北航中法工程师学院
Centrale Pékin

Algèbre 2

École Centrale de Pékin

Cours de mathématiques du cycle préparatoire

9 mars 2022

Table des matières

Avant-propos

Vous trouverez au fil de ce cours différents symboles :

- Le symbole "  ", situé dans la marge, signifie que le point correspondant est un point délicat (il s'agit d'un *virage dangereux*).
- Le symbole "□" est un marqueur signifiant la fin d'une démonstration.
-  Ce cours peut comporter des fautes de frappe, des coquilles, voire des erreurs d'argumentation. Ainsi, il faut toujours être vigilant lorsque vous suivez et que vous travaillez ce cours. Vérifier que les exemples sont justes et que les preuves n'ont pas de fautes est un exercice très utile (et indispensable) en mathématiques pour comprendre les notions et comprendre leurs utilisations.

Vous trouverez aussi des notations mathématiques :

$\mathcal{R}$	une relation binaire
$\equiv$	pour certaines relations d'équivalence
$x \preccurlyeq y$, $x \leq y$	pour une relation d'ordre
$\mathbb{N}$	l'ensemble des entiers naturels
$\mathbb{Z}$	l'ensemble des entiers relatifs
$\mathbb{Q}$	l'ensemble des nombres rationnels
$\mathbb{R}$	l'ensemble des entiers relatifs
$\mathbb{C}$	l'ensemble des nombres complexes
$(G, \times)$	un groupe
e_G	l'élément neutre d'un groupe G
g^{-1}	l'inverse dans un groupe d'un élément g
$\langle g \rangle$	le sous-groupe de G engendré par g
$(H, +)$	un groupe commutatif (parfois)
$a \equiv b \bmod n$	la relation de congruence modulo n (n divise $b - a$)
$\mathbb{Z}/n\mathbb{Z}$	l'ensemble des classes d'équivalence pour la relation de congruence modulo n
$(A, +, \times)$	un anneau
0_A	l'élément nul d'un anneau A pour l'addition $+$
1_A	l'élément unitaire d'un anneau A pour la multiplication $\times$
a^{-1}	l'inverse dans A d'un élément a inversible
I	un idéal de l'anneau A
$\langle a \rangle$	l'idéal de A engendré par a
$(\mathbb{Z}/n\mathbb{Z}, +, \times)$	l'anneau des classes d'équivalence modulo n
$\mathbb{K}$	un corps (en général $\mathbb{R}, \mathbb{C}$ ou $\mathbb{Q}$)
$\mathbb{Z}/p\mathbb{Z}$	le corps à p éléments, avec p premier
$Frac(A)$	le corps des fractions d'un anneau intègre A
$\mathbb{K}[X]$	l'anneau des polynômes à une indéterminée à coefficients dans $\mathbb{K}$
$\mathbb{K}(X)$	le corps des fractions rationnelles à coefficients dans $\mathbb{K}$

Chapitre 1 Relations binaires

Table des matières du chapitre

On étudie dans ce chapitre la notion de relation. Sur un ensemble E, on veut souvent comparer les élément ou les regrouper. (l'âge des gens, le pays d'origine des gens, l'ordre des mots dans le disctionnaire,...). On définit la notion de relation en mathématiques.

1.1 Premières définitions

Définition 1
Soient E et F deux ensembles. Soit G une patrie de $E \times F$.
On appelle **relation binaire** \关系\ le triplet $\mathcal{R} = (E, F, G)$.
Si $(x, y) \in G$, on dit que x **est en relation avec** y, et on le note $x\mathcal{R}y$.
On parle de la relation $\mathcal{R}$.

On a donc $G = \{(x, y) \in E \times F \mid x\mathcal{R}y\}$.

L'ordre dans un couple est important. On peut avoir $x\mathcal{R}y$ mais pas $y\mathcal{R}x$.

Remarque 2 — *On peut définir les fonctions $f : E \to F$ avec des relations binaires : pour tout $(x, y) \in E \times F$, on a $x\mathcal{R}y$ si et seulement si $y = f(x)$.*
Le fait d'associer à chaque élément $x \in E$ une image $f(x) \in F$ permet de construire une relation.

Dans la suite du chapitre, on s'intéresse aux relations sur E et E. Ce sont les relations les plus utiles en mathématiques.
Lorsque $E = F$, la relation $\mathcal{R}$ est appelée **relation binaire sur** E.

On note souvent une relation $\mathcal{R}$ avec un symbole $\equiv$, $\leq$, $\sim$, $\subset$...

Exemples 3 *Donnons quelques exemples de relations binaires sur un ensemble :*

- *la relation d'égalité $=$ sur E,*
- *les relations d'inégalité $\leq$, $<$ sur $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ ou $\mathbb{N}$,*
- *la relation d'inclusion $\subset$ sur $\mathcal{P}(E)$ (ensemble des parties de E),*
- *la relation de comparaison $\leq$ sur $Fonct(E, \mathbb{R})$ (fonctions de E dans $\mathbb{R}$), définie par $f \leq g$ si $f(x) \leq g(x)$ $\forall x \in E$,*
- *la relation de divisibilité $\mid$ sur $\mathbb{Z}$, définie par $m \mid n$ s'il existe $k \in \mathbb{Z}$ tel que $n = mk$.*
- *pour tout $n \in \mathbb{N}$, la relation de congruence modulo n sur $\mathbb{Z}$, notée $\equiv \mod n$, définie par $a \equiv b \mod n$ s'il existe $k \in \mathbb{Z}$ tel que $a = b + kn$.*
- *pour tout $\alpha \in \mathbb{R}$, la relation de congruence modulo α sur $\mathbb{R}$, notée $\equiv \mod \alpha$, définie par $a \equiv b \mod \alpha$ s'il existe $k \in \mathbb{Z}$ tel que $a = b + k\alpha$.*
- *la relation « avoir le même signe » sur $\mathbb{R}^*$.*

On définit des propriétés intéressantes pour les relations.

Définition 4
Soit E un ensemble. Soit $\mathcal{R}$ une relation binaire sur E.

- $\mathcal{R}$ est dite **réflexive** \自反性\ si : pour tout $x \in E$, on a $x\mathcal{R}x$,
- $\mathcal{R}$ est dite **symétrique** \对称性\ si : pour tout $(x, y) \in E^2$, si $x\mathcal{R}y$ alors $y\mathcal{R}x$,
- $\mathcal{R}$ est dite **antisymétrique** \反对称性\ si : pour tout $(x, y) \in E^2$, si $x\mathcal{R}y$ et $y\mathcal{R}x$ alors $x = y$,
- $\mathcal{R}$ est dite **transitive** \传递性\ si : pour tout $(x, y, z) \in E^3$, si $x\mathcal{R}y$ et $y\mathcal{R}z$ alors $x\mathcal{R}z$.

Exemples 5

- *La relation d'égalité $=$ sur E est réflexive, symétrique, antisymétrique et transitive.*
  On remarque qu'une relation peut donc être symétrique et antisymétrique.
- *La relation $\leq$ sur $\mathbb{R}$ est réflexive, antisymétrique et transitive.*
  Elle n'est pas symétrique car par exemple $2 \leq 3$ mais $3 \not\leq 2$.
- *La relation $<$ sur $\mathbb{R}$ est symétrique et transitive.*
  Elle n'est ni réflexive, ni antisymétrique. Par exemple, $1 \not< 1$.
- *La relation de divisibilité sur $\mathbb{Z}$ est réflexive et transitive.*
  Elle n'est ni symétrique, ni antisymétrique. En effet, on a $1|2$ mais $2 \nmid 1$, et $1|-1$ et $-1|1$ mais $1 \neq -1$.
- *La relation d'inclusion $\subset$ sur $\mathcal{P}(E)$ est réflexive, antisymétrique et transitive.*
  Elle n'est pas symétrique car par exemple $\{1\} \subset \{1, 2\}$ mais $\{1, 2\} \not\subset \{1\}$.
- *La relation « avoir le même signe » sur $\mathbb{R}^*$ est réflexive, symétrique et transitive.*
  Elle n'est pas antisymétrique car par exemple, $1\mathcal{R}2$ et $2\mathcal{R}1$ mais $1 \neq 2$.

Nous allons étudier deux grandes familles de relations.

1.2 Relations d'équivalence

La première famille est celle des relations d'équivalence.
Une telle relation permet d'identifier des éléments de E qui sont en relation muuelle, pour regarder les ensembles d'éléments qui sont en relation. Par exemple, la nationalité.

1.2.1 Définition et exemples

Définition 6
Soit E un ensemble et $\mathcal{R}$ une relation binaire sur E.
On dit que $\mathcal{R}$ est une **relation d'équivalence** \等价关系\ sur E si $\mathcal{R}$ est réflexive, symétrique et transitive.

Une relation d'équivalence est souvent notée $\equiv$ ou $\sim$. On parle d'éléments de E "équivalents", "semblables".

Exemples 7

- *La relation d'égalité $=$ sur E est une relation d'équivalence.*
- *La relation « avoir le même signe » sur $\mathbb{R}^*$ est une relation d'équivalence.*
- *Pour tout $n \in \mathbb{N}$, la relation de congruence modulo n sur $\mathbb{Z}$ est une relation d'équivalence.*
  ***Preuve** — Soit $n \in \mathbb{N}$.*
  - ***Réflexivité :** Soit $p \in \mathbb{Z}$. On a $p = p + 0 \times n$ et $0 \in \mathbb{Z}$ donc $p \equiv p \bmod n$. Donc la relation de congruence modulo n est réflexive.*
  - ***Symétrie :** Soit $(p, q) \in \mathbb{Z}^2$. Supposons que $p \equiv q \bmod n$. Alors il existe $k \in \mathbb{Z}$ tel que $p = q + kn$. Donc $q = p - kn = p + (-k)n$ et $-k \in \mathbb{Z}$. Donc $q \equiv p \bmod n$. Donc la relation de congruence modulo n est symétrique.*
  - ***Transitivité :** Soit $(p, q, r) \in \mathbb{Z}^3$. Supposons que $p \equiv q \bmod n$ et $q \equiv r \bmod n$. Montrons que $p \equiv r \bmod n$.*
    Il existe $k_1 \in \mathbb{Z}$ tel que $p = q + k_1 n$ et il existe $k_2 \in \mathbb{Z}$ tel que $q = r + k_2 n$. Donc $p = r + k_2 n + k_1 n = r + (k_1 + k_2)n$ et $(k_1 + k_2) \in \mathbb{Z}$. Donc $p \equiv r \bmod n$. Donc la relation de congruence modulo n est transitive.

  Cela termine la preuve. □
- *Pour tout $\alpha \in \mathbb{R}$, la relation de congruence modulo α sur $\mathbb{R}$ est une relation d'équivalence.*
  ***Preuve** — Identique à la preuve précédente.* □
- *Si $(A_i)_{i \in I}$ est une partition de E ($A_i \cap A_j = \emptyset$ si $i \neq j$, et $\cup_{i \in I} A_i = E$), la relation d'appartenance à un sous-ensemble A_i est une relation d'équivalence. ($x\mathcal{R}y$ si $\exists i \in I$ tel que $x, y \in A_i$)*

Remarque 8 — *Comme $\mathcal{R}$ est symétrique, on a $x\mathcal{R}y$ si et seulement si $y\mathcal{R}x$.*

1.2.2 Classes d'équivalence et ensemble quotient

Définition 9
Soient E un ensemble et $\mathcal{R}$ une relation d'équivalence sur E. Soit x un élément de E.
On appelle **classe d'équivalence** de x \x的等价类\ pour la relation $\mathcal{R}$ (ou plus simplement classe de x) l'ensemble des éléments y de E qui sont en relation avec x :

$$\mathrm{Cl}(x) = \{y \in E \text{ tels que } x\mathcal{R}y\}.$$

On la note $\mathrm{Cl}(x)$ ou $\overline{x}$.

Exemples 10

- *La classe d'équivalence de* 1 *pour la relation d'équivalence « avoir le même signe » sur* $\mathbb{R}^*$ *est l'ensemble des nombres réels non nuls de même signe que* 1*, c'est-à-dire l'ensemble des nombres réels strictement positifs :* $\mathrm{Cl}(1) = \mathbb{R}_+^*$.
- *Soit* $n \in \mathbb{N}$*. Soit* $r \in \mathbb{Z}$*. La classe d'équivalence de* r *pour la relation de congruence modulo* n *dans* $\mathbb{Z}$ *est*

$$\begin{aligned}\mathrm{Cl}(r) &= \{p \in \mathbb{Z} \mid p \equiv r \bmod n\}\\ &= \{p \in \mathbb{Z} \mid \exists k \in \mathbb{Z}, p = r + kn\}\\ &= \{r + kn \mid k \in \mathbb{Z}\}\\ &= n\mathbb{Z} + r\end{aligned}$$

Proposition 11
Soient E un ensemble et $\mathcal{R}$ une relation d'équivalence sur E.
Pour tout $(x, y) \in E^2$, on a $\mathrm{Cl}(x) = \mathrm{Cl}(y)$ si et seulement si $x\mathcal{R}y$.

Preuve — Soit $(x, y) \in E^2$.

▷ Supposons que $\mathrm{Cl}(x) = \mathrm{Cl}(y)$.
Comme $\mathcal{R}$ est réflexive, on a $y\mathcal{R}y$ donc $y \in \mathrm{Cl}(y)$. Or, par hypothèse, $\mathrm{Cl}(x) = \mathrm{Cl}(y)$, donc $y \in \mathrm{Cl}(x)$. Donc, par définition d'une classe d'équivalence, on a $x\mathcal{R}y$.

◁ Supposons que $x\mathcal{R}y$. Soit $z \in \mathrm{Cl}(x)$. Alors $x\mathcal{R}z$.
Comme $x\mathcal{R}y$, on a, par symétrie de $\mathcal{R}$, $y\mathcal{R}x$. Donc par transitivité de $\mathcal{R}$, comme $y\mathcal{R}x$ et $x\mathcal{R}z$, on a $y\mathcal{R}z$. Donc $z \in \mathrm{Cl}(y)$. D'où $\mathrm{Cl}(x) \subset \mathrm{Cl}(y)$.
Par symétrie des rôles de x et y, on a de la même façon $\mathrm{Cl}(y) \subset \mathrm{Cl}(x)$. Ainsi, on obtient $\mathrm{Cl}(x) = \mathrm{Cl}(y)$.

□

Notons donc que si $y \in \mathrm{Cl}(x)$ alors $\mathrm{Cl}(y) = \mathrm{Cl}(x)$.

Définition 12
Soient E un ensemble et $\mathcal{R}$ une relation d'équivalence sur E. Soit C une classe d'équivalence pour $\mathcal{R}$.
On appelle **représentant** de la classe d'équivalence C tout élément x de C.
On a alors $C = Cl(x)$.

Exemple 13 — *Nous avons vu que* $\mathbb{R}_+^*$ *est une classe d'équivalence (celle de* 1*) pour la relation d'équivalence « avoir le même signe » sur* $\mathbb{R}^*$.
Tout élément de $\mathbb{R}_+^*$ *est un représentant de cette classe. Des représentants de cette classe sont donc par exemple* 1*, ou* π*, ou* $\sqrt{2}$*... Ainsi,* $\mathbb{R}_+^* = \mathrm{Cl}(1) = \mathrm{Cl}(\pi) = \mathrm{Cl}(\sqrt{2})$...

Proposition 14
Soient E un ensemble et $\mathcal{R}$ une relation d'équivalence sur E.
L'ensemble des classes d'équivalence de E forme une partition de E, c'est-à-dire :

- Elles sont non vides,
- Elle sont deux à deux disjointes,
- Leur réunion est égale à l'ensemble E.

Preuve —

- Par définition, une classe d'équivalence C est toujours la classe d'équivalence d'un élément x de E : $C = \mathrm{Cl}(x)$.
  Comme $x\mathcal{R}x$ par réflexivité de $\mathcal{R}$, on a $x \in Cl(x) = C$ et C est non vide.
- Soient C_1 et C_2 deux classes d'équivalence. Supposons $C_1 \cap C_2 \neq \emptyset$. Soient x_1 un représentant de C_1 et x_2 un représentant de C_2. Ainsi, $C_1 = \mathrm{Cl}(x_1)$ et $C_2 = \mathrm{Cl}(x_2)$.
  Par hypothèse, il existe $x \in C_1 \cap C_2$. En particulier, $x \in C_1$ donc $x\mathcal{R}x_1$ et $x \in C_2$ donc $x\mathcal{R}x_2$. Par symétrie et transitivité de $\mathcal{R}$, $x_1\mathcal{R}x_2$. Donc d'après la proposition précédente, $\mathrm{Cl}(x_1) = \mathrm{Cl}(x_2)$, soit $C_1 = C_2$.
  Ainsi, deux classes sont soit égales soit disjointes.

- Soit $x \in E$. Comme on a $x \in \mathrm{Cl}(x)$, x appartient à la réunion des classes d'équivalence pour $\mathcal{R}$. Donc E est inclus dans la réunion des classes d'équivalence de $\mathcal{R}$.
  L'inclusion réciproque est évidente car une classe d'équivalence est une partie de E. Donc la réunion est égale à E.

Ainsi, l'ensemble des classes d'équivalence de E forme une partition de E. □

Remarque 15 — *Ainsi, toute relation d'équivalence sur E donne une partition de E, et toute partition de E donne une relation d'équivalence sur E.*
Chaque relation d'équivalence sur E correspond à une partition de E. (penser par exemple au pays de naissance, cela partionne l'ensemble des êtres humains)

Exemples 16

- *La relation « avoir le même signe » sur $\mathbb{R}^*$ a exactement deux classes d'équivalence : $\mathbb{R}_+^*$ et $\mathbb{R}_-^*$. Ces deux classes d'équivalence forment bien une partition de $\mathbb{R}^*$.*

  Preuve — *Soit C une classe d'équivalence et considérons x un représentant de C. Si x est positif, alors $C = \mathrm{Cl}(x) = \mathbb{R}_+^*$. Si x est négatif, alors $C = \mathrm{Cl}(x) = \mathbb{R}_-^*$. Les classes $\mathbb{R}_+^*$ et $\mathbb{R}_-^*$ sont bien sûr distinctes.* □
- *Pour tout $n \in \mathbb{N}$, la relation de congruence modulo n sur $\mathbb{Z}$ possède exactement n classes d'équivalence : les ensembles $n\mathbb{Z} + r = \{nk + r \mid k \in \mathbb{Z}\}$ avec $r \in \{0, \dots, n-1\}$. On les note souvent $\overline{0}$, $\overline{1}$, …, $\overline{n-1}$.*
  On a choisi comme représentant des différentes classes les entiers 0, 1, …, $n-1$.

  Preuve — *Soit C une classe d'équivalence et considérons p un représentant de C. Comme $p \in \mathbb{Z}$, on peut effectuer la division euclidienne de p par n. Il existe donc $k \in \mathbb{Z}$ et $r \in \{0, \dots, n-1\}$ tel que $p = kn + r$. Donc $p \equiv r \bmod n$.*
  Donc $C = \mathrm{Cl}(r) = n\mathbb{Z} + r$.
  De plus, les n classes d'équivalence $n\mathbb{Z} + r$ où $r \in \{0, \dots, n-1\}$ deux à deux disjointes car si r_1 et r_2 sont deux éléments distincts de $\{0, \dots, n-1\}$ alors r_1 n'est pas congru à r_2 modulo n. □

Définition 17
Soient E un ensemble et $\mathcal{R}$ une relation d'équivalence sur E.
L'ensemble des classes d'équivalence de E pour la relation $\mathcal{R}$ s'appelle **l'ensemble quotient de E par $\mathcal{R}$**.
On le note $E/\mathcal{R}$. C'est un sous-ensemble de $\mathcal{P}(E)$ (ensemble des parties de E).

Exemples 18

- *L'ensemble quotient de $\mathbb{R}^*$ par la relation « avoir le même signe » est l'ensemble $\{\mathbb{R}_-^*, \mathbb{R}_+^*\}$.*
- *L'ensemble quotient de E par la relation d'égalité $=$ est l'ensemble $\{\{x\}, x \in E\}$.*
- *Soit $n \in \mathbb{Z}$. L'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n est l'ensemble $\{n\mathbb{Z}, n\mathbb{Z} + 1, \dots, n\mathbb{Z} + n - 1\} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$. On note cet ensemble $\mathbb{Z}/n\mathbb{Z}$.*
- *Pour $f : E \to F$, la relation « avoir la même image par f » est une relation d'équivalence. L'ensemble quotient de E par cette relation d'équivalence est $\{f^{-1}(\{y\}), y \in Im(f)\}$. (A vérifier.)*

Les relations d'équivalence servent à étudier les éléments d'un ensemble E de façon simplifiée.
Par exemple, la congruence modulo n sert à étudier les entiers de $\mathbb{Z}$ seulement selon le reste de leur division euclidienne par n. La relation « signe » sur $\mathbb{R}$ étudie les nombres réels selon leur signe.
La relation « avoir le même rang » chez les matrices $n \times p$ étudie les matrices selon leur rang (ou les familles de p vecteurs de $\mathbb{K}^n$ selon leur rang).

1.3 Relations d'ordre et ensembles ordonnés

La deuxième grande famille de relations est celle des relations d'ordre. Une telle relation permet de hiérarchiser, d'ordonner les éléments.
Cela généralise l'ordre sur les nombres entiers/réels, ou l'ordre des mots dans le dictionnaire.

1.3.1 Définitions et exemples

Définition 19
Soient E un ensemble et $\mathcal{R}$ une relation binaire sur E.
On dit que $\mathcal{R}$ est une **relation d'ordre** \偏序\ sur E si $\mathcal{R}$ est réflexive, antisymétrique et transitive.
Dans ce cas, on dit que $(E, \mathcal{R})$ est un **ensemble ordonné**.

Remarques 20 *Une relation d'ordre est souvent notée $\preccurlyeq$, ou $\leq$,….*
Les écritures $x \preccurlyeq y$ et $y \succcurlyeq x$ sont équivalentes.

Souvent, $x \preccurlyeq y$ se lit « x plus petit que y » mais ce n'est qu'une convention.

La notation $x \preccurlyeq y \preccurlyeq z$ signifie $x \preccurlyeq y$ et $y \preccurlyeq z$.

Exemples 21

- *La relation $\leq$ sur $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ ou $\mathbb{N}$ est une relation d'ordre.*
- *La relation d'inclusion $\subset$ sur $\mathcal{P}(E)$ est une relation d'ordre.*
- *La relation $\leq$ sur $Fonct(E, \mathbb{R})$ (fonctions de E dans $\mathbb{R}$) est une relation d'ordre.*
- *La relation $<$ n'est pas une relation d'ordre sur $\mathbb{R}$ car elle n'est pas réflexive. En effet, $1 \not< 1$.*
- *La relation sur $\mathbb{C}$: $z\mathcal{R}z'$ si $|z| \leq |z'|$, n'est pas une relation d'ordre car elle n'est pas antisymétrique. On a $-1\mathcal{R}1$ et $1\mathcal{R}-1$ mais $1 \neq -1$.*
- *La relation de divisibilité sur $\mathbb{N}$ est une relation d'ordre.*
  ***Preuve** —*
  - ***Réflexivité :** Pour tout $n \in \mathbb{N}$, on a $n = n \times 1$ donc $n|n$. Donc la relation de divisibilité sur $\mathbb{N}$ est réflexive.*
  - ***Antisymétrie :** Soit $(p, q) \in \mathbb{N}^2$. Supposons que $p|q$ et $q|p$. Alors il existe $k_1 \in \mathbb{N}$ tel que $p = k_1 \times q$ et il existe $k_2 \in \mathbb{N}$ tel que $q = k_2 \times p$. Donc $p = k_1 \times k_2 \times p$. Donc $p(1 - k_1k_2) = 0$.*
    Si $p = 0$ alors $q = k_2 \times p = k_2 \times 0 = 0$ donc $p = q = 0$.
    Sinon, $k_1k_2 = 1$ et comme k_1 et k_2 sont des entiers naturels, on a $k_1 = k_2 = 1$. Donc $p = k_1 \times q = q$. Donc la relation de divisibilité sur $\mathbb{N}$ est antisymétrique.
  - ***Transitivité :** Soit $(m, n, p) \in \mathbb{N}^3$ tel que $m|n$ et $n|p$. Montrons que $m|p$. Il existe $k_1 \in \mathbb{N}$ tel que $n = k_1 \times n$ et il existe $k_2 \in \mathbb{N}$ tel que $p = k_2 \times n$. Donc $p = k_2 \times k_1 \times m$ et $k_1 \times k_2 \in \mathbb{N}$. Donc $m|p$. Donc la relation de divisibilité sur $\mathbb{N}$ est transitive.*

  Ainsi, la relation de divisibilité sur $\mathbb{N}$ est une relation d'ordre. □
- *La relation de divisibilité sur $\mathbb{Z}$ n'est pas une relation d'ordre car elle n'est pas antisymétrique.*

Remarque 22 — *Dans $\mathbb{R}$ muni de la relation d'ordre usuelle $\leq$, on peut comparer deux à deux tous les éléments (on a toujours $x \leq y$ ou $y \leq x$).*
Ce n'est pas le cas pour toutes les relations d'ordre, par exemple pour l'inclusion sur $\mathcal{P}(E)$.
Dans une relation d'ordre $\mathcal{R}$, deux éléments de E ne sont pas toujours comparables.
On fait donc la définition suivante.

Définition 23
Soit $(E, \preccurlyeq)$ un ensemble ordonné.

- On dit que l'ordre $\preccurlyeq$ est **total** \全序\ si, pour tout $(x, y) \in E^2$, on a $x \preccurlyeq y$ ou $y \preccurlyeq x$.
  On dit que $(E, \preccurlyeq)$ est un **ensemble totalement ordonné**.
- Sinon, on dit que l'ordre est **partiel** et l'ensemble $(E, \preccurlyeq)$ est appelé **ensemble partiellement ordonné**.

Quand on a $x \preccurlyeq y$ ou $y \preccurlyeq x$, on dit que les éléments x et y sont **comparables**.

Exemples 24

- *L'ensemble $(\mathbb{R}, \leq)$ est un ensemble totalement ordonné.*
- *Si E contient plus de deux éléments, l'ensemble $(\mathcal{P}(E), \subset)$ est un ensemble partiellement ordonné.*
  En effet, pour a et b des éléments distincts de E on a $\{a\} \not\subset \{b\}$ et $\{b\} \not\subset \{a\}$.
- *La relation de divisibilité sur $\mathbb{N}$ est une relation d'ordre partiel. Par exemple, on a $2 \nmid 3$ et $3 \nmid 2$.*

La négation de $x \preccurlyeq y$ est : x et y ne sont pas comparables ou x et y sont comparables et $y \prec x$.
Il faut bien se souvenir que si $\preccurlyeq$ n'est pas une relation d'ordre totale, on peut avoir x et y qui ne sont pas comparables.

1.3.2 Majorant et minorant

Définition 25
Soient $(E, \preccurlyeq)$ un ensemble ordonné et A une partie de E.

- Soit $M \in E$. On dit que M est un **majorant** \上界\ de A si : pour tout $a \in A$, on a $a \preccurlyeq M$.
- Soit $m \in E$. On dit que m est un **minorant** \下界\ de A si : pour tout $a \in A$, on a $m \preccurlyeq a$.

Exemples 26

- *Dans $(\mathbb{R}, \leq)$, l'ensemble $\mathbb{R}_-$ est l'ensemble des minorants de $\mathbb{R}_+$.*
  $\mathbb{R}_+$ n'admet pas de majorant.

  ***Preuve** — En effet, supposons que M soit un majorant de $\mathbb{R}_+$. Alors, comme $M+1 \in \mathbb{R}_+$, on a $M+1 \leq M$, ce qui est absurde.* □
- *Pour la relation d'inclusion, $\emptyset$ est un minorant de $\mathcal{P}(E)$ et E est un majorant de $\mathcal{P}(E)$.*
- *Pour la relation de divisibilité sur $\mathbb{N}$, l'ensemble $\{1,2\}$ est l'ensemble des minorants de l'ensemble $\{4,6\}$ et l'ensemble des multiples de 12, $12\mathbb{N}$, est l'ensemble des majorants.*
  Pour $A \subset \mathbb{N}$, 0 est un majorant de A pour la relation de divisibilité.

  ***Preuve** —*
  - *Soit m un minorant de $\{4,6\}$. Alors $m|4$ et $m|6$ donc $m|6-4=2$. Donc $m=1$ ou $m=2$. 1 et 2 divisent évidemment 4 et 6. Donc l'ensemble des minorants est $\{1,2\}$.*
  - *Soit M un majorant de $\{4,6\}$. Alors $4|M$ et $6|M$ donc $12 = \text{ppcm}(4,6)|M$. Donc M est un multiple de 12. 4 et 6 divisent évidemment tout multiple de 12. Donc l'ensemble des majorants est $\{12n \mid n \in \mathbb{N}\}$.*

  □

Remarque 27 — *Un majorant ou un minorant d'une partie A, s'ils existent, ne sont pas forcément uniques. C'est ce que l'on vient de voir.*

Définition 28

- *On dit que A est une partie **majorée** si A admet au moins un majorant M.*
  Autrement dit, A est majorée s'il existe $M \in E$ tel que pour tout $a \in A$, $a \preccurlyeq M$.
  On dit aussi que M majore A ou que A est majorée par M.
- *On dit que A est une partie **minorée** si A admet au moins un minorant m.*
  Autrement dit, A est minorée s'il existe $m \in E$ tel que pour tout $a \in A$, $m \preccurlyeq a$.
  On dit aussi que m minore A ou que A est minorée par m.
- *On dit que A est **bornée** si A est majorée et minorée.*
  Autrement dit, A est bornée s'il existe $(m,M) \in E^2$ tel que pour tout $a \in A$, $m \preccurlyeq a \preccurlyeq M$.

Exemples 29

- *Pour la relation $\leq$ sur $\mathbb{R}$, $\mathbb{R}_+$ est une partie minorée, par exemple par 0.*
  La partie $\mathbb{R}_+$ n'est pas majorée car elle n'admet pas de majorant.
- *Pour la relation d'inclusion, la partie $\mathcal{P}(E)$ est minorée (par $\emptyset$) et majorée (par E).*
  $\mathcal{P}(E)$ est donc une partie bornée pour l'inclusion.
- *Pour la relation de divisibilité sur $\mathbb{N}$, l'ensemble $\{4,6\}$ est minoré, par exemple par 2, et majoré, par exemple par 12. C'est donc une partie bornée pour la relation de divisibilité.*

1.3.3 Maximum et minimum

Définition 30
Soient $(E, \preccurlyeq)$ un ensemble ordonné et A une partie de E.

- On dit que A admet un **maximum** \最大値\ s'il existe $M \in A$ tel que pour tout $a \in A$, on a $a \preccurlyeq M$.
- On dit que A admet un **minimum** \最小値\ s'il existe $m \in A$ tel que pour tout $a \in A$, on a $m \preccurlyeq a$.

Remarque 31 — *Un maximum (resp. minimum) de A est donc un majorant (resp. minorant) de A qui appartient à A.*

Proposition 32 *Soient $(E, \preccurlyeq)$ un ensemble ordonné et A une partie de E.*

- *Si A admet un maximum alors celui-ci est unique, et est noté $\max(A)$.*
- *Si A admet un minimum alors celui-ci est unique, et est noté $\min(A)$.*

Preuve —

- Supposons que A admette deux maximums M_1 et M_2. Montrons que $M_1 = M_2$. Par définition du maximum, M_1 et M_2 sont des éléments de A et sont des majorants de A. Comme M_1 est un majorant de A et $M_2 \in A$, on a $M_2 \preccurlyeq M_1$. De même, M_2 étant un majorant de A et $M_1 \in A$, on a $M_1 \preccurlyeq M_2$. Donc par antisymétrie de $\preccurlyeq$, on en déduit que $M_1 = M_2$. Donc, si A admet un maximum alors celui-ci est unique.
- La preuve est analogue au cas précédent.

□

Remarque 33 — *S'ils existent, on peut donc parler* du *maximum et* du *minimum d'une partie A (car ils sont uniques), mais on parle toujours d'*un *majorant et d'*un *minorant de A (car ils ne sont en général pas uniques).*

Exemples 34

- 0 *est le minimum de* $\mathbb{R}_+$. $\mathbb{R}_+$ *n'admet pas de maximum.*
- *Pour la relation d'inclusion,* $\emptyset$ *est le minimum de* $\mathcal{P}(E)$*, et* E *est son maximum.*
- *Dans* $(\mathbb{N}, |\ )$*, l'ensemble* $\{4,6\}$ *n'admet pas de minimum ni de maximum. En effet, aucun des minorants* $\{1,2\}$ *et aucun des majorants* $\{12n \mid n \in \mathbb{N}^*\}$ *n'appartient à* $\{4,6\}$.
- *Dans* $(\mathbb{R}, \leq)$*, soit* $I = [0,1[$. *Le minimum de* I *est* 0 *et* I *n'admet pas de maximum.*

  Preuve — *Supposons que* I *admette un maximum* M. *Alors* $M \in [0,1[$ *donc* $M < 1$. *Posons* $M' = \dfrac{M+1}{2}$. *Alors* $M' \in [0,1[$ *et* $M < M'$*, contredisant la maximalité de* M. *Donc* I *n'admet pas de maximum.* □
- *Dans* $(\mathbb{R}, \leq)$*, soit* $A = \left\{\dfrac{1}{n} \mid n \in \mathbb{N}^*\right\}$. *Le maximum de* A *est* 1 *et* A *n'admet pas de minimum.*

  Preuve —
  - *On a* $1 = \dfrac{1}{1}$ *donc* $1 \in A$ *et pour tout* $n \in \mathbb{N}^*$, $\dfrac{1}{n} \leq 1$ *donc* A *admet un maximum et* $\max(A) = 1$.
  - *Supposons que* A *admette un minimum* m. *Alors* $m \in A$ *et il existe* $n_0 \in \mathbb{N}^*$ *tel que* $m = \dfrac{1}{n_0}$. m *étant un minorant, pour tout* $n \in \mathbb{N}^*$, $m \leq \dfrac{1}{n}$. *En particulier, pour* $n = n_0 + 1$*, on a* $\dfrac{1}{n_0} \leq \dfrac{1}{n_0+1}$*, ce qui est absurde.*
    Donc A *n'admet pas de minimum.*

  □

On rappelle trois propriétés fondamentales de l'ensemble $\mathbb{N}$.

