Sorbonne Université

LU2MA205
Fondements d'Analyse et d'Algèbre

Graham Foote
grahamwfoote@gmail.com

Esteban Wahler
esteban.wahler@gmail.com

Marco Maculan

Leonardo Zapponi

Promotion 2023-2024

Motivation

Ce document a pour but de laisser une trace écrite du cours de l'UE LU2MA205 de la Licence intensive de Mathématiques de Sorbonne Université, prodigué au premier semestre de L2 (S3). Ce papier était à l'origine principalement destiné aux étudiants de ce parcours, et rédigé pour que l'ensemble de ceux-là aient une référence sous forme écrite pour travailler cette UE, mais nous avons aussi pensé ensuite en faire profiter aux futures générations de Maths intensives. Ce cours a été rédigé sur la base de références bibliographiques d'Algèbre, tels que des cours et des livres, et de recherches internet.

Note au lecteur

L'ordre des notions abordées dans ce polycopié ne suit pas la progression chronologique du cours prodigué par nos deux professeurs. Nous avons en effet fait le choix d'un ordre qui nous a semblé naturel et cohérent à notre échelle et selon notre vision des choses à ce moment-là. De plus, il y a plusieurs approfondissements importants, comme les deux derniers théorèmes d'isomorphismes, le théorème de factorisation ou encore des notions et résultats de théorie des groupes par exemple, mais aussi des détails de rédaction ajoutés aux démonstrations faites en cours. Tout ici n'est donc pas exigible au partiel de fin octobre.

Introduction

Dans ce cours, nous allons construire les ensembles $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ de manière naturelle. Pour ce faire, nous aurons besoin de notions d'algèbre générale que sont les structures algébriques. Dans un premier temps, nous ferons des rappels et approfondissements sur les relations binaires. Ensuite, nous reverrons les principales structures algébriques et récapitulerons les plus importants résultats à leurs propos tout en insistant sur les applications entre structures par des approfondissements détaillés. Cela nous munira en passant d'un socle assez solide pour envisager la construction des ensembles usuels jusqu'à $\mathbb{C}$. Ensuite, nous nous attaquerons à des problèmes de cardinalité, puis nous approfondirons ce que l'on appelle l'algèbre commutative et enfin nous irons sur le terrain des polynômes en parlant des nombres algébriques et polynômes minimaux par exemple.

Remerciements

Nous voulons à présent remercier nos deux professeurs Marco Maculan et Leonardo Zapponi qui nous ont accompagnés dans cette incursion mathématique alors que nous étions que des mathématiciens débutants. Plus généralement, merci à la promotion 2023-2024 pour les commentaires et les retours. Bonne lecture !

Table des matières

1 Algèbre générale

1.1 Relations binaires

Définition. Soit E un ensemble. Une *relation binaire* sur E est une partie R de $E \times E$. Lorsque $(x, y) \in R$ on dit que x et y sont en relation par R et on écrit xRy.

Définition. Une relation binaire R sur E est

- *réflexive* : pour tout $x \in E,\ xRx$
- *symétrique* : pour tous $(x, y) \in E^2,\ xRy \implies yRx$
- *antisymétrique* : pour tous $(x, y) \in E^2,\ (xRy \text{ et } yRx) \implies x = y$
- *transitive* : pour tous $(x, y, z) \in E^3,\ (xRy \text{ et } yRz) \implies xRz$.

Définition. Une relation binaire R sur E est une *relation d'équivalence* si elle est réflexive, symétrique et transitive.

Exemple. La relation $xRy \iff 2 \mid x - y$ sur $\mathbb{Z}$ est une relation d'équivalence.

Définition. Une relation binaire R sur E est une *relation d'ordre* si elle est réflexive, antisymétrique et transitive. C'est une relation d'ordre *total* si l'on peut comparer n'importe quels éléments de E, *i.e.* $\forall (x, y) \in E^2,\ xRy$ ou yRx. C'est une relation d'ordre *partiel* sinon.

Exemple. La relation $\leqslant$ sur $\mathbb{N}$ est une relation d'ordre (mais pas sur $\mathbb{Z}$).

Définition. Un ensemble *partiellement ordonné* est un ensemble muni d'une relation d'ordre partiel. Un ensemble *totalement ordonné* est un ensemble muni d'une relation d'ordre total.

Définition. Soit R une relation d'équivalence sur un ensemble E.
Pour tout $x \in E$, la *classe d'équivalence* de x est l'ensemble $[x] := \{y \in E,\ yRx\}$.
L'ensemble de toutes les classes d'équivalence est l'ensemble *quotient* de E par R et est noté E/R. On a $E/R \subseteq P(E)$.

Exemple. Si $(x, y)R(x', y') \iff x = x'$ sur $\mathbb{R}^2$, la classe du vecteur (x, y) est l'ensemble des vecteurs (x', y') qui ont la même première coordonnée que lui et l'ensemble quotient est donc l'ensemble des droites verticales de $\mathbb{R}^2$.

Définition. La *projection canonique* associée à une relation R sur E est l'application

$$\begin{aligned} \pi \ : \ E &\longrightarrow E/R \\ x &\longmapsto [x]. \end{aligned}$$

Elle est surjective par construction.

Théorème. Si R est une relation d'équivalence sur E, alors E/R est une partition de E. Réciproquement, pour toute partition $(A_i)_{i\in I}$ de E il existe une unique relation d'équivalence R telle que $E/R = \{A_i : i \in I\}$.

Démonstration. Pour le sens direct : d'une part, montrons qu'une classe d'équivalence est non vide. En effet, nous considérons une relation d'équivalence R, qui est donc réflexive et on a xRx, d'où $x \in \overline{x}$ pour tout $x \in E$ donc toute classe d'équivalence est non vide. De plus, si pour tout $x \in E$, on a $x \in \overline{x}$ alors la réunion des classes d'équivalence est E tout entier puisque chaque élément x est au moins dans sa propre classe d'équivalence. Enfin, considérons $\overline{x}$ et $\overline{y}$ deux classes d'équivalence. On suppose que $\overline{x} \cap \overline{y} \neq \varnothing$, il existe donc $z \in \overline{x} \cap \overline{y}$ qui vérifie xRz et yRz. Par symétrie on a aussi xRz et zRy et par transitivité on en déduit xRy donc x et y sont en relation d'où $\overline{x} = \overline{y}$. Par contraposée, on a donc $\overline{x} \neq \overline{y} \Longrightarrow \overline{x} \cap \overline{y} = \varnothing$.
Pour la réciproque, on considère la relation R telle que

$$\forall (x, y) \in E^2, \quad xRy \iff \exists i \in I, x \in A_i \text{ et } y \in A_i.$$

Montrons que c'est une relation d'équivalence.
Dans un premier temps, R est réflexive car $xRx \iff x \in A_i$ et $x \in A_i$. De plus, R est symétrique car $x \in A_i$ et $y \in A_i$ est équivalent à $y \in A_i$ et $x \in A_i$. Enfin, R est transitive car si xRy et yRz alors x et z sont tous deux dans A_i donc xRz.

□

1.2 Structures algébriques

1.2.1 Généralités

Définition. On appelle *loi de composition interne* une application $* : E \times E \longrightarrow E$.

— Une loi de composition interne $*$ sur E est dite *associative* si

$$\forall (x, y, z) \in E^3, \quad (x * y) * z = x * (y * z).$$

— Une loi de composition interne $*$ sur E est dite *commutative* si

$$\forall (x, y) \in E^2, \quad x * y = y * x.$$

— Une loi de composition interne $*$ sur E est dite *distributive* par rapport à $\overline{*} : E \times E \longrightarrow E$ si

$$\forall (x, y, z) \in E^3, \quad x * (y \overline{*} z) \; = \; x * y \overline{*} x * z$$

$$\text{et} \quad (y \overline{*} z) * x \; = \; y * x \overline{*} z * x.$$

En effet, on ne suppose pas la loi $*$ commutative ici, mais elle l'est la plupart du temps.

— On dit que $e \in E$ est un *élément neutre* pour $*$ si

$$\forall x \in E, \quad x * e = e * x = x.$$

— Soit $e \in E$ un élément neutre de E pour $*$. On appelle *symétrique* de $x \in E$ un élément $x' \in E$ tel que

$$x * x' = x' * x = e.$$

Pour la loi additive notée $+$, le symétrique est appelé *opposé* et sera noté $-x$.
Pour la loi multiplicative notée $\times$, le symétrique est appelé *inverse* et sera noté x^{-1}.

Définition. Un *magma* $(M, *)$ est un couple composé d'un ensemble M et d'une loi de composition interne $*$ sur M. C'est la structure algébrique la plus simple, *i.e.* celle nécessitant le moins d'hypothèses.

Définition. Un *monoïde* $(E, *, e)$ est un magma associatif et unifère, *i.e.* tel que la loi $*$ est associative et possédant un élément neutre e.

Proposition. L'élément neutre d'une structure algébrique est unique.

Démonstration. Si $e, e' \in M$ sont deux éléments neutres pour $* : e = e * e' = e'$, donc $e = e'$.

□

Proposition. Propriétés diverses de l'inverse.
Soient $(M, *, e)$ un monoïde avec e l'élément neutre associé et $x, y, z \in M$.

1. *Unicité de l'inverse* : Si x est inversible, alors x possède un unique inverse.
2. *Simplification par un élément inversible* :
   — Si $x * y = x * z$ et si x est inversible : $y = z$
   — Si $y * x = z * x$ et si x est inversible : $y = z$
3. *Inversibilité d'un produit* : Si x et y sont inversibles, $x * y$ l'est aussi et : $(x * y)^{-1} = y^{-1} * x^{-1}$
4. *Puissances négatives* : Pour tout $n \in \mathbb{N}$, si x est inversible, alors x^n l'est aussi et : $(x^n)^{-1} = (x^{-1})^n$. Cet élément est noté x^{-n}. La notation x^k a donc un sens pour tout $k \in \mathbb{Z}$.
5. *Inversibilité de l'inverse* : Si x est inversible, alors x^{-1} l'est aussi et : $(x^{-1})^{-1} = x$.

Démonstration.

1. Si on suppose qu'un élément x admet deux inverses x' et x'', alors on a $x' = x' * e = x' * (x * x'') = (x' * x) * x'' = e * x'' = x''$.
2. Si $x * y = x * z$ avec x inversible, $y = 1 * e = (x^{-1} * x) * y = x^{-1} * (x * y) = x^{-1} * (x * z) = (x^{-1} * x) * z = e * z = z$. On fait le même raisonnement pour l'autre identité.
3. Effectuons le calcul : $(x * y) * (y^{-1} * x^{-1}) = x * (y * y^{-1}) * x^{-1} = x * e * x^{-1} = e * x * x^{-1} = e * e = e$. Cet énoncé s'effondre si l'on n'a pas l'hypothèse de commutativité !
4. On démontre cette propriété par récurrence sur $k \in \mathbb{N}$ à partir de l'identité précédente.
5. On a tout simplement $x^{-1} * x = x * x^{-1} = e$, d'où par définition de l'inversibilité, x est l'inverse de x^{-1}.

