : G \twoheadrightarrow G/H$ induit une **bijection croissante**

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

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 2.1 (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 2.2. 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 $\{0\}$.

3 Ensembles munis de deux opérations

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.

3.1 Les matrices $\mathrm{M}_n(\mathbb{R})$

Fixons $n \geq 1$. L'ensemble $\mathrm{M}_n(\mathbb{R})$ 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 $(\mathrm{M}_n(\mathbb{R}), +)$ 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 3.1. 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).

3.2 Les polynômes $\mathbb{R}[X]$

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

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_d X^d, \qquad a_i \in \mathbb{R},$$

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 frappante et 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 2 se transpose.

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

3.3 Tableau comparatif

Propriété	$\mathbb{Z}$	$\mathbb{Z}/n\mathbb{Z}$	$\mathbb{R}[X]$	$\mathrm{M}_n(\mathbb{R})$
$(E, +)$ 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.

4 Anneaux : définition abstraite

Définition 4.1 (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 $1_A \cdot a = a \cdot 1_A = a$ 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 4.1. 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 4.1 (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. □

4.1 Premiers exemples

Exemple 4.1. Les exemples fondamentaux d'anneaux :

(a) $(\mathbb{Z}, +, \times)$: anneau commutatif, intègre (cf. semaine 2).

(b) $(\mathbb{Z}/n\mathbb{Z}, +, \times)$: anneau commutatif à n éléments.

(c) $(\mathrm{M}_n(\mathbb{K}), +, \times)$ pour un corps $\mathbb{K}$: anneau non commutatif si $n \geq 2$.

(d) $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$: anneaux commutatifs (et même des corps).

(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. Vérifier que si $(A, +, \times)$ est un anneau, alors pour tout $n \geq 1$, $\mathrm{M}_n(A)$ est un anneau (commutatif si et seulement si $n = 1$ et A commutatif).

Exercice 3. 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 2.1).