Proposition 35
Dans l'ensemble ordonné $(\mathbb{N}, \leq)$, on a :

- Toute partie non vide de $\mathbb{N}$ admet un minimum,
- Toute partie non vide majorée de $\mathbb{N}$ admet un maximum,
- $\mathbb{N}$ n'a pas de maximum.

1.3.4 Borne supérieure et borne inférieure

Le maximum et le minimum d'une partie A sont des éléments intéressants quand on veut étudier A avec la relation d'ordre $\preccurlyeq$.
Souvent, A possède des minorants et des majorants, mais pas de minimum ou de maximum. (penser à $]a,b[$ dans $\mathbb{R}$)
On généralise ces définitions avec les définitions suivantes.

Définition 36
Soient $(E, \preccurlyeq)$ un ensemble ordonné et A une partie de E.

- On appelle **borne supérieure** \上確界\ de A, si elle existe, le plus petit des majorants de A.
  On la note alors $\sup(A)$. Cet élément est aussi appelé **supremum** de A.
- On appelle **borne inférieure** \下確界\ de A, si elle existe, le plus grand des minorants de A.
  On la note alors $\inf(A)$. Cet élément est aussi appelé **infimum** de A.

Remarque 37 — *La borne supérieure (resp. inférieure) n'existe pas nécessairement.*
Mais, si elle existe, elle est unique par unicité du minimum des majorants de A *(resp. maximum des minorants).*

Méthode 38 — *Pour démontrer que* A *admet une borne supérieure (respectivement inférieure) égale à* M *(resp.* m*),*

1. *on commence par montrer que* M *(resp.* m*) est un majorant (resp. minorant) de* A *:*
   pour tout $a \in A$*, on a* $a \preccurlyeq M$ *(resp.* $m \preccurlyeq a$*),*
2. *puis on montre que tout majorant (resp. minorant) de* A *est supérieur (resp. inférieur) à* M *(resp.* m*) :*
   pour tout M' *majorant de* A *(resp.* m' *minorant d* A*), on a* $M \preccurlyeq M'$ *(resp.* $m' \preccurlyeq m$*).*

On montre ainsi que M *est le plus petit des majorants (respectivement* m *est le plus grand des minorants).*


La différence entre $\max(A)$ et $\sup(A)$ est que $\max(A)$ est un élément de A alors que $\sup(A)$ n'est pas forcément un élément de A.

On a cependant le résultat suivant.

PROPOSITION 39
Soient $(E, \preccurlyeq)$ un ensemble ordonné et A une partie de E.

- Si A possède un maximum alors A possède une borne supérieure, et $\max(A) = \sup(A)$.
- Si A possède un minimum alors A possède une borne inférieure, et $\min(A) = \inf(A)$.

Preuve —

- Supposons que A possède un maximum M. Alors M est un majorant de A.
  De plus, comme $M \in A$, pour tout majorant M' de A, on a $M \preccurlyeq M'$.
  Donc M est le plus petit des majorants. Donc A admet une borne supérieure et $M = \sup(A)$.
- Preuve analogue à la précédente.

□

EXEMPLES 40

- *Pour l'ordre usuel sur $\mathbb{R}$, 0 est le maximum donc la borne inférieure de $\mathbb{R}_+$:* $\inf(\mathbb{R}_+) = 0$.
  Par contre, $\mathbb{R}_+$ n'admet pas de borne supérieure car $\mathbb{R}_+$ n'est pas majoré.
- *Pour la relation d'inclusion sur $\mathcal{P}(E)$, $\emptyset$ est le minimum de $\mathcal{P}(E)$ donc sa borne inférieure ($\emptyset = \inf(P(E))$), E est le maximum de $\mathcal{P}(E)$ donc sa borne supérieure.*
- *Pour la relation de divisibilité, la borne inférieure de $\{4, 6\}$ est 2 et la borne supérieure est 12.*

  ***Preuve** — Nous avons vu que l'ensemble des minorants est $\{1, 2\}$. Donc le plus grand des minorants existe et vaut 2. Donc $\sup(\{4, 6\}) = 2$. L'ensemble des majorants est $\{12n \mid n \in \mathbb{N}^*\}$. Donc le plus petit des majorants existe et vaut 12. Donc $\inf(\{4, 6\}) = 12$.* □
- *Dans $(\mathbb{R}, \leq)$, $[0, 1[$ n'admet pas de maximum mais admet une borne supérieure égale à 1.*
  Sa borne inférieure est égale à son minimum, 0.
  ***Preuve** — Nous avons déjà vu que $[0, 1[$ n'admet pas de maximum.*
  Montrons que $[0, 1[$ admet une borne supérieure égale à 1.
  Pour tout $x \in [0, 1[$, on a $x \leq 1$. Donc 1 majore $[0, 1[$.
  Montrons que 1 est le plus petit des majorants. Soit M un majorant de $[0, 1[$. Pour tout $n \in \mathbb{N}^*$, $1 - \frac{1}{n} \in [0, 1[$, donc $1 - \frac{1}{n} \leq M$. En laissant tendre n vers $+\infty$, on en déduit que $1 \leq M$.
  Donc 1 est le plus petit des majorants de $[0, 1[$ et $\sup(A) = 1$. □
- *Dans $(\mathbb{R}, \leq)$, l'ensemble $A = \left\{\frac{1}{n} \mid n \in \mathbb{N}^*\right\}$ n'admet pas de minimum mais admet une borne inférieure égale à 0.*
  Sa borne supérieure est égale à son maximum, 1. ($\sup(A) = \max(A) = 1$).
  ***Preuve** — Nous avons déjà vu que A n'admet pas de minimum.*
  Montrons que A admet une borne inférieure égale à 0.
  Pour tout $n \in \mathbb{N}^*$, $0 \leq \frac{1}{n}$. Donc 0 est un minorant de A.
  Montrons que 0 est le plus grand des minorants. Soit m un minorant de A. Comme m minore A, pour tout $n \in \mathbb{N}^*$, on a $m \leq \frac{1}{n}$. En laissant tendre n vers $+\infty$, on obtient $m \leq 0$.
  Donc 0 est le plus grand des minorants de A et $\inf(A) = 0$. □

D'après les deux derniers exemples, une partie A peut avoir une borne supérieure (resp. inférieure) mais ne pas avoir de maximum (resp. minimum).

Cas particulier de l'ensemble ordonné $(\mathbb{R}, \leq)$

Citons deux propriétés fondamentales de $\mathbb{R}$. On admet ces propriétés qui découlent de la construction de $\mathbb{R}$. La démonstration de nombreux théorèmes d'analyse repose sur ces propriétés.

PROPOSITION 41 (Propriété de la borne supérieure/inférieure)
Dans l'ensemble ordonné $(\mathbb{R}, \leq)$,

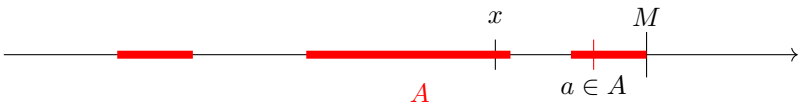
- Toute partie A non vide et majorée admet une borne supérieure,
- Toute partie A non vide et minorée admet une borne inférieure.

REMARQUE 42 — *La propriété de la borne supérieure est un résultat d'existence, elle ne donne pas la valeur de cette borne supérieure.*

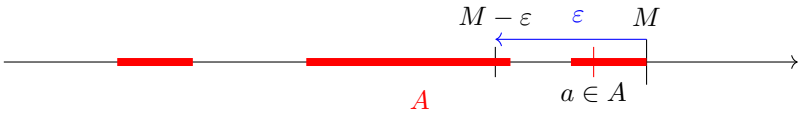
Dans certains cas, on a une idée de la borne supérieure, par exemple, on a vu que $\sup([0,1[) = 1$*, et on le démontre en revenant à la définition de la borne supérieure.*
Dans d'autres cas, on ne connaît pas cette valeur. Mais cette propriété permet de justifier que la borne supérieure existe.

PROPOSITION 43 (Caractérisation de la borne supérieure)
Soit A une partie non vide et majorée de $\mathbb{R}$. Soit $M \in \mathbb{R}$.

Alors $M = \sup(A)$ si et seulement si $\begin{cases} 1)\ M \text{ majore } A \\ 2)\ \text{pour tout } x \in \mathbb{R} \text{ tel que } x < M, \text{ il existe } a \in A \text{ tel que } x < a \leq M. \end{cases}$

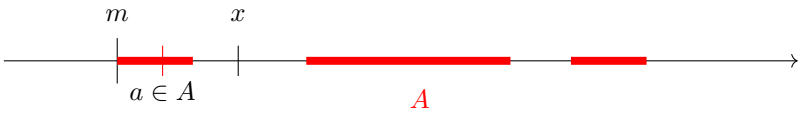


soit encore, si et seulement si $\begin{cases} 1)\ M \text{ majore } A, \\ 2)\ \text{pour tout } \varepsilon > 0, \text{ il existe } a \in A \text{ tel que } M - \varepsilon < a \leq M. \end{cases}$

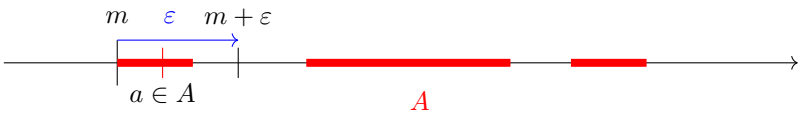


PROPOSITION 44 (Caractérisation de la borne inférieure)
Soit A une partie non vide minorée de $\mathbb{R}$. Soit $m \in \mathbb{R}$.

Alors $m = \inf(A)$ si et seulement si $\begin{cases} 1)\ m \text{ minore } A \\ 2)\ \text{pour tout } x \in \mathbb{R} \text{ tel que } x > m, \text{ il existe } a \in A \text{ tel que } m \leq a < x. \end{cases}$



soit encore, si et seulement si $\begin{cases} 1)\ m \text{ minore } A, \\ 2)\ \text{pour tout } \varepsilon > 0, \text{ il existe } a \in A \text{ tel que } m \leq a < m + \varepsilon. \end{cases}$



EXEMPLE 45 — *Retrouvons la valeur de la borne inférieure de l'exemple* $A = \left\{ \frac{1}{n} \mid n \in \mathbb{N}^* \right\}$.

1) 0 *minore* A.

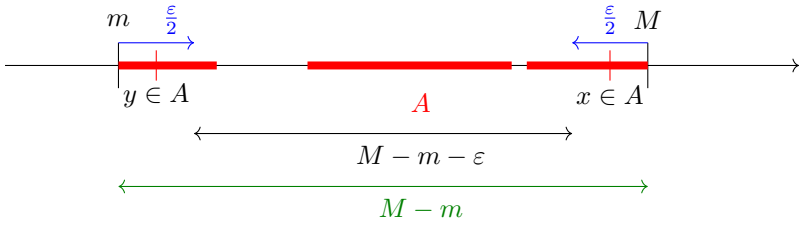
2) *Soit* $\varepsilon > 0$. *Comme* $\lim\limits_{n \to +\infty} \frac{1}{n} = 0$, *il existe* $n_0 \in \mathbb{N}^*$ *tel que* $0 < \frac{1}{n_0} \leq \varepsilon$ *et* $\frac{1}{n_0} \in A$.

Donc, avec la caractérisation de la borne supérieure, on obtient que $\inf(A) = 0$.

EXEMPLE 46 — *Soit* A *une partie non vide et bornée de* $\mathbb{R}$. *Posons* $E = \left\{ |x - y| \mid (x, y) \in A^2 \right\}$.
E *est donc l'ensemble des distances entre deux points de* A.

- A *étant non vide, on peut trouver un élément* $x \in A$. *Alors, comme* $(x, x) \in A^2$, $|x - x| = 0 \in E$. *Donc* E *est une partie non vide de* $\mathbb{R}$.
- A *étant bornée, il existe* $b \in \mathbb{R}$ *tel que pour tout* $x \in A$, *on ait* $|x| \leq b$.
  Soit $(x, y) \in A^2$. *Par inégalité triangulaire, on a* $|x - y| \leq |x| + |y| \leq b + b = 2b$. *Donc* E *est majoré par* $2b$.
- E *étant une partie non vide et majorée de* $\mathbb{R}$, *elle admet donc une borne supérieure, que l'on note* δ.

– *Déterminons δ.*
A étant non vide et bornée, A est en particulier non vide et minorée, donc $m = \inf(A)$ existe.
De même, A est en particulier non vide et majorée, donc $M = \sup(A)$ existe.
Montrons que $\delta = M - m = \sup(A) - \inf(A)$.



1) *Pour tout $(x, y) \in A^2$, on a $m \leq x \leq M$ et $m \leq y \leq M$. Donc $-(M-m) \leq x - y \leq M - m$, soit $|x - y| \leq M - m$.*
Donc $M - m$ majore E. C'est-à-dire $\delta \leq M - m$.
2) *Soit $\varepsilon > 0$. D'après la caractérisation de la borne supérieure (en prenant $\varepsilon' = \frac{\varepsilon}{2}$), il existe $x \in A$ tel $M - \dfrac{\varepsilon}{2} < x \leq M$.*
D'après la caractérisation de la borne inférieure (en prenant $\varepsilon' = \frac{\varepsilon}{2}$), il existe $y \in A$ tel que $m \leq y < m + \dfrac{\varepsilon}{2}$.
Alors $M - m - \varepsilon < x - y \leq |x - y|$.
En posant $d = |x - y|$, on a donc $d \in E$ et $M - m - \varepsilon < d \leq M - m$.
Donc, d'après la propriété de caractérisation de la borne supérieure, on obtient $\sup(E) = \delta = M - m = \sup(A) - \inf(A)$.

PROPOSITION 47
Soient a et b deux nombres réels.

- Si, pour tout $\varepsilon > 0$, on a $a \geq b - \varepsilon$ alors $a \geq b$.
- Si, pour tout $\varepsilon > 0$, on a $a \leq b + \varepsilon$ alors $a \leq b$.

Preuve — Traitons le premier point, le deuxième point se traitant de manière analogue.
Supposons que pour tout $\varepsilon > 0$, on a $a \geq b - \varepsilon$. On pose $B = \{b - \varepsilon \mid \varepsilon \in \mathbb{R}_+^*\}$.
On a $\sup(B) = b$ d'après la caractérisation de la borne supérieure et, par hypothèse, a est un majorant de B. La borne supérieure étant le plus petit des majorants, on en déduit que $b \leq a$. D'où le résultat. □

PROPOSITION 48 (Caractérisation séquentielle de la borne sup./inf.)
Soit A une partie non vide de $\mathbb{R}$. Soit $(m, M) \in \mathbb{R}^2$.

- Supposons que A est majorée.

Alors $M = \sup(A)$ si et seulement si $\begin{cases} 1)\ M \text{ majore } A \\ 2)\ \text{il existe une suite } (a_n)_{n\in\mathbb{N}} \text{ d'éléments de } A \text{ qui converge vers } M. \end{cases}$

- Supposons que A est minorée.

Alors $m = \inf(A)$ si et seulement si $\begin{cases} 1)\ m \text{ minore } A \\ 2)\ \text{il existe une suite } (a_n)_{n\in\mathbb{N}} \text{ d'éléments de } A \text{ qui converge vers } m. \end{cases}$

Preuve — Traitons le cas de la borne supérieure. A étant une partie non vide majorée de $\mathbb{R}$, A admet une borne supérieure.

• Supposons que $M = \sup(A)$.

Alors, par définition de la borne supérieure, M majore A. D'où le premier point.

Construisons une suite d'éléments de A qui converge vers M. Pour tout $n \in \mathbb{N}$, on va utiliser la caractérisation de la borne supérieure avec $\varepsilon = \dfrac{1}{n+1} > 0$. Pour tout $n \in \mathbb{N}$, il existe $a_n \in A$ tel que $M - \dfrac{1}{n+1} < a_n \leq M$. La suite $(a_n)_{n\in\mathbb{N}}$ est donc une suite d'éléments de A. De plus, en laissant tendre n vers $+\infty$, on en déduit que $M \leq \lim\limits_{n\to+\infty} a_n \leq M$, soit $\lim\limits_{n\to+\infty} a_n = M$. On a donc construit une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de A qui converge vers M.

• Réciproquement, soit $M \in \mathbb{R}$. Supposons que M majore A et qu'il existe une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de A qui converge vers M. Utilisons la caractérisation de la borne supérieure.

1) Par hypothèse, M majore de A.

2) Soit $\varepsilon > 0$. Comme $\lim_{n\to+\infty} a_n = M$, il existe $n_0 \in \mathbb{N}$ tel que pour tout $n \geq n_0$, $a_n > M - \varepsilon$. En particulier, on a $a_{n_0} \in A$ et $M - \varepsilon < a_{n_0} \leq M$.

Donc, par la caractérisation de la borne supérieure, $M = \sup(A)$.

□

EXEMPLE 49 — *Retrouvons la valeur de borne inférieure de l'exemple* $A = \left\{ \frac{1}{n} \mid n \in \mathbb{N}^* \right\}$.

1) *A est minoré par* 0.

2) *Posons, pour tout* $n \in \mathbb{N}^*$, $u_n = \frac{1}{n}$. *Pour tout* $n \in \mathbb{N}^*$, $u_n \in A$ *et* $u_n \to 0$ *lorsque n tend vers* $+\infty$. *La suite* $(u_n)_{n\in\mathbb{N}^*}$ *d'éléments de A converge donc vers* 0.

Donc, d'après la caractérisation séquentielle de la borne supérieure, on a $\inf(A) = 0$.

EXEMPLE 50 — *Soit* $B = \left\{ \frac{q}{2^p + q} \mid (p, q) \in \mathbb{N}^{*2} \right\}$. *Montrer que B admet un sup. et un inf., et les calculer.*

• *Remarquons que B est non vide et pour tout* $(p, q) \in \mathbb{N}^{*2}$, $\frac{q}{2^p + q} \leq \frac{q}{q} = 1$ *donc B est majoré par* 1.
B étant une partie de $\mathbb{R}$ *non vide majorée, B admet une borne supérieure.*

1) 1 *majore B.*

2) *Posons, pour tout* $n \in \mathbb{N}^*$, $u_n = \frac{n}{2 + n}$. *Alors, pour tout* $n \in \mathbb{N}^*$, $u_n \in B$ *et* $(u_n)_{n\in\mathbb{N}^*}$ *converge vers* 1.

Donc, par la caractérisation séquentielle de la borne supérieure, on a $\sup(B) = 1$.

• *Remarquons que B est non vide et pour tout* $(p, q) \in \mathbb{N}^{*2}$, $0 \leq \frac{q}{2^p + q}$ *donc B est minoré par* 0. *B étant une partie de* $\mathbb{R}$ *non vide minorée, B admet une borne inférieure.*

1) 0 *minore B.*

2) *Posons, pour tout* $n \in \mathbb{N}^*$, $v_n = \frac{1}{2^n + 1}$. *Alors, pour tout* $n \in \mathbb{N}^*$, $v_n \in B$ *et* $(v_n)_{n\in\mathbb{N}^*}$ *converge vers* 0.

Donc, d'après la caractérisation séquentielle de la borne inférieure, on a $\inf(B) = 0$.

Chapitre 2 Structures algébriques : Groupes

Table des matières du chapitre

2.1 Loi de composition interne, Notion de groupe

Loi de composition interne

Dans tout ce chapitre, si cela n'est pas précisé, E désigne un ensemble.

Définition 1
Soit E un ensemble.
On appelle **loi de composition interne** (ou opération) sur E toute fonction $\varphi : E \times E \to E$. L'image $\varphi(a, b)$ (écriture préfixe) sera souvent notée $a * b$ (écriture infixe), et la loi de composition sera appelée $*$.

Exemples 2— *Les ensembles et opérations suivants :* $(\mathbb{Z}, +)$, $(\mathcal{P}(E), \cap)$, $(\mathbb{R}^3, \wedge)$, *où* $\wedge$ *est le produit vectoriel, sont des ensembles munis d'une loi de composition interne.*

Définition 3
Soit $(E, *)$ un ensemble muni d'une loi de composition interne $*$.
Une partie $F \subset E$ de E est dite **stable par** $*$ si l'on a $x * y \in F$ pour tous $x, y \in F$.

La restriction de $*$ à $F \times F$ est alors appelée loi induite sur F.

Remarque 4 — *Si* F *n'est pas stable par* $*$*, on ne peut pas parler de loi induite (car elle n'est pas bien définie !).*

Exemple 5 —

1. *Pour* $(\mathbb{C}, +)$*, les ensembles* $\mathbb{R}$*,* $\mathbb{Q}$*,* $\mathbb{Z}$ *et* $\mathbb{N}$ *sont des parties stables pour la loi d'addition.*
   Ces parties peuvent donc être considérées comme étant munies de la loi induite par $+$ *sur* $\mathbb{C}$*.*
2. *La composition de fonctions* $\circ$ *définit une loi interne sur* $\mathcal{F}(E)$*, l'ensemble des fonctions d'un ensemble* E *dans lui même.*
   En particulier, le sous-ensemble des bijections de E *dans* E*,* $\mathrm{Bij}\,(E)$*, est stable par* $\circ$*.*

Groupe : Définition et exemples

Définition 6
Soit $(G, \star)$ un ensemble muni d'une loi de composition interne.
On dit que $(G, \star)$ est un **groupe** \群\ si la loi $\star$ vérifie les propriétés suivantes :

1. La loi $\star$ est **associative** \运算$*$满足结合律\ :
$$\forall x, y, z \in G, \text{ on a } x * (y * z) = (x * y) * z\,;$$
2. L'ensemble G possède un **élément neutre** \单位元\ pour la loi $\star$:
$$\exists e \in G, \text{ tel que } \forall x \in G,\ e * x = x * e = x\,;$$

3. tout élément est inversible \可逆的\ :

$$\forall x \in G,\ \exists y \in G \text{ tel que } x * y = y * x = e.$$

On appelle y le **symétrique** de x que l'on notera parfois y^{-1} (l'inverse) ou $-y$ (l'opposé).

De plus, le groupe $(G, \star)$ est **commutatif** (ou **abélien** \阿贝尔群/交换群/加群\) si la loi est commutative : $\forall x, y \in G,\ x * y = y * x$.

EXEMPLE 7 — *Nous allons d'abord donner quelques exemples que nous avons déjà rencontrés.*

1. *Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de la loi d'addition $+$ sont des groupes, qui sont abéliens.*
2. *L'ensemble $\mathbb{N}$ muni de l'addition n'est pas un groupe. (Pourquoi ?)*
3. *Les ensembles de matrices $\mathscr{M}_{n,p}(\mathbb{K})$ munis de la loi d'addition sont des groupes, qui sont abéliens.*
4. *Les ensembles $\mathbb{K}[X]$ munis de la loi d'addition sont des groupes, qui sont abéliens.*
5. *Les espaces vectoriels E munis de leur loi d'addition de vecteurs sont des groupes, qui sont commutatifs.*
6. *Les ensembles $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de la multiplication ne sont pas des groupes. (Pourquoi ?)*
   Mais $\mathbb{Q}^*$, $\mathbb{R}^*$ et $\mathbb{C}^*$ munis de la multiplication le sont, et sont commutatifs.
7. *Les ensembles de matrices inversibles $GL_n(\mathbb{K})$ munis de la multiplication matricielle sont des groupes. Si $n \geq 2$ ces groupes ne sont pas abéliens.*
   Par exemple $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ sont des matrices inversibles, mais $AB \neq BA$.

EXERCICE 1 —

1. *Montrer que l'ensemble $\mathbb{U}$ des nombres complexes de module 1 est un groupe pour la loi de multiplication.*
2. *Soit $G = \{0, 1\}$ et la loi $+$ donnée par la tableau :*

$+$	0	1
0	0	1
1	1	0

   , c'est-à-dire $0+0=0$, $1+0=0+1=1$ et $1+1=0$. Montrer que $(G,+)$ est un groupe. On le notera par la suite $(\mathbb{Z}/2\mathbb{Z}, +)$.
3. *L'ensemble $\mathscr{P}(E)$ muni de l'union est-il un groupe ? Et avec l'intersection ? Et avec la différence symétrique Δ : $A \Delta B = (A \cap \overline{B}) \cup (\overline{A} \cap B)$?*
   Pour vérifier l'assiciativité, on peut utiliser le fait que pour tout $A \in \mathscr{P}(E)$ la fonction :

$$\begin{array}{rccl} \chi_A : & E & \to & \mathbb{Z}/2\mathbb{Z} \\ & x & \mapsto & \begin{cases} 1 \text{ si } x \in A \\ 0 \text{ sinon} \end{cases} \end{array}$$

   et montrer que l'on a $\chi_{A \Delta B} = \chi_A + \chi_B$.

REMARQUE 8 — *Soit $(G, \star)$ un groupe. Alors G possède un unique élément neutre.*

En effet, pour e, e' deux éléments neutres de G, on a $e \star e' = e'$ et $e \star e' = e$, donc $e = e'$.

DÉFINITION 9

Soit $(G, \star)$ un groupe. Pour tout élément $x \in G$ et tout entier $n \in \mathbb{Z}^*$, on notera :

- x^{-1} le **symétrique** de x (ou **l'inverse** de x) ;
- $x^0 := e$;
- $x^n := \underbrace{x \star \ldots \star x}_{n \text{ fois}}$ si n est strictement positif ;
- $x^n := \underbrace{x^{-1} \star \ldots \star x^{-1}}_{-n \text{ fois}}$ si n est strictement négatif.

REMARQUE 10 — *Avec cette notation, pour tout $x \in G$ et tous $n, m \in \mathbb{Z}$ et $k \in \mathbb{N}^*$, on a :*

$$x^n \star x^m = x^{n+m} \quad \text{et} \quad (x^n)^k = \underbrace{x^n \star \ldots \star x^n}_{k \text{ fois}} = x^{kn}.$$

PROPOSITION 11
Soit $(G, \star)$ un groupe. Soient $a, b \in G$.
Alors, on a $(a \star b)^{-1} = b^{-1} \star a^{-1}$.

Preuve — On a $(a \star b) \star (b^{-1} \star a^{-1}) = e_G$, et $(b^{-1} \star a^{-1}) \star (a \star b) = e_G$. □

Si les éléments a et b ne commutent pas, alors $(a \star b)^{-1} = b^{-1} \star a^{-1} \neq a^{-1} \star b^{-1}$.

PROPOSITION 12
Soient $(G_1, \star_1)$ et $(G_2, \star_2)$ deux groupes.

L'ensemble $G = G_1 \times G_2$ muni de la loi produit :
$$\begin{array}{rccc} \star & G \times G & \to & G \\ & ((g_1, g_2), (h_1, h_2)) & \mapsto & (g_1 \star_1 h_1, g_2 \star_2 h_2) \end{array}$$
est lui aussi un groupe.
On l'appelle **produit direct** des groupes G_1 et G_2.

Preuve — Il faut vérifier les trois conditions de la définition d'un groupe :

1. Par définition de la loi produit $\star$, celle-ci est associative.
2. Soient e_1 et e_2 les deux éléments neutres de G_1 et G_2. L'élément (e_2, e_2) est alors l'élément neutre de $G_1 \times G_2$ pour la loi produit. (Le vérifier.)
3. Soit (x, y) appartenant à $G_1 \times G_2$. Alors (x^{-1}, y^{-1}) est l'inverse de (x, y) pour la loi $\star$.

□

2.2 SOUS-GROUPES ET ORDRE D'UN ÉLÉMENT

Notion de sous-groupe

DÉFINITION 13
Soit $(G, \star)$ un groupe. Soit H un sous-ensemble de G.
On dit que H est un **sous-groupe** \子群\ de $(G, \star)$ s'il vérifie les propriétés suivantes :

1. L'élément neutre e appartient à H ;
2. Pour tous x, y appartenant à H, le produit $x \star y$ appartient à H (autrement dit H est stable par la loi $\star$) ;
3. Pour tout x appartenant à H, l'inverse de x appartient à H.

Si H est un sous-groupe de G, on notera $H < G$.

PROPOSITION 14
Soient $(G, \star)$ un groupe et H un sous-groupe de G.
Alors l'ensemble H muni de la loi $\star$ restreinte à H est un groupe.

Preuve — Il faut vérfier les conditions de la définition de groupe :

1. Comme H est un sous-groupe, il possède un élément neutre e, qui est celui de G.
2. La loi $\star$ restreinte à H est associative puisqu'elle l'est sur G.
3. L'ensemble H est un sous-groupe, donc chaque élément de H possède un inverse dans H.

□

La proposition suivante donne un critère simple pour montrer qu'un sous-ensemble est un sous-groupe.

PROPOSITION 15
Soient $(G, \star)$ un groupe et H un sous-ensemble de G.
Les propriétés suivantes sont équivalentes :

1. H est un sous-groupe ;
2. H est non vide, et pour tous x, y appartenant à H, $x \star y^{-1}$ appartient à H.

Preuve — Commençons par montrer que le premier point implique le second. Comme H est un sous-groupe il contient e et est donc non-vide. Soient $x, y \in H$. Comme H est un sous-groupe on a $y^{-1} \in H$. Donc $x \star y^{-1} \in H$.

Soit maintenant H un sous-ensemble de G satisfaisant le second point.

1. Comme H est non-vide, il contient un élément x. Par hypothèse, l'élément neutre $e = x \star x^{-1}$ appartient donc à H.
2. Soit $x \in H$. Puisque e appartient à H, $x^{-1} = e \star x^{-1}$ appartient lui aussi à H.
3. Soit $x, y \in H$. Puisque y^{-1} appartient à H, $x \star y = x \star (y^{-1})^{-1}$ appartient lui aussi à H.

Donc H est un sous-groupe de G. □

Exemple 16 —

1. *Soit $(G,\star)$ un groupe et e_G son élément neutre. L'ensemble $\{e_G\}$ est un sous-groupe de G. On l'appelle le sous-groupe trivial de G.*
2. *Soit $n\in\mathbb{Z}$ un entier. L'ensemble $n\mathbb{Z}=\{nk, k\in\mathbb{Z}\}$ des multiples de n est un sous-groupe de $(\mathbb{Z},+)$.*
3. *L'ensemble $\mathbb{U}=\{z\in\mathbb{C},\ |z|=1\}$ est un sous-groupe de $(\mathbb{C}^*,\times)$.*
   Pour $n>0$, l'ensemble $\mathbb{U}_n=\{z\in\mathbb{C},\ z^n=1\}$ est un sous-groupe de $\mathbb{U}$ (Pourquoi ?).
4. *Soit E un ensemble et A une partie de E. L'ensemble des bijections $f:E\to E$ telles que $f(x)=x$, $\forall x\in A$, est un sous-groupe de $(Bij(E),\circ)$.*
5. *Soient E un ensemble et x un élément de E.*
   L'ensemble des parties de E qui ne contiennent pas x est un sous-groupe de $(\mathcal{P}(E),\Delta)$. (Le vérifier)

Remarque 17 —
• *Soit $(G,\star)$ un groupe et H un sous-groupe de G. Soit $x\in H$. Alors H contient tous les x^n, $n\in\mathbb{Z}$.*
• *Pout G un groupe, et X,Y des sous-groupes de G, la relation : $X<Y$ si X est un sous-groupe de Y, est une relation d'ordre. Cette relation d'ordre n'est pas totale en général.*

Il faut bien penser à vérifier que le sous-ensemble H est non-vide pour montrer que c'est un sous-groupe. L'ensemble vide $\emptyset$ est un sous-ensemble de G, mais pas un sous-groupe.

Exercice 2 —

1. *Une homothétie \位似\ sur $\mathbb{R}^3$ est une fonction de la forme*

$$h_\lambda : \begin{array}{ccc}\mathbb{R}^3 & \to & \mathbb{R}^3\\ (x_1,x_2,x_3) & \mapsto & (\lambda x_1,\lambda x_2,\lambda x_3)\end{array},$$

   où λ est un réel non nul. Montrer que l'ensemble des homothéties muni la composition de fonctions est un groupe. Montrer que ce groupe est abélien.
2. *Une **translation** sur $\mathbb{R}^3$ est une fonction de la forme*

$$t_a : \begin{array}{ccc}\mathbb{R}^3 & \to & \mathbb{R}^3\\ (x_1,x_2,x_3) & \mapsto & (x_1+a_1,x_2+a_2,x_3+a_3)\end{array}$$

   où $a=(a_1,\dots,a_3)$ est un vecteur de $\mathbb{R}^3$. Montrer que l'ensemble des translations muni de la composition de fonctions est un groupe. Montrer que ce groupe est abélien.

Proposition 18 (Intersection de sous-groupes)
Soient $(G,\star)$ un groupe et $(H_i)_{i\in I}$ une famille de sous-groupes de G.
Alors le sous-ensemble $\cap_{i\in I}H_i$ est un sous-groupe de G.

Preuve — Ce sous-ensemble contient e et est donc non-vide. Soient $x,y\in\cap_{i\in I}H_i$. Pour tout $i\in I$, x et y appartiennent à H_i. D'après la proposition précédente, on a donc $x\star y^{-1}\in H_i$ pour tout $i\in I$. Ainsi, $x\star y^{-1}$ appartient $\cap_{i\in I}H_i$. Donc $\cap_{i\in I}H_i$ est bien un sous-groupe de G. □

Proposition 19
Soient $(G,\star)$ un groupe et H et K deux sous-groupes.
L'ensemble $H\cup K$ est un sous-groupe de G si et seulement si H est inclus dans K ou K est inclus dans H.

Preuve — Si H est inclus dans K ou K est inclus dans H, alors $H\cup K$ est un sous-groupe de G.

Réciproquement, soient H et K deux sous-groupes tels que $H\cup K$ soit un sous-groupe. Supposons que H ne soit pas inclus dans K. Il existe alors $x\in H\backslash K$.

Soit $y\in K$. Comme $H\cup K$ est un sous-groupe de G, $x\star y$ appartient à $H\cup K$. Comme $x\notin K$, $x\star y$ n'appartient pas à K. En effet, on aurait sinon $x=(x\star y)\star y^{-1}\in K$.