□

1.2.2 Théorie des groupes

Définition. Un *groupe* $(G, *)$ est un couple composé d'un ensemble G et d'une loi de composition interne $*$ associative sur G, pour laquelle il existe un élément neutre e_G et pour laquelle tout élément $x \in G$ possède un symétrique $x^{-1} \in G$.
Un *groupe abélien* est un groupe dont la loi de composition interne est également commutative.
Un groupe $(G, +)$ est un *groupe additif* et un groupe $(G^*, \times)$ est un *groupe multiplicatif*.

Exemples. L'ensemble $\mathbb{Z}$ muni de l'addition est un groupe, noté $(\mathbb{Z}, +)$. En effet, la loi $+$ est associative, possède l'élément neutre $e = 0$ et tout nombre entier dans $\mathbb{Z}$ possède un symétrique (ici opposé) dans $\mathbb{Z}$.
De même, $(\mathbb{R}^*, \times)$ est un groupe car la loi $\times$ est associative, possède l'élément neutre $e = 1$ et tout nombre réel dans $\mathbb{R}^*$ possède un symétrique (ici inverse) dans $\mathbb{R}^*$.

Définition. Un *sous-groupe* $(H, *)$ de $(G, *)$ est une partie de G telle que
- H contient l'élément neutre e_G
- $\forall (x, y) \in H^2,\ x * y \in H$
- le symétrique selon la loi $*$ de tout élément de H est dans H.

Autrement dit, H contient e_G et est stable par $*$ et par passage au symétrique : $xy^{-1} \in H$.

Exemples. $(\mathbb{R}_+^*, \times)$ est un sous-groupe de $(\mathbb{R}^*, \times)$ car $e = 1 \in \mathbb{R}_+^*$, pour $x, y \in \mathbb{R}_+^*,\ z = x \times y \in \mathbb{R}_+^*$ et pour tout $x \in \mathbb{R}_+^*,\ x^{-1} \in \mathbb{R}_+^*$.
De même, l'ensemble des nombres pairs dans $\mathbb{Z}$, que l'on note ici P, muni de l'addition est un sous-groupe de $(\mathbb{Z}, +)$ puisque $0 \in P$, P est stable par produit et l'opposé d'un nombre pair est pair.

Définition. Soit G un groupe. On dit qu'un sous-groupe H de G est *distingué* (ou *normal*) si pour tout $g \in G,\ gH = Hg$. Autrement dit, H est un sous-groupe normal de G si $\forall h \in H, \forall g \in G, ghg^{-1} \in H$. Dans ce cas, on note $H \lhd G$.

Définition. Soient G un groupe et H un sous-groupe de G. Un ensemble de la forme $gH \coloneqq \{gh,\ h \in H\}$ avec $g \in G$ est appelé *classe à gauche modulo H*.
L'ensemble des classes à gauche modulo H est noté G/H.

Définition. Soient G un groupe et H un sous-groupe de G. On appelle *indice* de H dans G, et on le note $[G : H]$, le nombre de classes à gauche modulo H, lorsqu'il est fini.

Définition. Soient G un groupe et P une partie de G. On appelle *sous-groupe engendré* par P, que l'on note $\langle P \rangle$, le plus petit sous-groupe de G contenant P.

Théorème. Soient $(G, *)$ un groupe, P une partie de G et $P^{-1} = \{x^{-1},\ x \in P\}$. Alors
$$\langle P \rangle = \{x_1 \cdots x_n,\ n \geqslant 0,\ x_i \in P \cup P^{-1}\}.$$

Démonstration. Soit $H = \{x_1 \cdots x_n,\ n \geqslant 0,\ x_i \in P \cup P^{-1}\}$, montrons que H est le plus petit sous-groupe de G contenant P, *i.e.* $H = \langle P \rangle$.
Soit $x \in P \subset \langle P \rangle$, alors $x^{-1} \in \langle P \rangle$ car $\langle P \rangle$ est un sous-groupe de G, donc $P^{-1} \subset \langle P \rangle$ et $P \cup P^{-1} \subset \langle P \rangle$. Puisque $\langle P \rangle$ est un sous-groupe, on a $x_1 \cdots x_n \in \langle P \rangle$ pour tous $x_1, ..., x_n \in P \cup P^{-1}$, d'où $H \subset \langle P \rangle$.
Réciproquement, montrons simplement que H est un sous-groupe de G contenant P puisque $\langle P \rangle$ est le plus petit sous-groupe de G vérifiant cette propriété (il sera donc nécessairement inclus ou égal à H). En prenant $n = 1$ et $x_1 \in P \subset P \cup P^{-1}$, on a bien $P \subset H$; en prenant $n = 0$, on a $1_G \in H$, donc H est non vide. Montrons que pour $x, y \in H$, $xy^{-1} \in H$: si $x \in P \cup P^{-1}$, alors $x^{-1} \in P \cup P^{-1}$ donc si $x = x_1 \cdots x_n$ et $y = y_1 \cdots y_m$,

on a

$$xy^{-1} = x_1 \cdots x_n \cdot y_m^{-1} \cdots y_1^{-1} \in H,$$

ce qui montre finalement que H est un sous-groupe de G (en plus de contenir P), donc par double inclusion que $H = \langle P \rangle = \{x_1 \cdots x_n,\ n \geqslant 0,\ x_i \in P \cup P^{-1}\}$.

□

Définition. Soient G un groupe et P une partie de G. On dit que P est une *partie génératrice* de G si elle l'engendre, *i.e.* $G = \langle P \rangle$.

Définition. Un groupe est *monogène* s'il peut être engendré par un élément. Un groupe est *cyclique* s'il est fini et monogène.

Exemples. Le groupe $(\mathbb{Z}, +)$ est monogène. Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique d'ordre n.

Définition. Soient $G_1, ..., G_n$ des groupes. On définit une loi de composition interne sur le produit $G_1 \times ... \times G_n$ en posant pour tous $(x_1, y_1), ..., (x_n, y_n) \in G_1 \times ... \times G_n$: $(x_1, ..., x_n) \times (y_1, ..., y_n) \coloneqq (x_1 \times y_1, ..., x_n \times y_n)$.
Muni de cette loi, $G_1 \times ... \times G_n$ est un groupe d'élément neutre $(1_{G_1}, ..., 1_{G_n})$ appelé le *groupe produit* $G_1 \times ... \times G_n$. On dit aussi que c'est le groupe produit des groupes $G_1, ..., G_n$.

Définition. On appelle *ordre* d'un groupe $(G, *)$, noté $|G|$, le cardinal de l'ensemble G. On a $|(G, *)| \coloneqq Card(G)$. On appelle *groupe fini* (resp. *groupe infini*) un groupe dont l'ordre est fini (resp. infini).

Proposition. Soient G un groupe et $x \in G$. Alors, on a $\langle x \rangle = \{x^n,\ n \in \mathbb{Z}\}$.

Démonstration. Le théorème précédent nous dit que $\langle x \rangle = \{x^{\varepsilon_1} \cdots x^{\varepsilon_n},\ n \geqslant 0,\ \varepsilon_i = \pm 1\}$. Montrons donc que $\{x^{\varepsilon_1} \cdots x^{\varepsilon_n},\ n \geqslant 0,\ \varepsilon_i = \pm 1\} = \{x^n,\ n \in \mathbb{Z}\}$ par double inclusion.
On a $x^{\varepsilon_1} \cdots x^{\varepsilon_n} = x^{\varepsilon_1 + ... + \varepsilon_n}$ avec $\varepsilon_1 + ... + \varepsilon_n = n \in \mathbb{N} \subset \mathbb{Z}$ ou $\varepsilon_1 + ... + \varepsilon_n = -n \in \mathbb{Z}$, d'où l'on tire l'inclusion dans le sens direct. Réciproquement, on peut écrire x^n comme $x^n = x^1 \cdots x^1$ (pour $\varepsilon_i = 1$) ou bien comme $x^n = x^{-1} \cdots x^{-1}$ (pour $\varepsilon_i = -1$), d'où l'on tire l'inclusion dans le sens indirect, et donc l'égalité.

□

Définition. Soit G un groupe. On dit que $x \in G$ est *d'ordre fini* si $\langle x \rangle$ est un groupe fini. Dans ce cas, l'ordre de x est l'ordre de $\langle x \rangle$, et on le note $ord(x)$.

Théorème de Lagrange. Soient $(G, *)$ un groupe fini et H un sous-groupe de G. Alors $|H| \mid |G|$.

Démonstration. Posons R une relation sur G telle que $xRy \iff x^{-1}y \in H$. Montrons d'abord que c'est une relation d'équivalence.
En effet, $xRx \iff x^{-1}x = e \in H$. De plus, si xRy, alors $x^{-1}y \in H$. Puisque H est un sous-groupe de G, on a $(x^{-1}y)^{-1} = y^{-1}x \in H$, soit yRx. Enfin, pour $z \in G$, si xRy et yRz, on a $x^{-1}y \in H$ et $y^{-1}z \in H$. Or, puisque H est un sous-groupe de G, il est stable par produit, d'où $x^{-1}yy^{-1}z = x^{-1}z \in H$, d'où xRz. On a $[x] = \{y \in G,\ yRx\} = \{y \in G,\ y^{-1}x \in H\} = \{y \in G,\ x^{-1}y \in H\}$. Montrons que $[x] = xH = xy,\ y \in H$ par double inclusion.
Soit $y \in [x]$, alors $x^{-1}y \in H$. On écrit $y = xx^{-1}y = xz,\ z \in H$ donc $y \in xH$. Réciproquement, soit $y \in xH$. Alors, y s'écrit $y = xz,\ z \in H$. On part de $x^{-1}y = x^{-1}xz = z \in H$ d'où $x^{-1}y \in H$, soit xRy ou encore yRx, donc $y \in [x]$.
Montrons que xH contient autant d'éléments que H, *i.e.* que xH et H sont en bijection. Soient $y_1, y_2 \in H$. Si $xy_1 = xy_2$, alors $x^{-1}xy_1 = x^{-1}xy_2$, soit $y_1 = y_2$. Par contraposée, on a $y_1 \neq y_2 \implies xy_1 \neq xy_2$. Donc tous les termes de H sont différents deux à deux. Cela montre que xH et H contiennent autant d'éléments. Cela veut dire que $\mathrm{Card}([x]) = \mathrm{Card}(H) = |H|$. De plus, les classes de x forment une partition de G, *i.e.* les classes sont disjointes et de cardinal $|H|$.
Soit α une classe de $x \in G$, on a alors $G = \dot{\bigcup_{\alpha \in G/R}}$ avec $\mathrm{Card}(\alpha) = |H|$. Alors

$$|G| = \sum_{\alpha \in G/R} \mathrm{Card}(\alpha) = \sum_{\alpha \in G/R} |H| = |H| \cdot \mathrm{Card}(G/R), \qquad \text{d'où} \qquad |H| \mid |G|.$$

□

Définition. Soit E un ensemble non vide. On appelle *permutation* de E toute bijection de E sur E, et *groupe symétrique* de E l'ensemble des permutations de E, noté $\mathfrak{S}_E$. Le magma $(\mathfrak{S}_E, \circ)$ est un groupe d'élément neutre Id_E.