Ainsi, on a $x\star y\in H$. Comme $x\in H$, on a donc $y=x^{-1}\star(x\star y)\in H$. On en conclut donc que K est inclus dans H. □

Exercice 3 — *Soient n,m deux entiers. Montrer que $n\mathbb{Z}\cup m\mathbb{Z}$ est un groupe si et seulement si $n|m$ ou $m|n$.*

PROPOSITION 20
Les sous-groupes de $(\mathbb{Z}, +)$ sont de la forme $n\mathbb{Z}$, avec $n \in \mathbb{N}$ uniquement déterminé.

Preuve — Soit H un sous-groupe de $\mathbb{Z}$ (sous-entendu pour l'addition). Si $H = \{0\}$, alors $n = 0$ convient.

Sinon, posons $n \in H \setminus \{0\}$ le plus petit entier naturel non nul appartenant à H (son existence est assurée). Alors, $n\mathbb{Z} = \{kn, k \in \mathbb{Z}\}$ est contenu dans H. Réciproquement, soit $a \in H$. La division euclidienne de a par n donne

$$a = nq + r,\ 0 \leq r < n.$$

On a alors $r = p - nq \in H$, avec $0 \leq r < n$. Par minimalité de n on a donc $r = 0$, donc $a = nq \in n\mathbb{Z}$. Ainsi, $H \subset n\mathbb{Z}$.

On termine la preuve en vérifiant que pour tout $n \in \mathbb{Z}$, $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. □

Sous-groupe engendré par une partie

PROPOSITION-DÉFINITION 21
Soient $(G, \star)$ un groupe et S une partie de G.
On appelle sous-groupe **engendré** \生成的子群\ par S le plus petit sous-groupe contenant S.
On note $\langle S \rangle$ ce sous-groupe. Il est caractérisé par la relation :

$$\langle S \rangle = \bigcap_{S \subset H < G} H.$$

Lorsque S est un singleton $\{x\}$, on note $\langle x \rangle$ le groupe engendré par $\{x\}$.
On l'appelle aussi le sous-groupe engendré par x.

Preuve — Soit S un partie de G. On pose $A := \{H < G \text{ tels que } S \subset H\}$. L'ensemble A n'est pas vide car il contient G. D'après la proposition 18, l'ensemble $\langle S \rangle := \bigcap_{H \in A} H$ est un sous-groupe de G. Ce sous-groupe contient S. De plus, tout sous-groupe H de G contenant S appartient à A et donc contient $\langle S \rangle$. $\langle S \rangle$ est donc le plus petit sous-groupe contenant S. □

REMARQUE 22 — *Soit $(G, \star)$ un groupe et S une partie de G.*
L'ensemble A de tous les produits $a_1 \star \ldots \star a_n$, avec $a_i \in S$ ou $a_i^{-1} \in S$ pour tout $i \in [\![1, n]\!]$, est un sous-groupe de G (le vérifier).
De plus, tous les sous-groupes de G contenant S contiennent A (Pourquoi ?).
A est donc le sous-groupe engendré par S.

En particulier, pour $x \in G$ le sous-groupe engendré par x est

$$\langle x \rangle = \{x^n / \ n \in \mathbb{Z}\}.$$

EXEMPLE 23 —

1. *Le sous-groupe de $\mathbb{Z}$ engendré par 1 est $\mathbb{Z}$: $\langle 1 \rangle = \mathbb{Z}$.*
2. *Le sous-groupe de $\mathbb{Z}$ engendré par n est $n\mathbb{Z}$: $\langle n \rangle = n\mathbb{Z}$.*
3. *Pour $a_1, \ldots, a_r \in \mathbb{Z}$, on a $\langle \{a_1, \ldots, a_n\} \rangle = \text{pgcd}(a_1, \ldots, a_n)\mathbb{Z}$ (voir chapitre Arithmétique).*

EXERCICE 4 — *Montrer qu'il n'existe pas de partie finie S de $\mathbb{Q}$ telle que $\langle S \rangle = \mathbb{Q}$.*

DÉFINITION 24
Soit $(G, \star)$ un groupe.
Le groupe G est **monogène** s'il existe $a \in G$ tel que $G =< a >$.
L'élément a est appelé un **générateur** de G.

Si G est monogène et fini, on dit que G est un groupe **cyclique** \循环群\.

PROPOSITION 25
Soit $(G, \star)$ un groupe.
Si G est monogène, alors il est abélien.

Preuve — Soit x un élément G tel que $G = \langle x \rangle$. Soient $x, y \in G$. Il existe alors $n, m \in \mathbb{Z}$ tels que $x^n = y$ et $x^m = z$ (voir la remarque 22). On a donc :

$$y \star z = x^n \star x^m = x^{n+m} = x^m \star x^n = z \star y.$$

□

Exemple 26 —

1. *Tout sous-groupe de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$ et est donc monogène.*
2. *Pour $n \geq 1$, l'ensemble $\mathcal{U}_n$ des racines n-ièmes de l'unité muni de la multiplication est un groupe.*
   Il est cyclique, et $\chi = \exp\left(\dfrac{2i\pi}{n}\right)$ est un générateur du groupe.
   Le groupe $(\mathcal{U}_n, \times)$ est un groupe à n éléments. Il existe ainsi des groupes finis de toutes les tailles possibles.
3. *L'ensemble $\mathcal{U}_\infty = \{z \in \mathbb{C},\ \exists n \in \mathbb{N},\ z^n = 1\}$ est-il un groupe monogène ?*

Ordre d'un élément

Définition 27
Soit $(G, \star)$ un groupe fini.
On appelle **ordre** de G le nombre d'éléments de G (c'est le cardinal de G).
On le note $|G|$ (ou $\mathrm{Card}(G)$).

Définition 28
Soient $(G, \star)$ un groupe et $a \in G$.

Si le sous-groupe $\langle a \rangle$ est fini, alors l'**ordre** de a, noté $\mathrm{ord}(a)$, est le cardinal de ce sous-groupe.
Sinon, on dit que a est d'ordre infini.

Exemple 29 — *Dans $(\mathbb{C}^*, \times)$, i est un élément d'ordre 4. En effet, on a :*

$$i^0 = 1, \quad i^1 = i, \quad i^2 = -1, \quad i^3 = -i, \quad i^4 = 1 = i^0,$$

donc $\langle i \rangle = \{1, i, -1, -i\}$.

Exemple 30 — *Soit $E = \{1, 2, 3\}$. Pour $f : E \to E$ avec $f(1) = 2$, $f(2) = 3$, $f(3) = 1$, pn a $f \in Bij(E)$.*
Dans le groupe $(Bij(E), \circ)$, f est un élément d'ordre 3. En effet, on a :

$$f^0 = Id, \quad f^1 = f, \quad f^2 \neq f \text{ et } Id, \quad f^3 = Id,$$

donc $\langle f \rangle = \{Id, f, f^2\}$.

Proposition 31
Soient $(G, \star)$ est un groupe et $x \in G$.
L'élement x est d'ordre fini si et seulement s'il existe $k \in \mathbb{N}^*$ tel que $x^k = e$.
Dans ce cas, $\mathrm{ord}(x)$ est le plus petit entier n strictement positif tel que $x^n = e$.

Preuve — Supposons qu'il existe $k \in \mathbb{N}^*$ tel que $x^k = e$. Soit $n \in \mathbb{N}^*$ le plus petit entier tel que $x^n = e$. Montrons alors que $\langle x \rangle = \{e, x, \ldots, x^{n-1}\}$, ce qui prouvera que x est d'ordre fini et que $\mathrm{ord}(x) = n$.

On sait que $\langle x \rangle = \{x^k, k \in \mathbb{Z}\}$. Ainsi, on a $\{e, x, \cdots, x^{n-1}\} \subset \langle x \rangle$. Réciproquement, soit $k \in \mathbb{Z}$. On effectue la division euclidienne de k par n : $k = qn + r$ avec $0 \leq r \leq n - 1$. On a alors :

$$x^k = x^{qn+r} = x^{qn}\, x^r = (x^n)^q\, x^r = x^r \in \{e, x, \ldots, x^{n-1}\},$$

ce qui prouve que $\langle x \rangle = \{e, x, \ldots, x^{n-1}\}$. Donc x est d'ordre fini et $\mathrm{ord}(x) = n$.

Réciproquement, supposons que x est d'ordre fini n. Montrons alors qu'il existe un entier r strictement positif tel que $x^r = e$.

L'ensemble $\{e, x, \ldots, x^n\}$ comporte ainsi au plus n éléments distincts. Il y a donc $0 \leq k < k' \leq n$ tels que $x^k = x^{k'}$. Cela donne $x^{k'-k} = e$. Comme $k' - k > 0$, il existe donc un entier strictement positif r tel que $x^r = e$. La première moitié de la preuve nous dit alors que $n = \mathrm{ord}(x)$ est le plus petit entier tel que $x^n = e$, ce qui conclut. □

Remarque 32 — *En réutilisant l'idée de la division euclidienne, on montre que si $x \in G$ est d'ordre fini n, alors on a $x^k = e$ si et seulement si n divise k.*

De plus, tout groupe $(G, \star)$ possède un unique élément d'ordre 1 : son élément neutre e_G.

PROPOSITION 33
Soit $(G, \star)$ un groupe fini de cardinal n.
Alors, pour tout $x \in G$, il existe un entier $p \in [\![1, n]\!]$ tel que $x^p = e$.

Preuve — Comme G est fini et comme $\langle x \rangle < G$, alors $\langle x \rangle$ est fini et $\text{ord}(x) \leq n$. La proposition précédente permet de conclure. □

REMARQUE 34 — *Les groupes pouvant se définir de façon très formelle, comment classifier les groupes, comment les identifier ?*

On retrouvera des ensembles de nature très différente comme $\mathbb{Z}/n\mathbb{Z}$, $\mathcal{U}_n$, groupes de rotations... mais qui ont en fait les mêmes propriétés.

2.3 MORPHISMES DE GROUPES, ISOMORPHISMES

Définitions et premières propriétés

Les groupes sont des ensembles importants en mathématiques, on les retrouve dans beaucoup de domaines et dans beaucoup de situations. Avec des ensembles, on regarde des fonctions définies sur ces ensembles.
Pour les espaces vectoriels on regarde les applications linéaires, les fonctions sur des e.v. qui préservent la structure d'espace vectoriel. Pour les groupes, nous allons regarder les fonctions qui préservent la structure de groupe.

DÉFINITION 35
Soit $(G, *)$ et $(H, \triangle)$ deux groupes.
Une fonction $\varphi : G \to H$ est un **morphisme de groupes** (\同态\) si l'on a :

$$\forall x, y \in G,\ \varphi(x * y) = \varphi(x) \triangle \varphi(y).$$

De plus, on dit que φ est :

1. un endomorphisme de groupes si $G = H$.
2. un **isomorphisme** de groupes(\同构\) si φ est bijective.
3. un automorphisme de groupes si φ est un endomorphisme bijectif.

EXEMPLE 36 —

1. *Pour $(G, \star_1)$ et $(H, \star_2)$ deux groupes, la fonction $\varphi : x \in G \mapsto e_H \in H$ est toujours un morphisme de groupes.*
   *On l'appelle **morphisme trivial** de G vers H.*
2. *L'application $n \mapsto 2n$ est-elle un morphisme de groupes sur $(\mathbb{Z}, +)$?*
3. *Soit $(G, \star)$ un groupe et $h \in G$ fixé.*
   La fonction $\varphi : g \in G \mapsto hg \in G$ est-elle un morphisme de groupes ? Est-elle bijective ?
4. *Soit $(G, \star)$ un groupe et $h \in G$ fixé.*
   La fonction $\varphi : g \in G \mapsto hgh^{-1} \in G$ est-elle un morphisme de groupes ? Est-elle bijective ?
5. *La fonction $\theta \to e^{i\theta}$ est un morphisme de groupes de $(\mathbb{R}, +)$ dans $(\mathbb{C}^*, \times)$. Est-elle bijective ?*

Les morphismes de groupes sont les fonctions $f : G \to H$ qui préservent la structure de groupe de G vers H (autrement dit, les fonctions qui sont compatibles avec les lois de ces groupes).

PROPOSITION 37
Soient $(G, *)$, $(H, \triangle)$ des groupes. Soit $\varphi : G \to H$ un morphisme de groupes. Alors :

1. On a $\varphi(e_G) = e_H$ et $\varphi(x^{-1}) = \varphi(x)^{-1}$ pour tout $x \in G$;
2. Si G' est un sous-groupe de G, alors $\varphi(G') = \{\varphi(x),\ x \in G'\}$ est un sous-groupe de H ;
3. Si H' est un sous-groupe de H, alors $\varphi^{-1}(H') = \{x \in G$,tels que $\varphi(x) \in H'\}$ est un sous-groupe de G.

Preuve — 1) On a $f(e_G) = f(e_G * e_G) = f(e_G) \triangle f(e_G)$, donc $e_H = f(e_G)$.

Le restant des preuves est à faire en exercice. □

Proposition 38
Soient $(G,*)$, $(H,\triangle)$ des groupes et $\varphi : G \to H$ un morphisme de groupes. Soit $x \in G$ d'ordre fini n.
Alors on a $\varphi(x)^n = e_H$.

De plus, $\text{ord}(\varphi(x))$ divise $\text{ord}(x)$.

Preuve — On a $\varphi(x)^n = \varphi(x^n) = \varphi(e_G) = e_H$. Avec la remarque 32, on en déduit que l'ordre de $\varphi(x)$ divise $n = \text{ord}(x)$, ce qui conclut. □

Remarque 39 — *Ce résultat permet de montrer que des fonctions φ données ne sont pas des morphismes. Cela permet aussi de compter le nombre de morphismes possibles entre deux groupes finis G et H.*
En effet, pour $x \in G$ d'ordre n, $\varphi(x)$ doit être un élément de H dont l'ordre divise n. Le nombre de possibilités est parfois très réduit (voire limité à 1 seule possibilité : le morphisme trivial).

Exemple 40 — *Soient $G = \mathbb{Z}/2Z = \{0,1\}$ et $H = \mathbb{Z}$, munis de leurs lois respectives (comme vu précédemment). Soit $\varphi : G \to H$ un morphisme de groupes.*

On a alors $\varphi(0) = 0$. Dans $\mathbb{Z}/2Z$, l'élément 1 est d'ordre 2 (car $1+1=0$).
Or, dans Z, tout entier n non-nul est d'ordre infini, tandis que 0 est d'ordre 1.

Comme φ est un morphisme de groupes, on doit donc avoir $\varphi(1) = 0$. Ainsi le seul morphisme de groupes de $Z/2Z$ vers $\mathbb{Z}$ est le morphisme trivial.

Définition 41
Soient $(G,*)$, $(H,\triangle)$ des groupes. Soit $\varphi : G \to H$ un morphisme de groupes.
On appelle **noyau** de φ l'image réciproque de e_H.
On le note $\text{Ker}(\varphi) = \varphi^{-1}(\{e_H\})$ (de l'allemand "*Ker*nel" = "noyau").

Le noyau de φ, $\text{Ker}(\varphi)$, est un sous-groupe de G.

Proposition 42
Soient $(G,*)$, $(H,\triangle)$ des groupes et $\varphi : G \to H$ un morphisme de groupes.
Le morphisme φ est injectif si et seulement si $\ker\varphi = \{e_G\}$.

Preuve — Si la fonction φ est injective on a bien $\text{Ker}\varphi = \{e_G\}$ puisque $\varphi(e_G) = e_H$.

Réciproquement, supposons que $\text{Ker}\varphi = \{e_G\}$. Soient $x, x' \in G$ tels que $\varphi(x) = \varphi(x')$. On a alors alors $\varphi(x)\triangle\varphi(x')^{-1} = e_H$, donc $\varphi(x * x'^{-1}) = e_H$. Cela donne $x * x'^{-1} = e_G$, c'est-à-dire $x = x'$. Donc φ est injectif. □

Exemple 43 — *La fonction $\varphi : z \in (\mathbb{C}^*, \times) \mapsto |z| \in (\mathbb{R}_+^*, \times)$ est un morphisme de groupes, et $\text{Ker}(\varphi) = \varphi^{-1}(\{1\}) = \mathbb{U}$. Ainsi, $(\mathbb{U}, \times)$ est un sous-groupe de $(\mathbb{C}, \times)$ et φ n'est pas injectif.*

Isomorphismes de groupes

Définition 44
Soient $(G,*)$, $(H,\triangle)$ deux groupes.
On dit que G et H sont **isomorphes** s'il existe un isomorphisme de groupes φ entre G et H.
On le note $G \simeq H$.

Proposition 45
Soient $(G,*)$, $(G',\triangle)$ deux groupes et $\varphi : G \to G'$ un isomorphisme de groupes.
Alors $\varphi^{-1} : G' \to G$ est encore un isomorphisme de groupes.

Preuve — Il faut montrer que $\varphi^{-1} : G' \to G$ est un morphisme de groupes.

On a pour commencer $\varphi^{-1}(e_{G'}) = e_G$. Soient $y, y' \in G'$. Comme $\varphi(x)$ est surjective, il existe $x, x' \in G$ tels que $\varphi(x) = y$ et $\varphi(x') = y'$. Le calcul donne :

$$\begin{array}{rcl} \varphi^{-1}(y\triangle y') & = & \varphi^{-1}(\varphi(x)\triangle\varphi(x')) \\ & \underset{\varphi \text{ morphisme}}{=} & \varphi^{-1}(\varphi(x * x')) \\ & = & x * x' = \varphi^{-1}(y) * \varphi^{-1}(y') \end{array}$$

□

Remarque 46 — *La relation "$\mathcal{GRH}$ si G et H sont des groupes isomorphes" est ainsi une relation d'équivalence sur la classe de tous les groupes.*
Les classes d'équivalence pour cette relation (la relation "à isomorphisme près") sont des classes de groupes qui sont tous isomorphes.
Quand on étudie la structure d'un groupe, ce qui nous intéresse est le comportement entre les éléments. Deux groupes isomorphes vont avoir exactement la même structure, ce qui fait que l'on étudie souvent les groupes "à isomorphisme près".
Ainsi, être capable de classer les groupes pour cete relation d'équivalence, de dire si G est isomorphe à H ou non, est une chose très importante en théorie des groupes.

Remarque 47 — *Soient G, H deux groupes isomorphes (via $\varphi : G \to H$).*

- *Alors G et H ont même cardinal.*
- *Tout élément $x \in G$ d'ordre fini n est envoyé sur un élément $\varphi(x) \in H$ d'ordre fini n.*
- *On a une bijection entre les solutions de l'équation $x^n = e_G$ et celles de $y^n = e_H$.*
  Plus généralement, on a une bijection entre les solutions de $x^n = g$ et celles de $y^n = \varphi(g)$.
- *De même, G est abélien si et seulement si H est abélien.*

Ces résultats sont utiles pour montrer que deux groupes ne sont pas isomorphes.
Cela permet aussi de voir quels éléments de la "structure" d'un groupe sont totalement identiques entre G et H quand $G \simeq H$.

Exemple 48 —

1. *$(\mathbb{Z}, +)$ n'est pas isomorphe à $(\mathbb{Q}, +)$. (Le vérifier.)*
2. *$(\mathbb{Q}, +)$ n'est pas isomorphe à $(\mathbb{R}, +)$. (Le vérifier.)*
3. *Il existe une infinité de morphismes de groupes sur $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. (Les $x \mapsto nx$ sont des morphismes de groupes additifs, par exemple).*
4. *Un groupe fini et un groupe infini ne peuvent pas être isomorphes.*
5. *Le groupe $(\bigcup_{n\geq 1} \mathbb{U}_n, \times)$ de toutes les racines n-èmes de l'unité n'est pas isomorphe à $\mathbb{Z}$,$\mathbb{Q}$,$\mathbb{R}$,$\mathbb{C}$. (Le démontrer.)*
6. *Le groupe $(\mathbb{R}, +)$ est isomorphe à $(]0, +\infty[, \times)$. (Chercher une fonction f qui sera l'isomorphisme.)*
7. *Le sous-groupe de $(\mathbb{U}, \times)$ engendré par e^i est isomorphe à $\mathbb{Z}$.*

Exemple 49 —

1. *Soit G un groupe. Soient H, K deux sous-groupes de G tels que $H \cap K = \{e\}$, $HK = G$, et $hk = kh$ pour tous $(h, k) \in H \times K$.*
   Alors, $\varphi : (h, k) \in H \times K \mapsto hk \in G$ est un isomorphisme de groupes.
   On vérifie en effet que c'est un morphisme de groupes car les éléments de H et K commutent entre eux. Ce morphisme est surjectif car $HK = G$. Enfin, $\varphi(h, k) = hk = e$ implique que $h = k^{-1}$, d'où $h, k \in H \cap K = \{e\}$, donc $\mathrm{Ker}(\varphi) = \{(e, e)\}$, ce qui veut dire que φ est injectif.
2. *Les groupes $(\mathbb{R}^{+*}, \times)$ et $(\mathbb{R}, +)$ sont isomorphes via $x \mapsto \ln x$.*
   Par contre, $(\mathbb{R}^*, \times)$ et $(\mathbb{R}, +)$ ne sont pas isomorphes. L'équation $x \star x = e_G$ a deux solutions dans le premier groupe (elle vaut $x^2 = 1$) et seulement une dans le second (elle vaut $2x = 0$).
   On peut montrer cependant que $(\mathbb{R}^*, \times)$ est isomorphe à $(\mathbb{R}^{+*} \times \{-1, 1\}, \times)$.

Remarque 50 — *Un enjeu de la théorie des groupes est de classifier les groupes à isomorphisme près (classes d'équivalence) et de trouver un représentant simple à décrire ou à utiliser.*

2.4 Le groupe $\mathbb{Z}/n\mathbb{Z}$

Un groupe monogène G est un groupe engendré par un élément a.
On a donc un morphisme surjectif de groupes :

$$\varphi : (\mathbb{Z}, +) \to (G, *), \quad k \mapsto a^k.$$

Le noyau de ce morphisme est un sous-groupe de $\mathbb{Z}$, il est donc de la forme $n\mathbb{Z}$.

Si $n = 0$, alors φ injectif et est donc un isomorphisme.

Sinon, on montrera que G est isomorphe à un groupe cyclique d'ordre n, le groupe $\mathbb{Z}/n\mathbb{Z}$.

Exemple 51 — *Le groupe $\mathbb{U}_n$ des racines n-ièmes de l'unité est un groupe cyclique d'ordre n.*
On montrera que ce groupe est isomorphe au groupe $\mathbb{Z}/n\mathbb{Z}$, une fois que celui-ci sera construit.

Relation de congruence

Définition 52
Soit $\varepsilon \in \mathbb{R}$. On définit sur $\mathbb{R}$ la relation de **congruence modulo** ε par :

$$x \equiv y \bmod \varepsilon \iff x - y \in \varepsilon\mathbb{Z} = \{\varepsilon k,\, k \in \mathbb{Z}\}.$$

Proposition 53
Pour $x \in \mathbb{R}$, l'ensemble des éléments y tels que $x \equiv y \bmod \varepsilon$ est :

$$\bar{x} = x + \varepsilon\mathbb{Z} = \{x + \varepsilon k,\, k \in \mathbb{Z}\}.$$

Si $\varepsilon \neq 0$, alors pour tout $x \in \mathbb{R}$ il existe un unique $y \in [0, \varepsilon[$ tel que $x \equiv y \bmod \varepsilon$. C'est-à-dire :

$$\exists!(y, k) \in [0, \varepsilon[\times\mathbb{Z},\ x = y + k\varepsilon.$$

Preuve — Pour l'existence et l'unicité de y, on peut procéder par analyse-synthèse en se demandant quel est le lien entre k et $\frac{x}{\varepsilon}$. □

Remarque 54 — *Pour $n \in \mathbb{N}$, on notera encore $p \equiv q \bmod n$ la relation de congruence induite sur $\mathbb{Z}$, qui est celle définie dans les chapitres Relations et Arithmétique.*
Ces relations de congruence sont des relations d'équivalence.

On sait que les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$. Pour les sous-groupes de $(\mathbb{R}, +)$, nous avons la proposition suivante qui donne une information très importante à leur sujet.

Proposition 55
Tout sous-groupe de $(\mathbb{R}, +)$ est soit dense dans $\mathbb{R}$, soit de la forme $a\mathbb{Z}$, $a \in \mathbb{R}^+$.

Preuve — Notons tout d'abord que $a\mathbb{Z}$ est bien un sous-groupe de $\mathbb{R}$.
Soit G un sous-groupe de $\mathbb{R}$. Si G a un seul élément, alors $G = \{0\}$ et $a = 0$ convient.
On suppose que G a au moins deux éléments. On pose :

$$H = \{|y - x| \mid x, y \in G, x \neq y\} = G \cap \mathbb{R}^{+*} \quad \text{et} \quad a = \inf H.$$

Comme H est une partie non vide de $\mathbb{R}$ minorée par 0, a existe. On distingue deux cas :

1. Si $a = 0$, par caractérisation de la borne inférieure, alors il existe une suite $(\varepsilon_n)_{n\in\mathbb{N}} \in H^{\mathbb{N}} \subset G^{\mathbb{N}}$ strictement décroissante et qui tend vers 0.
   Soit $]x, z[$ un intervalle non vide de $\mathbb{R}$. Montrons alors que $G \cap]x, z[\neq \emptyset$: on choisit ε_n tel que $\varepsilon_n < z - x$. La proposition précédente appliquée à x et ε_n donne :
   $$x = k\varepsilon_n + y,\ 0 \leq y < \varepsilon_n.$$
   On a alors $(k+1)\varepsilon_n \in G$ et $x < k\varepsilon_n + \varepsilon_n < z$, donc $G \cap]x, z[\neq \emptyset$.
2. Si $a \neq 0$, on montre d'abord que $a \in H$: Si ce n'était pas le cas, par caractérisation de la borne inférieure, il existerait une suite strictement décroissante $(a_n) \in H^{\mathbb{N}}$ qui tend vers a. Comme $H \subset G$, on aurait alors $a_n - a_{n+1} \in H \setminus \{0\}$ avec $a_n - a_{n+1} \to 0$, ce qui contredit le fait que $a \neq 0$.
   Enfin, tout $z \in H$ est de la forme $z = ka + z'$ avec $0 \leq z' < a$. Par définition de H et de a, on doit avoir $z' = 0$, donc $H \subset a\mathbb{N}$. L'inclusion réciproque se montre facilement. On en déduit donc que $G = a\mathbb{Z}$.

□

§ *1. Construction de $\mathbb{Z}/n\mathbb{Z}$, Groupe $(\mathbb{Z}/n\mathbb{Z}, +)$*

Définition 56
Soit $n \in \mathbb{N}$. Pour $p \in \mathbb{Z}$, on note $\overline{p} := p + n\mathbb{Z} = \{p + nk,\, k \in \mathbb{Z}\}$ l'ensemble des entiers congrus à p modulo n.
Ce sont les **classes d'équivalences** pour la relation de congruence modulo n.
L'entier p est ainsi un **représentant** de la classe d'équivalence $\overline{p}$.

On définit $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$ l'ensemble des classes d'équivalence modulo n.
$\mathbb{Z}/n\mathbb{Z}$ est l'ensemble quotient de la relation d'équivalence de congruence modulo n. (voir chapitre Relations)

On peut remarquer que pour r le reste de la division euclidienne de p par n, on a $0 \leq r < n$ et $\overline{r} = \overline{p}$.
Autrement dit, chaque classe d'équivalence $\overline{p}$ possède un représentant compris entre 0 et $n - 1$.
Ainsi, l'ensemble $\overline{p}$ est bien un élément de l'ensemble d'ensembles $\mathbb{Z}/n\mathbb{Z}$. (déjà démontré dans le chapitre Relations)

PROPOSITION-DÉFINITION 57 (Opérations sur $\mathbb{Z}/n\mathbb{Z}$)
Soit $n \in \mathbb{N}$. Pour tous $p, q \in \mathbb{Z}$, on a :

$$\overline{p} + \overline{q} = \{a + b,\ a \in \overline{p}, b \in \overline{p}\} = \overline{p+q},$$
$$\overline{p} \times \overline{q} = \{ab,\ a \in \overline{p}, b \in \overline{p}\} = \overline{pq},$$

les opérations d'addition et de multiplication étant ici celles définies pour des sous-ensembles de $\mathbb{Z}$.
Ces opérations définissent ainsi des lois de composition internes sur $\mathbb{Z}/n\mathbb{Z}$, notées $\overline{+}$ et $\overline{\times}$.
Ces lois de composition sont associatives et commutatives.
La loi $\overline{+}$ admet pour élément neutre $\overline{0}$ et la loi $\overline{\times}$ admet pour élément neutre $\overline{1}$.
Enfin, $\left(\mathbb{Z}/n\mathbb{Z}, \overline{+}\right)$ est un groupe.

Preuve — Soient $p, q \in \mathbb{Z}$. On a :

$$\overline{p} + \overline{q} = \{(p + kn) + (q + rn),\ k, r \in \mathbb{Z}\} = \{(p + q) + sn,\ s \in \mathbb{Z}\} = \overline{p+q},$$
$$\overline{p} \times \overline{q} = \{(p + kn)(q + rn),\ k, r \in \mathbb{Z}\} = \{pq + n(kq + rp + n),\ k, r \in \mathbb{Z}\} = \{pq + ns,\ s \in \mathbb{Z}\} = \overline{pq}.$$

Ainsi, la somme de deux classes de $\mathbb{Z}/n\mathbb{Z}$ est encore une classe de $\mathbb{Z}/n\mathbb{Z}$, et le produit de deux classes de $\mathbb{Z}/n\mathbb{Z}$ est encore une classe de $\mathbb{Z}/n\mathbb{Z}$.
Comme la somme et le produit d'ensembles sont commutatifs, les lois $\overline{+}$ et $\overline{\times}$ sont donc commutatives sur $\mathbb{Z}/n\mathbb{Z}$.
De même, la somme et le produit d'ensembles sont associatifs $(A + (B + C) = (A + B) + C$ et $(A \times (B \times C) = (A \times B) \times C)$, les lois $\overline{+}$ et $\overline{\times}$ sont donc associatives sur $\mathbb{Z}/n\mathbb{Z}$.
On a : $\overline{0+p} = \overline{p} = \overline{p+0}$ et $\overline{1 \times p} = \overline{p \times 1} = \overline{p}$.

□

REMARQUE 58 —

1. *Soit $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ et $k \in \mathbb{N}$, on note $k\overline{a} = \overline{a} \overline{+} \cdots \overline{+} \overline{a}$, la somme de k copies de a. On a $k\overline{a} = \overline{ka}$.*
2. *Le symétrique pour la loi $\overline{+}$ de $\overline{p}$ est $\overline{-p}$.*
3. *Le groupe $(\mathbb{Z}/n\mathbb{Z}, \overline{+})$ est un groupe de cardinal n, qui est commutatif. ($\overline{p} + \overline{q} = \overline{q} + \overline{p}$)*
4. *La fonction $k \in \mathbb{Z} \mapsto \overline{k} \in \mathbb{Z}/n\mathbb{Z}$, est un morphisme de groupes surjectif, de noyau $n\mathbb{Z}$.*
5. *Pour $n = 0$, $\mathbb{Z}/0\mathbb{Z}$ est ainsi isomorphe à $\mathbb{Z}$ de façon triviale. (la relation de congruence modulo 0 est la relation d'égalité)*
   Ce cas n'est pas très intéressant. Ce cas sera souvent écarté par la suite.
6. *Pour $n = 1$, on a $\mathbb{Z}/1\mathbb{Z} = \{\overline{0}\}$. Ce groupe ne contient donc que son élément neutre.*
   *On appelle un tel groupe le **groupe trivial**. (le groupe à 1 élément)*

Lorsqu'il n'y a pas d'ambiguité avec les lois de $\mathbb{Z}$, les lois $\overline{+}$ et $\overline{\times}$ de $\mathbb{Z}/n\mathbb{Z}$ pourront être notées $+$ et $\times$.

EXEMPLE 59 —

1. *Écrire les tables d'addition et de multiplication de $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}$.*
2. *Le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est-il cyclique ? Ecrire la table d'addition du groupe $\mathbb{Z}/2\mathbb{Z}$. Est-elle similaire à celle de $\mathbb{Z}/4\mathbb{Z}$?*
3. *Le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ est-il cyclique ?*

L'ensemble $(\mathbb{Z}/n\mathbb{Z}, \overline{\times})$ muni de sa loi multiplicative n'est pas un groupe !
Cela vient du fait que certains éléments de $\mathbb{Z}/n\mathbb{Z}$ n'admettent pas d'inverse pour la loi $\overline{\times}$, comme par exemple $\overline{0}$.
Même si les lois additives et multiplicatives sont toutes deux associatives et commutatives, les structures de $(\mathbb{Z}/n\mathbb{Z}, \overline{+})$ et $(\mathbb{Z}/n\mathbb{Z}, \overline{\times})$ sont très différentes.
Il faut faire attention à ne pas les confondre (par ex., $\overline{2 + 2 + 2}$ est en général différent de $\overline{2.2.2}$).

PROPOSITION 60
Soit $n \in \mathbb{N}^*$. Le groupe $\left(\mathbb{Z}/n\mathbb{Z}, \overline{+}\right)$ possède des générateurs.
Ce sont exactement les classes $\overline{m}$, avec $\text{pgcd}(m, n) = 1$. (on a $\mathbb{Z}/n\mathbb{Z} = \langle \overline{m} \rangle$)

Preuve — Si $\overline{m}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$, alors on a $1 \in \overline{km}$ pour un $k \in [\![1, n-1]\!]$, ce qui s'écrit

$$1 = km + ln \text{ avec } l \in \mathbb{Z}.$$

Ainsi, (voir chapitre Arithmétique) on a $\text{pgcd}(m, n) = 1$.
Réciproquement, si $\text{pgcd}(m, n) = 1$, la relation de Bézout $1 = km + ln$ montre que $1 \in \overline{km} = k\overline{m}$. Pour tout $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, on a donc $\overline{a} = (ak)\overline{m}$, ce qui donne $\mathbb{Z}/n\mathbb{Z} = \langle \overline{m} \rangle$. Donc $\overline{m}$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, \overline{+})$. □

Définition 61
Soit $n \geq 1$. On définit $\varphi(n)$ le nombre de générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$.
L'entier $\varphi(n)$ est appelé **l'indicatrice d'Euler** de n.
On a donc $\varphi(n) = Card(\{1 \leq m \leq n-1 \text{ tels que } \text{pgcd}(m,n) = 1\})$.