1.2.3 Théorie des anneaux

Définition. Un *anneau* $(A, +, \times)$ est un ensemble muni de deux lois de composition interne, notées $+$ et $\times$, telles que
- $(A, +)$ est un groupe abélien,
- la loi $\times$ est associative et distributive par rapport à $+$,
- il existe un élément neutre pour la loi $\times$ noté 1_A.

Un *anneau commutatif* est un anneau dont la loi $\times$ est également commutative.

Exemples. $(\mathbb{Z}, +, \times)$ est un anneau commutatif car $(\mathbb{Z}, +)$ est un groupe abélien, la loi $\times$ est associative, distributive par rapport à $+$ et commutative et il existe un élément neutre pour la loi $\times$, noté 1.
Enfin, $(M_n(\mathbb{R}), +, \times)$ est un anneau mais il n'est pas commutatif car toutes les matrices ne vérifient pas $A \times B = B \times A$.

Définition. Un anneau commutatif *intègre* (d'élément neutre 0_A pour la loi $+$) est un anneau commutatif tel que

$$\forall (a, b) \in A^2, \qquad a \times b = 0_A \implies a = 0_A \ \text{ ou } \ b = 0_A.$$

Exemples. $(\mathbb{Z},+,\times)$ et $(\mathbb{R},+,\times)$ sont des anneaux commutatifs intègres. Cependant, pour $n \geqslant 2$, $(M_n(\mathbb{R}),+,\times)$ n'est pas intègre (et toujours pas commutatif).

Proposition (Calculs dans un anneau intègre) (admis). Soient A un anneau commutatif et $a, b \in A$. Alors

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

On appelle ces identités respectivement le binôme de Newton et la factorisation de Bernoulli.

Définition. Un élément $a \in A$ est dit *inversible* s'il existe un élément $b \in A$ tel que $a \times b = b \times a = 1_A$. On dit alors que b est l'inverse de a.

Notation. L'ensemble des éléments inversibles de A est noté $A^\times$.

Définition. Un *sous-anneau* $(P,+,\times)$ de $(A,+,\times)$ est une partie de A telle que
- $1_A \in P$
- $\forall (x,y) \in P^2,\ x - y \in P$
- $\forall (x,y) \in P^2,\ x \times y \in P$.

Autrement dit, un sous-anneau contient l'élément neutre pour $\times$, et est stable par soustraction et produit.

Exemple. $(\mathbb{Z},+,\times)$ est un sous-anneau de $(\mathbb{R},+,\times)$.

Notation. $(A^*,\times)$ est un groupe, il est souvent noté simplement $A^\times$ aussi.

Définition. Soit $(A,+,\times)$ un anneau. Un *idéal* I de A est une partie de A telle que
- $(I,+)$ est un sous-groupe de $(A,+)$,
- $\forall x \in I,\ \forall a \in A,\ \ ax \in I$ et $xa \in I$.

Exemple. $3\mathbb{Z}$ est un idéal de l'anneau $(\mathbb{Z},+,\times)$ car $(3\mathbb{Z},+)$ est un sous-groupe de $(\mathbb{Z},+)$ et le produit d'un élément de I et d'un élément de $\mathbb{Z}$ est dans I : $3z \times z' = 3(z \times z') \in 3\mathbb{Z}$ pour $z, z' \in \mathbb{Z}$ car le produit de deux entiers $z, z' \in \mathbb{Z}$ est dans $\mathbb{Z}$.

Définition. Soit $(A,+,\times)$ un anneau commutatif. Un idéal I de A est dit *principal* s'il existe $x \in A$ tel que $I = xA$. On note cet idéal $< x >$.

Définition. On dit qu'un anneau est *principal* si tous ses idéaux non nuls sont principaux.

Proposition. Soit A un anneau intègre et B un sous-anneau de A. Alors B est intègre.

Démonstration. A étant intègre, on a $\forall (a,b) \in A^2,\ ab = 0 \implies a = 0$ ou $b = 0$. En particulier cette proposition est valable sur B étant donné que $B \subseteq A$.

□

Remarque. Tout anneau principal est intègre. La réciproque est fausse.

Lemme. Soit $\mathfrak{a} \subseteq A$ un idéal de A. Alors $\mathfrak{a} = A \iff 1 \in \mathfrak{a}$.

Démonstration.
- Si $\mathfrak{a} = A$, alors $\mathfrak{a}$ contient tous les éléments de A, en particulier 1.
- Si $1 \in \mathfrak{a}$, alors $\forall a \in A,\ a = a \cdot 1 \in \mathfrak{a} \implies \mathfrak{a} = A$.

□

Définition. Soient $a_1, ..., a_n \in A$ et $x_1, ..., x_n \in A$. On note $< x_1, ..., x_n >$ l'idéal

$$\{x_1 a_1 + ... + x_n a_n,\ (a_1, ..., a_n) \in A^n\}.$$

C'est l'idéal *engendré* par $x_1, ..., x_n$.
Un idéal engendré par un nombre fini d'éléments est un idéal de *type fini*.
Un idéal engendré par un seul élément $a \in A$, *i.e.* de la forme $aA = \{ab,\ b \in A\}$, est un idéal *monogène*.

1.2.4 Corps

Définition. Un *corps* $(K, +, \times)$ est un ensemble muni des lois $+$ et $\times$ telles que
- $(K, +)$ et $(K^*, \times)$ sont des groupes abéliens,
- La loi $\times$ est distributive par rapport à $+$.

Un *corps commutatif* est un corps dont la loi $\times$ est également commutative.

Exemple. $(\mathbb{C}, +, \times)$ est un corps commutatif car $(\mathbb{C}, +)$ et $(\mathbb{C}^*, \times)$ sont des groupes abéliens et la loi $\times$ est distributive par rapport à $+$.

Remarque. Tous les éléments non nuls d'un corps sont inversibles.

Définition. Un *sous-corps* L de K est une partie de K stable par $+$ et $\times$.

Exemple. $(\mathbb{R}, +, \times)$ est un sous-corps de $(\mathbb{C}, +, \times)$.

1.2.5 Espaces vectoriels

Définition (Espace Vectoriel). Un *espace vectoriel* $(V, +, \cdot)$ est un groupe abélien auquel on associe un corps $\mathbb{K}$ tel que on peut définit une multiplication externe par un scalaire :

$$V \times \mathbb{K} \longrightarrow V$$
$$(v, \lambda) \longmapsto \lambda \cdot v$$

vérifiant aussi quelques axiomes pour $u, v \in V$ et $\lambda, \mu \in \mathbb{K}$:

1. $\lambda(u + v) = \lambda u + \lambda v$ (distributivité du scalaire sur les vecteurs)
2. $(\lambda + \mu)v = \lambda v + \mu v$ (distributivité du vecteur sur les scalaires)
3. $(\lambda\mu)v = \lambda(\mu v)$ (quasi-associativité)
4. $1v = v$ (neutre multiplicatif)

Définition (Sous-espace vectoriel). Un *sous-espace vectoriel* est un sous-groupe stable par multiplication par un scalaire.

Remarque (Sous-espace vectoriel en pratique). En pratique, ce qu'on est ramené à faire c'est de montrer que quelque chose est un sous-espace vectoriel d'un espace vectoriel de référence. Ainsi, il ne faut que montrer la stabilité par la somme et par multiplication par un scalaire du sous-espace vectoriel considéré.

Définition (Espace engendré). Soit $U \subset V$. Le sous-espace vectoriel *engendré* par U est :

$$\langle U \rangle = \{a_1u_1 + \cdots a_nu_n \mid a_1...a_n \in \mathbb{K}\ ,\ u_1...u_n \in U\}$$

Définition (Finiment engendré). On dit que V est *finiment engendré* s'il existe $U \subset V$ fini tel que $V = \langle U \rangle$.

1.2.6 Modules

Définition. Un *module* $(M, +, \cdot)$ sur un anneau commutatif $(A, +, \times)$ (ou A-module) est un espace vectoriel muni de la multiplication par un scalaire dans l'anneau A, *i.e.* $(M, +)$ est un groupe abélien et $\cdot$ est associative, distributive par rapport à $+$ et possède un élément neutre noté 1.
La notion de module généralise celle d'espace vectoriel.

Définition. N est un *sous-module* de $(M, +, \cdot)$ s'il contient 0 et si pour tous $x, y \in N$ et $\alpha \in A$, $x + y \in N$ et $\alpha x \in N$.

Définition. Un A-module M est dit de *type fini* s'il est engendré par une partie finie $S \subset M$.
Il est dit *libre* s'il existe une famille $(x_i)_{i\in I}$ telle que tout élément x de M s'écrive de manière unique sous la forme $x = \sum_{i\in I} \alpha_i x_i$ avec $(\alpha_i)_{i\in I}$ des éléments de A non tous nuls.

Exemple. $\mathbb{Z}/n\mathbb{Z}$ est un $\mathbb{Z}$-module de type fini car il est engendré par $\overline{1}$ mais il n'est pas libre car dans un module libre on a $\alpha x = 0 \Longrightarrow \alpha = 0$ ou $x = 0$, or ici on peut trouver $(a, b) \neq (0, 0)$ tels que $ab = n = \overline{0}$.

1.3 Applications entre structures algébriques

1.3.1 Morphismes

Définition. Soient $(G, *)$ et $(H, \overline{*})$ deux groupes et $f : G \longrightarrow H$ une application.
On dit que f est un *morphisme de groupes* (ou homomorphisme de groupes) entre G et H si
$$\forall (x, y) \in G^2, \quad f(x * y) = f(x) \,\overline{*}\, f(y).$$

Définition. Soient $(A, +, \times)$ et $(B, +, \times)$ deux anneaux et $f : A \longrightarrow B$ une application.
On dit que f est un *morphisme d'anneaux* (ou homomorphisme d'anneaux) entre A et B si
- $\forall (x, y) \in A^2,\ f(x + y) = f(x) + f(y)$
- $\forall (x, y) \in A^2,\ f(x \times y) = f(x) \times f(y)$
- $f(1_A) = 1_B$.