Nous verrons avec d'autres théorèmes comment calculer l'indicatrice d'Euler de n'importe quel entier n.
Pour terminer cette section sur les groupes $(\mathbb{Z}/n\mathbb{Z}, +)$, nous allons étudier les équations diophantiennes.

2.5 Équations diophantiennes

2.5.1 Equations diophantiennes

Définition 62
Une équation diophantienne est une équation à coefficients entiers et dont les solutions sont cherchées parmi les nombres entiers.

Donnons un premier exemple de résolution d'une équation diophantienne. Cela permettra de donner la forme générale des solutions d'une équation diophantienne à 2 inconnues.

Soient a, b, c dans $\mathbb{Z}$ avec a et b non nuls. On se propose de résoudre dans $\mathbb{Z}^2$ l'équation d'inconnue (x, y) :

$$ax + by = c.$$

Notons $d = \text{pgcd}(a, b)$. Supposons que l'équation admette une solution (x_0, y_0).
Comme d divise a et b, d divise alors $ax_0 + by_0 = c$. Donc si d ne divise pas c, l'équation n'a pas de solutions.

Dans la suite, on suppose donc que d divise c. On a donc $c = dc'$ pour un $c' \in \mathbb{Z}$. Il existe aussi $a', b' \in \mathbb{Z}$ tels que $a = da'$, $b = db'$, et $\text{pgcd}(a', b') = 1$. En divisant par $d \neq 0$, on a alors $ax + by = c$ si et seulement si $a'x + b'y = c'$.
On est donc ramené à étudier l'ensemble des solutions dans $\mathbb{Z}^2$ de $a'x + b'y = c'$, avec $\text{pgcd}(a', b') = 1$.

Comme a' et b' sont premiers entre eux, le théorème de Bézout nous dit qu'il existe $(u, v) \in \mathbb{Z}^2$ tel que

$$a'u + b'v = 1.$$

En multipliant par c', on otient $a'(c'u) + b'(c'v) = c'$. Ainsi, $(x_0, y_0) = (c'u, c'v) \in \mathbb{Z}^2$ est une solution de l'équation $a'x + b'y = c'$, donc cette équation admet donc au moins une solution.

Soit $(x, y) \in \mathbb{Z}^2$ une solution de l'équation $a'x + b'y = c'$. Comme on a

$$a'x_0 + b'y_0 = c',$$

on en déduit que

$$a'(x - x_0) + b'(y - y_0) = 0,$$

soit encore

$$a'(x - x_0) = b'(y_0 - y).$$

On a ainsi $a' \mid b'(y_0 - y)$. Comme a' et b' sont premiers entre eux, le théorème de Gauss nous dit que $a' \mid y_0 - y$.
Il existe donc $k \in \mathbb{Z}$ tel que $y_0 - y = ka'$, c'est-à-dire $y = y_0 - ka'$.

On a ainsi $a'(x - x_0) = b'ka'$, donc $x - x_0 = kb'$, soit $x = x_0 + kb'$.

Réciproquement, soit $k \in \mathbb{Z}$. On a $a'(x_0 + kb') + b'(y_0 - ka') = a'x_0 + b'y_0 = c$, donc $(x_0 + kb', y_0 - ka')$ est une solution de l'équation.

Ainsi, l'ensemble des solutions de $a'x + b'y = c'$, et donc de $ax + by = c$, est

$$\mathcal{S} = \{(x_0 + kb', y_0 - ka') \mid k \in \mathbb{Z}\}.$$

Proposition 63
Soient a, b, c dans $\mathbb{Z}$ avec a et b non nuls. Alors, l'équation diophantienne d'inconnue (x, y) :

$$ax + by = c,$$

possède des solutions si et seulement si $\text{pgcd}(a, b)$ divise c.
Si cette équation possède des solutions, on peut trouver une solution (x_0, y_0) en utilisant l'algorithme d'Euclide pour a et b et en le remontant.
L'ensemble des solutions de l'équation est alors

$$\mathcal{S} = \{(x_0 + kb', y_0 - ka') \mid k \in \mathbb{Z}\}.$$

Illustrons cette méthode sur un exemple.

Exemple 64 — *Résolvons dans $\mathbb{Z}^2$ l'équation $36x + 21y = 9$.*

On a $\text{pgcd}(36, 21) = 3$ et $3 \mid 9$ donc cette équation admet des solutions dans $\mathbb{Z}^2$.

Par division par 3, l'ensemble des solutions de $36x + 21y = 9$ est égal à l'ensemble des solutions de $12x + 7y = 3$.

Appliquons l'algorithme d'Euclide étendu pour déterminer des coefficients de Bézout de 12 et 7.

$$\begin{array}{rclcrcl} 12 &=& 7 \times 1 + 5 & | & 7 &=& 0 \times 12 + 1 \times 7 \\ 7 &=& 5 \times 1 + 2 & | & 5 &=& 1 \times 12 - 1 \times 7 \\ 5 &=& 2 \times 2 + 1 & | & 2 &=& -1 \times 12 + 2 \times 7 \\ 2 &=& 1 \times 2 + 0 & | & 1 &=& 3 \times 12 - 5 \times 7 \end{array}$$

En multipliant par 3, on obtient

$$3 = 9 \times 12 - 15 \times 7,$$

donc $(x_0, y_0) = (9, -15)$ est une solution de l'équation $12x + 7y = 3$.

Soit $(x, y) \in \mathbb{Z}^2$ une solution de l'équation $12x + 7y = 3$. Par soustraction d'équations, on obtient $12(x - x_0) = 7(y_0 - y)$. Donc $12 \mid 7(y_0 - y)$. Comme 12 et 7 sont premiers entre eux, le théorème de Gauss donne $12 \mid y_0 - y$. Il existe donc $k \in \mathbb{Z}$ tel que $y = y_0 - 12k$. Donc $12(x - x_0) = 7 \times 12k$, soit $x = x_0 + 7k$.

Réciproquement, pour tout $k \in \mathbb{Z}$, on a :

$$12(x_0 + 7k) + 7(y_0 - 12k) = 12 \times 9 + 7 \times (-15) = 3$$

donc $(x_0 + 7k, y_0 - 12k)$ est solution de $12x + 7y = 3$.

Ainsi, l'ensemble des solutions de l'équation $12x + 7y = 3$, et donc de $36x + 21y = 9$, est

$$\mathcal{S} = \{(9 + 7k, -15 + 12k) \mid k \in \mathbb{Z}\}.$$

Exemple 65 — *$42x + 66y = 10$ n'admet aucune solution dans $\mathbb{Z}^2$ car $\text{pgcd}(42, 66) = 6$ ne divise pas 10.*

Pour résoudre certaines équations diophantiennes, on peut essayer de résoudre cela modulo n, avec n bien choisi. S'il n'y a pas de solutions modulo n, alors il n'y en a pas dans $\mathbb{Z}$.

Exemple 66 — *L'équation $x^2 + y^2 = 8z + 7$ n'a pas de solutions dans $\mathbb{Z}$.*

Preuve — *Supposons qu'une solution $(x, y, z) \in \mathbb{Z}^3$ existe. Alors modulo 8, on a $x^2 + y^2 \equiv 8z + 7 \bmod 8$, soit $x^2 + y^2 \equiv 7 \bmod 8$.*

Calculons les carrés modulo 8 :

- $0^2 \equiv 0 \bmod 8$,
- $1^2 \equiv 1 \bmod 8$,
- $2^2 \equiv 4 \bmod 8$,

- $3^2 \equiv 1 \bmod 8$,
- $4^2 \equiv 0 \bmod 8$,
- $5^2 \equiv (-3)^2 \bmod 8 \equiv 1 \bmod 8$,

- $6^2 \equiv (-2)^2 \bmod 8 \equiv 4 \bmod 8$,
- $7^2 \equiv (-1)^2 \bmod 8 \equiv 1 \bmod 8$

Donc $x^2 + y^2$ est congru à $0, 1, 2, 3, 4$ ou 5 modulo 8. Ceci contredit le fait que $x^2 + y^2 \equiv 7 \bmod 8$.

L'équation n'admet donc pas de solutions dans $\mathbb{Z}$. □

Maintenant que les équations diophantiennes à 2 inconnues sont résolues, nous allons regarder des équations à valeurs et à solutions dans $\mathbb{Z}/n\mathbb{Z}$: les équations diophantiennes modulaires.

2.5.2 Equations diophantiennes modulaires, théorème chinois

Rappelons que la relation de congruence modulo n est compatible avec les opérations d'addition et de multiplication d'entiers. Par rapport à ces opérations, l'élément neutre pour l'addition $+$ est 0 ($a + 0 \equiv a \bmod n$) et l'élément neutre pour la multiplication $\times$ est 1 ($a \times 1 \equiv a \bmod n$).

Tout comme pour les matrices, avoir $ab \equiv 0 \bmod n$ n'implique par que $a \equiv 0 \bmod n$ ou $b \equiv 0 \bmod n$.
Par exemple, pour $n = 6$, on a $2 \times 3 \equiv 0 \bmod 6$ mais $2 \not\equiv 0 \bmod 6$ et $3 \not\equiv 0 \bmod 6$.

Dans $\mathbb{Z}/n\mathbb{Z}$, il faut ainsi distinguer les éléments $\overline{a}$ avec lesquels on peut effectuer une division des autres. (la division est l'opération réciproque à la multiplication, mais on ne peut pas diviser par n'importe quel élément)

Définition 67
Soient $a, n \in \mathbb{Z}$, avec $n \neq 0$. On dit que a est inversible modulo n s'il existe un élément $u \in \mathbb{Z}$ tel que $au \equiv 1 \bmod n$.
L'entier u est alors un inverse de a modulo n.
Dans $\mathbb{Z}/n\mathbb{Z}$, on a alors $\overline{a}.\overline{u} = \overline{1}$.
L'entier a est inversible modulo n si et seulement si la classe $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

Proposition 68
Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$.
Alors, a est inversible modulo n si et seulement si a et n sont premiers entre eux.
Ainsi, la classe $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $\overline{a}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$.

Preuve — L'entier a est inversible modulo n si et seulement s'il existe $u \in \mathbb{Z}$ tel que $au \equiv 1 \bmod n$, donc si et seulement s'il existe $(u, v) \in \mathbb{Z}^2$ tel que $ua = 1 + vn$, c'est-à-dire $au + n(-v) = 1$. Donc, d'après le théorème de Bézout, a est inversible modulo n si et seulement si a et n sont premiers entre eux.
Enfin, on a vu dans un résultat précédent que les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les classes $\overline{m}$ avec $\text{pgcd}(m, n) = 1$. □

Méthode 69 — *Si a est inversible modulo n, on peut toujours trouver un inverse en calculant la relation de Bézout $au + nv = 1$, puisque a et n sont premiers entre eux. Un inverse de a modulo n sera alors u.*

Tous les inverses de a modulo n seront de la forme $b = u + kn$, $k \in \mathbb{Z}$, car ils correspondent à la première coordonnée x des solutions (x, y) de l'équation diophantienne $ax + ny = 1$.

Exemple 70 — *$18 = 2 \times 3^2$ et $49 = 7^2$ sont premiers entre eux donc 18 est inversible modulo 49.*

Déterminons à l'aide de l'algorithme d'Euclide étendu une relation de Bézout entre 18 et 49.

$$\begin{array}{rcl|rcl} 49 &=& 18 \times 2 + 13 & 18 &=& 0 \times 49 + 1 \times 18 \\ 18 &=& 13 \times 1 + 5 & 13 &=& 1 \times 49 - 2 \times 18 \\ 13 &=& 5 \times 2 + 3 & 5 &=& -1 \times 49 + 3 \times 18 \\ 5 &=& 3 \times 1 + 2 & 3 &=& 3 \times 49 - 8 \times 18 \\ 3 &=& 2 \times 1 + 1 & 2 &=& -4 \times 49 + 11 \times 18 \\ 2 &=& 1 \times 2 + 0 & 1 &=& 7 \times 49 - 19 \times 18 \end{array}$$

On en déduit que $1 \equiv (-19) \times 18 \bmod 49 \equiv 30 \times 18 \bmod 49$. Donc 30 est un inerse de 18 modulo 49 (et -19 aussi).

Exemple 71 — *Déterminons les solutions de l'équation $7x \equiv= 10 \bmod 37$.*

Les entiers 7 et 37 étant premiers entre eux, 7 est inversible modulo 37.

L'algorithme d'Euclide étendu donne :

$$\begin{array}{rcl|rcl} 37 &=& 7 \times 5 + 2 & 7 &=& 0 \times 37 + 1 \times 7 \\ 7 &=& 2 \times 3 + 1 & 2 &=& 1 \times 37 - 5 \times 7 \\ 2 &=& 1 \times 2 + 0 & 1 &=& -3 \times 37 + 16 \times 7 \end{array}$$

Donc, $1 \equiv 16 \times 7 \bmod 37$, et 16 est un inverse de 7 modulo 37.

De même, 16 est inversible modulo 37 et 7 est l'un de ses inverses. Ainsi, on a : $7x \equiv= 10 \bmod 37 \Leftrightarrow x \equiv= 160 \bmod 37 \Leftrightarrow x \equiv= 12 \bmod 37$ L'équation $7x \equiv= 10 \bmod 37$ admet donc pour solutions les entiers de la forme $x = 12 + 37k$, $k \in \mathbb{Z}$.
Dans $\mathbb{Z}/37\mathbb{Z}$ on a montré que $\overline{7}$ est inversible, d'inverse $\overline{16}$.

Ainsi, on a

$$\overline{7x} = \overline{10} \Leftrightarrow \overline{10}.\overline{7}.\overline{x} = \overline{16}.\overline{10} \Leftrightarrow \overline{x} = \overline{160} = \overline{12}.$$

Dans $\mathbb{Z}/37\mathbb{Z}$ *cette équation admet une unique solution, qui est* $\overline{12}$.

Pour un système d'équations diophantiennes modulaires, avec plusieurs modulo différents, on peut transformer ce système en un système plus petit avec un seul modulo commun. C'est le théorème des restes chinois.

THÉORÈME 72 (Théorème des restes chinois)
Soient $m_1, m_2 \in \mathbb{N}^*$ premiers entre eux. Soient $a, b \in \mathbb{Z}$.
Alors le système de congruences d'inconnue $x \in \mathbb{Z}$:

$$\begin{cases} x \equiv a \bmod m_1 \\ x \equiv b \bmod m_2 \end{cases}$$

admet une solution dans $\mathbb{Z}$.
De plus, si $x_0 \in \mathbb{Z}$ est une solution, alors l'ensemble des solutions dans $\mathbb{Z}$ est $x_0 + m_1 m_2 \mathbb{Z} = \{x_0 + m_1 m_2 k \mid k \in \mathbb{Z}\}$.
Autrement dit, pour x_0 une solution du système d'équations, on a :

$$\begin{cases} x \equiv a \bmod m_1 \\ x \equiv b \bmod m_2 \end{cases} \Leftrightarrow \begin{cases} x \equiv x_0 \bmod m_1 m_2 \end{cases}$$

Preuve — Comme m_1 et m_2 sont premiers entre eux, le théorème de Bézout donne l'existence de $(u, v) \in \mathbb{Z}^2$ tel que $m_1 u + m_2 v = 1$.

On a donc

$$\begin{cases} m_1 u \equiv 0 \bmod m_1 \\ m_1 u \equiv 1 \bmod m_2 \end{cases} \quad \text{et} \quad \begin{cases} m_2 v \equiv 1 \bmod m_1 \\ m_2 v \equiv 0 \bmod m_2 \end{cases}.$$

D'où :

$$\begin{cases} b m_1 u + a m_2 v \equiv b \times 0 + a \times 1 \equiv a \bmod m_1 \\ b m_1 u + a m_2 v \equiv b \times 1 + a \times 0 \equiv b \bmod m_2 \end{cases}.$$

Ainsi, $x_0 = b m_1 u + a m_2 v$ est une solution du système de congruences

$$\begin{cases} x \equiv a \bmod m_1 \\ x \equiv b \bmod m_2 \end{cases}.$$

Soit $x \in \mathbb{Z}$. Alors x est solution du système si et seulement si

$$\begin{cases} x \equiv x_0 \bmod m_1 \\ x \equiv x_0 \bmod m_2 \end{cases},$$

soit encore si et seulement si $m_1 \mid x - x_0$ et $m_2 \mid x - x_0$. Comme m_1 et m_2 étant premiers entre eux, la proposition 71 nous dit que x est solution si et seulement $m_1 m_2 \mid x - x_0$, soit encore si et seulement s'il existe $k \in \mathbb{Z}$ tel que $x = x_0 + m_1 m_2 k$.

Ce qui donne le résultat. □

REMARQUE 73 — *La solution d'un tel système de congruences est donc unique modulo* $m_1 m_2$.

EXEMPLE 74 — *Déterminons les solutions du système de congruences :*

$$\begin{cases} x \equiv 3 \bmod 5 \\ x \equiv 6 \bmod 13 \end{cases}.$$

5 *et* 13 *sont premiers entre eux. Utilisons l'algorithme d'Euclide étendu pour trouver une relation de Bézout entre* 5 *et* 13 *:*

$$\begin{array}{rcl|rcl} 13 & = & 5 \times 2 + 3 & 5 & = & 0 \times 13 + 1 \times 5 \\ 5 & = & 3 \times 1 + 2 & 3 & = & 1 \times 13 - 2 \times 5 \\ 3 & = & 2 \times 1 + 1 & 2 & = & -1 \times 13 + 3 \times 5 \\ 2 & = & 1 \times 2 + 0 & 1 & = & 2 \times 13 - 2 \times 5 \end{array}$$

On a donc :

$$\begin{cases} 2 \times 13 \equiv 1 \bmod 5 \\ 2 \times 13 \equiv 0 \bmod 13 \end{cases} \quad \textit{et} \quad \begin{cases} -5 \times 5 \equiv 0 \bmod 5 \\ -5 \times 5 \equiv 1 \bmod 13 \end{cases}$$

Ains, $3 \times (2 \times 13) + 6 \times (-5 \times 5) = -72$ *est une solution du système de congruences. On a* $-72 \equiv 3 \bmod 5$ *et* $-72 \equiv 6 \bmod 13$. *D'après le théorème des restes chinois, on a donc :*

$$\begin{cases} x \equiv 3 \bmod 5 \\ x \equiv 6 \bmod 13 \end{cases} \Leftrightarrow \Big\{ x \equiv -72 \bmod 65$$

L'ensemble des solutions est donc $\{-72 + 5 \times 13k \mid k \in \mathbb{Z}\} = \{-72 + 65k \mid k \in \mathbb{Z}\} = \{-7 + 65k' \mid k' \in \mathbb{Z}\}$.

En regardant les groupes $\mathbb{Z}/n\mathbb{Z}$, le théorème des restes chinois s'exprime aussi :

THÉORÈME 75 (Théorème d'isomorphisme chinois)
Soient $m_1, m_2 \in \mathbb{N}^*$ premiers entre eux.
Soit $\phi : (\mathbb{Z}/(m_1m_2)\mathbb{Z}) \to (\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})$ définie par $\phi(\overset{-(m_1m_2)}{c}) = (\overset{-(m_1)}{c}, \overset{-(m_2)}{c})$.
Alors, ϕ est un isomorphisme de groupes.
Soit $um_1 + vm_2 = 1$ une relation de Bézout pour m_1 et m_2. On a alors :

$$\phi^{-1}(\overset{-(m_1)}{a}, \overset{-(m_2)}{b}) = \overset{-(m_1m_2)}{avm_2 + bum_1}.$$

Ainsi, on a

$$(\mathbb{Z}/(m_1m_2)\mathbb{Z}, +) \simeq ((\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z}), +).$$

Preuve — En prenant $c_1, c_2 \in \mathbb{Z}$ et en regardant les classes d'équivalences de $0, c_1, c_2, c_1 - c_2$ modulo m_1, m_2, m_1m_2, on montre que ϕ est un morphisme de groupes.
Soit $c \in \mathbb{Z}$ tel que $\overset{-(m_1m_2)}{c} \in Ker(\phi)$.
On a alors $\overset{-(m_1)}{c} = \overset{-(m_1)}{0}$, $\overset{-(m_2)}{c} = \overset{-(m_2)}{0}$, donc $m_1 \mid c$ et $m_2 \mid c$.
Comme m_1 et m_2 sont premiers entre eux, on obtient $m_1m_2 \mid c$, c'est-à-dire $\overset{-(m_1m_2)}{c} = \overset{-(m_1m_2)}{0}$.
Le morphisme de groupes ϕ est donc injectif.
Comme les groupes $\mathbb{Z}/(m_1m_2)\mathbb{Z}$ et $(\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})$ sont de cardinal m_1m_2, on en déduit que la fonction ϕ est bijective. Donc ϕ est un isomorphisme de groupes.
Calculons sa bijection réciproque ϕ^{-1}.
Comme $\text{pgcd}(m_1, m_2) = 1$, d'après le théorème de Bézout il existe $u, v \in \mathbb{Z}$ tels que $um_1 + vm_2 = 1$.
On a donc $\phi(\overset{-(m_1m_2)}{um_1}) = (\overset{-(m_1)}{0}, \overset{-(m_2)}{1})$ et $\phi(\overset{-(m_1m_2)}{vm_2}) = (\overset{-(m_1)}{1}, \overset{-(m_2)}{0})$.
Pour $a, b \in \mathbb{Z}$, les propriétés des classes d'équivalences pour la congruence modulo n nous donne alors :

$$\overset{-(m_1m_2)}{\phi(avm_2 + bum_1)} = \overset{-(m_1)}{(a.1 + b.0}, \overset{-(m_2)}{a.0 + b.1}) = (\overset{-(m_1)}{a}, \overset{-(m_2)}{b}).$$

On obtient ainsi que $\phi^{-1}(\overset{-(m_1)}{a}, \overset{-(m_2)}{b}) = \overset{-(m_1m_2)}{avm_2 + bum_1}$.

□

Le Théorème des restes chinois se généralise par récurrence à un système de r équations modulaires, $r \geq 2$, où « les modulo » sont deux à deux premiers entre eux.

THÉORÈME 76 (Théorème des restes chinois généralisé)
Soient m_1,...,$m_r \in \mathbb{N}$ des entiers non nuls et premiers entre eux deux à deux.

Alors le système de congruences d'inconnue $x \in \mathbb{Z}$:

$$\begin{cases} x \equiv a_1 \bmod m_1 \\ \quad \vdots \\ x \equiv a_r \bmod m_r \end{cases}$$

admet une solution dans $\mathbb{Z}$.
De plus, si $x_0 \in \mathbb{Z}$ est solution alors l'ensemble des solutions est $x_0 + m_1 \dots m_r\mathbb{Z}$.
Autrement dit, pour x_0 une solution, on a :

$$\begin{cases} x \equiv a_1 \bmod m_1 \\ \quad \vdots \\ x \equiv a_r \bmod m_r \end{cases} \Leftrightarrow \Big\{ x \equiv x_0 \bmod m_1 \dots m_r$$

Preuve — On démontre le résultat par récurrence sur $r \geq 2$, en utilisant le théorème des restes chinois. □

Méthode 77 — *Pour résoudre le système de congruences :*

$$\begin{cases} x \equiv a_1 \bmod m_1 \\ \quad \vdots \\ x \equiv a_r \bmod m_r \end{cases},$$

où les entiers m_i sont premiers entre eux deux à deux, on introduit, pour tout $i \in \{1, \ldots, r\}$, les entiers $M_i = m_1 \times \ldots \times m_{i-1} \times \cancel{m_i} \times m_{i+1} \times \ldots \times m_r = \Pi_{1 \leq j \leq r,\, j \neq i} m_j$.

Soit $i \in \{1, \ldots, r\}$. Par hypothèse, m_i est premier avec tous les m_j, $j \neq i$, et donc avec leur produit M_i.

M_i est donc inversible modulo m_i et il existe donc $y_i \in \mathbb{Z}$ tel que $y_i M_i \equiv 1 \bmod m_i$. De plus, comme pour tout $j \neq i$ on a $m_j \mid M_i$, alors $y_i M_i \equiv 0 \bmod m_j$.
Cela donne ainsi :

$$\begin{cases} y_i M_i \equiv 0 \bmod m_1 \\ \quad \vdots \\ y_i M_i \equiv 1 \bmod m_i \\ \quad \vdots \\ y_i M_i \equiv 0 \bmod m_r \end{cases}.$$

En pratique, on détermine un tel y_i à l'aide d'une relation de Bézout entre m_i et M_i.

Puis, l'entier $x_0 = \sum_{i=1}^{r} a_i y_i M_i = a_1 y_1 M_1 + \ldots + a_r y_r M_r$ est alors une solution du système de congruences.

L'ensemble des solutions est alors $\{x_0 + m_1 \ldots m_r k \mid k \in \mathbb{Z}\}$.

Exemple 78 — *Résolvons le système :*

$$\begin{cases} x \equiv 2 \bmod 4 \\ x \equiv 3 \bmod 5 \\ x \equiv 1 \bmod 9 \end{cases}.$$

Posons $M_1 = 5 \times 9 = 45$, $M_2 = 4 \times 9 = 36$ et $M_3 = 4 \times 5 = 20$.

$m_1 = 4$ et $M_1 = 45$ sont premiers entre eux et $1 = 45 - 11 \times 4$, donc :

$$\begin{cases} 45 \equiv 1 \bmod 4 \\ 45 \equiv 0 \bmod 5 \\ 45 \equiv 0 \bmod 9 \end{cases}.$$

$m_2 = 5$ et $M_2 = 36$ sont premiers entre eux et $1 = 36 - 5 \times 7$, donc :

$$\begin{cases} 36 \equiv 0 \bmod 4 \\ 36 \equiv 1 \bmod 5 \\ 36 \equiv 0 \bmod 9 \end{cases}.$$

$m_3 = 9$ et $M_3 = 20$ sont premiers entre eux et :

$$\begin{aligned} 20 &= 1 \times 20 + 0 \times 9 \\ 9 &= 0 \times 20 + 1 \times 9 \\ 2 &= 1 \times 20 - 2 \times 9 \\ 1 &= -4 \times 20 + 9 \times 9. \end{aligned}$$

Donc :

$$\begin{cases} -4 \times 20 \equiv 0 \bmod 4 \\ -4 \times 20 \equiv 0 \bmod 5 \\ -4 \times 20 \equiv 1 \bmod 9 \end{cases}.$$

Finalement, $x_0 = 2 \times 45 + 3 \times 36 + 1 \times (-4) \times 20 = 118$ *est une solution du système de congruences. D'après le théorème des restes chinois, on a donc :*

$$\begin{cases} x \equiv 2 \bmod 4 \\ x \equiv 1 \bmod 5 \\ x \equiv 1 \bmod 9 \end{cases} \Leftrightarrow \Big\{ x \equiv 118 \bmod 180$$

L'ensemble des solutions est donc $\{118 + 4 \times 5 \times 9k \mid k \in \mathbb{Z}\} = \{118 + 180k \mid k \in \mathbb{Z}\}$.

A nouveau, en regardant les groupes $\mathbb{Z}/n\mathbb{Z}$, le théorème des restes chinois généralisé nous donne un isomorphisme de groupes.

THÉORÈME 79 (Théorème d'isomorphisme chinois généralisé)
Soit $r \geq 2$. Soient $m_1, \ldots, m_2 \in \mathbb{N}^*$ premiers entre eux deux à deux.
Soit $\phi : (\mathbb{Z}/(m_1 \ldots m_r)\mathbb{Z}) \to (\mathbb{Z}/m_1\mathbb{Z}) \times \ldots \times (\mathbb{Z}/m_r\mathbb{Z})$ définie par $\phi(\overset{-(m_1 \ldots m_r)}{c}) = (\overset{-(m_1)}{c}, \ldots, \overset{-(m_r)}{c})$.
Alors, ϕ est un isomorphisme de groupes.
Pour tout $1 \leq i \leq r$, soient $u_i m_i + v_i \Pi_{j \neq i} m_j = 1$ des relations de Bézout pour m_i et $\Pi_{j \neq i} m_j$. On a alors :

$$\phi^{-1}(\overset{-(m_1)}{a_1}, \ldots, \overset{-(m_r)}{a_r}) = \sum_{i=1}^{r} \overset{-(m_1 \ldots m_r)}{a_i v_i \Pi_{j \neq i} m_j}.$$

Ainsi, on a

$$(\mathbb{Z}/(m_1 \ldots m_r)\mathbb{Z}, +) \simeq ((\mathbb{Z}/m_1\mathbb{Z}) \times \ldots \times (\mathbb{Z}/m_r\mathbb{Z}), +).$$

Preuve — Preuve par récurrence sur $r \geq 2$, en utilisant le Théorème d'isomorphisme chinois. □

Le théorème des restes chinois (version généralisée), le théorème de Bézout, et l'algorithme d'Euclide sont les trois résultats qui permettent d'étudier facilement tous les systèmes d'équations modulaires.
Le théorème d'isomorphisme chinois permet de comprendre comment le théorème des restes chinois fonctionne du point de vue des groupes. Il donne en réalité un peu plus d'informations car on a un isomorphisme de groupes (pas uniquement une bijection), et car on a une expression explicite de l'isomorphisme inverse.
L'expression de cet isomorphisme inverse est très utile lorsque l'on travaille sur les $\mathbb{Z}/n\mathbb{Z}$ (dans les exemples d'équations modulaires on l'a utilisée, sans le dire, pour trouver une solution particulière).

REMARQUE 80 — *Soit* $n \in \mathbb{N}^*$. *On écrit* $n = \Pi_{i=1}^{r} p_i^{a_i}$ *la décomposition de* n *en produits de facteurs premiers. On a alors*

$$\mathbb{Z}/n\mathbb{Z} \simeq (\mathbb{Z}/(p_1)^{a_1}\mathbb{Z}) \times \ldots \times (\mathbb{Z}/(p_r)^{a_r}\mathbb{Z}).$$

Pour étudier tous les groupes $\mathbb{Z}/n\mathbb{Z}$, *on peut ainsi se ramener à étudier seulement les groupes* $\mathbb{Z}/p^a\mathbb{Z}$, *avec* p *premier.*

REMARQUE 81 — *Ce théorème permet de caractériser les produits de groupes* $\Pi_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z}$. *On peut alors les distinguer, à isomorphisme de groupe près.*
Par exemple, $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$ *est isomorphe à* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z}$, *qui est isomorphe à* $\mathbb{Z}/150\mathbb{Z}$.
Par contre, $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$ *est isomorphe à* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z})^2$, *qui est isomorphe à* $\mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. *Ces deux groupes le même cardinal, mais l'équation* $5x = 0$ *possède* 5 *solutions dans le premier anneau, et* 25 *solutions dans le second. Ils ne sont donc pas isomorphes.*
Il existe toute une théorie pour classer les produits de groupes $\mathbb{Z}/n\mathbb{Z}$, *et celle-ci est basée sur le théorème d'isomorphisme chinois ainsi que sur les propriétés des isomorphismes de groupes.*

EXEMPLE 82 — *Soient* p *un nombre premier et* $a, b \geq 1$.
• *Le groupe* $(\mathbb{Z}/p^a\mathbb{Z})^b$ *n'est pas isomorphe à* $(\mathbb{Z}/(p^a)^b\mathbb{Z})$ *si* $b > 1$.
En effet, dans $\mathbb{Z}/p^{ab}\mathbb{Z}$, *l'élément* $\bar{1}$ *est d'ordre* p^{ab}.
S'il existait un isomorphisme f *entre ces deux groupes, alors* $f(\bar{1})$ *serait d'ordre* p^{ab}.
Mais, pour tout $\bar{x} = (\bar{k_1}, \ldots, \bar{k_b}) \in (\mathbb{Z}/p^a\mathbb{Z})^b$, *on a* $p^a.\bar{x} = 0$. *Donc* $\bar{x}$ *est d'ordre au plus* $p^a < p^{ab}$.
• *Un exemple simple est ainsi :* $(\mathbb{Z}/5\mathbb{Z})^2 \not\simeq \mathbb{Z}/25\mathbb{Z}$.

Nous pouvons maintenant revenir à l'étude des groupes en général.

2.6 Groupes monogènes, Théorème de Lagrange

Théorème 83 (Caractérisation des groupes monogènes)
Soit $(G, \star)$ un groupe monogène engendré par a.

1. Si G est d'ordre infini, alors $\varphi : k \in \mathbb{Z} \mapsto a^k \in G$ est un isomorphisme de groupes.
   On a donc $G \simeq \mathbb{Z}$.
2. Si G est cyclique d'ordre n, alors $\overline{\varphi} : \overline{k} \in \mathbb{Z}/n\mathbb{Z} \mapsto a^k \in G$ est un isomorphisme de groupes.
   On a donc $G \simeq \mathbb{Z}/n\mathbb{Z}$.

Preuve — Comme G est monogène, le morphisme φ est surjectif. Comme $\mathrm{Ker}(\varphi)$ est un sous-groupe de $\mathbb{Z}$, son noyau est de la forme $n\mathbb{Z}$.
Ainsi, le morphisme φ est injectif si et seulement si $n = 0$, si et seulement si G est d'ordre infini.
Sinon, on a $\mathrm{Ker}(\varphi) = n\mathbb{Z}$ pour un $n \in \mathbb{N}^*$. Alors, on a $\varphi(k) = \varphi(l)$ ssi $k - l \in n\mathbb{Z}$. Autrement dit, on a $\varphi(k) = \varphi(l)$ si et seulement si $\overline{k} = \overline{l}$.
On en déduit donc que l'application $\overline{\varphi}$ est bien définie. Cette fonction est surjective (son image est la même que celle de φ), et c'est bien un morphisme de groupes car

$$\overline{\varphi}(\overline{k} - \overline{l}) = a^{k-l} = a^k(a^l)^{-1} = \overline{\varphi}(\overline{k})(\overline{\varphi}(\overline{l}))^{-1}.$$

Enfin, par construction de $\overline{\varphi}$, son noyau est réduit à 0. $\overline{\varphi}$ est donc un isomorphisme de groupes, et G est d'ordre n. □

Ainsi, l'étude des groupes cycliques (groupes finis engendrés par un seul élément) se ramène à l'étude des groupes $(\mathbb{Z}/n\mathbb{Z}, \overline{+})$ pour $n \geq 1$.