Définition. Si $(A, +, \times)$ et $(B, +, \times)$ sont deux corps et que $f : A \longrightarrow B$ est un morphisme d'anneaux, alors on dit que f est un *morphisme de corps* entre A et B.

Définition. Si $f : E \longrightarrow F$ est un morphisme bijectif entre deux groupes (resp. anneaux, resp. corps), on dit que f est un *isomorphisme de groupes* (resp. d'anneaux, resp. de corps).
On dit que E et F sont *isomorphes* et on note $E \simeq F$.

Exemple. Le morphisme
$$\begin{array}{rccc} f & : & (\mathbb{R}^*, \times) & \longrightarrow & (\mathbb{R}_+^*, \times) \\ & & x & \longmapsto & e^x \end{array}$$
est un isomorphisme de groupes.

Définition. Lorsqu'un morphisme $f : E \longrightarrow F$ est injectif, il induit un isomorphisme entre E et $Im(f) \coloneqq \{f(x),\ x \in E\}$.
On dit que $f : E \longrightarrow F$ est un *plongement* de E dans F et que F est une *extension* de E.

Définition. Soit $f : G \longrightarrow G'$ un morphisme de groupes. On note $ker(f) = \{x \in G,\ f(x) = e_{G'}\}$. On appelle cet ensemble le *noyau* du morphisme f.

Définition (Morphisme d'espaces vectoriels). C'est ce qu'on appelle dans le jargon mathématique les *applications linéaires*, c'est-à-dire les fonctions $f : U \longrightarrow V$ vérifiant, pour $a, b \in U$ et $\lambda \in \mathbb{K}$:
- $f(a + b) = f(a) + f(b)$
- $f(\lambda a) = \lambda f(a)$

Lorsque f est bijective, on dit que c'est un *isomorphisme* entre U et V.

Définition. Soient $(M, +, \cdot)$ et $(M', +, \cdot)$ deux A-modules et $f : M \longrightarrow M'$ une application.
On dit que f est un *morphisme de A-modules* (ou homomorphisme de A-modules) entre M et M' si

$$\forall x, y \in M,\ \forall \alpha \in A, \quad f(x + y) = f(x) + f(y) \quad \text{et} \quad f(\alpha x) = \alpha f(x).$$

Si de plus f est bijective, on dit que c'est un *isomorphisme de A-modules*. De plus, on note $ker(f) \coloneqq f^{-1}\big(\{0\}\big)$ son noyau et $Im(f) \coloneqq f(M)$ son image ; ce sont des sous-modules de M et M', respectivement.

1.3.2 Groupes quotient

Soient G un groupe et H un sous-groupe de G. On s'intéresse à la relation d'équivalence R telle que $xRy \iff x^{-1}y \in H$. On avait montré que, pour tout $x \in G$, $\overline{x} = xH$.
L'idée de cette partie est de définir une structure de groupe sur G/R de manière à ce que la projection canonique $\pi : G \longrightarrow G/R$ soit un morphisme de groupes, *i.e.* qu'on ait pour tous $x, y \in G$, $\overline{x}\ \overline{y} = \overline{xy}$. Pour que cela soit vrai, nous devons imposer une condition sur le sous-groupe H, à savoir qu'il soit distingué, *i.e.* $xH = Hx$, ce qui nous amène à la proposition suivante.

Proposition. Soient G un groupe et $H \lhd G$. Alors l'application

$$\begin{aligned} f\ :\ G/R \times G/R &\longrightarrow G/R \\ (\overline{x}, \overline{y}) &\longmapsto \overline{xy} \end{aligned}$$

est bien définie et induit sur G/R une structure de groupe.

Démonstration. Vérifions que si $\overline{x_1} = \overline{x_2}$ et $\overline{y_1} = \overline{y_2}$, alors $\overline{x_1 y_1} = \overline{x_2 y_2}$. Par définition de la relation d'équivalence, il existe $h, h' \in H$ tels que $x_2 = x_1 h$ et $y_2 = y_1 h'$. On a alors $x_2 y_2 = x_1 h y_1 h' = x_1 y_1 (y_1^{-1} h y_1) h'$. Comme $H \lhd G$, on a $y_1^{-1} h y_1 \in H$ et donc $(y_1^{-1} h y_1) h' = h'' \in H$, soit $\overline{x_1 y_1} = \overline{x_2 y_2}$ et f est bien définie.
Vérifions maintenant que G/R muni de cette loi interne est un groupe. Pour tout $\overline{x} \in G/R$,

on a $\overline{1}_G\overline{x} = \overline{1_G x} = \overline{x}$ et de même $\overline{x}\overline{1}_G = \overline{x 1_G} = \overline{x}$. Donc $\overline{1}_G$ est un élément neutre pour cette loi. De plus, pour tous $\overline{x}, \overline{y}, \overline{z} \in G/R$, $(\overline{x}\ \overline{y})\overline{z} = \overline{xy}\ \overline{z} = \overline{(xy)z} = \overline{x(yz)} = \overline{x}\ \overline{yz} = \overline{x}(\overline{y}\ \overline{z})$. Enfin, $\overline{x}\ \overline{x^{-1}} = \overline{xx^{-1}} = \overline{1}_G$, donc $\overline{x}$ admet $\overline{x^{-1}}$ comme classe symétrique, ce qui conclut quant à la structure de groupe de G/R muni de cette loi.

□

Définition. Si G est un groupe et H un sous-groupe distingué de G, on appelle *groupe quotient* de G par H le groupe $G/H := G/R$ pour R la relation d'équivalence telle que pour tous $x, y \in G$, $xRy \iff x^{-1}y \in H$.

Remarque. La notation coïncide de manière tout à fait cohérente avec celle de l'ensemble des classes à gauche modulo H vue plus haut.

1.3.3 Théorèmes d'isomorphisme

Théorème (Premier théorème d'isomorphisme). Soient G et G' deux groupes et $f : G \longrightarrow G'$ un morphisme. Alors le morphisme de groupes $\tilde{f} : G/ker(f) \longrightarrow G'$ est un morphisme et on a $G/ker(f) \simeq Im(f)$, *i.e.* $G/ker(f)$ et $Im(f)$ sont isomorphes.

Démonstration. Montrons d'abord que $\tilde{f}$ est un morphisme injectif de groupes.
Soit $\tilde{x} \in G/ker(f)$. On a $\tilde{f}(\tilde{x}) = 1_{G'}$ si et seulement si $f(x) = 1_{G'}$, *i.e.* si et seulement si $x \in ker(f)$, ce qui revient à dire que $\tilde{x} = \tilde{1}$ avec $\tilde{1} := 1_{G/ker(f)}$. Ainsi, $ker(\tilde{f})$ est réduit à l'élément neutre. Par équivalence, $\tilde{f}$ est injective.
Puisque $\tilde{f} : G/ker(f) \longrightarrow G'$ est un morphisme injectif, il induit un isomorphisme de $G/ker(f)$ sur $Im(\tilde{f})$. Or, on a

$$Im(\tilde{f}) = \{\tilde{f}(\tilde{x}),\ \tilde{x} \in G/ker(f)\} = \{f(x),\ x \in G\} = Im(f),$$

donc $\tilde{f}$ induit un isomorphisme de $G/ker(f)$ sur $Im(f)$, d'où $G/ker(f) \simeq Im(f)$.

□

Exemple. Soit $det : (GL_n(\mathbb{R}), \times) \longrightarrow (\mathbb{R}^*, \times)$ un morphisme de groupes.
On sait en fait que $SL_n(\mathbb{R}) := \{M \in M_n(\mathbb{R}),\ det(M) = 1\}$ est un sous-groupe de $GL_n(\mathbb{R}) := \{M \in M_n(\mathbb{R}),\ det(M) \neq 0\}$.
De plus, on remarque que $SL_n(\mathbb{R})$ est le noyau de l'application det puisque le 1 qui apparaît à droite de l'égalité dans la définition de $SL_n(\mathbb{R})$ est l'élément neutre du groupe produit $(\mathbb{R}^*, \times)$. Ainsi, d'après le théorème d'isomorphisme tout juste énoncé, on a $(GL_n(\mathbb{R}), \times)/(SL_n(\mathbb{R}), \times) \simeq (\mathbb{R}^*, \times)$, c'est-à-dire que $(GL_n(\mathbb{R}), \times)/(SL_n(\mathbb{R}), \times)$ et $(\mathbb{R}^*, \times)$ sont isomorphes.

Théorème (Deuxième théorème d'isomorphisme). Soient G un groupe, N un sous-groupe normal de G et H un sous-groupe de G. Alors $N \cap H$ est un sous-groupe normal de H, et on a l'isomorphisme suivant :

$$H/(H \cap N) \simeq HN/N$$

Démonstration. Pour pouvoir parler du groupe quotient HN/N, il faut d'abord montrer que HN est un groupe et que N est un sous-groupe normal. Soient hn et $h'n'$ deux éléments de HN. On a :

$$hnh'n' = hh'(h'^{-1}nh')n'$$

avec $hh' \in H$, et puisque N est normal dans G, on a $h'^{-1}nh' \in N$ et finalement $n' \in N$. Donc $hnh'n' \in HN$, ce qui montre que HN est stable par multiplication.
D'autre part, on a les inclusions de groupes $N \subset HN \subset G$, et N est normal dans G, donc il est également normal dans HN.
Établissons maintenant l'isomorphisme en utilisant le premier théorème d'isomorphisme. On dispose d'un morphisme injectif $j : H \longrightarrow HN$ définie par $j(h) = h$, et de la surjection canonique $\pi : HN \longrightarrow HN/N$. On s'assure du fait que l'ensemble d'arrivée est bien un groupe puisque N est normal dans G. En composant ces deux morphismes, on obtient un nouveau morphisme qu'on note f :

$$\begin{aligned} f \coloneqq \pi \circ j \ : \ H &\longrightarrow HN/N \\ h &\longmapsto hN \end{aligned}$$

Montrons que le morphisme f est surjectif : pour $h \in H$ et $n \in N$, soit $(hn)N \in HN/N$. Puisque $n \in N$, $hnN = hN$, donc $hnN = f(h)$.
Montrons que le noyau de f est $H \cap N$: $f(h) = hN$ est l'élément neutre N de $HN/N \iff h \in N$. Comme h est déjà dans H, cela revient à dire que h est dans $N \cap H$.
Le premier théorème d'isomorphisme assure que $N \cap H$ est un sous-groupe normal de H, et que le morphisme induit $\tilde{f} : H/(N \cap H) \longrightarrow HN/N$ est un isomorphisme.

□

(Méta-)Lemme (Factorisation ensembliste). Soit $f : A \longrightarrow B$ une application entre deux ensembles A et B et $\pi : A \longrightarrow C$ une application surjective entre A et un troisième ensemble C. Alors les propositions suivantes sont équivalentes :

1. Il existe une unique application $g : C \longrightarrow B$ telle que $g \circ \pi = f$
2. Pour tout $a_1, a_2 \in A$, $\pi(a_1) = \pi(a_2) \implies f(a_1) = f(a_2)$.

On parle de factorisation parce qu'en quelque sorte, on divise (au sens de la composition) l'application f par l'application π.

Démonstration. On montre d'abord 1. $\implies$ 2. : on suppose l'existence d'une application g telle que $g \circ \pi = f$. Soient $a_1, a_2 \in A$ tels que $\pi(a_1) = \pi(a_2)$. Alors en appliquant g à cette égalité on obtient $f(a_1) = g(\pi(a_1)) = g(\pi(a_2)) = f(a_2)$.
On montre ensuite 2. $\implies$ 1. : soit $c \in C$. Puisque π est surjective, $\pi^{-1}(c) \neq \emptyset$. Alors $\forall a' \in \pi^{-1}(c)$, on a $\pi(a') = \pi(a) = c$ et donc $f(a) = f(a')$ par 2. En conséquence l'ensemble $f(\pi^{-1}(c))$ est un singleton, et l'élément $b \in B$ tel que $f(\pi^{-1}(c)) = b$ est uniquement défini pour c fixé. Ainsi on peut dire suivant l'usage que $c \longmapsto b \in f(\pi^{-1}(c))$ est une application bien définie. Appelons g cette application. En suivant la construction de g, on vérifie que $g \circ \pi = f$. Cette égalité donne aussi l'unicité de g. En effet, soit $g' : C \longrightarrow B$ une application telle que $g' \circ \pi = f$. Pour montrer que $g = g'$, on vérifie l'égalité $g'(c) = g(c)$ pour tout $c \in C$. On fixe c et on choisit $a \in \pi^{-1}(c) \subset A$. Puisque $g \circ \pi = f = g' \circ \pi$, on obtient $g(c) = g(\pi(a)) = f(a) = g'(\pi(a)) = g'(c)$. Donc la réciproque est vraie.

□

Lemme (Théorème de factorisation). Soient G et G' des groupes et soit $f : G \longrightarrow G'$ un morphisme. Soit H un sous-groupe distingué de G tel que $H \subseteq \mathrm{Ker}(f)$. Alors il existe un unique morphisme de groupes $\overline{f} : G/H \longrightarrow G'$ tel que $f = \overline{f} \circ \pi$, où π est la projection canonique de G sur G/H. Ce morphisme de groupes est défini par

$$\overline{f}(\overline{x}) = f(x), \quad \forall \overline{x} \in G/H.$$

Démonstration. Remarquons tout d'abord qu'un morphisme $f : G \longrightarrow G'$ est constant sur les classes d'équivalence (pour la relation associée à H) si et seulement si $H \in \mathrm{Ker}(f)$. En effet, si $H \in \mathrm{Ker}(f)$, alors pour tous $x \in G$ et $h \in H$, on a

$$f(xh) = f(x)f(h) = f(x).$$

Réciproquement, si f est constante sur chaque classe d'équivalence, elle est constante sur H. Mais H contient 1, et l'on a donc

$$f(h) = f(1_G) = 1_{G'}, \quad \forall h \ \in H,$$

c'est-à-dire $H \in \mathrm{Ker}(f)$. Le théorème de factorisation ensembliste fournit l'existence et l'unicité d'une application $\overline{f}$ vérifiant les propriétés voulues. De plus, pour tous $x_1, x_2 \in G$, on a :

$$\overline{f}(\overline{x_1}.\overline{x_2}) = \overline{f}(\overline{x_1 x_2})) = f(x_1 x_2) = f(x_1)f(x_2) = \overline{f}(\overline{x_1})\overline{f}(\overline{x_2}),$$

ce qui termine la démonstration.

□

Théorème (Troisième théorème d'isomorphisme). Soient G un groupe et H et K deux sous-groupes normaux de G tels que $K \subset H$. Alors H/K est un sous-groupe normal de G/K et on a l'isomorphisme suivant :

$$(G/K)(H/K) \simeq G/H$$

Démonstration. Soit $\pi : G \longrightarrow G/H$ la projection canonique. Comme $K \subset H = Ker(\pi)$, le théorème de factorisation montre que π induit un morphisme de groupes :

$$\begin{array}{rccc} \tilde{\pi} : & G/K & \longrightarrow & G/H \\ & \tilde{x} & \longmapsto & \overline{x}, \end{array}$$

où $\tilde{x}$ et $\overline{x}$ désignent respectivement les classes à gauche de x modulo K et modulo H. Le morphisme $\tilde{\pi}$ est évidemment surjectif. De plus, pour tout $x \in G$, on a

$$\overline{x} = \overline{1} \iff x \in H \iff \tilde{x} \in H/K.$$

Autrement dit, $\mathrm{Ker}(\tilde{\pi}) = H/K$. Ainsi, H/K est distingué dans G/K, et par le premier théorème d'isomorphismes, on a :

$$(G/K)(H/K) \simeq G/H,$$

ce qui achève la démonstration.

□

2 Construction des ensembles usuels

2.1 Construction de $\mathbb{N}$

Dans cette sous-section, nous allons construire l'ensemble qui nous permettra de construire tous les autres ensembles de nombres que nous utilisons chaque jour : c'est les entiers naturels, notés $\mathbb{N}$. Intuitivement, on sait que $\mathbb{N} = \{0, 1, 2, 3...\}$, pourquoi est-ce le cas ? Nous partons de peu pour construire $\mathbb{N}$ avec la méthode de Von Neumann qui consiste à définir les entiers naturels comme des nombres ordinaux, c'est-à-dire les nombres qui servent à décrire la position d'un élément dans un ensemble totalement ordonné.

Nous nous plaçons dans la théorie des ensembles de Zermelo-Fraenkel pour pouvoir utiliser *l'axiome de l'infini*. Plus précisément, l'axiome peut être écrit de la manière suivante, pour X un ensemble totalement ordonné :

Il existe un ensemble auquel appartient l'ensemble vide et qui est clos par application du successeur $x \longmapsto X \cup x$.

Donnons sens à cette phrase : nous pouvons associer l'ensemble vide (qui existe et qui est unique par les axiomes de Zermelo-Fraenkel) au nombre 0 et le fait d'être *"clos par application du successeur"* peut être interprété comme une manière de construire le prochain entier naturel étant donné la construction d'un certain nombre d'autres entiers naturels. Cela ne vous rappelle-t-il pas quelque chose ? Il s'agit en effet d'une démonstration par récurrence ! On peut construire le $n^{\text{ème}}$ entier naturel à partir des $n-1$ entiers naturels qui le précèdent. Formalisons cette construction intuitive.

Soit X un ensemble. Nous définissions le *successeur* de X, noté $s(X)$, comme un sous-ensemble des parties de X (c'est à dire que $s(X) \subset \mathcal{P}(X) \coloneqq \{A : A \subset X\}$) vérifiant $s(X) \coloneqq X \cup \{\{x\}, x \in X\}$, où les $\{x\}$ sont les singletons de l'ensemble X. Cette application nous permet entièrement de construire $\mathbb{N}$ ainsi que de démontrer ses propriétés algébriques. On pose

$$\emptyset = \{\} = 0$$

où au milieu on a l'ensemble qui ne contient RIEN, même pas *l'ensemble vide*. Cette subtilité est importante pour pouvoir construire le prochain entier naturel, à savoir 1. On applique la fonction successeur à 0 (c'est-à-dire à l'ensemble vide) :

$$\mathrm{s}(\emptyset) = \{\emptyset\} = \{0\} = 1.$$

Appliquons ce même procès pour les quelques entiers suivants :

$$\begin{gathered}\mathrm{s}(\mathrm{s}(\emptyset)) = \{\emptyset, \{\emptyset\}\} = \{0, 1\} = 2 \\ \mathrm{s}(\mathrm{s}(\mathrm{s}(\emptyset))) = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{0, 1, 2\} = 3 \\ \mathrm{s}(\mathrm{s}(\mathrm{s}(\mathrm{s}(\emptyset)))) = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\} = \{0, 1, 2, 3\} = 4.\end{gathered}$$

On construit ainsi par récurrence les entiers naturels : pour un entier n, on applique n fois la fonction successeur à l'ensemble vide. On conclut alors que $\mathbb{N} \coloneqq \{0, 1, 2, 3, 4, ...\}$.
On remarque deux choses intéressantes avec cette construction de $\mathbb{N}$:

- $\forall n \in \mathbb{N}, n = \{i, i \in [\![0, n-1]\!]\} = \{0, 1, ..., n-1\}$
- $\forall n \in \mathbb{N}$, le cardinal de l'ensemble qui le définit est n.

D'où l'existence et l'explicitation des entiers naturels $\mathbb{N}$ par la méthode de Von Neumann.

Pour les motivé(e)s, je vous encourage à voir la construction des entiers naturels par les axiomes de Peano, nommés comme tel en l'honneur du mathématicien italien Giuseppe Peano. Je vous donne ici les 5 axiomes de Peano, qui sont ceux qu'il a utilisés pour faire sa construction de $\mathbb{N}$:

1. L'élément appelé zéro et noté 0 est un entier naturel
2. Tout entier naturel n a un unique successeur, noté $s(n)$
3. Aucun entier naturel n'a 0 pour successeur
4. Deux entiers naturels ayant le même successeur sont égaux
5. Si une propriété P est vraie pour 0 et si qu'elle soit vraie pour n implique qu'elle soit vraie pour $s(n)$, alors elle vraie pour tout n.

Construction de l'addition.

Nous gardons toutes les notations pour la construction de $\mathbb{N}$ pour en définir ses propriétés.

Définition (Addition sur $\mathbb{N}$). Soient $n, m \in \mathbb{N}$. On définit l'opération "additionner n" comme :

$$\begin{aligned} +_n \ : \ \mathbb{N} &\longrightarrow \mathbb{N} \\ m &\longmapsto \begin{cases} +_n(m) = 0 & \text{si } m = 0 \\ +_n\big(s(m)\big) = s\big(+_n(m)\big) & \text{sinon} \end{cases} \end{aligned}$$

Remarque. Pour alléger l'abstraction au début, il faut garder en tête ce que cette application nous dit avec la notation usuelle d'addition :

$$\begin{aligned} +_n \ : \ \mathbb{N} &\longrightarrow \mathbb{N} \\ m &\longmapsto \begin{cases} n + m = n & \text{si } m = 0 \\ n + s(m) = s(n + m) & \text{sinon} \end{cases} \end{aligned}$$

Théorème (Élément neutre pour l'addition dans $\mathbb{N}$). Pour tout $n \in \mathbb{N}$, $n+0 = 0+n = n$.