Exemple 84 — *Pour tout $n \geq 1$, le groupe $\mathbb{U}_n$ des racines n-ièmes de l'unité est un groupe cyclique, d'ordre n, engendré par $\exp(\frac{2i\pi}{n})$. Le groupe multiplicatif $(\mathbb{U}_n, \times)$ est donc isomorphe au groupe additif $(\mathbb{Z}/n\mathbb{Z}, \overline{+})$.*

Cela veut dire que ces deux groupes ont exactement la même structure et les mêmes propriétés.

Exemple 85 — *Le groupe $(\mathbb{Q}, +)$ possède des sous-groupes stricts qui ne sont pas monogènes.*
Pour $G = \{\frac{p}{2^n},\ p \in \mathbb{Z},\ n \geq 0\}$, G est un sous-groupe de $\mathbb{Q}$.
Si G était monogène, alors G serait isomorphe à $(\mathbb{Z}, +)$. Soit $f : G \to \mathbb{Z}$ isomorphisme. Alors, pour $k \in \mathbb{N}$, on a $k.x = 1$ dans G si et seulement si $f(k.x) = f(x + \ldots + x) = k.f(x) = f(1)$ dans $\mathbb{Z}$.
Dans G, l'équation $2^n.x = 1$ possède exactement 2^n solutions. Dans $\mathbb{Z}$, l'équation $2^n y = f(1) = r$ ne possède des solutions que si 2^n divise r. En prenant $n \geq r$ cette équation ne possède donc pas de solutions, et l'isomorphisme f ne peut donc pas exister.
Autre méthode : *Si G était monogène, on aurait $G = \langle a \rangle$, pour un $a \in \mathbb{Q}$. Mais on a $\langle a \rangle = \{n.a,\ n \in \mathbb{Z}\} = a\mathbb{Z}$. En écrivant $a = \frac{p}{2^n}$, on remarque alors que $\frac{a}{2}$ est dans G, alors que $\frac{a}{2}$ n'est pas dans $a\mathbb{Z}$. Donc G n'est pas monogène.*

Théorème 86
Soit G un groupe fini de cardinal n. Alors :

$$\forall a \in G,\ a^n = e.$$

Preuve — Si G est commutatif, on a une preuve très élémentaire : La fonction $\psi : g \in G \mapsto ag \in G$ est bijective (attention, ce n'est pas un morphisme !), car injective entre deux ensembles finis de même cardinal. On en déduit donc que :

$$\prod_{g \in G} g = \prod_{g \in G} ag = a^n \prod_{g \in G} g.$$

Par simplication, on obtient $a^n = e$.
Si G n'est pas commutatif, la preuve résulte immédiatement du théorème de Lagrange que l'on va démontrer. □

Théorème 87 (Théorème de Lagrange)
Soit G un groupe fini et H un sous-groupe de G.
Alors, l'ordre de H divise l'ordre de G : $\mathrm{Card}(H) \mid \mathrm{Card}(G)$.

Preuve — On définit la relation suivante sur G : $x \equiv y$ si $xy^{-1} \in H$.

L'ensemble des éléments en relation avec x est $Hx = \{yx,\ y \in H\}$. D'après l'argument de la preuve précédente, ces ensembles ont autant d'éléments que H, c'est-à-dire $\mathrm{Card}(H)$. De plus pour $x, x' \in G$ on a soit $Hx = Hx'$ si $x \equiv x'$, soit $Hx \cap Hx' = \emptyset$ si $x \not\equiv x'$. Ces ensembles sont donc soit égaux, soit disjoints.
Cette relation est en fait une relation d'équivalence, dont toutes les classes d'équivalence ont le même cardinal.

Soit p le nombre d'ensembles distincts de la forme Hx, pour un $x \in G$. Comme ces ensembles sont disjoints, et comme leur réunion est G tout entier, on obtient $\mathrm{Card}(G) = p\mathrm{Card}(H)$, ce qui démontre le résultat. □

Corollaire 88
Soit G un groupe fini.
Alors pour tout $a \in G$, l'ordre de a divise l'ordre de G : $\text{ord}(a) \mid \text{Card}(G)$.

Preuve — Soit $a \in G$. On prend $H = \langle a \rangle$. Alors on a $\text{Card}(H) = \text{ord}(a)$. Le théorème de Lagrange nous dit donc que l'ordre de a divise l'ordre de G. □

Pour G un groupe fini et $a \in G$, comme l'ordre de G, n est un multiple de l'ordre de a, on $a^n = e$. Cela termine la preuve du Théorème 86.

Remarque 89 — *Le théorème de Lagrange et ses conséquences sont des résultats très importants en théorie des groupes.*
Ils apportent des informations sur des groupes finis qui peuvent être très gros et compliqués (par exemple $Bij(\{1, \dots, n\})$, groupe à $n!$ éléments, ou l'un de ses sous-groupes).

Les groupes finis commutatifs ne sont qu'un cas particulier des groupes finis, et les groupes cycliques (les $\mathbb{Z}/n\mathbb{Z}$ à isomorphisme près) ne sont qu'un cas particulier des groupes finis commutatifs. (par exemple, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ n'a rien à voir avec $\mathbb{Z}/8\mathbb{Z}$) Un groupe fini non-commutatif se comporte très différemment d'un groupe fini commutatif. On a besoin des théorèmes comme le théorème de Lagrange pour étudier, obtenir des informations sur ces groupes.

Exemple 90 — *Soit G un groupe d'ordre 105. On a $105 = 3.5.7$.*
Pour H un sous-groupe de G, le cardinal de H vaut alors $1, 3, 5, 7, 15, 21, 35$ ou 105.
Pour $a \in G$, l'ordre de a vaut alors $1, 3, 5, 7, 15, 21, 35$ ou 105.
Si on a un élément a d'ordre 105, alors G est cyclique et $G \simeq \mathbb{Z}/105\mathbb{Z}$.

Pour a un élément d'ordre 5 et b un élément d'ordre 7, le sous-groupe $\langle \{a, b\} \rangle$ est alors de cardinal 35 ou 105, car son cardinal est un multiple de 5 et de 7, et est un diviseur de 105.

Proposition 91
Soit G un groupe fini d'ordre p, avec p premier.
Alors G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.
Autrement dit, $\mathbb{Z}/p\mathbb{Z}$ est l'unique groupe (à isomorphisme près) d'ordre p.

Preuve — Comme p est premier, ses diviseurs sont 1 et p. Pour tout $a \in G$, l'ordre de a dans G est donc 1 ou p. Or, le seul élément d'ordre 1 dans un groupe est son élément neutre.

Comme on a $p \geq 2$, G contient au moins un autre élément que son élément neutre, et il contient donc un élément a d'ordre p. On a donc $G = \langle a \rangle \simeq \mathbb{Z}/p\mathbb{Z}$, ce qui conclut. □

Cela démontre au passage qu'un groupe fini d'ordre p est commutatif et monogène.
Ce n'est pas vrai en général quand $\text{Card}(G)$ n'est pas un nombre premier.

Exemple 92 — *Quel est le plus petit entier n tel qu'il existe un groupe non commutatif de cardinal n ?*

Proposition 93
Soient G, H deux groupes cycliques, d'ordres n et m.
Alors, le produit direct $G \times H$ est cyclique si et seulement si n et m sont premiers entre eux.

Preuve — Le groupe $G \times H$ est d'ordre $n.m$. Ses éléments sont de la forme (x, y) avec $x \in G$ et $y \in H$.
On va regarder l'ordre possible des éléments de $G \times H$ suivant la valeur de $\text{pgcd}(n, m)$.
Pour $k \in \mathbb{N}$, on a $(x, y)^k = (x^k, y^k)$.
Ainsi, on a $(x, y)^k = (e_G, e_H)$ si et seulement si $ord(x) \mid k$ et $ord(y) \mid k$, si et seulement si $ppcm(ord(x), ord(y)) \mid k$.
Par définition de l'ordre de l'élément (x, y), on en déduit que $ord((x, y)) = ppcm(ord(x), ord(y))$.
D'après le théorème de Lagrange on a $ord(x) \mid n$ et $ord(y) \mid m$. On a donc

$$ppcm(ord(x), ord(y)) \leq ppcm(n, m) = \frac{nm}{\text{pgcd}(n, m)}.$$

Ainsi, si $\text{pgcd}(n, m) \neq 1$, on remarque que tous les éléments de $G \times H$ sont d'ordre au plus $\frac{nm}{\text{pgcd}(n,m)}$. Ce groupe ne possède donc pas d'élément d'ordre nm, donc il ne peut pas être cyclique.
Si $\text{pgcd}(n, m) = 1$, soient a un générateur de G et b un générateur de H.
Alors on a $ord(a) = n$ et $ord(b) = m$.
D'après ce qui précède, on a donc $ord((a, b)) = ppcm(ord(a), ord(b)) = nm$.
Le groupe $G \times H$ possède un élément d'ordre nm, donc il est cyclique. □

Remarque 94 — *Un groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*
Ainsi, la proposition précédente nous dit que si n et m ne sont pas premiers entre eux, alors $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ n'est pas cyclique.
Si m et n sont premiers entre eux, on sait avec le théorème d'isomorphisme chinois que $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}) \simeq \mathbb{Z}/(nm)\mathbb{Z}$, qui est un groupe cyclique.
En exemple simple, on pourra penser à $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ qui n'est pas cyclique (3 éléments d'ordre 2 et 1 d'ordre 1), alors que $\mathbb{Z}/6\mathbb{Z}$ est cyclique (2 éléments d'ordre 6, 2 d'ordre 3, 1 d'ordre 2, 1 d'ordre 1).

Remarque 95 (Bilan sur les groupes) — *Les familles de groupes que l'on utilise ou aborde souvent sont :*

1. *$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, pour la loi additive $+$;*
2. *$\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$, pour la loi multiplicative $\times$.*
   Le groupe $\mathbb{U}$ des complexes de module 1, pour la lo $\times$;
3. *Les groupes quotients $\mathbb{Z}/n\mathbb{Z}$, $n \geq 1$, pour la loi additive $+$;*
4. *Les groupes de bijections $Bij(E)$, pour la loi de composition $\circ$.*
   Les groupes de permutation S_n, pour $n \geq 1$, pour la loi de composition $\circ$ (voir Géom. 2).
   Les groupes d'isométrices du plan ou de l'espace, $Isom(E)$, pour la loi $\circ$ (voir Géom. 2).
   Les groupes d'isométries qui préservent un polygone régulier, D_n, pour la loi $\circ$ (voir Géom. 2) ;
5. *Les groupes de matrices inversibles $Gl_n(\mathbb{K})$, pour la loi multiplicative $\times$;*
6. *Les anneaux A, pour la loi $+$ (voir chapitre Anneaux) ;*
7. *Les groupes des inversibles d'un anneau, $A^\times$, pour la loi multiplicative $\times$ (voir chap. Anneaux) ;*

Remarque 96 (Propriétés des groupes) —
Les types de groupes que nous avons vus sont :

1. *Groupes monogènes : $\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}$, sous-groupes de ces groupes.*
2. *Groupes commutatifs finis : Produits d'un nombre fini de $\mathbb{Z}/n_i\mathbb{Z}$ avec les n_i non-tous premiers entre eux. Sous-groupes de ces groupes.*
3. *Groupes commutatifs : $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, $\mathbb{Z}^n$, $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$, $(\mathbb{U}, \times)$. Produits d'un nombre fini (ou infini) de groupes commutatifs. Sous-groupes de groupes commutatifs.*
4. *Groupes finis (non commutatifs) : $(S_n, \circ)$. Groupes d'isométries du plan/de l'espace. Produits d'un nombre fini de ces groupes.*
5. *Groupes généraux : $(Bij(E), \circ)$ pour E infini, $(Gl_n(\mathbb{K}), \times)$. Produits et sous-groupes de ces groupes.*

Chapitre 3 Structure algébrique : Anneaux

3.1 Structure d'anneau

Définition

Définition 1
Soit $(A, +, \times)$ un ensemble muni de deux lois de composition internes.
On dit que $(A, +, \times)$ est un **anneau** \环, **ring**\ si :

1. $(A, +)$ est un groupe commutatif, d'élément neutre noté 0_A ;
2. La loi $\times$ est associative et admet un élément neutre noté 1_A, avec $1_A \neq 0_A$;
3. La loi $\times$ est distributive à gauche et à droite par rapport à $+$:

$$\forall x, y, z \in A,\ x \times (y + z) = (x \times y) + (x \times z) \text{ et } (x + y) \times z = (x \times z) + (y \times z).$$

De plus, on dit que A est un anneau **commutatif** si la loi $\times$ est commutative ($x \times y = y \times x$).

Remarque 2 — *Dans le cas d'un anneau A, le symétrique d'un élément a pour la loi $+$ est noté $-a$ (**opposé** de a) et le symétrique de a pour la loi $\times$, s'il existe, est noté a^{-1} (**inverse** de a).*
Les notations 0_A et 1_A sont très générales, et on les abrège parfois en 0 et 1 (élément neutre pour l'addition, élément neutre pour la multiplication).
On notera souvent ab pour $a \times b$.
On écrira souvent "Soit A un anneau", les lois $+$ et $\times$ étant sous-entendues.

Exemples 3

1. *$(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{R}, +, \times)$ sont des anneaux commutatifs.*
2. *Pour E un ensemble non-vide et $\mathcal{F}(E, \mathbb{C})$ l'ensemble des fonctions de E dans $\mathbb{C}$, $(\mathcal{F}(E, \mathbb{C}), +, \times)$ est un anneau commutatif.*
   Cela reste vrai si l'on remplace $\mathbb{C}$ par un anneau A. (Le vérifier)
3. *En particulier, $(\mathbb{K}^{\mathbb{N}}, +, \times)$ est un anneau. C'est l'ensemble des suites à coefficients dans un corps $\mathbb{K}$ muni de l'addition et de la multiplication termes à termes.*
4. *$(\mathbb{K}[X], +, \times)$ est un anneau. C'est l'ensemble des polynômes à coefficients dans un corps $\mathbb{K}$, pour l'addition et la multiplication de polynômes.*
5. *Soit E un ensemble. L'ensemble $\mathcal{P}(E)$ muni de la différence symétrique et de l'intersection est un anneau. On le note $(\mathcal{P}(E), \Delta, \cap)$. (Le vérifier)*

Exemples 4 1. *Pour $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, $(\mathscr{M}_n(\mathbb{K}), +, \times)$ est un anneau.*
   Si $n \geq 2$, cet anneau n'est pas commutatif. (Le vérifier)
2. *Pour E un $\mathbb{K}$-espace vectoriel, $(\mathcal{L}(E), +, \circ)$ est un anneau.*
   Si $\dim(E) \geq 2$, cet anneau n'est pas commutatif.
3. *Pour A un anneau, $(\mathcal{F}(A, A), +, \circ)$ n'est pas un anneau. En effet, on a bien $(f + g) \circ g = f \circ g + f \circ h$, mais en général on a $f \circ (g + h) \neq f \circ g + f \circ h$.*
4. *Pour G un groupe commutatif et pour pour $Gr(G, G)$ l'ensemble des morphismes de groupes sur $(G, +)$, $(Gr(G, G), +, \circ)$ est un anneau. (Le vérifier)*
   On peut donc construire des anneaux uniquement à partir de groupes ! (en considérant des ensembles d'endomorphismes)

Remarque 5 — *Dans la littérature mathématique, on peut aussi définir un anneau sans demander l'existence de l'élément unitaire 1_A. Un anneau possédant un élément unitaire 1_A est alors appelé anneau unitaire.*
Mais, il y a déjà beaucoup de choses à dire sur les anneaux unitaires, et c'est ce que ce chapitre étudie. Les "anneaux unitaires" sont appelés "anneaux" ici.

Propriétés élémentaires

Proposition 6
Soit $(A, +, \times)$ un anneau. On a alors :

1. Pour tout $a \in A$, $0_A \times a = a \times 0_A = 0_A$.
2. La soustraction définit une loi interne $- : (a, b) \in A \times A \mapsto a - b \in A$.
   Elle vérifie :
   (a) $a - a = 0_A$
   (b) $a(b - c) = ab - ac$ car $a(b - c) + ac = a(b - c + c) = ab$.
   (c) $a \times (-b) = -(a \times b)$.

Preuve — 1) On a $0_A \times a = (1_A - 1_A) \times a = a - a = 0_A$. On obtient de même que $a \times 0_A = 0_A$. □

Remarque 7 — *La loi $-$ ainsi définie n'est pas associative.*
La soustraction étant la réciproque de l'addition, les propriétés de cette loi découlent toutes de celles de $+$.

Remarque 8 — *Comme on suppose $0_A \neq 1_A$ dans la définition de A, un anneau contient donc toujours au moins deux éléments.*
Existe-t-il un anneau contenant exactement deux éléments ?

Un ensemble $(A, +, \times)$ vérifiant toutes les conditions d'un anneau mais avec $0_A = 1_A$ est réduit à un seul élément, c'est-à-dire $A = \{0_A\}$. En effet, pour tout $x \in A$ on a alors $x = 1_A.x = 0_A.x = 0_A$.
Cet "anneau" étant très particulier et rapidement décrit (l'anneau nul), on l'enlève de notre étude en demandant à ce que $0_B \neq 1_B$.

Proposition-Définition 9
Soit $(A_i, +_i, \times_i)_{i \in [\![1,n]\!]}$ une famille d'anneaux.
On appelle anneau produit l'ensemble $(A_1 \times \ldots \times A_n, +, \times)$ où les lois $+$ et $\times$ sont définies par :

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$$

et

$$(a_1, \ldots, a_n) \times (b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n).$$

Cet ensemble est un anneau.
On a $0_A = (0_{A_1}, \ldots, 0_{A_n})$ et $1_A = (1_{A_1}, \ldots, 1_{A_n})$.

Preuve — On vérifie que les opérations définies possèdent bien tous les axiomes d'un anneau. □

Les exemples classiques d'anneaux commutatifs sont $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{K}[X]$, voire un produit de certains d'entre eux.
Il ne faut pas hésiter à les utiliser pour tester si un résultat sur les anneaux commutatifs est vrai, ou voir s'il est faux (chercher un contre-exemple).
On verra par la suite un autre exemple fondamental d'anneau, les $\mathbb{Z}/n\mathbb{Z}$.
Les exemples classiques d'anneaux non-commutatifs sont les $\mathscr{M}_n(\mathbb{K})$ ($n \geq 2$). Il ne faut pas hésiter à les utiliser (pour $n = 2, 3, 4$) afin de tester si un résultat sur les anneaux commutatifs est vrai, ou voir s'il est faux (chercher un contre-exemple).

3.2 Éléments inversibles

Groupe des éléments inversibles

Définition 10
Soit A un anneau et $a \in A$.
On dit que a **inversible** s'il admet un symétrique pour la loi $\times$: $b \in A$ tel que $ab = ba = 1_A$.
Ce symétrique est appelé inverse de a, et est noté a^{-1}.
On note $A^\times$ l'ensemble des éléments inversibles de l'anneau A. C'est le **groupe des inversibles** de A.

Proposition 11
L'ensemble des éléments inversible d'un anneau A, $A^\times$, est un groupe pour la multiplication $\times$.
Si A est commutatif, alors ce groupe est abélien.

Preuve — L'ensemble $A^\times$ contient 1_A, l'élément neutre pour la multiplication, donc est non-vide. Montrons que $A^\times$ est stable par $\times$. Soient $a, b \in A^\times$. On a $(ab)(b^{-1}a^{-1}) = 1_A$ et $(b^{-1}a^{-1})(ab) = 1_A$, donc $ab \in A$. La loi $\times$ est associative sur A, donc sur A^*. Enfin, par définition, tout élément de $A^\times$ est inversible. □

REMARQUE 12 — *Attention à ne pas confondre $A^* = A \setminus \{0_A\}$ et $A^\times$ l'ensemble des inversibles de A. Dans cerains cas (par ex $\mathbb{R}, \mathbb{C}, \mathbb{Q}$), ces deux ensembles sont égaux.*

On a par contre $\mathbb{Z}^\times = \{-1, 1\}$. De même, $\mathscr{M}_n(\mathbb{K})^\times = GL_n(\mathbb{K}) \neq \mathscr{M}_n(\mathbb{K})^*$.

EXEMPLE 13 —

1. *Nous avons vu (chapitre Matrices) que $GL_2(\mathbb{R}) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix}, ad - bc \neq 0\}$.*
2. *Pour E un ensemble non-vide et A un anneau, on a $\mathcal{F}(E, A)^\times = \mathcal{F}(E, A^\times)$.*

DÉFINITION 14
Soit $(A, +, \times)$. Soit $a \in A$ non-nul. Alors :

1. Pour $n \geq 0$, on définit $0_A^n = 0_A$ (donc $0_A^0 = 0_A$) ;
2. Pour $n \geq 1$, on définit $a^n = a \times \ldots \times a$ (n fois) ;
3. Pour $n = 0$, on définit $a^0 = 1_A$;
4. Si a est inversible, pour $n < 0$, on définit $a^n = a^{-1} \times \ldots \times a^{-1}$ ($-n$ fois).

REMARQUE 15 — *On retrouve alors les propriétés habituelles.*
Pour $k, m, n \in \mathbb{N}$ et $a \in A$, on a :

$$a^m \times a^n = a^{m+n} \quad \text{et} \quad (a^n)^k = a^{kn}.$$

Si $a \in A$ est inversible, cela reste vrai pour a^n, pour tout $n \in \mathbb{Z}$.

Nous allons étudier à nouveau les ensembles $\mathbb{Z}/n\mathbb{Z}$, avec cette fois ses lois additive et multiplicative.

3.3 L'ANNEAU $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

Soit $n \geq 2$.
On rappelle que les opérations $\overline{+}$ et $\overline{\times}$ vérifient :

$$\forall a, b \in \mathbb{Z},\ \bar{a} \overline{+} \bar{b} = \overline{a + b},\ \text{et}\ \bar{a} \overline{\times} \bar{b} = \overline{ab},$$

où $\forall a \in \mathbb{Z}$, $\bar{a} = a + n\mathbb{Z}$ est la classe d'équivalence de a pour la relation de congruence modulo n sur $\mathbb{Z}$.

PROPOSITION 16
Soit $n \geq 2$. $(\mathbb{Z}/n\mathbb{Z}, \overline{+}, \overline{\times})$ est un anneau, qui est commutatif.
Son élément neutre pour l'addition est $\bar{0}$, l'élément nul de $\mathbb{Z}/n\mathbb{Z}$.
Son élément neutre pour la multiplication est $\bar{1}$, l'élément unitaire de $\mathbb{Z}/n\mathbb{Z}$.

Preuve — (Le vérifier) □

REMARQUE 17 — • *Les anneaux de la forme $\mathbb{Z}/n\mathbb{Z}$ sont des anneaux avec un nombre fini d'éléments. On va alors trouver des phénomènes très différents de $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.*
• *Par exemple, dans $\mathbb{Z}/n\mathbb{Z}$, on a $\sum_{k=1}^{n} 1 = 1 + \ldots + 1 (n \text{ fois}) = 0$.*
• *De même, pour n qui n'est pas permier (par ex. $n = 2.3$), en écrivant $n = a.b$ avec $a, b \in \{1, \ldots, n-1\}$, on va avoir $\bar{a} \neq 0$, $\bar{b} \neq 0$ dans $\mathbb{Z}/n\mathbb{Z}$, mais $\bar{a}\bar{b} = \bar{ab} = \bar{n} = 0$. (le produit de deux nombres non-nuls peut être nul)*
• *Autre exemple de phénomène. Dans $\mathbb{Z}/8\mathbb{Z}$ on a vu avec les congruences que $\bar{1}^2 = \bar{3}^2 = \bar{5}^2 = \bar{7}^2 = \bar{1}$. Ainsi, l'équation $x^2 = \bar{1}$ possède plus de 2 solutions.*

REMARQUE 18 — *Dans la suite du cours, quand les lois d'addition et de multiplication seront claires (quand on sait sur quel anneau on travaille), on notera $+$ à la place de $\overline{+}$ et $\times$ à la place de $\overline{\times}$ pour les lois de $\mathbb{Z}/n\mathbb{Z}$.*

Le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$

PROPOSITION-DÉFINITION 19
Soit $n \geq 2$. Pour $(\mathbb{Z}/n\mathbb{Z})^\times$ l'ensemble des éléments de $\mathbb{Z}/n\mathbb{Z}$ inversibles, on a :

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{m},\ m \in \mathbb{Z} \text{ avec } \operatorname{pgcd}(m, n) = 1\}.$$

C'est un groupe fini et abélien.
On a aussi $\operatorname{Card}(\mathbb{Z}/n\mathbb{Z}^\times) = \varphi(n)$, où $\varphi(n)$ est **l'indicatrice d'Euler** de n.

Preuve — Ce résultat a déjà été traité au chapitre Arithmétique, avec le théorème de Bézout. □

Exemple 20 — *Le groupe des inversibles de l'anneau est* $(\mathbb{Z}/8\mathbb{Z})^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$.
C'est un groupe abélien à 4 *éléments. On a donc* $\varphi(8) = 4$. *On remarque que l'on a de plus :* $\overline{3}^2 = \overline{5}^2 = \overline{7}^2 = \overline{1}$.
Ainsi, le groupe $((\mathbb{Z}/8\mathbb{Z})^\times, \times)$ *possède un élément d'ordre* 1 $(\overline{1})$ *et trois éléments d'ordre* 2 $(\overline{3}, \overline{5}, \overline{7})$.

Le groupe $(\mathbb{Z}/8\mathbb{Z})^\times$ *n'est donc pas isomorphe au groupe* $(\mathbb{Z}/4\mathbb{Z}, +)$, *groupe abélien d'ordre* 4, *car ce groupe contient un élément d'ordre* 4 $(\overline{3})$.
En comparant les tables d'opérations, on peut montrer que $((\mathbb{Z}/8\mathbb{Z})^\times, \times)$ *est isomorphe à* $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$.

Proposition 21
Soit p un nombre premier.

1. Alors on a $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z}^*$.
   Ainsi, on obtient $\varphi(p) = p - 1$.
2. Pour tout $k \geq 1$, on a $\varphi(p^k) = p^k - p^{k-1}$.

Preuve — On a $\varphi(p^k) = \text{Card}(\{0 \leq n \leq p^k - 1 \text{ tels que } \text{pgcd}(p^k, n) = 1\})$. Soit $n \in \mathbb{N}$. Comme p est un nombre premier, on a $\text{pgcd}(n, p^k) = 1$ si et seulement si p ne divise pas n.

Or, il y a exactement p^{k-1} multiples de p compris entre 0 et $p^k - 1$: les entiers $p.m$ avec $0 \leq m \leq p^k - 1$.

On obtient donc $\varphi(p^k) = p^k - p^{k-1}$, ce qui conclut. □

On rappelle le théorème d'arithmétique suivant :

Théorème 22 (Petit théorème de Fermat)
Soient p un nombre premier et $a \in \mathbb{Z}$ avec $\text{pgcd}(a, p) = 1$. Alors, on a :

$$a^{p-1} \equiv 1 \bmod p$$

$$\text{c'est-à-dire } \overline{a}^{p-1} = \overline{1} \text{ dans } \mathbb{Z}/p\mathbb{Z}.$$

Nous pouvons maintenant apporter une généralisation à ce résultat, et apporter une preuve utilisant les ensembles $\mathbb{Z}/n\mathbb{Z}$.

Théorème 23
Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$ avec $\text{pgcd}(a, n) = 1$. Alors, on a :

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

$$\text{c'est-à-dire } \overline{a}^{\varphi(n)} = \overline{1} \text{ dans } \mathbb{Z}/n\mathbb{Z}.$$

Preuve — L'élément $\overline{a}$ est alors contenu dans le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$, qui est de cardinal $\varphi(n)$. Le théorème de Lagrange permet alors de conclure. □

On verra par la suite une généralisation du théorème d'isomorphisme chinois. Il faudra d'abord définir ce que sont les morphismes d'anneaux (les fonctions qui "préservent" la structure d'anneau).

3.4 Anneaux intègres

Ensemble des diviseurs de 0

Définition 24
Soit $a \in A$, avec $a \neq 0$. On dit que a est un **diviseur de zéro** s'il existe $b \in A$ non-nul tel que $ab = 0$.

Remarque 25 — *Si* $a \in A$ *est un diviseur de* 0, *alors* a *n'est pas inversible.*
En effet, si a *était inversible on aurait* $b = a^{-1}ab = 0_A$, *ce qui est impossible.*

Exemple 26 —

1. *Les anneaux* $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ *n'ont pas de diviseurs de* 0.
2. $\mathscr{M}_2(\mathbb{K})$ *a des diviseurs de* 0. *On a :*

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

   La "relation" a et b diviseurs de 0 *n'est pas réflexive.*
3. *L'anneau* $\mathcal{F}(I, \mathbb{R})$ *a-t-il des diviseurs de* 0 *? (Les déterminer.)*
4. *Un anneau produit* $A \times B$ *possède toujours des diviseurs de* 0. *Pour* $a \in A$,$b \in B$ *non-nuls,* $(a, 0)$ *et* $(0, b)$ *sont des diviseurs de* 0.

Exercice 5 — *Soit* $n \in \mathbb{N}$, $n \geq 2$. *Montrer que les diviseurs de* $\overline{0}$ *dans l'anneau* $\mathbb{Z}/n\mathbb{Z}$ *sont exactement les* $\overline{m}$ *tels que :*

$$n \text{ de divise pas } m, \quad \text{et} \quad \operatorname{pgcd}(m, n) > 1.$$

Ainsi, tous les éléments de $\mathbb{Z}/n\mathbb{Z}$ *qui ne sont pas inversibles et qui sont différents de* $\overline{0}$ *sont des diviseurs de* $\overline{0}$

Exemple 27 — *Les diviseurs de* $\overline{0}$ *de l'anneau* $\mathbb{Z}/8\mathbb{Z}$ *sont* $\{\overline{2}, \overline{4}, \overline{6}\}$.

Pour p premier, l'anneau $\mathbb{Z}/p\mathbb{Z}$ *n'a pas de diviseurs de* $\overline{0}$.

Anneaux intègres

Définition 28
Soit A un anneau. On dit que A est **intègre** s'il n'a pas de diviseurs de zéro.

Proposition 29
Soit A un anneau intègre.

1. $\forall a, b \in A$, si $ab = 0$ alors $a = 0_A$ ou $b = 0_A$.
2. $\forall a, b, c \in A$ avec $a \neq 0_A$, si $ab = ac$ alors $b = c$.
3. $\forall a, b, c \in A$ avec $a \neq 0_A$, si $ba = ca$ alors $b = c$.

Preuve — 1) Par définition. 2) $a(b - c) = 0_A$ 3) $(b - c)a = 0_A$. □

Remarque 30 — *Dans un anneau intègre, tous les éléments non-nuls ne sont pas forcément inversibles, mais on peut simplifier une équation en la factorisant.*
Cela est par exemple le cas dans l'anneau $\mathbb{Z}$.

Proposition 31
Soit A un anneau intègre. Soient $b_1, \ldots, b_n \in A$ (pas forcément distincts).
Alors, on a $(x - b_1) \ldots (x - b_n) = 0$ si et seulement si $x = b_i$ pour un $1 \leq i \leq n$.
L'équation $(x - b_1) \ldots (x - b_n) = 0$ possède donc au plus n solutions.

Remarque 32 —
• *Si A est un anneau intègre, alors l'équation* $x^2 = 1$ *a pour unique solution* 1 *et* -1 *car l'équation s'écrit* $(x - 1_A)(x + 1_A) = 0_A$.
• *Si l'on trouve une équation polynômiale dans A de la forme* $\Pi_i(x - b_i) = 0$ *qui possède plus de n solutions, on sait donc immédiatement que l'anneau A n'est pas intègre.*
• *Dans un anneau produit* $A \times B$ *tel que* $1_A \neq -1_A$ *et* $1_B \neq -1_B$, *il y a au moins 4 solutions à cette équation et donc* $A \times B$ *n'est jamais intègre.*
• *Dans* $\mathcal{M}_2(\mathbb{R})$, *pour tout* $\theta \in \mathbb{R}$, $S(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$ *vérifie* $x^2 = 1$.
Les anneaux $\mathscr{M}_n(\mathbb{K})$ *ne sont jamais intègres pour* $n \geq 2$.

Exemple 33 —

- *Les anneaux* $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ *sont intègres.*

- *Les anneaux $\mathbb{Z}/p\mathbb{Z}$ pour p premier sont intègres.*
- *Les anneaux $\mathbb{K}[X]$ sont intègres.*
- *Les anneaux $\mathbb{Z}/n\mathbb{Z}$, pour $n \geq 2$ non premier, ne sont pas intègres.*
- *Les anneaux $\mathscr{M}_n(\mathbb{K})$, pour $n \geq 2$, ne sont pas intègres. (Le vérifier.)*
- *Les anneaux produits $A \times B$ ne sont pas intègres.*
- *Les anneaux $\mathcal{F}(E, A)$ ne sont pas intègres si $Card(E) \geq 2$.*

3.5 Calcul dans les anneaux

Dans un anneau A, si deux éléments a et b ne commutent pas ($ab \neq ba$), on ne peut appliquer aucune formule de factorisation/développement d'expressions polynômiales en a et en b.
Par exemple, on a $(a+b)^2 = a^2 + ab + ba + b^2 \neq a^2 + 2ab + b^2$, ou $(a-b)(a+b) = a^2 - b^2 + ab - ba \neq a^2 - b^2$.
La propriété de commutativité (sur l'anneau A tout entier, ou seulement entre deux éléments a et b) permet d'effectuer beaucoup de calculs dans l'anneau avec des résultats de factorisation/développement que l'on connaît déjà sur $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Proposition 34
Soit $(A, +, \times)$ un anneau. Soient $a, b \in A$ qui commutent ($a \times b = b \times a$). Alors, on a :

1. $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$, $\forall n \geq 1$ **(Formule du binôme)** ;
2. $a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^{n-k-1} b^k$, $\forall n \geq 2$ **(Formule de Bernoulli)** ;
3. $a^{2n+1} + b^{2n+1} = (a+b) \sum_{k=0}^{2n} (-1)^k a^{2n-k} b^k$, $\forall n \geq 1$.

Preuve — La formule du binôme (parfois appelée formule du binôme de Newton) se démontre par récurrence sur n. La formule de Bernoulli s'obtient en développant le terme de droite :

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

La dernière formule découle de la formule de Bernouilli (on remplace b par $-b$ et n par $2n+1$). □

Remarque 35 —

1. *Vous devez connaître ces formules et leurs cas particuliers quand n est petit, comme par exemple*
   (a) $a^3 - b^3 = (a-b)(a^2 + ab + b^2)$;
   (b) $a^3 + b^3 = (a+b)(a^2 - ab + b^2)$.
2. *Pour $a_1, \cdots, a_m \in A$ qui commutent deux à deux on a aussi :*

$$(a_1 + \cdots + a_m)^k = \sum_{i_1 + \cdots i_m = k} \binom{k}{i_1 \cdots i_m} a_1^{i_1} \cdots a_m^{i_m}, \quad \textbf{(Formule du multinôme)}$$

Corollaire 36
On retrouve la formule de la somme géométrique : $1 - a^n = (1-a) \sum_{k=0}^{n-1} a^k$.

Si $1 - a$ est inversible, on a alors : $\sum_{k=0}^{n-1} a^k = (1-a)^{-1}(1-a^n)$.

Exercice 6 — *On dit qu'un élément $a \in A$ est **nilpotent** s'il existe $n \in \mathbb{N}^*$ tel que $a^n = 0$. ("nil" : "nul", "potent" : "puissance")*
*On appelle **indice de nilpotence** de a le plus petit $n \geq 1$ tel que $a^n = 0$.*

1. *Pour $A = \mathscr{M}_n(\mathbb{R})$ avec $n = 2, 3$ ou 4, trouver des exemples de matrices nilpotentes. (On pourra chercher des matrices triangulaires supérieures/inférieures).*

2. *Soient $a, b \in A$ qui commutent et sont nilpotents d'indices p et q. Montrer que $a+b$ est nilpotent et majorer son indice de nilpotence.*
3. *Si a et b ne commutent plus, peut-on encore dire quelque chose sur $a+b$? (Si non, on cherchera un contre-exemple)*
4. *Si a est nilpotent d'indice p, que peut-on dire de $1-a$?*

3.6 Sous-anneaux, Idéaux

Sous-anneaux

Définition 37
Soit $(A, +, \times)$ un anneau et $B \subset A$.
On dit que B est un **sous-anneau** de A si :

1. $(B, +)$ est un sous-groupe de $(A, +)$;
2. $1_A \in B$;
3. la loi $\times$ est stable sur B : $\forall x, y \in B$, on a $x \times y \in B$.

Remarque 38 —

- *Pour B un sous-anneau de A, l'ensemble $(B, +, \times)$ muni de la restriction de $+$ et $\times$ à B est un anneau.*
- *Z est un sous-anneau de $\mathbb{Q}$, qui est un sous-anneau de $\mathbb{R}$, qui est un sous-anneau de $\mathbb{C}$.*
- *$\mathbb{K}$ est un sous-anneau de $\mathbb{K}[X]$.*
- *$\mathbb{K}_n[X]$ n'est pas un sous-anneau de $\mathbb{K}[X]$. $X\mathbb{K}[X]$ n'est pas un sous-anneau non plus.*
- *Il est important de vérifier que B contient l'élément 1_A :*
  Pour $n \geq 2$, $n\mathbb{Z}$ n'est pas un sous-anneau de $\mathbb{Z}$. Il vérifie toutes les propriétés nécessaires sauf celle de l'existence d'un élément neutre pour la multiplication.
- *Soit E un ensemble et E' un sous-ensemble strict de E. Alors les ensembles $\mathcal{F}(E, \mathbb{C})$ et $\mathcal{F}(E', \mathbb{C})$ sont des anneaux.*
  On peut identifier $\mathcal{F}(E', \mathbb{C})$ à un sous-ensemble de $\mathcal{F}(E, \mathbb{C})$ (le sous-ensemble des fonctions $f : E \to \mathbb{C}$ telles que $f(x) = 0$ si $x \notin E'$), mais ce sous-ensemble n'est pas un sous-anneau de $\mathcal{F}(E, \mathbb{C})$ car il ne contient pas la fonction constante égale à 1.

Proposition 39
Soit $(A, +, \times)$ un anneau et $B \subset A$. B est un sous-anneau de A si et seulement si :

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

L'intérêt de cette proposition est qu'à partir d'anneaux déjà connus ($\mathbb{C}$, $\mathscr{M}_n(\mathbb{K})$,$\mathcal{F}(E, \mathbb{C})$) on peut facilement montrer qu'un sous-ensemble B de l'un de ces anneaux est lui aussi un anneau, sans avoir à revérifier tous les axiomes définissant un anneau.

Exemple 40 — • *On pose $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2},\ (a, b) \in \mathbb{Z}^2\}$. C'est un sous-anneau de $(\mathbb{R}, +, \times)$.*
• *On pose $\mathbb{Z}[X] = \{P \in \mathbb{Q}[X],\ \text{avec } P \text{ à coefficients dans } \mathbb{Z}\}$.*
C'est un sous-anneau de $(\mathbb{Q}[X], +, \times)$.

Exercice 7 — • *Montrer que $\mathbb{Z}[i] := \{a + ib,\ (a, b) \in \mathbb{Z}^2\}$ est un sous-anneau de $\mathbb{C}$.*

- *Soit $n \geq 2$. Montrer que l'ensemble des matrices diagonales $\mathcal{D}_n(\mathbb{K})$ et que l'ensemble des matrices triangulaires supérieures $\mathcal{T}_n(\mathbb{K})$ sont des sous-anneaux de $\mathscr{M}_n(\mathbb{K})$.*

Remarque 41 — *Pour $S \subset A$, on peut définir le sous-anneau engendré par S comme le plus petit sous-anneau de A contenant S, et obtenir une écriture de ce sous-anneau : $\{\sum_{k=1}^{n} \pi_{i=1}^{m_k} a_i,\ n \geq 1, m_1, \ldots, m_n \geq 1,\ a_i \in S \cup \{1\}\}$. Contrairement aux sous-groupes engendrés par une partie, cet objet mathématique n'est pas très intéressant dans ce chapitre.*

Les anneaux $\mathscr{M}_n(\mathbb{K})$ et $\mathbb{K}[X]$ sont aussi des $\mathbb{K}$-e.v.
Cela permet de définir des sous-anneaux un peu particuliers.

Proposition-Définition 42
Soient $n \geq 1$ et $\mathbb{K}$ un corps. Soient $A \in \mathscr{M}_n(\mathbb{K})$ et $P \in \mathbb{K}[X]$.
On définit $\mathbb{K}[A] = Vect(A^k,\ k \geq 0)$ et $\mathbb{K}[P] = Vect(P^k,\ k \geq 0)$.
Alors, $\mathbb{K}[A]$ est un sous-anneau de $\mathscr{M}_n(\mathbb{K})$ et $\mathbb{K}[P]$ est un sous-anneau de $\mathbb{K}[X]$.
$\mathbb{K}[P]$ est un sous-anneau commutatif et intègre (car $\mathbb{K}[X]$ est commutatif et intègre).
$\mathbb{K}[A]$ est un sous-anneau commutatif.

Preuve — Les ensembles $\mathbb{K}[A]$ et $\mathbb{K}[P]$ sont des sous-ev, donc ce sont des sous-groupes pour la loi additive $+$.
On a 0 et 1 contenus dans ces ensembles.
On montre facilement que pour $B_1, B_2 \in \mathbb{K}[A]$ (resp. $\in \mathbb{K}[P]$), on a $B_1.B_2 \in \mathbb{K}[A]$ (resp. $\in \mathbb{K}[P]$). (A vérifier.)
Cela démontre que ces ensembles sont des sous-anneaux.

On montre de même que pour $B_1, B_2 \in \mathbb{K}[A]$, on a $B_1B_2 = B_2B_1$, donc $\mathbb{K}[A]$ est commutatif.
Comme $\mathbb{K}[X]$ est un anneau commutatif et intègre, le sous-anneau $\mathbb{K}[P]$ est commutatif et intègre. □

Remarque 43 — • *Les sous-anneaux $\mathbb{K}[A]$ et $\mathbb{K}[P]$ sont construits en utilisant la structure de $\mathbb{K}$-algèbre de $\mathscr{M}_n(\mathbb{K})$ et $\mathbb{K}[X]$, que l'on étudiera plus tard. Cela fournit quelques sous-anneaux que l'on peut étudier.*
• *La commutativité de $\mathbb{K}[A]$ est très utile pour faire des calculs. (déjà vu au chapitre Matrices)*
• *Le sous-anneau $\mathbb{K}[A]$ n'est pas intègre en général.*
Par exemple, si $A^2 = I_n$ (symétrie), $A^2 = A$ (projection), $A^m = 0$ (nilpotent), ou $A = Diag(\lambda_1, \ldots, \lambda_n)$ (diagonal), avec $A \neq \lambda I_n$, alors le sous-anneau $\mathbb{K}[A]$ n'est pas intègre.
On peut trouver $B_1, B_2 \in \mathbb{K}[A]$ non-nulles telles que $B_1B_2 = 0$.

Par rapport aux sous-groupes qui sont seulement stables pour la loi $+$, les sous-anneaux doivent être stables pour les lois $+$ et $\times$ et en plus contenir l'élément 1.
Pour tout $a \in A$ non-inversible, l'ensemble des multiples de a, aA, n'est donc pas un sous-anneau.
On va définir un objet mathématique différent des sous-anneaux pour étudier cela, les idéaux.

Idéaux d'un anneau commutatif

Définition 44
Soient A un anneau commutatif et $I \subset A$.
On dit que I est un **idéal** de A si :

1. $(I, +)$ est un sous-groupe de $(A, +)$;
2. $\forall x \in I$, $\forall a \in A$, on a $ax \in I$ (on dit que I est **absorbant** pour la loi $\times$).

Exemple 45 —

1. *Le singleton $\{0_A\}$ et A sont des idéaux de A.*
2. *Pour $a \in A$, l'ensemble aA des multiples de a est un idéal de A.*
3. *La définition d'idéal ne concerne que les anneaux commutatifs, afin d'avoir $ax = xa$.*
   On ne s'intéresse pas aux anneaux non-commutatifs (ex : matrices) dans ce cas.
4. *$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ne sont pas des idéaux de $\mathbb{C}$ car ils ne sont pas absorbants pour la multiplication. Pourtant, ce sont des sous-anneaux de $\mathbb{C}$.*
5. *Si un idéal I contient un élément inversible, alors $I = A$. En particulier, les idéaux de $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont $\{0\}$ et l'anneau tout entier.*
6. *Tout sous-anneau B strict d'un anneau A n'est pas un idéal de A, car B contient 1_A mais ne contient pas A tout entier.*
7. *Pour tout $n \in \mathbb{Z}$, $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$. Pourtant, le seul sous-anneau de $\mathbb{Z}$ est $\mathbb{Z}$ lui-même.*
8. *Pour $n \in \mathbb{Z}^*$, $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$ mais ce n'est pas un idéal de $\mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$.*
9. *Pour E un ensemble et E' un sous-ensemble de E, l'ensemble $\{f : E \to \mathbb{C}, t.q. f(x) = 0\, \forall x \notin E'\}$ est un idéal de $\mathcal{F}(E, \mathbb{C})$.*

Remarque 46 — *Un idéal I d'un anneau A est un sous-ensemble qui est en partie similaire à un sous-anneau (identique pour l'addition, mêmes règles de multiplication).*
Par contre, il ne contient en général pas d'élément neutre pour la multiplication (pas de 1).

La définition de sous-anneau de $(A,+,\times)$ ne dépend que des opérations sur A, et non de tous les éléments de A (par exemple, Z est un sous-anneau de $\mathbb{Q}$, de $\mathbb{R}$ et de $\mathbb{C}$, mais les nombres réels et complexes n'interviennent nulle part).
Pour un idéal, la condition d'absorbance implique un lien entre les éléments de I et ceux de A.

Pour B un sous-anneau de A et I un idéal de B, on ne sait pas si I est un idéal de A.

Par exemple, $2\mathbb{Z}$ est un idéal de $\mathbb{Z}$ mais n'est pas un idéal de $\mathbb{Q}$,$\mathbb{R}$ ou $\mathbb{C}$. La condition d'absorbance fait entrer les nombres rationnels/réels/complexes dans les multiplications possibles, et $2\mathbb{Z}$ ne contient pas tout cela.

Remarque 47 — *Soient A un anneau commutatif et I un idéal de A.*
Pour $x_1,\dots,x_n \in I$ et $a_1,\dots,a_n \in A$, on a alors $\sum_{k=1}^{n} a_k x_k \in I$.
En effet, chaque $a_k x_k$ est dans I, et $(I,+)$ est un groupe.

Proposition 48
Soit $(A,+,\times)$ un anneau commutatif et $(I_k)_{k\in E}$ une famille d'idéaux de A indexée par un ensemble E. Alors

1. $\bigcap_{k\in E} I_k$ est un idéal de A.
2. Si E est de cardinal fini, alors $\sum_{k\in E} I_k$ est un idéal de A.
3. $\sum_{k\in E} I_k = \left\{ \sum_{k=1}^{n} x_i, \quad \text{avec } x_i \in \bigcup_{k\in E} I_k,\ \forall i \in [\![1,n]\!],\ \forall n \in \mathbb{N}^* \right\}$ est un idéal de A.

Preuve — Il faut vérifier que ces ensembles satisfont bien les conditions pour être un idéal. □

Proposition-Définition 49
Soient A un anneau commutatif et $S \subset A$ non-vide.
On définit $\langle S\rangle = \{\sum_{k=1}^{n} a_k s_k,\ n \geq 1,\ s_1,\dots,s_n \in S,\ a_1,\dots,a_n \in A\}$.
Alors $\langle S\rangle$ est un idéal de A. On l'appelle **idéal engendré par** S.
C'est le plus petit idéal de A contenant S.

Preuve — • On a bien $0 \in \langle S\rangle$.
Par définition de $\langle S\rangle$, pour $x_1, x_2 \in S$ on a bien $x_1 - x_2 \in \langle S\rangle$. Donc $\langle S\rangle$ est un sous-groupe de $(A,+)$. Soient $x \in \langle S\rangle$ et $a \in A$. On a $x = \sum_{k=1}^{n} a_k s_k$. Alors, $ax = \sum_{k=1}^{n} a a_k s_k = \sum_{k=1}^{n} b_k s_k$, avec $b_1,\dots,b_n \in A$.
Donc ax est encore un élément de $\langle S\rangle$, ce qui montre que $\langle S\rangle$ est un idéal de A.
• Soit I un idéal de A contenant S.
Alors, I contient les éléments de la forme $\sum_{k=1}^{n} a_k s_k$, $\forall n \geq 1$, $\forall a_1,\dots,a_n \in A$, $\forall s_1,\dots,s_n \in S$.
Donc I contient $\langle S\rangle$. □

Contrairement aux sous-anneaux, l'idéal engendré par une partie S a une définition assez simple. Ces idéaux sont assez intéressants.

Proposition 50
Soient A un anneau commutatif, $S_1, S_2 \subset A$ non-vides, et $x_1 \dots, x_n \in A$, avec $n \geq 2$. Alors

1. $\langle x_1\rangle = x_1 A = \{ax_1,\ a \in A\}$;
2. $\langle S_1 \cup S_2\rangle = \langle S_1\rangle + \langle S_2\rangle$;
3. $\langle x_1,\dots,x_n\rangle = x_1A + x_2A + \dots + x_nA$.

Preuve —

1. On vérifie facilement que $x_1A = \{ax_1,\ a \in A\}$ est un idéal de A, qui contient x_1. (A vérifier.)
   Réciproquement, un idéal I de A qui contient x_1 contient les ax_1, $\forall a \in A$.
   Donc, $\langle x_1\rangle = x_1A$ par minimalité de $\langle x_1\rangle$.
2. D'après une proposition précédente, $\langle S_1\rangle + \langle S_2\rangle$ est un idéal de A. Et cet idéal contient $S_1 \cup S_2$.
   Réciproquement, soit I un idéal contenant $S_1 \cup S_2$. Comme I contient S_1 et S_2, I contient $\langle S_1\rangle$ et $\langle S_2\rangle$, donc I contient $\langle S_1 \cup S_2\rangle$.
   Par minimalité de l'idéal engendré par une partie, on en déduit que $\langle S_1 \cup S_2\rangle = \langle S_1\rangle + \langle S_2\rangle$.
3. La preuve de ce résultat est identique à celle du point 1). (Ou bien on utilise 1) et 2) et une récurrence sur $n \geq 2$)

□

On retrouve avec cette proposition l'ensemble des multiples d'un élément x, ensembles que l'on a utilisés dans $\mathbb{Z}$ et dans $\mathbb{K}[X]$ pour définir le *pgcd*, le *ppcm*, et étudier ces outils.
Tout le travail sur les ensembles $n\mathbb{Z}$ et $P\mathbb{K}[X]$ était en fait un travail sur des idéaux.
On peut réaliser le même travail sur d'autres anneaux, les anneaux principaux.

3.7 Anneaux principaux

Définition 51
Soit $(A, +, \times)$ un anneau commutatif, et I un idéal de A.

1. On dit que l'idéal I est **principal** s'il existe $a \in A$ tel que $I = aA$.
2. On dit que l'anneau A est **principal** si A est intègre et si tout idéal de A est principal.

Exemple 52 — *1. L'anneau $(\mathbb{Z}, +, \times)$ est un anneau principal.*

2. Les corps $(\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z})$ sont des anneaux principaux.

3. Les anneaux $\mathbb{Z}/n\mathbb{Z}$ avec n non-premier ne sont pas des anneaux principaux car ils ne sont pas intègres.

Exemple 53 — *1. Tous les anneaux qui ne sont pas intègres ne sont pas principaux ($\mathbb{Z}/n\mathbb{Z}$ avec n non-premier, $\mathcal{F}(E, \mathbb{K})$,...).*

2. L'anneau $(\mathbb{Z}[X], +, \times)$ des polynômes à coefficients entiers n'est pas un anneau principal.
En effet, l'idéal $\langle 2, X\rangle$ n'est pas un idéal principal de $\mathbb{Z}[X]$. (Le vérifier.)

Remarque 54 —
• *Un anneau A qui est principal peut avoir un sous-anneau qui n'est pas principal (On montrera par la suite que $\mathbb{Q}[X]$ est principal, alors que son sous-anneau $\mathbb{Z}[X]$ ne l'est pas).*
De même, un anneau A qui n'est pas principal peut avoir un sous-anneau principal ($\mathbb{Z}[X]$ n'est pas principal, mais il contient $\mathbb{Z}$ qui est principal).
• *Le produit d'anneau principaux $A \times B$ n'est jamais principal, car le produit d'anneaux intègres n'est pas intègre. Par contre, tous les idéaux de $A \times B$ sont encore principaux.*

Preuve — Soit J un idéal de $A \times B$.
On pose $J_A = \{x \in A$, tels que $\exists y \in B$ avec $(x, y) \in J\}$, et $J_B = \{y \in B$, tels que $\exists x \in A$ avec $(x, y) \in J\}$.
Alors, on a $J_A \times \{0_B\} = (1, 0).J$, et $\{0_A\} \times J_B = (0, 1).J$.
Comme A et B sont principaux, on a a et b tels que $J_A = aA$ et $J_B = bB$.
On a ainsi $J_A \times \{0\} = aA \times 0B = (a, 0).(A \times B)$ et $J_B = 0A \times bB = (0, b).(A \times B)$.
En combinant les relations, on obtient :

$$J = (1, 1)J = (1, 0).J + (0, 1).J = (a, 0).(A \times B) + (0, b).(A \times B) = (a, b).(A \times B),$$

ce qui montre que l'idéal J est principal. □

Définition 55
Soit A un anneau commutatif intègre. Soient a,$b \in A$.

1. On dit que a divise b s'il existe $c \in A$ tel que $b = ac$. On le note $a|b$.
2. On dit que deux éléments a et b sont **associés** si a divise b et b divise a.

Exemple 56 —

1. *1 et -1 sont associés dans $\mathbb{Z}$.*
Tout entier n non-nul est associé à un entier strictement positif.
2. *Dans $\mathbb{R}[X]$, $X^2 + 1$ et $2X^2 + 2$ sont associés.*
3. *Dans $\mathbb{K}[X]$, deux polynômes P et Q sont associés si et seulement si $P(X) = \lambda Q(X)$ pour un $\lambda \in \mathbb{K}^*$.*
Tout polynôme P non-nul est associé à un polynôme unitaire.

Proposition 57
Soit A un anneau commutatif intègre.
Alors a divise b si et seulement si $\langle b\rangle = bA \subset aA = \langle a\rangle$.

Preuve — Si $a|b$, alors $b = ac$ et donc $\forall x \in bA$ on a $x = x'b = acx' \in aA$.
Réciproquement, si $bA \subset aA$, alors, $b \in bA \subset aA$ s'écrit ac, d'où $a|b$. □

Remarque 58 — *Soit A un anneau commutatif et intègre.*

1. *Deux éléments $a, b \in A$ sont associés si et seulement si ils sont égaux, à un facteur inversible près.*
Si on a $a = bc$ et $b = c'a$, on a alors $a = cc'a$. Comme A est intègre on obtient $cc' = 1$, donc c est inversible d'inverse c'.
Et donc, a est égal à b multiplié par un élément inversible (un élément de $A^\times$).

2. *La relation "être associés" est donc une relation d'équivalence. (Le vérifier.)*
3. *La relation "être associés" revient à travailler "à un multiple inversible près".*
   Dans $\mathbb{K}[X]$, cela revient à travailler "au coefficient dominant près".
   Dans $\mathbb{Z}$, cela revient à travailler "au signe près".
4. *On va généraliser les résultats de pgcd, ppcm, d'éléments premiers entre eux, d'éléments irréductibles, de factorisation que l'on a obtenus sur $\mathbb{Z}$ et sur $\mathbb{K}[X]$ aux anneaux principaux.*
   Par nature, un élément inversible de A ne se factorise pas (c'est comme -1 dans $\mathbb{Z}$ ou un polynôme constant dans $\mathbb{K}[X]$).

Propriétés de l'anneau $(\mathbb{K}[X], +, \times)$

THÉORÈME 59
L'anneau $(\mathbb{K}[X], +, \times)$ est principal.
Soit I un idéal de $\mathbb{K}[X]$ qui n'est pas réduit à $\{0\}$. Alors il existe un unique polynôme unitaire P tel que $I = P\mathbb{K}[X]$.

Preuve — On sait que l'anneau $(\mathbb{K}[X], +, \times)$ est intègre. Soit I un idéal de $\mathbb{K}[X]$. Il faut montrer que I est principal.
On procède comme avec $\mathbb{Z}$ (voir chapitre Arithmétique). Si $I = \{0\}$, alors $I = 0\mathbb{K}[X]$.
Si $I \neq \{0\}$, soit P un polynôme de I non-nul de plus petit degré. Si λ est son coefficient dominant, alors $\lambda^{-1}P \in I$. On peut donc supposer que P est unitaire.
Soit $Q \in I$. On effectue la division euclidienne de Q par P :

$$Q = RP + S, \text{ avec } \deg S < \deg P.$$

Alors $S = RP - Q \in I$, ce qui donne $S = 0$ et par définition de P. Cela montre que $I \subset P\mathbb{K}[X]$. Réciproquement, pour $P \in I$ on a $P\mathbb{K}[X] \subset I$ car I est un idéal.
On a donc montré que tout idéal I de $\mathbb{K}[X]$ est bien principal.
Supposons que $P\mathbb{K}[X] = Q\mathbb{K}[X]$ avec P, Q unitaires. Alors il existe $A, B \in \mathbb{K}[X]$ tels que $P = AQ$ et $Q = BP$. On obtient $\deg(P) = \deg(Q)$ et $\deg(A) = \deg(B) = 0$, c'est-à-dire $A(X) = \lambda$ pour $\lambda \in \mathbb{K}^*$. Comme P et Q sont unitaires, on a donc $P = Q$, ce qui démontre l'unicité voulue. □

REMARQUE 60 — *La preuve de ce théorème utilise la division euclidienne de polynômes dans $\mathbb{K}[X]$.*
*Les anneaux $\mathbb{K}[X]$ et $\mathbb{Z}$ sont appelés **anneaux euclidiens** (des anneaux possédant une division euclidienne).*
La preuve du théorème permet en fait de montrer qu'un anneau qui possède une division euclidienne (un anneau euclidien) est un anneau intègre.
Nous verrons par la suite la petite différence entre un anneau principal sans division euclidienne et un anneau principal avec division euclidienne.

Dans cette section, nous allons étudier toutes les propriétés des anneaux principaux (les conséquences de la petite hypothèse "tous les idéaux sont principaux"). Ces résultats sont une généralisation des propriétés arithmétiques de $\mathbb{Z}$ et de $\mathbb{K}[X]$ (voir Algèbre 1).

PGCD et PPCM, Théorèmes de Bézout et de Gauss dans les anneaux principaux

PROPOSITION 61
Soit A un anneau intègre. Soient $z, z' \in A$.
Alors, on a $zA = z'A$ si et seulement si z et z' sont associés.
Ainsi, l'idéal principal $I = zA = \langle z \rangle$ possède un unique élément générateur à association près.

Preuve — D'après une remarque précédente, comme A est intègre, si z et z' sont associés on a $z = cz'$ avec c inversible.
Alors $z \subset z'A$ donc $zA \subset z'A$, et $z' = c^{-1}z$ donc $z' \subset zA$ d'où $z'A \subset zA$.
Cela donne bien $zA = z'A$.
Réciproquement, si $zA = z'A$ on a $z = cz'$ et $z' = dz$ pour des éléments $c, d \in A$. Donc z et z' sont associés. □

REMARQUE 62 — *Dans l'étude des propriétés des anneaux principaux (divisiblité, factorisations), les éléments inversibles ne sont pas très intéressants (ce sont des éléments qui divisent tout le monde, comme -1 dans $\mathbb{Z}$ ou comme $\lambda \neq 0$ dans $\mathbb{K}[X]$).*
Ainsi, la majorité des résultats sera à association près, c'est-à-dire à un représentant de classe d'équivalence près pour la relation d'association.
Dans $\mathbb{Z}$, ce représentant sera un nombre positif. Dans $\mathbb{K}[X]$, ce sera un polynôme unitaire.
Par contre, dans le cas général, il n'y a pas de méthode pour choisir un représentant particulier dans la relation

"être associé". On pensera donc bien à préciser que l'unicité d'un élément ou d'une factorisation sera "à association près".

Définition 63
Soit A un anneau principal. Soient x,$y \in A$.
On définit le **plus grand diviseur commun** de x et y, noté $\text{pgcd}(x, y)$ ou $x \wedge y$, comme l'unique élément de A (à association près) tel que :

$$\langle x, y\rangle = xA + yA = \text{pgcd}(x, y)A.$$

On définit le plus petit diviseur commun de x et y, noté $\text{ppcm}(x, y)$ ou $x \vee y$, comme l'unique élément de A (à association près) tel que :

$$xA \cap yA = \text{ppcm}(x, y)A.$$

Définition 64
Soit A un anneau principal. Soient x,$y \in A$.
On dit que x et y sont **premiers entre eux** si $\text{pgcd}(x, y) = 1$.

Proposition 65 (Théorème de Bézout)
Soit A un anneau principal. Soient x,$y \in A$.
Les élémnts x et y sont premiers entre eux si et seulement s'il existe $u, u \in A$ tels que $ux + vy = 1$.

Preuve — On a $\text{pgcd}(x, y) = 1$ ssi $xA + yA = A$. Cela implique qu'il existe $u, v \in A$ tels que $1 = ux + vy$.

Réciproquement, si l'on a $1 = xu + vy$, alors $xA + yA$ contient $1.A = A$, d'où $xA + yA = A$. □

Remarque 66 — *On peut alors montrer de l'exacte même façon qu'avec les entiers que* $\text{pgcd}(x, y)$ *et* $\text{ppcm}(x, y)$ *sont bien les plus grands commun diviseur et plus petit commun multiple pour le relation de divisibilité, à association près.*

Proposition 67
Soit A un anneau principal. Soient x,$y \in A$ et $s \in A$.
Alors s est égal à $\text{pgcd}(x, y)$ à association près si et seulement si :

1. $s \mid x$ et $s \mid y$,
2. Pour tout $t \in A$ tel que $t \mid x$ et $t \mid y$, on a $t \mid s$.

Autrement dit, s est le plus grand diviseur de x et de y.

Proposition 68
Soit A un anneau principal. Soient x,$y \in A$ et $s \in A$.
Alors s est égal à $\text{ppcm}(x, y)$ à association près si et seulement si :

1. $x \mid s$ et $y \mid s$,
2. Pour tout $t \in A$ tel que $x \mid t$ et $y \mid t$, on a $s \mid t$.

Autrement dit, s est le plus petit multiple de x et de y.

Proposition 69 (Théorème de Gauss)
Soit A un anneau principal. Soient $x, y, z \in A$.
Si x divise yz et $\text{pgcd}(x, y) = 1$, alors $x|z$.

Preuve — la preuve est identique au cas des entiers. D'après e théorème de Bézout, il existe $u, v \in A$ tels que $ux + vy = 1$. Cela donne $xuz + yvz = z$. Comme $x|yz$, on a $x|(xuz + yvz) = z$. □

Remarque 70 — *Si l'anneau A est principal mais ne possède pas de division euclidienne (s'il n'est pas euclidien), on sait que pour $x, y \in A$ il existe $u, v \in A$ tels que $xu + yv = pgcd(x, y)$, mais on n'a aucune méthode pour calculer u et v.*
La division euclidienne, dont découle l'algorithme d'Euclide, est une propriété qui permet de calculer $pgcd(x, y)$ et de calculer les nombres u, v.

Conséquences de ces théorèmes

Proposition 71
Soit A un anneau principal. Soient $a, b, c \in A$.

Si a et b premiers entre eux et si $a \mid c$ et $b \mid c$, alors $ab \mid c$.

Preuve — Supposons que $a \mid c$ et $b \mid c$ avec $\text{pgcd}(a,b) = 1$. Le théorème de Bézout nous dit qu'il existe alors des entiers $u, v \in A$ tels que $au + bv = 1$. On a donc $c = auc + bvc$. Comme $a \mid c$, on a on a $ab \mid bc$. Comme $b \mid c$, on a on a $ab \mid ac$. Donc, ab divise $acu + bcv = c$. □

Corollaire 72
Soit A un anneau principal. Soient $a_1,\ldots,a_n,c \in A$.
Si les a_i sont premiers entre eux deux à deux et si $a_i \mid c$ pour tout $1 \leq i \leq n$, alors $a_1 \times a_2 \times \ldots a_n \mid c$.

Preuve — Cette généralisation de la proposition précédente se démontre par récurrence sur $n \geq 2$. □

Si a et b ne sont pas premiers entre eux, on ne peut rien dire ! Par exemple, dans $\mathbb{Z}$, $4 \mid 4$ et $2 \mid 4$ mais $4 \times 2 = 8$ ne divise pas 4.

Exemple 73 — *Si* $4 \mid n$ *et* $3 \mid n$ *alors* $12 \mid n$ *car* 4 *et* 3 *sont premiers entre eux.*

Proposition 74
Soit A un anneau principal. Soient $a, b, c \in A$.
Si a est premier avec b et si a est premier avec c, alors a est premier avec bc.

Preuve — Supposons a premier avec b et avec c. D'après le théorème de Bézout, il existe $u_1, u_2, v_1, v_2 \in A$ tels que $1 = au_1 + bv_1$ et $1 = au_2 + cv_2$. Par multiplication, on obtient :

$$1 = a(au_1u_2 + u_1cv_2 + bv_1u_2) + bc(v_1v_2).$$

Ainsi, d'après le théorème de Bézout, a et bc sont premiers entre eux. □

Corollaire 75
Soit A un anneau principal. Soient $a,b_1,\ldots,b_n \in \mathbb{Z}$.
Si a est premier avec b_i pour tout $i \in \{1,\ldots,n\}$, alors a est premier avec $b_1 \times b_2 \times \ldots \times b_n$.

Preuve — Cette généralisation de la proposition précédente se démontre par récurrence sur $n \geq 2$. □

Proposition 76
Soit A un anneau principal. Soient $a, b \in A$.
Si a est premier avec b alors a^m est premier avec b^n pour tous $m, n \in \mathbb{N}$.

Preuve — Soient $m, n \in \mathbb{N}$. Si $m = 0$ ou $n = 0$ on a $a^m = 1$ ou $b^n = 1$, et dans ce cas le résultat est vrai.

Supposons $m, n \neq 0$. Comme a est premier avec b, le corollaire précédent nous dit que a est premier avec b^n. Comme b^n est premier avec a, le corollaire précédent nous dit que b^n est premier avec a^m. □

Exemple 77 — *Soit* A *un anneau principal. Soit* $a \in \mathbb{N}^*$. *Comme* a *est premier avec* $a-1$ *et avec* $a+1$, a *est premier avec* $(a-1)(a+1) = a^2 - 1$.

Proposition 78
Soit A un anneau principal. Soient $a, b \in A$. Posons $d = \text{pgcd}(a,b)$.
Alors il existe des éléments a' et b' de A tels que

$$a = da',\ b = db', \quad \text{et} \quad \text{pgcd}(a', b') = 1.$$

Preuve — Si $(a,b) = (0,0)$, alors $a' = b' = 1$ conviennent.