Démonstration. On définit l'ensemble $A \coloneqq \{n \in \mathbb{N} : n + 0 = 0 + n = n\}$.
On remarque que par définition de l'addition, on a $0 \in A$. Supposons que $k \in A$, alors $k + 0 = 0 + k = k$. Alors $0 + s(k) = s(0 + k) = s(k)$ d'après la définition de l'addition par 0 et par hypothèse de récurrence respectivement. Encore une fois, par définition de l'addition par 0 on a $s(k) + 0 = s(k)$. On conclut que $k \in A \implies s(k) \in A$. Ainsi tous les éléments k qui sont dans cet ensemble sont les entiers naturels. Ainsi $A = \mathbb{N}$, ce qui achève la démonstration par l'axiome de récurrence.

□

Théorème (Explicitation du successeur). Pour tout $n \in \mathbb{N}$, $s(n) = n + 1$.

Démonstration. On définit $B \coloneqq \{n \in \mathbb{N} : s(n) = n + 1\}$
D'abord, on a $0 \in B$ car $s(0) = 1 = 0+1$ par le théorème précédent. Supposons que $k \in B$, alors $s(k) = k + 1$. Ainsi, $s(s(k)) = s(s(k) + 0) = s(k) + s(0) = s(k) + 1$. Alors on a que $k \in B \implies s(k) \in B$. Donc $B = \mathbb{N}$.

□

Théorème (Associativité de l'addition dans $\mathbb{N}$). Pour tous $\ell, m, n \in \mathbb{N},\ \ell + (m+n) = (\ell + m) + n$.

Démonstration. Fixons ℓ et m et faisons une récurrence sur k.
Soit $C \coloneqq \{n \in \mathbb{N} : \ell + (m+n) = (\ell+m)+n\}$. Nous avons $0 \in C$ car $\ell + (m+0) = \ell + m = (\ell+m)+0$. Supposons que $k \in C$, alors $(\ell+m)+k = \ell+(m+k)$. Montrons que $s(k) \in C$.
Nous avons : $(\ell+m)+s(k) = s((\ell+m)+k) = s(\ell+(m+k)) = \ell+s(m+k) = \ell+(m+s(k))$.
Ainsi $k \in C \implies s(k) \in C$. Donc $C = \mathbb{N}$.

□

Lemme. Pour tout $n \in \mathbb{N},\ 1 + n = n + 1$.

Démonstration. Soit $D \coloneqq \{n \in \mathbb{N} : 1 + n = n + 1\}$. Alors $0 \in D$. Supposons que $k \in D$, alors $1+k = k+1 = s(k)$. Ainsi on a $1+s(k) = s(1+k) = s(k+1) = s(k+s(0)) = s(s(k+0)) = s(s(k)) = s(k)+1$. Donc on a bien que $s(k) \in D$, donc $D = \mathbb{N}$.

□

Théorème (Commutativité de l'addition dans $\mathbb{N}$). Pour tous $n, m \in \mathbb{N},\ n + m = m + n$.

Démonstration. Fixons m et soit $E \coloneqq \{n \in \mathbb{N} : n + m = m + n\}$.
Par le premier théorème $0 \in E$ et par le lemme précédent, $1 \in E$.
Supposons que $k \in E$, alors $m + k = k + m$. On considère $m + s(k)$:
$m+s(k) = s(m+k) = s(k+m) = (k+m)+1 = k+(m+1) = k+(1+m) = (k+1)+m = s(k) + m$. Ainsi $E = \mathbb{N}$.

□

Théorème (Structure de $(\mathbb{N}, +)$). L'ensemble $(\mathbb{N}, +)$ est un monoïde commutatif.

Démonstration. Tout ce qu'on a fait sert de démonstration.

□

Construction de la multiplication.

Définition (Multiplication sur $\mathbb{N}$). Soient $n, m \in \mathbb{N}$. On définit l'opération "multiplier par n" récursivement comme :

$$\begin{aligned} \times_n \ : \ \mathbb{N} &\longrightarrow \mathbb{N} \\ m &\longmapsto \begin{cases} \times_n(m) = 0 & \text{si } n = 0 \\ \times_n(m) = n \times s(m) = (n \times m) + n & \text{sinon} \end{cases} \end{aligned}$$

Proposition (Propriétés algébriques de la multiplication). On peut vérifier que cette opération est associative, commutative et qu'elle admet un élément neutre : 1. De plus, elle est distributive par rapport à l'addition : $a \times (b + c) = a \times b + a \times c$.

□

2.2 Construction de $\mathbb{Z}$

Dans cette sous-section, après avoir construit l'ensemble $\mathbb{N}$ des entiers naturels, nous allons construire l'ensemble $\mathbb{Z}$ des entiers relatifs en symétrisant le monoïde commutatif $(\mathbb{N}, +)$ car en effet, il est absolument naturel et fondamental de définir l'opposé d'un entier naturel, et dans le même temps une nouvelle opération : la soustraction. Pour ce faire, il va nous falloir construire la soustraction à partir l'addition, ce qui est délicat sachant que cette opération est totalement banalisée pour nous à ce jour. Nous allons alors considérer de manière astucieuse une relation d'équivalence particulière et construire ainsi $\mathbb{Z}$ à partir des classes d'équivalence des éléments de cette relation. Avant de commencer, je souhaitais préciser que dans cette construction tous les calculs et toutes les vérifications redondantes seront faites pour donner l'exemple de rédaction, tandis que ceux pour la construction de $\mathbb{Q}$ seront parfois laissés au lecteur. Maintenant, allons-y !

On s'intéresse à des couples d'entiers dans $\mathbb{N} \times \mathbb{N}$. On pose $(a, b) \sim (c, d) \iff a + d = b + c$. On a en tête de voir (a, b) comme l'entier relatif $a - b$. Deux éléments en relation par celle-ci sont reliés par un $\sim$, en référence à une relation d'équivalence, qu'elle est elle-même par ailleurs, et nous allons le vérifier.
Elle est réflexive car $(a, b) \sim (a, b) \iff a + b = b + a$, ce qui est vrai par commutativité sur $\mathbb{N}$. Elle est symétrique car $(a, b) \sim (c, d) \implies (c, d) \sim (a, b)$ puisque $a + d = b + c \iff c + b = d + a$ par symétrie de la relation d'égalité. Enfin, elle est transitive car si $(a, b) \sim (c, d)$ et $(c, d) \sim (e, f)$, alors on a $a + d = b + c$ et $c + f = d + e$ soit, en additionnant $a + d + c + f = b + c + d + e$ qu'on simplifie en $a + f = b + e$ par injectivité du successeur défini plus haut ; il vient $(a, b) \sim (e, f)$.

Il est très important de comprendre que l'on a considéré cette relation d'équivalence car on avait en tête de définir et comprendre quand est-ce que l'on a $a - b = c - d$, c'est-à-dire que la classe d'équivalence de n est l'ensemble infini de couples d'entiers naturels dont la différence est lui-même. En ce sens, on peut définir de manière formelle et élégante $\mathbb{Z}$ comme le quotient de l'ensemble des couples d'entiers naturels par notre relation d'équivalence, *i.e.* $\mathbb{Z} \coloneqq (\mathbb{N} \times \mathbb{N})/\sim$.

On considèrera dans la suite les applications

$$\begin{array}{rccl} P & : & \mathbb{N} & \longrightarrow & \mathbb{Z} \coloneqq (\mathbb{N} \times \mathbb{N})/\sim \\ & & n & \longmapsto & [n, 0] \end{array}$$

et

$$\begin{array}{rccl} N & : & \mathbb{N} & \longrightarrow & \mathbb{Z} \coloneqq (\mathbb{N} \times \mathbb{N})/\sim \\ & & n & \longmapsto & [0, n] \end{array}$$

qui sont des projections canoniques injectives (avec $[n, 0]$ la classe d'équivalence de l'entier $n - 0 = n$ par $\sim$). On peut justifier cela par le fait que $(n, 0) \sim (m, 0) \implies n = m$ pour P et $(0, n) \sim (0, m) \implies m = n$.
Nous allons d'ailleurs montrer plus bas que $[0, n]$ est l'opposé de $[n, 0]$ pour l'addition, que nous allons elle-même définir formellement ci-dessous.

Construction de l'addition. Soient $x, y \in \mathbb{Z}$. On pose $x = [a, b]$, $y = [c, d]$ et $x + y \coloneqq [a + c, b + d]$. En effet, l'idée ici est de retrouver par construction les propriétés usuelles de l'addition que l'on connaît sur $\mathbb{Z}$.
On va vérifier avant tout que cette loi additive est bien définie, *i.e.* qu'elle ne dépend pas du représentant des classes d'équivalence considérées. On pose $x = [a', b']$ et $y = [c', d']$. Alors on a $x = [a, b] = [a', b']$, soit $a + b' = a' + b$. De même, on a $y = [c, d] = [c', d']$, soit $c + d' = c' + d$. En sommant les deux égalités, on obtient

$$a + c + b' + d' = b + d + a' + c' \qquad \text{d'où} \qquad [a + c, b + d] = [a' + c', b' + d'].$$

Vérifions dans un second temps que notre loi additive est associative, commutative et qu'elle possède un élément neutre (ce qui montrera que $\mathbb{Z}$ se voit muni d'une structure de groupe abélien, noté $(\mathbb{Z},+)$ pour rappel, dans un premier temps).
En effet, pour $x=[a,b]$, $y=[c,d]$ et $z=[e,f]$, on a

$$x+(y+z)=x+[c+e,d+f]=[a+c+e,\ b+d+f]$$

et aussi

$$(x+y)+z=[a+c,b+d]+z=[a+c+e,\ b+d+f],$$

d'où $x+(y+z)=(x+y)+z$ et la loi est bien associative.
De plus, on a $x+y=[a+c,b+d]=[c+a,d+b]=y+x$, donc la loi est bien commutative.
Ensuite, on propose $e=[0,0]$ pour l'élément neutre. On a alors $x+e=[a+0,b+0]=[a,b]=[0+a,0+b]=e+x=x$, donc il existe bien un élément neutre et c'est précisément $e=[0,0]$.
Enfin, pour tous $n,m\in\mathbb{N}$ on a $P(n)+P(m)=[n,0]+[m,0]=[n+m,0]=P(n+m)$.