Supposons que $(a,b) \neq (0,0)$. Comme $d = \text{pgcd}(a,b)$, on sait que $d \mid a$ et $d \mid b$. Les nombres $a' = \frac{a}{\text{pgcd}(a,b)}, b' = \frac{b}{\text{pgcd}(a,b)}$ sont donc bien définis, et tels que $a = da'$ et $b = db'$. On a alors $d = \text{pgcd}(a,b) = \text{pgcd}(da', db') = d\,\text{pgcd}(a', b')$. Donc, comme d est non nul, on a $\text{pgcd}(a', b') = 1$. □

Eléments irréductibles d'un anneau principal, décomposition en facteurs irréductibles

Définition 79
Soit A un anneau principal. Soit $a \in A$.
On dit que a est un élément **irréductible de** A si a n'est pas inversible et si les seuls diviseurs de a sont les éléments inversibles et les éléments associés à a.

Un élément irréductible de A est donc un élément a non-inversible dont les diviseurs sont 1 et a, à association près.
Tout comme un nombre premier est un entier dont les diviseurs sont, au signe près, 1 et lui-même.

EXEMPLE 80 — *Voir exemples dans $\mathbb{Z}$ et dans $\mathbb{K}[X]$.*

LEMME 81
Soit A un anneau principal. Soient $a, b \in A$ avec a irréductible.
Alors, on a $pgcd(a,b) = a$ si $a \mid b$, et $pgcd(a,b) = 1$ sinon (égalités à association près).

Preuve — Si $a \mid b$ on a $pgcd(a,b) \mid a$ et $a \mid pgcd(a,b)$, donc a et $pgcd(a,b)$ sont associés.
Sinon, a ne divise pas b. Comme $pgcd(a,b)$ divise a et divise b, et comme a est irréductible, on en déduit que 1 et $pgcd(a,b)$ sont associés. C'est-à-dire que $pgcd(a,b) = 1$ (à association près). □

LEMME 82 (Théorème d'Euclide)
Soit A un anneau principal. Soient $a, b, c \in A$ avec c irréductible.
Si $c \mid ab$, alors $c \mid a$ ou $c \mid B$.

Preuve — Supposons que $c \mid ab$.

• Si c divise a, c'est bon.

• Sinon, c ne divise pas a. D'après le lemme précédent on a alors $\text{pgcd}(a,c) = 1$ (à association près), donc c et a sont premiers entre eux. Le théorème de Gauss nous dit alors que c divise b, ce qui conclut la preuve. □

THÉORÈME 83 (Décomposition en produit de facteurs irréductibles)
Soit A un anneau euclidien. Soit $a \in A$ non-nul et non-inversible.
Alors a se décompose, de manière unique à l'ordre près des termes et à association près, en produit de facteurs irréductibles :

$$a = \epsilon p_1(X)^{\alpha_1} \times p_2(X)^{\alpha_2} \dots p_N(X)^{\alpha_N},$$

où les p_i sont des éléments irréductibles deux à deux premiers entre eux, les α_i sont des entiers non nuls, et où ϵ est un élément inversible de A.

Contrairement aux anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$, on ne peut pas utiliser la division euclidienne (en fait $|n|$ et $\deg(P)$) pour montrer rapidement l'existence de la décomposition en facteurs irréductibles de a.
On va alors utiliser le fait que A est principal pour démontrer le lemme suivant.

LEMME 84
Soit A un anneau principal. Soit $(J_n)_{n\geq 0}$ une suite d'idéaux de A.
Si la suite $(J_n)_{n\geq 0}$ est croissante pour l'inclusion ($J_n \subset J_{n+1}$), alors elle est stationnaire : il existe n_0 tel que $J_n = J_{n_0}$, $\forall n \geq n_0$.

Preuve — On pose $J = \bigcup_{n\geq 0} J_n$.
On montre que J est alors un idéal de A. (facile à vérifier)
Comme A est principal, on en déduit qu'il existe $b \in A$ tel que $J = bA$.
On remarque que l'on a $b \in J$.
Comme J est une réunion d'ensembles, il existe donc un $n_0 \geq 0$ tel que $b \in J_{n_0}$.
On a ainsi $bA \subset J_{n_0}$. Vu que $J_{n_0} \subset J$, on en déduit que $J = J_{n_0}$.
Ainsi, pour tout $n \geq n_0$, on a $J_n = J = J_{n_0}$. □

Preuve — **Existence :** Comme a est non-nul et non-inversible, il possède au moins un diviseur irréductible.
Supposons par l'absurde que a possède une infinité de diviseurs irréductibles qui sont premiers entre eux (qui sont distincts à association près).
On peut alors trouvr une suite $(p_n)_{n\geq 0}$ de nombres irréductibles premiers entre eux, tels que $p_n \mid a$ $\forall n \geq 0$.
D'après les résultats de divisibilité précédents, on en déduit que $p_1 p_2 \dots p_n \mid a$, $\forall n \geq 0$.
On pose alors $b_n = \frac{a}{p_1 \dots p_n}$, et on définit l'idéal $J_n = b_n A$.
On remarque facilement que $J_n \subset J_{n+1}$ car $b_{n+1} \mid b_n$.
Comme on a $b_{n+1} p_{n+1} = b_n$, avec p_{n+1} non-inversible, on en déduit que b_n et b_{n+1} ne sont pas associés, donc $J_n \neq J_{n+1}$ d'après une proposition précédente.
On obtient alors une suite $(J_n)_{n\geq 0}$ d'idéaux de A, qui est croissante pour l'inclusion.
D'après le lemme précédent, cette suite est stationnaire. Cela contredit le fait que $J_n \neq J_{n+1}$, $\forall n \geq 0$.

Ainsi, le nombre a possède un nombre fini N de diviseurs irréductibles qui sont premiers entre eux deux à deux.
Soient $p_1, \dots, p_N$ des nombres irréductibles, premiers entre eux deux à deux, qui divisent a.
Avec le même argument, on montre que pour chaque i, il existe un entier α_i tel que $p_i^{\alpha_i} \mid a$ et $p_i^{\alpha_i+1} \not| a$. (chaque p_i ne divise pas a

une infinité de fois)
Le nombre $\epsilon = \frac{a}{\Pi_{i=1}^{N} p_i^{\alpha_i}}$ est alors bien défini. Ce nombre est non-nul et il ne peut posséder aucun diviseur irréductible. (ses seuls diviseurs possibles sont parmi les p_i, et aucun p_i ne peut diviser ϵ)
On en déduit donc que ϵ est inversible, ce qui prouve l'existence de cette décomposition.

Unicité :

La preuve de l'unicité est identique à celle de la décomposition des entiers en produit de facteurs premiers, à part le fait que tous les nombres irréductibles que l'on considère sont choisis à association près. □

Ainsi, tout éléent non-nul et non-inversible d'un anneau principal A possède une décomposition en produit de facteurs irréductible. Cette décomposition, nous l'avons vu en Algèbre 1, est très utile pour des calculs arithmétiques (*pgcd*, *ppcm*, divisibilité, factorisations,...)
Cependant, l'absence de division euclidienne a rendu la preuve plus difficile. On a eu le même résultat, mais avec moins d'outils, et il a fallu être bien plus malin pour l'obtenir.
Les idées de cette preuve sont bien plus difficiles que celles des autres preuves du chapitre. Cela montre qu'en mathématiques une notion peut paraître simple pour beaucoup de résultats, et subitement devenir très difficile.

Proposition 85
Soit A un anneau intègre. Soit $a \in A$ non-nul et non-inversible.
Soit $a = \epsilon p_1^{\alpha_1} \times \ldots \times p_N^{\alpha_N}$ la décomposition de a en produit de facteurs irréuctibles, avec p_i des nombres irréductibles premiers entre eux deux à deux, α_i des entiers naturels non nuls, et ϵ inversible.

Alors les diviseurs de a sont exactement les nombres de la forme $\epsilon' p_1^{\beta_1} \ldots p_N^{\beta_N}$ avec $0 \leq \beta_i \leq \alpha_i$ pour tout $1 \leq i \leq N$, et ϵ' inversible.

Le nombre a possède ainsi $\Pi_{i=1}^{N}(\alpha_i + 1)$ diviseurs distincts (à association près).

Preuve — La preuve est identique à celle du résultat pour les entiers, (voir Algèbre 1) à part le fait que l'on a ajouté un terme inversible en plus pour inclure tous les diviseurs à association près. □

Exemple 86 — • *Les diviseurs à association près de* $X^3 - 5X + 6 = (X-2)(X-3)$ *dans* $\mathbb{Q}[X]$ *sont les suivants :* 1, $X-2$, $X-3$, $(X-2)(X-3)$.
• *Dans* $\mathbb{Z}[X]$, *les diviseurs à association près de* $6X-6$ *sont* $1, 2, 3, 6, X-1, 2X-2, 3X-3, 6X-6$.

Proposition 87
Soit A un anneau unitaire. Soient $a, b \in A$ non-inversibles et non-unitaires.
On suppose que $a = \epsilon p_1^{\alpha_1} \times \ldots \times p_N^{\alpha_N}$ et $b = \epsilon' p_1^{\beta_1} \times \ldots \times p_N^{\beta_N}$, où les p_i sont des éléments irréductibles preiers entre eux deux à deux, les α_i, β_i sont des entiers naturels (éventuellement nuls), et ϵ, ϵ' sont inversibles. Alors on a :

- $\text{pgcd}(a,b) = p_1^{\min(\alpha_1,\beta_1)} \times \ldots \times p_N^{\min(\alpha_N,\beta_N)}$, (à association près)
- $\text{ppcm}(a,b) = p_1^{\max(\alpha_1,\beta_1)} \times \ldots \times p_N^{\max(\alpha_N,\beta_N)}$. (à association près)

Preuve — La preuve est identique à celle du résultat pour les entiers. (voir Algèbre 1) □

Proposition 88
Soit A un anneau unitaire. Soient $a, b \in A$.
Alors on a

$$\text{pgcd}(a,b) \times \text{ppcm}(a,b) = a \times b. \text{ (à association près)}$$

En particulier, si a et b sont premiers entre eux, on a $\text{ppcm}(a,b) = ab$.

Preuve — La preuve est identique à celle pour les entiers. (voir Algèbre 1) □

Remarque 89 (Bilan sur les anneaux étudiés) — *Voici les principales propriétés des anneaux que nous avons définies et étudiées. Elles sont triées par ordre décroissant, et accompagnées d'exemples.*

1. *Les anneaux :* $\mathscr{M}_n(\mathbb{K})$, $(Fonct(G,G), +, \circ)$ *(avec* G *un groupe commutatif), produits d'anneaux non-tous commutatifs,...*
2. *Les anneaux commutatifs :* $(Fonct(E,A), +, \times)$, $\mathbb{Z}/n\mathbb{Z}$, *produits d'anneaux commutatifs,...*
3. *Les anneaux intègres commutatifs :* $\mathbb{Z}[X], \mathbb{K}[a]$*(pour* $a \in A$ *)*, ...
4. *Les anneaux principaux :* $\mathbb{Z}, \mathbb{Z}[i], \mathbb{Z}[sqrt2], \mathbb{K}[X], \ldots$
5. *Les corps :* $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}, \mathbb{Q}[i], \mathbb{Q}[sqrt2], \ldots$

Chaque propriété supplémentaire permet de faciliter les calculs ou les études sur l'anneau A.
• Si A est commutatif, on peut alors effectuer des développements et factorisations, comme la formule du binôme, la somme géométrique, les identités remarquables.
• Si A est intègre, on peut alors résoudre des équations produit-nul ($ab = 0$) et donc simplifier beaucoup d'équations où un terme non-nul est en facteur.
• Si A est principal, il existe des éléments qui ne se factorisent pas, et tous les éléments se factorisent comme produit (à association près) d'éléments irréductibles. Cela aide aussi dans beaucoup de factorisations, à déterminer des divisibilités, et à résoudre certaines équations, en regardant ce qui se passe pour chaque facteur irréductible.
• Si A possède une division euclidienne, tous les éléments que l'on peut définir quand A est principal peuvent se calculer à l'aide de divisions euclidienne et de l'algorithme d'Euclide : diviseurs, pgcd,ppcm,...
• Si A est un corps (tous les éléments non-nuls sont inversibles), alors beaucoup de questions de factorisation et de divisibilité se résolvent instantanément. (nous étudierons les corps par la suite)
Les corps ne sont pas intéressants à étudier comme anneaux principaux (ils n'ont pas d'éléments irréductibles), mais ils sont très intéressants pour définir d'autres objets (anneaux $\mathbb{K}[X]$, $\mathbb{K}$-espaces vectoriels, $\mathbb{K}$-algèbres,...).

Remarque 90 — *Il existe aussi des anneaux qui ne vérifient pas toutes ces propriétés. Il n'y a pas forcément d'exemple très simple pour ces anneaux, mais leur existence montre que l'étude des anneaux en général est très riche.*
Cela montre aussi qu'il existe des anneaux possédant certains propriétés pratiques, mais qui peuvent être très différents des exemples "classiques" que nous avons étudiés dans ce cours.

1. *Anneaux intègres non-commutatifs : $\mathbb{H}$ (anneau des quaternions),...*
2. *Anneaux commutatifs, non-intègres, avec tous les idéaux principaux : $\mathbb{Z}/n\mathbb{Z}$ pour n non premier, produit d'anneaux principaux,...*
3. *Anneaux principaux sans division euclidienne : $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$, ... (pas facile du tout !)*

Nous avons étudié plusieurs propriétés d'anneaux (commutatif, intègre, principal), ainsi que certains exemples fondamentaux. Tout comme pour les groupes, nous allons nous intéresser aux fonctions qui préservent la structure d'anneau, les morphismes d'anneaux.

3.8 Morphismes d'anneaux, Isomorphismes

Définition 91
Soient $(A, +, \times)$ et $(B, \triangle, .)$ deux anneaux.
Une fonction $f : A \to B$ est un **morphisme d'anneaux** si :

1. f est un morphisme de groupes de $(A, +)$ dans $(B, \triangle)$: $\forall x, y \in A,\ f(x + y) = f(x) \triangle f(y)$;
2. $f(1_A) = 1_B$;
3. $\forall x, y \in A,\ f(x \times y) = f(x).f(y)$.

Un morphisme d'anneaux est ainsi une fonction qui est compatible avec les opérations d'addition ($+$ et $\triangle$), avec les opérations de multiplication ($\times$ et $.$), et telle que $f(1) = 1$.

Exemple 92 —

1. *Soit $(A, +, \times)$ un anneau. La fonction identité $Id : A \to A$ est un morphisme d'anneaux.*
2. *Si B est un sous-anneau de $(A, +, \times)$, alors l'injection $i : x \in B \mapsto x \in A$ est un morphisme d'anneaux. Ainsi, $x \in \mathbb{R} \mapsto x \in \mathbb{C}$ est un morphisme d'anneaux.*
3. *Soient E un ensemble et $x_0 \in E$. La fonction*
$$\varphi_{x_0} : \begin{array}{ccc} \mathcal{F}(E, \mathbb{R}) & \to & \mathbb{R} \\ g & \mapsto & g(x_0) \end{array}$$
est un morphisme d'anneaux (Pourquoi ?).
*On l'appelle **morphisme d'évaluation** en x_0.*
4. *La conjugaison complexe $z \in \mathbb{C} \mapsto \overline{z} \in \mathbb{C}$ est un morphisme d'anneaux.*
5. *Soit $n \in \mathbb{N}^*$. La fonction*
$$r : \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ x & \mapsto & \overline{x} \end{array}$$
est un morphisme d'anneaux.

6. *Soit I un intervalle de $\mathbb{R}$. La fonction*

$$D : \begin{array}{ccc} \mathcal{C}^1(I) & \to & \mathcal{C}^0(I) \\ f & \mapsto & f' \end{array}$$

n'est pas un morphisme d'anneaux (Pourquoi ?).

DÉFINITION 93
Soient $(A, +, \times)$, $(B, \triangle, .)$ deux anneaux, er $\varphi : A \to B$ un morphisme d'anneaux. On dit que :

- φ est un endomorphisme d'anneaux si $(B, \triangle, .) = (A, +, \times)$;
- φ est un **isomorphisme d'anneaux** si φ est bijective ;
- φ est un automorphisme d'anneaux si φ est un endomorphisme bijectif.

On dit que les anneaux A et B sont **isomorphes** s'il existe un isomorphisme d'anneaux entre A et B.

EXEMPLE 94 —

1. *Dans $\mathscr{M}_n(\mathbb{C})$, $Vect(I_n) = I_n.\mathbb{C}$ est un sous-anneau isomorphe à $\mathbb{C}$.*
2. *Dans $\mathscr{M}_n(\mathbb{K})$, l'ensemble des matrices diagonales est un sous-anneau, isomorphe à l'anneau $\mathbb{K}^n$.*
3. *Dans $\mathscr{M}_2(\mathbb{R})$, pour $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $Vect(I_2, A)$ est un sous-anneau qui est isomorphe à l'anneau $\mathbb{C}$. (Prendre $f(xI_2 + yA) = x + iy$.)*
4. *Dans $\mathbb{K}[X]$, $Vect(1) = 1.\mathbb{K}$ est un sous-anneau isomorphe à $\mathbb{K}$.*
5. *L'anneau $\mathbb{Q}[i]$ n'est pas isomorphe comme anneau à $\mathbb{Q}^2$.*

EXEMPLE 95 —

1. *Il n'existe aucun morphisme d'anneau de $\mathbb{Q}$ vers $\mathbb{Z}$. (Indication : Supposer que f existe et regarder $f(\frac{1}{2})$.)*
2. *Il n'existe aucun morphisme d'anneau de $\mathbb{R}$ vers $\mathbb{Q}$. (Indication : Supposer que f existe et regarder $f(\sqrt{2})$.)*
3. *Il n'existe aucun morphisme d'anneau de $\mathbb{C}$ vers $\mathbb{R}$. (Pourquoi ?)*
4. *Il existe un seul morphisme d'anneau de $\mathbb{Z}$ vers $\mathbb{Z}$. (Pourquoi ?)*
5. *Il existe un seul morphisme d'anneau de $\mathbb{Q}$ vers $\mathbb{Q}$. (Pourquoi ?)*
6. *Il existe une infinité de morphismes d'anneaux de $\mathbb{K}[X]$ vers $\mathbb{K}[X]$. (Lesquels ?)*
7. *Il existe un morphisme d'anneaux de $\mathbb{Z}/n\mathbb{Z}$ vers $\mathbb{Z}/m\mathbb{Z}$ si et seulement si $n \mid m$. (Pourquoi ?)*
8. *Les anneaux $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$ sont isomorphes. (Le démontrer.)*
9. *Les anneaux $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ne sont pas isomorphes. (Le démontrer.)*

REMARQUE 96 — *La relation "$A\mathcal{R}B$ si A et B sont des anneaux isomorphes" est une relation d'équivalence sur la classe de tous les anneaux.*
Quand on étudie la structure d'un anneau, ce qui nous intéresse est le comportement entre les éléments. Deux anneaux isomorphes vont avoir exactement la même structure, ce qui fait que l'on étudie souvent les anneaux "à isomorphisme près".
Ainsi, être capable de classer les anneaux pour cete relation d'équivalence, de dire si A est isomorphe à B ou non, est une chose très importante en théorie des anneaux.
Pouvoir reconnaître dans un anneau A des sous-anneaux dont on connaît toute la structure (par exemple des sous-anneaux de $\mathscr{M}_n(\mathbb{K})$ isomorphes à un $\mathbb{K}^d$, à $\mathscr{M}_d(\mathbb{K})$,...) est quelque chose de très important.
• Etudier les anneaux à isomorphisme près est similaire au fait d'étudier les espaces vectoriels à isomorphisme (d'e.v.) près.
Un $\mathbb{K}$-e.v. de dimension n se comporte exactement comme $\mathbb{K}^n$ (il est isomorphe à $\mathbb{K}^n$ avec le choix d'une base), ce qui permet de simplifier grandement l'étude de tous ces e.v., et aussi de simplifier l'étude des applications linéaires sur ces e.v.).

PROPOSITION 97
Soient A, B, C des anneaux.

- Pour $\varphi_1 : A \to B$, $\varphi_2 : B \to C$ des morphismes d'anneaux, alors $\varphi_2 \circ \varphi_1 : A \to C$ est un morphisme d'anneaux.
- Pour $\varphi : A \to B$ un isomorphisme d'anneaux, $\varphi^{-1} : B \to A$ est un isomorphisme d'anneaux.
- L'ensemble $MA(A)$ des endomorphismes d'anneaux sur A, muni des opérations $+$ et $\circ$.

- L'ensemble $MA(A)^\times$ des éléments inversibles de $MA(A)$ est exactement l'ensemble des isomorphismes d'anneaux sur A. C'est un groupe pour $\circ$.

Preuve — Il faut vérifier que les fonctions satisfont bien les axiomes d'un morphisme d'anneaux. Les raisonnements sont similaires à ceux pour la composée/l'inverse de morphismes de groupes.
Pour le point 3), il faut vérifier que cet ensemble est un sous-anneau de $Fonct(A)$. En effet, la somme de morphismes d'anneaux est un anneaux. Pour la composée, cela vient du point 1). Enfin, l'élément neutre Id_A est est bien dans $MA(A)$.
Pour le point 4), on vérifie facilement avec 2) qu'un morphisme d'anneau est bijectif si et seulement si il est inversible dans $MA(A)$. Ensuite, il faut vérifier que cet ensemble est un sous-groupe de $Bij(A)$. Cette vérification découle de 2) et de 1). □

Si les opérations sur des anneaux A et B sont sans ambiguité, on notera parfois "toutes les additions" $x + y$ et "toutes les multiplications" $x \times y$ ou $x.y$ ou xy.

PROPOSITION 98
Soient $(A, +, \times)$, $(B, \triangle, .)$ deux anneaux et $\varphi : A \to B$ un morphisme d'anneaux.

1. Si A' est un sous-anneau de A, alors $\varphi(A')$ est un sous-anneau de B.
2. Si B' est un sous-anneau de B, alors $\varphi^{-1}(B')$ est un sous-anneau de A.

De plus, si A' (ou B') est commutatif, alors $\varphi(A')$ (ou $\varphi^{-1}(B')$) l'est aussi.

Preuve — Il faut vérifier que $\varphi(A')$ et $\varphi^{-1}(B')$ satisfont les conditions pour être des sous-anneaux. □

REMARQUE 99 — *Le noyau d'un morphisme d'anneaux,* $\mathrm{Ker}(\varphi) := \varphi^{-1}(\{0_B\})$*, n'est pas un anneau (Pourquoi ?).*

EXEMPLE 100 — *La fonction* $\varphi : a + ib \in C \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathscr{M}_2(\mathbb{R})$ *est un morphisme d'anneaux, qui est injectif. Ainsi,* $\mathscr{M}_2(\mathbb{R})$ *contient un sous-anneau commutatif qui est isomorphe (comme anneau) à* $\mathbb{C}$.

PROPOSITION 101
Soient A, B des anneaux et $\varphi : A \to B$ un morphisme d'anneaux. Alors on a :

1. $\varphi(0_A) = 0_B$;
2. $\varphi(na) = n\varphi(a)$, $\forall a \in A$, $\forall n \in \mathbb{Z}$;
3. $\varphi(a^n) = \varphi(a)^n$, $\forall a \in A$, $\forall n \in \mathbb{N}$.

Preuve — Ces résultats s'obtiennent très bien avec les propriétés d'un morphisme d'anneau, voire avec une récurrence. (A vérifier .) □

PROPOSITION 102
Soient $(A, +, \times)$, $(B, \triangle, .)$ deux anneaux commutatifs et $\varphi : A \to B$ un morphisme d'anneaux.

1. Soit I un idéal de A. Alors $\varphi(I)$ est un idéal de $\varphi(A)$.
2. En particulier, pour $S \subset A$ on a $f(\langle S \rangle) = \langle f(S) \rangle$.
3. Soit J un idéal de B. Alors $\varphi^{-1}(J)$ est un idéal de A.
4. En particulier, $\mathrm{Ker}(\varphi)$ est un idéal de A.

Preuve —

1. On sait que $\varphi(A)$ est un sous-anneau de B et que $(\varphi(I), +)$ est un sous-groupe abélien. Soient $y \in \varphi(I)$ et $y' \in \varphi(A)$. Il existe $x \in I$,$x' \in A$ tels que $\varphi(x) = y$ et $\varphi(x') = y'$.
   On a $yy' = \varphi(x)\varphi(x') = \varphi(xx')$. Comme I est un idéal, on a $xx' \in I$, donc $\varphi(xx') \in \varphi(I)$. Donc $\varphi(I)$ est un idéal.
2. La vérification est assez facile par double-inclusion.
   On utilise le fait que, pour $a_1, \ldots, a_n \in A$ et $s_1, \ldots, s_n \in S$, on a
   $$f(\sum_{i=1}^{n} a_i s_i) = \sum_{i=1}^{n} f(a_i) f(s_i),$$
   car f est un morphisme d'anneaux.
3. De même, on sait que $(\varphi^{-1}(J), +)$ est un sous-groupe abélien. Soient $x \in \varphi^{-1}(J)$ et $x' \in A$. Comme J est un idéal et $\varphi(x) \in J$, on a $\varphi(xx') = \varphi(x)\varphi(x') \in J$. Ce qui implique que $xx' \in \varphi^{-1}(J)$.
4. Immédiat. (Pourquoi ?)

□

Exemple 103 —

- *Pour $n \in \mathbb{N}$ et $\varphi_n : a \in \mathbb{Z} \mapsto \overline{a} \in \mathbb{Z}/n\mathbb{Z}$, on a $\mathrm{Ker}(\varphi_n) = n\mathbb{Z}$.*
  On retrouve le fait que $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$.
  D'un autre côté, pour B un anneau commutatif et pour $\varphi : \mathbb{Z} \to B$ un morphisme d'anneaux, on a $\mathrm{Ker}(\varphi) = m\mathbb{Z}$ pour un $m \in \mathbb{N}$, car ces idéaux sont les seuls idéaux de $\mathbb{Z}$. ($\mathbb{Z}$ est un anneau principal)
- *Soit B un anneau quelconque et pour $\varphi : \mathbb{R} \to B$ un morphisme d'anneaux.*
  Comme $\varphi(\mathbb{R})$ est un sous-anneau commutatif de B, la restriction $\varphi : \mathbb{R} \to \varphi(\mathbb{R})$ est un morphisme entre anneaux commutatifs.
  Donc, $\mathrm{Ker}(\varphi)$ est un idéal de $\mathbb{R}$. Les idéaux de $\mathbb{R}$ sont $\{0\}$ et $\mathbb{R}$.
  Comme $\varphi(1) = 1_B \neq 0_B$, on a donc $\mathrm{Ker}(\varphi) = \{0\}$, donc un tel morphisme est toujours injectif.

Maintenant que nous avons défini les morphismes d'anneaux et les isomorphismes d'anneaux, nous pouvons revenir une dernière fois sur les ensembles $\mathbb{Z}/n\mathbb{Z}$. Nous allons généraliser les théorèmes des restes et d'isomorphisme chinois vus pour les groupes $\mathbb{Z}/n\mathbb{Z}$ aux anneaux $\mathbb{Z}/n\mathbb{Z}$.

3.9 Théorème d'isomorphisme chinois

Théorème 104 (Théorème d'isomorphisme chinois)
Soit $r \geq 2$. Soient $m_1, \ldots, m_2 \in \mathbb{N}^*$ premiers entre eux deux à deux.
Soit $\phi : (\mathbb{Z}/(m_1 \ldots m_r)\mathbb{Z}) \to (\mathbb{Z}/m_1\mathbb{Z}) \times \ldots \times (\mathbb{Z}/m_r\mathbb{Z})$ définie par $\phi(\overset{-(m_1 \ldots m_r)}{c}) = (\overset{-(m_1)}{c}, \ldots, \overset{-(m_r)}{c})$.
Alors, ϕ est un isomorphisme d'anneaux.
Pour tout $1 \leq i \leq r$, soient $u_i m_i + v_i \Pi_{j \neq i} m_j = 1$ des relations de Bézout pour m_i et $\Pi_{j \neq i} m_j$. On a alors :

$$\phi^{-1}(\overset{-(m_1)}{a_1}, \ldots, \overset{-(m_r)}{a_r}) = \sum_{i=1}^{r} \overset{-(m_1 \ldots m_r)}{a_i v_i \Pi_{j \neq i} m_j}.$$

Ainsi, les deux anneaux suivants sont isomorphes :

$$(\mathbb{Z}/(m_1 \ldots m_r)\mathbb{Z}, +, \times) \simeq ((\mathbb{Z}/m_1\mathbb{Z}) \times \ldots \times (\mathbb{Z}/m_r\mathbb{Z}), +, \times).$$

Preuve — On sait d'après la section "Groupe $\mathbb{Z}/n\mathbb{Z}$" que la fonction ϕ est bijective, que ϕ est un morphisme de groupes, et on connaît l'expression de ϕ^{-1}.
Il faut donc vérifier que ϕ est un morphisme d'anneaux, et la preuve sera terminée.
Soient $a, b \in \mathbb{Z}$.
Par définition de la multiplication sur un produit d'anneaux, on a

$$(\overset{-(m_1)}{a}, \ldots, \overset{-(m_r)}{a}) \times (\overset{-(m_1)}{b}, \ldots, \overset{-(m_r)}{b}) = (\overset{-(m_1)}{a} \times \overset{-(m_1)}{b}, \ldots, \overset{-(m_r)}{a} \times \overset{-(m_r)}{b}) = (\overset{-(m_1)}{ab}, \ldots, \overset{-(m_r)}{ab}).$$

On vient donc de montrer que

$$\phi(\overset{-(m_1 \ldots m_r)}{a}) \times \phi(\overset{-(m_1 \ldots m_r)}{b}) = \phi(\overset{-(m_1 \ldots m_r)}{ab}).$$

Cela termine la preuve. □

Exercice 8 — *1. Soient $m, n \in \mathbb{N}^*$ premiers entre eux. Montrer que l'on a $\varphi(nm) = \varphi(n)\varphi(m)$. (Indication : On pourra utiliser le théorème d'isomorphisme chinois, et chercher une bijection entre deux ensembles.)*

2. Soit $n \geq 2$. Soit $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ la décomposition en facteurs premiers de n. Exprimer $\varphi(n)$ en fonction des p_i et des α_i.

3. Calculer $\varphi(10)$,$\varphi(60)$, $\varphi(100)$, $\varphi(105)$.

Remarque 105 — *Le théorème d'isomorphisme chinois (pour les anneaux) permet d'étudier tous les anneaux $\mathbb{Z}/n\mathbb{Z}$ simplement en étudiant tous les anneaux $\mathbb{Z}/p^a\mathbb{Z}$, avec p premier.*

Remarque 106 — *Ce théorème aussi d'étudier le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$, qui est isomorphe à un produit direct de groupes de la forme $(\mathbb{Z}/p^a\mathbb{Z})^\times$, pour p premier. On a ainsi des résultats sur les anneaux qui permettent d'étudier certains groupes paticuliers. Par exemple, si n n'est pas de la forme p^b, $2p^b$ ou $4p^b$ avec p premier impair, alors le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique. (Résultat étudié en TD, cela utilise des propriétés élémentaires des groupes cycliques)*

REMARQUE 107 — *Ce théorème permet de caractériser les produits d'anneaux* $\Pi_{i=1}^{r}\mathbb{Z}/n_i\mathbb{Z}$. *On peut alors les distinguer, à isomorphisme d'anneau près.*
Par exemple, $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$ *est isomorphe à* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z}$, *qui est isomorphe à* $\mathbb{Z}/150\mathbb{Z}$.
Par contre, $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$ *est isomorphe à* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z})^2$, *qui est isomorphe à* $\mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. *Ces deux anneaux le même cardinal, mais l'équation* $5x = 0$ *possède* 5 *solutions dans le premier anneau, et* 25 *solutions dans le second. Ils ne sont donc pas isomorphes.*
Il existe toute une théorie pour classer les produits d'anneaux $\mathbb{Z}/n\mathbb{Z}$, *et celle-ci est basée sur le théorème d'isomorphisme chinois ainsi que sur les propriétés des isomorphismes d'anneau.*

Chapitre 4 Structure algébrique : Espaces Vectoriels

Définition 1
Soit $\mathbb{K}$ un corps. Soit E un ensemble.
On dit que E est un $\mathbb{K}$-espace vectoriel s'il possède deux lois $+ : E \times E \to E$ et $. : \mathbb{K} \times E \to E$ vérifiant :

1. $(E, +)$ est un groupe commutatif ;
2. Pour tous $x, y \in E$ et pour tous $\lambda, \mu \in \mathbb{K}$
   (a) $(\lambda + \mu).x = \lambda.x + \mu.x$;
   (b) $\lambda.(x + y) = \lambda.x + \lambda.y$;
   (c) $\lambda.(\mu.x) = (\lambda\mu).x$;
   (d) $1.x = x$.

Les éléments de E sont appelés vecteurs, et les éléments de $\mathbb{K}$ sont appelés des scalaires.

Les $\mathbb{K}$-espaces vectoriels ont été étudiés en Géométrie 1. Tous les résultats, les méthodes, les outils importants des espaces vectoriels ont été traités dans ce cours.

Remarque 2 — *1. Pour $(E, +, .)$ un $\mathbb{K}$-ev, $(E, +)$ est un groupe commutatif.*

2. *Chez les espaces vectoriels, les notions importantes sont celles de dimension, de familles libres/génératrices/bases.*
3. *Chez les espaces vectoriels, les morphismes d'e.v. sont les applications linéaires.*
   Un morphisme d'ev est en particulier un morphisme de groupes (pour la loi additive $+$).
4. *Un $\mathbb{K}$-e.v. de dimension n est isomorphe à l'e.v. $\mathbb{K}^n$. (L'isomorphisme se construit avec le choix d'une base.)*
5. *On étudie beaucoup les morphismes d'e.v. en dimension finie afin de caractériser leur comportement sur tout l'e.v.*
6. *L'ensemble des applications linéaires de $\mathbb{K}^n$ vers $\mathbb{K}^m$ est un $\mathbb{K}$-ev isomorphe à $\mathscr{M}_{m,n}(\mathbb{K})$.*
7. *L'ensemble des endomorphismes sur $\mathbb{K}^n$ est un $\mathbb{K}$-ev et un anneau, qui est isomorphe (comme $\mathbb{K}$-ev et comme anneau) à $\mathscr{M}_n(\mathbb{K})$.*
   On ramène ainsi l'étude des endomorphismes avec les opérations $+, ., \circ$ à l'étude des matrices, pour les opérations $+, ., \times$.
   Cet ensemble est ce que l'on appelle une $\mathbb{K}$-algèbre. Nous l'étudierons par la suite.