Construction de l'opposé. Soit $x=[a,b]\in\mathbb{Z}$. Alors il existe $y=[b,a]\in\mathbb{Z}$ tel que $x+y=e$ car en effet $x+y=[a+b,b+a]\sim[0,0]=e$ donc y est bien l'opposé de x pour l'addition.

Construction de la multiplication. Soient $x,y\in\mathbb{Z}$. On pose $x=[a,b]$, $y=[c,d]$ et $xy\coloneqq[ac+bd,ad+bc]$. Ici, l'idée de définir ainsi la multiplication est de retomber sur la propriété de multiplication telle que $(a-b)(c-d)=ac-ad-bc+bd=(ac+bd)-(ad+bc)$.
On va vérifier que cette loi multiplicative est bien définie. On pose $x=[a',b']$ et $y=[c',d']$. Alors on a $x=[a,b]=[a',b']$ soit $a+b'=a'+b$; de même $y=[c,d]=[c',d']$ soit $c+d'=c'+d$. En multipliant les deux égalités, on obtient

$$(a+b')(c+d')=(a'+b)(c'+d)\qquad\text{soit}\qquad ac+ad'+b'c+b'd'=a'c'+a'd+bc'+bd.$$

Or $a+b'=a'+b$ et $c+d'=c'+d$, donc

$$ac+ad'+b'c+b'd'=a'c'+a'd+bc'+bd\iff ac+a'd'+b'c+bd'=a'c'+ad+bc'+b'd$$
$$\iff ac+a'd'+b'c'+bd=a'c'+ad+bc+b'd'\iff ac+bd+a'd'+b'c'=ad+bc+a'c'+b'd',$$

d'où $[ac+bd,ad+bc]=[a'c'+b'd',a'd'+b'c']$.

Vérifions maintenant que la loi est associative, commutative, distributive et qu'elle possède un élément neutre (ce qui montrera plus largement avec les résultats précédents que $\mathbb{Z}$ se voit muni d'une structure d'anneau commutatif, noté $(\mathbb{Z},+,\times)$ pour rappel).
En effet, pour $x=[a,b]$, $y=[c,d]$ et $z=[e,f]$, on a

$$(xy)z=[ac+bd,ad+bc]\ [e,f]=[ace+bde+adf+bcf,\ acf+bdf+ade+bce]$$

et aussi

$$x(yz)=[a,b]\ [ce+df,cf+de]=[ace+adf+bcf+bde,\ acf+ade+bce+bdf].$$

On conclut sur l'associativité en mentionnant la commutativité de l'addition dans $\mathbb{N}$.
De plus, on a $xy=[ac+bd,ad+bc]$ et $yx=[ca+db,cb+da]$. Par commutativité du produit sur $\mathbb{N}$, on a bien $xy=yx$.
Ensuite, on a

$$x(y+z)=[a,b]\ [c+e,d+f]=[ac+ae+bd+bf,\ ad+af+bc+be].$$

D'autre part, on a

$$xy=[ac+bd,ad+bc]\qquad\text{et}\qquad xz=[ae+bf,af+be],$$

soit

$$xy + xz = [ac + bd, ad + bc] + [ae + bf, af + be] = [ac + bd + ae + bf,\ ad + bc + af + be],$$

d'où, par commutativité de la somme sur $\mathbb{N}$, $x(y + z) = xy + xz$, ce qui montre la distributivité.
Par ailleurs, on propose $e = [1, 0]$ pour l'élément neutre. On a alors $xe = [a \times 1 + b \times 0,\ a \times 0 + b \times 1] = [a, b] = [1 \times a + 0 \times b,\ 1 \times b + 0 \times a] = ex = x$, donc il existe bien un élément neutre et c'est précisément $e = [1, 0]$.
Enfin, pour tous $n, m \in \mathbb{N}$, $P(n)P(m) = [n, 0]\ [m, 0] = [nm + 0 \times 0, n \times 0 + 0 \times m] = [nm, 0] = P(nm)$.

Remarquons par ailleurs que l'on a un ordre total sur $\mathbb{Z}$, ce qui en fait un ensemble totalement ordonné. En effet

- $a \geqslant b \iff [a, b] \geqslant [0, 0] \iff \exists n \in \mathbb{N},\ a = b + n$, soit $a + 0 = b + n$ d'où $[a, b] = [n, 0] = P(n)$,
- $a \leqslant b \iff [a, b] \leqslant [0, 0] \iff \exists n \in \mathbb{N},\ b = a + n$, soit $b + 0 = a + n$ d'où $[a, b] = [0, n] = N(n)$.

Pour $n \in \mathbb{N}$, on note maintenant $n = P(n)$, d'où $-1 = [0, 1]$ et donc $x \leqslant y \implies -x \geqslant -y$. En effet, $x \leqslant y \iff a + d \leqslant b + c$. D'autre part, $-x = [b, a]$ et $-y = [d, c]$, d'où $-x \geqslant -y \iff b + c \geqslant a + d$ donc on a bien l'implication puisque l'on retrouve la même inégalité.

On a également la propriété suivante concernant les signes : $(-x)(-y) = xy$.
En effet, on a

$$[b, a]\ [d, c] = [bd + ac, bc + ad] \qquad \text{et} \qquad [a, b]\ [c, d] = [ac + bd, ad + bc].$$

Par commutativité de la somme sur $\mathbb{N}$, on retrouve bien $(-x)(-y) = xy$.

Par construction, on a bien retrouvé toutes les propriétés de l'ensemble $\mathbb{Z}$ que l'on connaît. C'est sur cette même idée de construction par l'exploitation d'une relation d'équivalence que l'on va se baser pour construire l'ensemble $\mathbb{Q}$ des rationnels dans la sous-section suivante.

2.3 Construction de $\mathbb{Q}$

Dans cette sous-section, nous allons construire l'ensemble $\mathbb{Q}$ des rationnels avec pour motivation de définir et manipuler des fractions ainsi que de définir l'inverse d'un nombre. Comme précisé dans l'introduction de la construction de $\mathbb{Z}$, certains calculs et vérifications redondantes seront ici laissés au lecteur, contrairement à la sous-section précédente où tout est très détaillé.

On considère la relation d'équivalence $\sim$ sur $\mathbb{Z} \times \mathbb{Z}^*$ telle que $(a, b) \sim (c, d) \iff ad = bc$. On a en tête de voir (a, b) comme le nombre rationnel $\dfrac{a}{b}$. Vérifions déjà que c'est bien une relation d'équivalence.
Elle est réflexive car $(a, b) \sim (a, b) \iff ab = ba$, ce qui est vrai par commutativité du produit sur $\mathbb{Z}$. Elle est symétrique car si $ad = bc$, alors $cb = da$ par commutativité du produit sur $\mathbb{Z}$ et symétrie de la relation d'égalité. Enfin, elle est transitive car si $ad = bc$ et $cf = de$, alors $fad = bcf$ et $bcf = edb$ soit $fad = edb$ ou encore $d(af - be) = 0$. Par intégrité de $\mathbb{Z}$, on a $d = 0$ ou $af - be = 0$, or $d \neq 0$ puisque c'est un dénominateur, ce qui implique $af = be$, *i.e.* $(a, b) \sim (e, f)$.

L'idée de considérer cette relation d'équivalence en particulier vient de la volonté de regrouper les fractions telles que $\frac{a}{b} = \frac{c}{d}$ car l'on sait qu'il y a une infinité de manières d'écrire un entier relatif comme une fraction de deux entiers relatifs (e.g. $2 = \frac{2}{1} = \frac{-2}{-1} = \frac{8}{4} = ...$). Tout cela nous montre que l'on peut définir $\mathbb{Q}$ comme le quotient de l'ensemble $\mathbb{Z} \times \mathbb{Z}^*$ par la relation d'équivalence $\sim$ fraîchement définie, *i.e.* $\mathbb{Q} \coloneqq (\mathbb{Z} \times \mathbb{Z}^*)/\sim$.

Construction de l'addition. Soient $x, y \in \mathbb{Q}$. On pose $x = [a, b]$, $y = [c, d]$ et $x + y \coloneqq [ad + bc, bd]$. On a l'idée de poser cette définition car on veut retrouver $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$.
Vérifions que cette loi additive est bien définie. Soient $x = [a', b']$ et $y = [c', d']$. On a $[a, b] = [a', b']$ et $[c, d] = [c', d']$ soit $ab' = a'b$ et $cd' = c'd$. On veut montrer que $[ad + bc, bd] = [a'd' + b'c', b'd']$, soit $b'd'(ad + bc) = bd(a'd' + b'c')$. On a bien

$$a'bdd' + bb'c'd = ab'dd' + bb'cd' = b'd'(ad + bc).$$

On vérifie trivialement que la loi est associative, commutative, avec opposé, élément neutre $[0, 1]$ et telle que l'application i définie comme

$$\begin{aligned} i \ : \ \mathbb{Z} &\longrightarrow \mathbb{Q} \\ a &\longmapsto [a, 1] \end{aligned}$$

est injective et vérifie $i(a) + i(b) = i(a + b)$.

Construction de la multiplication. Soient $x, y \in \mathbb{Q}$. On pose $x = [a, b]$, $y = [c, d]$ et $xy \coloneqq [ac, bd]$. On définit le produit ainsi car on veut retrouver $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.
Vérifions que c'est bien défini. Soient $x = [a', b']$ et $y = [c', d']$. On a $ab' = a'b$ et $cd' = c'd$, et on veut montrer que $[ac, bd] = [a'c', b'd']$. On a simplement

$$acb'd' = a'cbd' = a'c'bd.$$

On montre facilement par le calcul que la loi est associative, commutative, distributive selon la loi $+$, d'élément neutre $[1, 1]$ et telle que

$$\begin{aligned} i \ : \ \mathbb{Z} &\longrightarrow \mathbb{Q} \\ a &\longmapsto [a, 1] \end{aligned}$$

vérifie $i(a)i(b) = i(ab)$.

Construction de l'inverse. Soit $x \in \mathbb{Q}^*$ avec $0 = [0, 1]$. Alors $x = [a, b]$ avec $a \times 1 \neq b \times 0 \iff a \neq 0$. On a $y = [b, a]$ pour que $xy = [ab, ba] = [1, 1]$ car $\frac{ab}{ba} = 1$ et $[1, 1] = i(1)$.

L'ensemble $\mathbb{Q}$ est intègre. En effet

$$xy = [ac, bd] = [0, 1] \iff ac \times 1 = 0 \times bd = 0$$

donc $0 \in \{a, c\}$.
- Si $a = 0$, $x = [0, b] = [0, 1]$,
- Si $c = 0$, $y = [0, d] = [0, 1]$.