Remarque 3 — *Pour un $\mathbb{K}$-e.v. E de dimension finie (par exemple $\mathbb{R}^n$), on peut chercher à étudier les sous-groupes de $(E, +)$.*
Cela donne entre autres la théorie des réseaux (étude de certains sous-groupes de $\mathbb{R}^n$ les uns par rapport aux autres).

Exemple 4 (Sous-groupes de $\mathbb{K}^n$) — *Soient $\mathbb{K}$ un corps et $n \geq 1$. Soit $(e_1, \ldots, e_n)$ une base de $\mathbb{K}^n$. Soient $G_1, \ldots, G_n$ des sous-groupes de $\mathbb{K}$.*
Alors, $G = e_1G_1 + \ldots + e_nG_n = \{\sum_{i=1}^n g_ie_i,\ g_i \in G_i\}$ est un sous-groupe de $(\mathbb{K}^n, +)$.

Chapitre 5 Structure algébrique : Corps

5.1 Définition et premières propriétés

Définition 1
Soit $(\mathbb{K}, +, \times)$ un anneau.
On dit que l'anneau $\mathbb{K}$ est un **corps** s'il est commutatif et si tout élément non nul est inversible pour $\times$.

Remarque 2 —

- *Si $(K, +, \times)$ est un corps, alors $K^\times = \mathbb{K}^* := K \setminus \{0\}$.*
- *Ainsi, $(K^*, \times)$ est un groupe abélien.*

Exemple 3 — $\mathbb{R}$,$\mathbb{C}$, *et* $\mathbb{Q}$ *sont des corps pour les lois* $+$ *et* $\times$ *habituelles.*
$\mathbb{Q}[\sqrt{2}]$ *et* $\mathbb{Q}[i]$ *sont aussi des corps.*

Proposition 4
Soit $\mathbb{K}$ un corps.
Alors $\mathbb{K}$ est un anneau intègre.

Preuve — Tout élément non nul est inversible, donc ce n'est pas un diviseur de 0. □

Proposition 5
Soit $\mathbb{K}$ un corps.
Alors $\mathbb{K}$ est un anneau principal. Ses seuls idéaux sont $\{0\}$ et $\mathbb{K}$.

Preuve — On sait que $\mathbb{K}$ est commutatif et intègre.
Comme tous les éléments non-nuls de $\mathbb{K}$ sont inversibles, on en déduit que les seuls idéaux de $\mathbb{K}$ sont $\{0\}$ et $\mathbb{K}$.
Donc, $\mathbb{K}$ est bien un anneau principal. □

Remarque 6 —

- *La réciproque est fausse : $\mathbb{Z}$ est un anneau intègre mais ce n'est pas un corps.*
- *Un anneau commutatif A est un corps si et seulement si ses idéaux sont exactement $\{0\}$ et A, les idéaux triviaux. (Le vérifier.)*
- *Un corps est donc un cas très particulier d'anneau commutatif, intègre, principal. Ces particularités peuvent être utilisées pour construire des structures très utiles ($\mathbb{K}$-espaces vectoriels, matrices, polynômes, $\mathbb{K}$-algèbres,...).*
  Un corps est un anneau, mais il est tellement important qu'on lui consacre un chapitre à part entière.

Dans le cas des anneaux finis, il est facile de caractériser les corps.

Proposition 7
Soit $\mathbb{K}$ un anneau commutatif, intègre, et fini.
Alors $\mathbb{K}$ est un corps.

Preuve — Soit $a \in \mathbb{K}$ non-nul. Comme $\mathbb{K}$ est intègre, la fonction $\varphi_a : a \in \mathbb{K} \mapsto ab \in \mathbb{K},\ b \mapsto ab$ est injective.
Comme $\mathbb{K}$ est fini, la fonction φ_A est alors bijective. Ainsi, il existe $b \in \mathbb{K}$ tel que $ab = 1_\mathbb{K}$.
Comme $\mathbb{K}$ est commutatif, on a $ba = ab = 1_\mathbb{K}$, donc a est inversible, ce qui conclut. De même, $\psi_a : c \mapsto ca$ est injective, donc bijective et il existe c tel que $ca = 1_A$.
On multiplie par b à droite, et on obtient $b = c$, donc a est bien inversible.

□

Théorème 8 (Théorème de Wedderburn (1905))
Soit A un anneau intègre fini.
Alors A est un corps.

Preuve — Même sans l'hypothèse de commutativité, on peut démontrer que pour tout $a \in A$ non-nul a est inversible à l'aide des idées de la preuve précédente.

Cependant, un corps doit être commutatif pour sa loi de multiplication.
La fin de la démonstration de ce théorème (prouver qu'un tel anneau A est commutatif) nécessite des outils supplémentaires, que nous n'avons pas. Des preuves plus élémentaires existent, mais celles-ci sont plutôt longues et ne sont pas intéressantes pour ce cours. Ce théorème est surtout présenté pour montrer ce qu'il se passe chez les anneaux finis. □

EXEMPLE 9 — *Pour p est nombre premier, $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps.*
En effet, c'est un anneau commutatif, intègre, et fini.

Ainsi, la liste des corps usuels en mathématiques est : $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$ pour p premier.
On peut construire beaucoup d'autres corps de plusieurs façons différentes (corps des fractions, extensions de corps), mais les corps les plus courants sont ceux-là.

5.2 Sous-corps

DÉFINITION 10
Soit $(\mathbb{K}, +, \times)$ un corps. Soit L une sous-partie de $\mathbb{K}$.
On dit que L est un **sous-corps** de $\mathbb{K}$ si :

- L est un sous-anneau de $\mathbb{K}$;
- $(L, +, \times)$ est un corps.

Autrement dit, L est un sous-corps de $\mathbb{K}$ si c'est un sous-anneau de $\mathbb{K}$ et si pour tout $x \in L$ non-nul on a $x^{-1} \in L$.

PROPOSITION 11
Soit $(\mathbb{K}, +, \times)$ un corps. Soit L une sous-partie de $\mathbb{K}$.
Alors L est un sous-corps de $\mathbb{K}$ si et seulement si :

- $0 \in L$ et $1 \in L$;
- Pour tous $x, y \in L$, $x - y \in L$;
- Pour tous $x, y \in L$, $xy^{-1} \in L$.

EXEMPLE 12 — *Pour $n \in \mathbb{N}^*$, $\mathbb{Q}[\sqrt{n}] = \{a + b\sqrt{n},\ a, b \in \mathbb{Q}\}$ est un sous-corps de $\mathbb{R}$.*

$\mathbb{R}$ et $\mathbb{C}$ possèdent ainsi une infinité de sous-corps.

Par contre, $\mathbb{Q}$ ne possède qu'un seul sous-corps : lui-même.
En effet un sous-corps L de $\mathbb{Q}$ contient 1. En tant que sous-anneau il contient donc tous les $n.1 = n$, pour $n \in \mathbb{Z}$. En tant que sous-corps il contient donc tous les $\frac{1}{m}$ pour m non-nul. Donc L contient tous les $\frac{n}{m}$, $m \neq 0$, d'où $L = \mathbb{Q}$.

REMARQUE 13 — *On peut encore montrer qu'une intersection quelconque de sous-corps est un sous-corps et donc parler de sous-corps engendré par une partie d'un corps, mais étudier de façon intéressante ces objets demande des outils plus poussés d'algèbre.*

Par contre, un produit de corps ne donne pas un corps car ce n'est pas un anneau intègre.

Les corps usuels $\mathbb{R}, \mathbb{C}, \mathbb{Q}, Z/p\mathbb{Z}$ sont des objets relativement élémentaires mais dont les propriétés permettent de construire beaucoup de nouveaux objets et outils (matrices, polynômes, analyse réelle, analyse complexe,...)

EXEMPLE 14 (Construction d'un corps à 4 éléments via ses lois) — *Soit $G = \{0, 1, \alpha, \beta\}$ un ensemble.*
On veut déterminer une loi $+$ et une loi $\times$ telles que $(G, +, \times)$ soit un corps d'élément neutre 0 et 1 pour respectivement l'addition et la multiplication.
On commence par la multiplication : $\alpha\beta$ ne peut être égal à 0 car un corps est intègre, ni à α car sinon $\beta = 1$, ni à β car sinon $\alpha = 1$. Ainsi α^2 n'est pas égal à 0, 1 et clairement $\alpha^2 \neq \alpha$. On en déduit que $\alpha^2 = \beta$. De même, $\beta^2 = \alpha$.

On en déduit le tableau

$\times$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

On détermine maintenant la loi $+$: si $\alpha+1=0$, alors $\beta(\alpha+1)=\alpha\beta+\beta=\beta+1=0$, et ainsi $\alpha=\beta$, ce qui est exclu. On en déduit que $\alpha+1=\beta$ et de même $\beta+1=\alpha$.
De plus, $\alpha(\alpha+1)=\begin{cases}\alpha^2+\alpha=\alpha+\beta\\ \alpha\beta=1\end{cases}$ Donc $\alpha+\beta=1=2\alpha+1$ et aussi $2\alpha=0$. de même $2\beta=0=2\alpha+2$, d'où $1+1=0$. Ce qui donne le tableau

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

Il reste à vérifier que les lois sont bien associatives et distributives, ce que nous laissons en exercice.

Remarque 15 (Culture générale sur les corps finis) —
Avec la théorie des corps, on peut montrer qu'un corps fini possède forcément p^r éléments avec p premier et $r\in\mathbb{N}^*$.
De plus, on peut construire explicitement un corps à p^r éléments pour chaque nombre premier p et pour tout entier $r\geq 1$. Ces corps sont appelés corps finis.
Les corps $\mathbb{Z}/p\mathbb{Z}$ sont les corps finis à p éléments.
De même, la théorie des corps montre que les corps finis sont uniques à isomorphisme d'anneau près.

5.3 Le corps des réels $\mathbb{R}$

Rappelons quelques propriétés du corps des réels $\mathbb{R}$.

Théorème 16
Il existe un unique ensemble noté $\mathbb{R}$, contenant $\mathbb{Q}$, muni de deux lois $+$ et $\times$ et d'une relation d'ordre totale $\leq$ tels que :

1. $(\mathbb{R},+,\times)$ est un corps ;
2. $\leq$ prolonge l'ordre sur $\mathbb{Q}$ défini par :
$$\forall \frac{p}{q},\frac{p'}{q'}\in\mathbb{Q},\ \frac{p}{q}\leq\frac{p'}{q'}\iff pq'\leq p'q.$$
3. $\forall a,b,c\in\mathbb{R}$, $a\leq b\Rightarrow a+c\leq b+c$. Si $c\geq 0$, alors $ac\leq bc$.
4. Toute partie non vide majorée possède une borne supérieure *(Propriété de la borne supérieure).*

Remarque 17 — *L'axiome 4 est fondamental.*

1. *Il n'est pas vérifié sur $\mathbb{Q}$ (penser à $[0;\sqrt{2}]\cap\mathbb{Q}$).*
2. *C'est aussi l'axiome qui permet de prouver que toute suite réelle croissante majorée est convergente et converge vers sa borne supérieure.*
3. *On a aussi par symétrie que toute partie minorée non vide admet une borne inférieure.*

5.4 Corps et morphismes d'anneaux, Caractéristique d'un corps

Regardons comment les corps se comportent vis-à-vis des morphismes d'anneaux.

Proposition 18
Soient A un anneau et $\mathbb{K}$ un corps. Soit $f : \mathbb{K} \to A$ un morphisme d'anneaux.
Alors f est injectif.

Preuve — On a vu dans le cours que $Ker(f)$ est un idéal, car $Ker(f) = f^{-1}(\{0\})$.
Les seuls idéaux de $\mathbb{K}$ sont $\{0\}$ et $\mathbb{K}$. Comme on doit avoir $f(1) = 1$, on a ainsi $Ker(f) = \{0\}$. □

Proposition 19
Soient A un anneau et $\mathbb{K}$ un corps. Soit $g : A \to \mathbb{K}$ un morphisme d'anneaux.
Alors l'idéal $Ker(g)$ est premier : Pour tout $x \in Ker(g)$ avec $x = yz$, on a alors $y \in Ker(g)$ ou $z \in Ker(g)$.

Preuve — Si $x = yz$ on a alors $0 = g(x) = g(yz) = g(y)g(z)$.
Mais comme $\mathbb{K}$ est un corps, $\mathbb{K}$ est un anneau intègre, donc on a forcément $g(y) = 0$ ou $g(z) = 0$, d'où $y \in Ker(g)$ ou $z \in Ker(g)$. □

Corollaire 20
Soient $\mathbb{K}, L$ deux corps et $f : \mathbb{K} \to L$ un morphisme de corps.
Alors, f est injectif.
De plus, $\mathbb{K}$ est isomorphe à $f(\mathbb{K})$, donc le corps $\mathbb{K}$ s'identifie à un sous-corps de L.

Proposition-Définition 21
Soit $\mathbb{K}$ un corps. Soit $f : n \in \mathbb{Z} \mapsto n.1_K \in \mathbb{K}$.
Alors f est un morphisme d'anneaux.
On a $Ker(f) = \{0\}$ ou $Ker(f) = p\mathbb{Z}$ pour un nombre premier p.
On définit ainsi la caractéristique du corps $\mathbb{K}$ comme l'entier m tel que $Ker(f) = m\mathbb{Z}$.

Preuve — On a déjà montré que cette fonction est un morphisme d'anneaux.
On sait que $Ker(f)$ est un idéal de $\mathbb{Z}$, donc $Ker(f) = m\mathbb{Z}$ pour un certain $m \geq 0$.
Si $Ker(f) = \{0\}$, c'est bon. Sinon, on suppose que $m \geq 1$.
On ne peut pas avoir $m = 1$ car $Ker(f) \neq \mathbb{Z}$, donc on a $m \geq 2$. D'après la proposition précédente, l'idéal $Ker(f)$ est premier.
On montre alors que l'entier m est premier.
En effet, pour $m = ab$ on a $a \times b \in m\mathbb{Z} = Ker(f)$. D'après la proposition précédente on a donc $a \in m\mathbb{Z}$ ou $b \in m\mathbb{Z}$, c'est-à-dire $m \mid a$ ou $m \mid b$. On a donc $|a| = m$ ou $|b| = m$. Ainsi, les seuls diviseurs positifs de m sont m et 1, donc m est bien un nombre premier.
Cela termina la preuve. □

Exemple 22 —

- *Les corps $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}[i], \mathbb{Q}[\sqrt{2}]$ sont des corps de caractéristique 0 (caractéristique nulle).*
  Dans un corps de caractéristique nulle, on peut aujouter autant de fois un nombre x à lui-même, le résultat ne sera jamais nul. (si $x \neq 0$ et $n \geq 1$, alors $x + \ldots + x = n.x \neq 0$.)
- *Le corps $\mathbb{Z}/p\mathbb{Z}$ est un corps de caractéristique p.*

Remarque 23 —
• *En caractéristique nulle, on peut multiplier ou diviser une quantité par n'importe quel nombre entier n non-nul sans aucun problème.*
• *Dans un corps de caractéristique p, si on ajoute un nombre x p fois, on obtient 0 : $x + \ldots + x$ (p fois) $= p.x = 0$. Donc "multiplier par p" revient à multiplier par 0.*
• *De même, le nombre $p = p.1_{\mathbb{K}}$ est nul. On ne peut donc pas "diviser par p" dans un corps de caractéristique p. Cette différence de comportement entre ces corps est très importante lorsque l'on veut les étudier plus profondément.*
• *Par exemple, en caractéristique nulle le polynôme $X^2 - X - 2$ est à racines simples, tandis qu'en caractéristique 3 il possède une racine double ($X^2 - X - 2 = (X + 1)(X - 2) = (X + 1)^2$)*
Le polynôme $P(X) = X^7 - 7X + 2$ est premier avec son polynôme dérivé, sauf en caractéristique 7 où on a $P'(X) = 7X^6 - 7 = 0$.
• *La matrice $\begin{pmatrix} 2 & 3 \\ 0 & 5 \end{pmatrix}$ est inversible, sauf en caractéristique 2 ou 5.*
• *Quand on travaille avec des objets sur un corps $\mathbb{K}$ quelconque, et que l'on a des multiples du nombre $1_{\mathbb{K}}$, il y aura au moins une caractéristique p pour laquelle l'un de ces multiples sera nul, et il faudra éventuellement traiter ce cas à part.*

5.5 Corps des fractions d'un anneau commutatif intègre

Soit A un anneau intègre et commutatif.
Dans A, parmi les éléments a non-nuls on a des éléments inversibles, qui possèdent un inverse a^{-1} (c'est-à-dire comme $\frac{1}{a}$), et des éléments non-inversibles, pour lesquels la notion d'inverse n'a pas de sens.
Dans l'anneau $\mathbb{Z}$, les seuls éléments inversibles sont 1 et -1. Pour les autres entiers n, la notion d'inverse $\frac{1}{n}$ n'a pas de sens dans $\mathbb{Z}$.
Pourtant, on connaît l'ensemble des rationnels $\mathbb{Q}$, anneau lui aussi, dans lequel tout entier naturel n possède un inverse $\frac{1}{n}$. Si l'on regarde $\mathbb{Z}$ comme sous-anneau du corps $\mathbb{Q}$, alors la notion d'inverse d'un entier naturel n a toujours un sens (mais un sens dans $\mathbb{Q}$).
Le corps des fractions est une construction qui généralise ce contexte.

Proposition-Définition 24
Soit A un anneau commutatif et intègre.
Sur l'ensemble $A \times A^*$, on définit la relation suivante :

$$(a,b)\mathcal{R}(c,d) \text{ si } ad = bc.$$

1. La relation $\mathcal{R}$ est une relation d'équivalence sur $A \times A^*$.
   On note $\frac{a}{b}$ la classe d'équivalence de l'élément (a,b).
2. On a alors $\frac{a}{b} = \frac{c}{d}$ si et seulement si $ad = bc$.

On note $Frac(A)$ l'ensemble des classes d'équivalences de la relation $\mathcal{R}$.
Cet ensemble est appelé **corps des fractions** de l'anneau A.

Preuve —

1. On vérifie facilement que $\mathcal{R}$ est une relation d'équivalence (réflexive, symétrique, transitive).

□

Proposition-Définition 25
Soit A un anneau commutatif et intègre.
On pose sur $Frac(A)$ les opérations :

$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd},$$
$$\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}.$$

1. Les opérations $+$ et $\times$ sont bien définies sur $Frac(A)$. Elles ne dépendent pas des représentants (a,b) et (c,d) choisis pour les classes d'équivalence.
2. L'ensemble $(Frac(A), +, \times)$ est un anneau commutatif. Son élément nul est $\frac{0}{1}$ et son élément unitaire est $\frac{1}{1}$.
3. L'anneau $(Frac(A), +, \times)$ est un corps.
   Pour tout élément $\frac{a}{b} \in Frac(A)$ non-nul, cet élément est inversible, d'inverse $(\frac{a}{b})^{-1} = \frac{b}{a}$.
4. L'anneau A est isomorphe au sous-anneau $\{\frac{a}{1},\ a \in A\}$ de $Frac(A)$.
   On peut ainsi identifier A à un sous-anneau du corps $Frac(A)$.

Preuve —

1. Pour montrer que ces opérations sont bien définies, il faut montrer que si $\frac{a}{b} = \frac{a'}{b'}$ et si $\frac{c}{d} = \frac{c'}{d'}$, on a $\frac{ac}{bd} = \frac{a'c'}{b'd'}$ et $\frac{ad+cb}{bd} = \frac{a'd'+c'b'}{b'd'}$.
   Comme on a $ab' = a'b$ et $cd' = c'd$, avec $b, b', d, d' \neq 0$, la preuve est facile.
2. Il faut montrer que $(Frac(A), +, \times)$ vérifie tous les axiomes d'un anneau. Cela est assez facile.
   De même, il est facile de montrer que $Frac(A)$ est un anneau commutatif.
3. Dans $Frac(A)$, on a $\frac{a}{b} = \frac{0}{1}$ si et seument si $a = 0$.
   Ainsi, si $\frac{a}{b} \neq \frac{0}{1}$, on a $a \neq 0$, donc $\frac{b}{a}$ est bien défini, et on a

   $$\frac{a}{b}\frac{b}{a} = \frac{ba}{ba} = \frac{1}{1}.$$

   Cela montre que $Frac(A)$ est un corps.
4. On pose $f : a \mapsto \frac{a}{1}$.
   On vérifie alors que f est un morphisme d'anneaux ($f(a+b) = f(a) + f(b)$, $f(ab) = f(a)f(b)$, $f(1) = \frac{1}{1}$).
   De plus, on remarque que f es injectif : $Ker(f) = \{0\}$.
   Donc, l'anneau A est isomorphe à $f(A)$, sous-anneau de $Frac(A)$.

□

PROPOSITION 26
Soit A un anneau commutatif et intègre.
• Alors il existe un corps $\mathbb{K}$ tel que $A \subset \mathbb{K}$.
• Tout anneau commutatif et intègre peut être vu comme le sous-anneau d'un certain corps.
• Dans le corps $\mathbb{K}$, le sous-corps engendré par A est isomorphe à $Frac(A)$, le corps des fractions de A.

Preuve — • On prend $\mathbb{K} = Frac(A)$ pour l'existence d'un corps contenant A.
• Pour $\mathbb{K}$ un corps contenant A, on montre que le sous-corps engendré par A est exactement l'ensemble $L = \{ab^{-1},\ a \in A, b \in A^*\}$.
On peut alors définir une fonction $f : L \to Frac(A)$ avec $f(ab^{-1}) = \frac{a}{b}$.
On montre que la fonction f est bien définie en montrant que si $ab^{-1} = cd^{-1}$, alors $\frac{a}{b} = \frac{c}{d}$.
On montre alors facilement que f est un morphisme d'anneaux, qui est surjectif, et qui est injectif ($Ker(f) = \{0\}$).
Ainsi, ces deux corps sont isomorphes. □

EXEMPLE 27 —

- $\mathbb{Q}$ *est le corps des fractions de* $\mathbb{Z}$ *:* $Frac(\mathbb{Z}) = \mathbb{Q}$.
- *L'anneau des fractions rationnelles sur* $\mathbb{K}$ *est le corps des fractions de* $\mathbb{K}[X]$.
- *Le corps des fractions de* $\mathbb{Z}[i] = \{a + ib,\ a, b \in \mathbb{Z}\}$ *est* $\mathbb{Q}[i]$.

Chapitre 6 Structure algébrique : Algèbres

Nous abordons la dernière structure algébrique du chapitre. Après avoir vu groupes, anneaux, corps, et espaces vectoriels, regardons des ensembles qui possèdent à la fois une structure d'anneau et à la fois une structure de $\mathbb{K}$-espace vectoriel.

6.1 Structure de $\mathbb{K}$-algèbre, Sous-algèbres

Définition 1
Soit $\mathbb{K}$ un corps.
Une $\mathbb{K}$-algèbre est un quadruplet $(A, +, \times, .)$ tel que

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

De plus, si la loi $\times$ est commutative, on dit que l'algèbre est commutative.

Donnons maintenant les exemples fondamentaux qui motivent l'étude des $\mathbb{K}$-algèbres.

Exemple 2 — *Soit $\mathbb{K}$ un corps.*

1. *L'ensemble $(\mathbb{K}[X], +, \times, .)$ (polynômes à coefficients dans $\mathbb{K}$) est une $\mathbb{K}$-algèbre commutative.*
2. *L'ensemble $(\mathcal{M}_n(\mathbb{K}), +, \times, .)$ (matrices carrées) est une $\mathbb{K}$-algèbre.*
   Elle est non commutative si $n \geq 2$.
   De même $(\mathcal{L}(E), +, \circ, .)$ (endomorphismes sur E) est une $\mathbb{K}$-algèbre.
3. *$(\mathcal{F}(X, \mathbb{K}), +, \times, .)$ (fonctions de X dans $\mathbb{K}$) est une $\mathbb{K}$-algèbre.*
4. *$\mathbb{C}$ est une $\mathbb{R}$-algèbre et une $\mathbb{Q}$-algèbre.*
5. *$\mathbb{R}$ est une $\mathbb{Q}$-algèbre.*
6. *$\mathbb{Q}[\sqrt{2}]$ est une $\mathbb{Q}$-algèbre.*

Définition 3
Soit $(A, +, \times, .)$ une $\mathbb{K}$-algèbre.
Une **sous-algèbre** B est une partie $B \subset A$ telle que

1. $(B, +, \times)$ est un sous-anneau de $(A, +, \times)$;
2. $(B, +, .)$ est un sous-espace vectoriel de $(A, +, .)$.

Proposition 4
Si B est une sous-algèbre de $(A, +, \times, .)$, alors $(B, +, \times, .)$ est une algèbre.

Preuve — Par définition, il suffit de vérifier $\forall \lambda \in \mathbb{K}$, $\forall x, y \in B$, $(\lambda.x)y = \lambda.(xy) = x(\lambda.y)$, ce qui est vérifié sur A donc sur B.

□

Remarque 5 — *Le produit d'algèbres est une algèbre.*
Une intersection de sous-algèbres est une algèbre.
On peut définir la sous-algèbre engendrée par une partie S, et étudier ses différentes expressions.
Le plus souvent, pour montrer qu'un ensemble A est une algèbre, on montrera que c'est une sous-algèbre d'une algèbre connue. (polynômes, matrices, fonctions, ...)

Proposition-Définition 6
Soient $\mathbb{K}$ un corps, A une $\mathbb{K}$-algèbre, et $a \in A$.
On définit $\mathbb{K}[a] := Vect(a^k, k \geq 0)$.
L'ensemble $\mathbb{K}[a]$ est une sous-algèbre de A, qui est commutative.
C'est la sous-algèbre engendrée par a.

Preuve — On vérifie que $\mathbb{K}[a]$ est stable par addition, multiplication par un scalaire, par multiplication, et que l'ensemble contient 1_A.
Tous les éléments de $\mathbb{K}[a]$ s'écrivent comme des polynômes en a, ce qui permet de montrer facilement qu'ils commutent. □

6.2 Morphismes de $\mathbb{K}$-algèbres

Comme pour les autres objets, une fois leurs propriétés établies, on s'intéresse aux fonctions qui préservent la structure choisie.

Définition 7
Soit $(A, +, \times, .)$ et $(B, +, \times, .)$ deux $\mathbb{K}$-algèbres.
Un **morphisme d'algèbres** $\varphi : A \to B$ est une application vérifiant

1. $\varphi(1_A) = 1_B$;
2. $\forall x, y \in A$, $\varphi(xy) = \varphi(x)\varphi(y)$
3. $\forall x, y \in A$, $\forall \lambda, \mu \in \mathbb{K}$, $\varphi(\lambda x + \mu y) = \lambda\varphi(x) + \mu\varphi(y)$.

Exemple 8 —
- *La conjugaison complexe $z \mapsto \bar{z}$ est un morphisme de $\mathbb{R}$-algèbres.*
- *Sur $\mathbb{K}[X]$, $f : P \mapsto P \circ Q$ est un morphisme de $\mathbb{K}$-algèbres.*
- *Sur $\mathscr{M}_n(\mathbb{K})$, pour M inversible, $f : A \mapsto M^{-1}AM$ est un morphisme de $\mathbb{K}$-algèbres.*
- *Pour $a \in \mathbb{K}$, $f : P \in \mathbb{K}[X] \mapsto P(a) \in \mathbb{K}$ est un morphisme de $\mathbb{K}$-algèbres.*
- *Pour $x \in E$ et A une $\mathbb{K}$-algèbre, $\phi : g \in F(E, A) \mapsto g(x) \in A$ est un morphisme de $\mathbb{K}$-algèbres.*
  On l'appelle le morphisme d'évaluation en x.
- *Pour B une base de $\mathbb{K}^n$, la fonction $f \in \mathcal{L}(\mathbb{K}^n) \mapsto Mat_B(f) \in \mathscr{M}_n(\mathbb{K})$ est un morphisme de $\mathbb{K}$-algèbres.*
- *Sur $\mathbb{Q}[\sqrt{2}]$, $f : a + \sqrt{2}b \mapsto a - \sqrt{2}b$ est un morphisme de $\mathbb{K}$-algèbres.*
- *$f : P \in \mathbb{K}[X] \mapsto (x \mapsto P(x)) \in F(\mathbb{K}, \mathbb{K})$ est un morphisme de $\mathbb{K}$-algèbres.*
  Il est injectif si $\mathbb{K}$ est infini, et surjectif si $\mathbb{K}$ est fini. (Le vérifier.)

Proposition 9
Soient $\mathbb{K}$ un corps, A, B des $\mathbb{K}$-algèbres, et $f : A \to B$ un morphisme de $\mathbb{K}$-algèbres.
Soient $a \in A$ et $P(X) = a_nX^n + \ldots + a_0 \in \mathbb{K}[X]$.
• Alors, on a $f(P(a)) = P(f(a))$.
• Si $P(a) = 0$ alors on a $P(f(a)) = 0$.

Preuve — On a

$$f(P(a)) = f(\sum_{k=0}^{n} a_k a^k) = \sum_{k=0}^{n} f(a_k a^k) \sum_{k=0}^{n} a_k f(a^k) = \sum_{k=0}^{n} a_k f(a)^k) = P(f(a)).$$

Le second point découle du premier. □

Remarque 10 —
• *Ce résultat permet de déterminer l'existence ou non de morphismes de $\mathbb{K}$-algèbres entre deux algèbres A et B.*
• *Par exemple, dans la $\mathbb{R}$-algèbre $\mathbb{C}$, on a i qui est racine de $X^2 + 1$.*
Ainsi, un morphisme de $\mathbb{R}$-algèbres sur $\mathbb{C}$ doit envoyer 1 sur 1 et i sur $\pm i$. On a ainsi deux choix possibles de morphismes ($Id_{\mathbb{C}}$ et $z \mapsto \bar{z}$).
• *La $\mathbb{K}$-algèbre $\mathbb{K}[X]$ est engendrée par l'élément X en tant que $\mathbb{K}$-algèbre. (tous les polynômes sont des combinaisons linéaires de puissances de X) Ainsi, un morphisme d'algèbres $f : \mathbb{K}[X] \to B$ est entièrement déterminé par le choix de $f(X)$.*
Cela permet de montrer qu'un morphisme d'algèbres $f : \mathbb{K}[X] \to \mathbb{K}[X]$ est forcément de la forme $P \mapsto P \circ Q$. (Prendre $Q = f(X)$.)

Proposition-Définition 11 (Algèbre quotient)
Soit $\mathbb{K}$ un corps. Soit $P \in \mathbb{K}[X]$ un polynôme non nul de degré $n \geq 1$.
• On définit la relation de congruence modulo P, $A \equiv B \bmod (P)$, par $A - B \in P\mathbb{K}[X]$.
Alors, cette relation est une relation d'équivalence sur $\mathbb{K}[X]$.
• Les classes d'équivalence pour cette relation sont les $\overline{A} = A + P\mathbb{K}[X]$.
On peut remarquer que chaque classe d'équivalence contient un unique polynôme R de degré strictement inférieur à n. C'est le reste de la division euclidienne de A par P.

On note E l'ensemble des classes d'équivalence pour cette relation de congruence.
• On définit alors trois opérations sur E (deux opérations internes, une opération externe) ;

$$\overline{A}+\overline{B}=\overline{A+B},\ \overline{A}\times\overline{B}=\overline{AB} \text{ et } \lambda.\overline{A}=\overline{\lambda A}.$$

Alors, ces opérations sont bien définies, et $(E,+,\times,.)$ est une $\mathbb{K}$-algèbre.
On l'appelle l'algèbre quotient de $\mathbb{K}[X]$ par l'idéal $P\mathbb{K}[X]$.
• La fonction $\varphi : A\in\mathbb{K}[X]\mapsto\overline{A}\in E$, est un morphisme de $\mathbb{K}$-algèbres, et son noyau est $\ker\varphi=P\mathbb{K}[X]$.
• En tant qu'espace vectoriel, E est un $\mathbb{K}$-ev de dimension n, dont une base est $(\overline{1},\cdots,\overline{X^{n-1}})$.
• Dans la $\mathbb{K}$-algèbre E, l'élément $\overline{X}$ est annulé par le polynôme P : On a $P(\overline{X})=\overline{P(X)}=\overline{0}$.

Exemple 12 — • *On prend* $\mathbb{K}=\mathbb{R}$ *et* $P(X)=X^2+1$. *Décrire la* $\mathbb{K}$*-algèbre obtenue en quotientant* $\mathbb{R}[X]$ *par* $(X^2+1)\mathbb{R}[X]$.

- *On prend* $\mathbb{K}=Q$ *et* $P(X)=X^2+2$. *Décrire la* $\mathbb{K}$*-algèbre obtenue avec ce quotient. Quel anneau retrouve-t-on ?*
- *On prend* $\mathbb{K}=\mathbb{Z}/2\mathbb{Z}$ *et* $P(X)=X^2+X+1$. *Décrire la* $\mathbb{K}$*-algèbre obtenue avec ce quotient. Quel est son cardinal ? Montrer que* E *est un corps.*
- *On prend* $\mathbb{K}=\mathbb{Z}/3\mathbb{Z}$ *et* $P(X)=X^2+1$. *Décrire la* $\mathbb{K}$*-algèbre obtenue avec ce quotient. Quel est son cardinal ? Montrer que* E *est un corps.*

Cette construction est un outil très utile en théorie des anneaux et en théorie des corps. Ce cours est déjà trop long pour en parler plus en détail.
Construire des anneaux quotients/des algèbres quotients en utilisant une relation de congruence est très utile en mathématique pour produire des anneaux et des algèbres qui ont des comportements éventuellement nouveaux et différents.
Pour tout polynôme $P\in\mathbb{K}[X]$ irréductible, cela permet par exemple de construire une $\mathbb{K}$-algèbre A dans laquelle le polynôme P possède une racine.
En théorie des corps, on construit des corps de cardinal p^r, pour $r\geq 1$, avec cette technique.