L'inverse est unique. En effet, si $xy = 1 = xy'$, alors $x(y - y') = 0$. Or $x \neq 0$ donc par intégrité de $\mathbb{Q}$ on a $y = y'$.

On a un ordre total sur $\mathbb{Q}$, ce qui en fait un ensemble totalement ordonné.

Comme pour $\mathbb{Z}$, la clé de la construction est la définition de la relation d'équivalence. On a ainsi retrouvé toutes les propriétés sur $\mathbb{Q}$ et donc construit cet ensemble (qui est muni d'une structure de corps commutatif) par la même occasion.

2.4 Construction de $\mathbb{R}$

Enfin nous sommes arrivés à la construction des nombres réels $\mathbb{R}$! Nous supposons que sont construits les ensembles $\mathbb{N}, \mathbb{Z}$ et $\mathbb{Q}$. Ce n'est qu'au $19^{\text{ème}}$ siècle que les nombres réels sont construits rigoureusement. La manière que nous adoptons dans ce cours est la construction de $\mathbb{R}$ par les suites de Cauchy. Il existe cependant une autre construction très connue sous le nom de la méthode des coupures de Dedekind. Allons-y.

Définition (Suite de Cauchy rationnelle). Une *suite de Cauchy* est une suite $x = (x_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}}$ telle que

$$\forall R \in \mathbb{N}^*,\ \exists N_R \in \mathbb{N}^*,\ \forall m, n \geqslant N_R,\quad |x_m - x_n| \leqslant \frac{1}{R}.$$

Notation. N_R signifie que le N choisi dépend du R choisi auparavant.

Définition (Suite négligeable). Une suite $x = (x_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}}$ est dite *négligeable* si

$$\forall R \in \mathbb{N}^*,\ \exists N_R \in \mathbb{N}^*,\ \forall n \geqslant N_R,\quad |x_n| \leqslant \frac{1}{R}.$$

Notation (Suites de Cauchy, suites négligeables). On note :

1. $\mathcal{C} = \{\text{suites rationnelles de Cauchy}\}$
2. $\mathcal{N} = \{\text{suites rationnelles négligeables}\}$

Définition (Opérations séquentielles). Soient $x = (x_n)$ et $y = (y_n)$ deux suites. Alors

1. $x + y = (x_n + y_n)$ est la *somme* terme à terme des deux suites,
2. $xy = (x_n y_n)$ est le *produit* terme à terme des deux suites.

Proposition (Propriétés algébriques des opérations). Avec les mêmes notations, on peut vérifier sans peine que :

1. La somme est associative, commutative, elle admet un élément neutre (la suite $(x_n) = (0)$) ainsi qu'un opposé (la suite $(x_n) = (-x_n)$)
2. Le produit est associatif, commutatif, il admet un élément neutre (la suite $(x_n) = (1)$) et il est distributif par rapport à la somme.

□

Remarque (Non-intégrité de l'anneau $(A, +, \times)$). Il se peut qu'on ait deux suites qui soient toutes deux non nulles et qui ont pour autant un produit nul ! Par exemple :

$$x = (1, 0, 1, 0, 1, 0...)$$
$$y = (0, 1, 0, 1, 0, 1...)$$

Lemme (Toute suite de Cauchy est bornée). Si $x = (x_n)$ est de Cauchy, $\exists C > 0$ tel que $\forall n \in \mathbb{N},\ |x_n| \leqslant C$.

Démonstration. $\exists N \in \mathbb{N}^*$ tel que $|x_n - x_m| \leqslant 1,\ \forall m, n \geqslant N$. Donc $x_n \leqslant |x_N| + 1$ donc $C = max\{|x_1|, ..., |x_N|\}$ convient.

□

Proposition (Stabilité de Cauchy). Si deux suites x et y sont de Cauchy, alors leur somme $x + y$ et leur produit xy sont de Cauchy.

Démonstration. Soit $R \in \mathbb{N}^*$. Alors $\exists N_R \in \mathbb{N}^*$ tel que pour $m, n \geqslant N_R$, on a $|x_n - x_m| \leqslant \frac{1}{2R}$ et $|y_n - y_m| \leqslant \frac{1}{2R}$.
Pour démontrer que $x + y$ est de Cauchy, on considère

$$|(x_n - x_m) + (y_n - y_m)| = |(x_n + y_n) - (x_m + y_m)| \leqslant |(x_n + y_n)| + |(x_m + y_m)| \leqslant \frac{1}{2R} + \frac{1}{2R} = \frac{1}{R}.$$

Pour démontrer que xy est de Cauchy, on prend un C bien choisi de telle sorte que C borne à la fois la suite (x_n) et la suite (y_n), qui existe par le lemme précédent. Ainsi on considère

$$|x_n y_n - x_m y_m| \leqslant |x_n| \times |y_n y_m| + |y_m| \times |x_n + x_m| \leqslant \frac{C}{2R} + \frac{C}{2R} = \frac{C}{R},$$

ce qui achève notre démonstration.

□

Remarque (pour en finir avec les suites de Cauchy...). On remarque deux petites choses avant de partir sur les suites négligeables.
Premièrement, si $x \in \mathcal{C}$, alors $-x \in \mathcal{C}$.
Deuxièmement, toute suite constante est de Cauchy.
Ainsi, $\mathcal{C}$ hérite des opérations $+$ et $\times$ avec leurs propriétés habituelles.

Proposition (Premières propriétés des suites négligeables). Nous avons tout d'abord l'inclusion $\mathcal{N} \subset \mathcal{C}$. De plus :

1. $x \in \mathcal{N} \implies -x \in \mathcal{N}$ (stabilité des suites négligeables par multiplication de -1)
2. $x, y \in \mathcal{N} \implies x + y \in \mathcal{N}$ (stabilité des suites négligeables par la somme)
3. $x \in \mathcal{C}, y \in \mathcal{N} \implies xy \in \mathcal{N}$ (propriété absorbante des suites négligeables)

Démonstration. Nous allons démontrer la première inclusion ; la démonstration des propriétés numérotées constituent un bon exercice pour apprendre à manipuler les suites négligeables.
Soit $x = (x_n) \in \mathcal{N}$. Soit $R \geqslant 1$ un entier, alors $\exists N_R \geqslant 1$ tel que $\forall n \geqslant N_R,\ |x_n| \leqslant \frac{1}{2R}$.
Ceci implique que $|x_m - x_n| \leqslant |x_n| + |x_m| \leqslant \frac{1}{2R} + \frac{1}{2R} = \frac{1}{R},\ \ \forall m, n \geqslant N_R$.

□

Proposition (Stabilité de $\mathcal{N}$ par multiplication). $x \in \mathcal{N},\ y \in \mathcal{N} \implies xy \in \mathcal{N}$.

Démonstration. $\exists C > 0$ tel que $|x_n| \leqslant C,\ \forall n \in \mathbb{N}$. Soit $R \geqslant 1$, alors il existe N_R tel que $|y_n| \leqslant \frac{1}{C'R}$, où $C' \geqslant C$ sont deux entiers. Alors

$$|x_n y_n| \leqslant C \times \frac{1}{CR} = \frac{1}{R}.$$

□

Proposition (L'idéal des suites de Cauchy). L'ensemble $\mathcal{C}$ est un anneau. L'idéal de $\mathcal{C}$ est $\mathcal{N}$.

Démonstration. Toutes les propriétés pour démontrer ces deux affirmations ont été démontrées au cours de cette sous-section.

□

Définition (Quotient d'un anneau par son idéal). Soit A un anneau et $I \subset A$ un idéal de A. On définit la relation suivante pour $a, b \in A$:

$$a \sim b \iff a - b \in I$$

Remarque. On peut montrer que cette relation définit une relation d'équivalence.

Proposition (Suites de Cauchy quotientées par les suites négligeables). Montrons que pour $A = \mathcal{C}$ et $I = \mathcal{N}$, la relation précédente est bien une relation d'équivalence. On dit que deux suites de Cauchy rationnelles sont équivalentes si

$$(x_n) \sim (y_n) \iff \lim_{n\to\infty} (x_n - y_n) = 0.$$

Les trois propriétés sont bien vérifiées :

- Réflexivité : la suite nulle converge vers 0
- Symétrie : Si $\lim_{n\to\infty}(x_n) = 0$, alors $\lim_{n\to\infty}(-x_n) = 0$
- Transitivité : démontrée à l'aide de l'inégalité triangulaire. Soient $(x_n), (y_n)$ et (z_n) trois suites de Cauchy rationnelles, alors pour tout $n \in \mathbb{N}$, $|u_n - z_n| \leqslant |u_n - v_n| + |v_n - w_n|$.

□

Définition ($\mathbb{R}$)***.*** On définit les nombres réels $\mathbb{R}$ comme l'ensemble des classes d'équivalence des suites de Cauchy rationnelles pour la relation d'équivalence $\sim$ précédente, *i.e.* $\mathbb{R} \coloneqq \mathcal{C}/\mathcal{N}$.

2.5 Construction de $\mathbb{C}$

Dans cette sous-section, nous allons construire le corps des nombres complexes $\mathbb{C}$ en utilisant la notion d'idéal déjà définie plus haut ainsi que la division euclidienne d'un

polynôme par un autre.

Soient $(A, +, *)$ un anneau et I un idéal de A.

On définit deux lois de composition interne $+$ et $\times$ sur A/I par
- $\forall a, b \in A,\ (a+I)+(b+I) = a+b+I$
- $\forall a, b \in A,\ (a+I)\times(b+I) = ab+I$.

Par construction, $(A/I, +, \times)$ est un anneau commutatif.

La projection sur le quotient A/I définie par

$$\begin{aligned} \pi\ :\ A &\longrightarrow A/I \\ a &\longmapsto a+I \end{aligned}$$

est alors un morphisme d'anneaux de noyau I.

Posons $A = \mathbb{R}[X]$ et $I = \langle X^2+1\rangle = (X^2+1)\mathbb{R}[X]$. Prenons $P(X) = 2X^3 - 3X^2 + 4X - 5$. On écrit

$$\begin{array}{rr|l} 2X^3 - 3X^2 + 4X - 5 & & X^2+1 \\ \cline{3-3} -2X^3 \qquad\quad -2X & & 2X-3 \\ \cline{1-2} -3X^2 + 2X - 5 & & \\ 3X^2 \qquad\quad +3 & & \\ \cline{1-2} 2X - 2 & & \end{array}$$

et on a donc $P(X) \equiv (2X-2)[X^2+1]$. De manière plus générale, on peut dire que

$$\mathbb{R}[X]\ /\ \langle X^2+1\rangle\ = \{aX+b+I,\ a, b \in \mathbb{R}\}.$$

Somme :

$$(aX+b+I) + (cX+d+I)\ =\ (a+c)X + (b+d) + I.$$

Multiplication :

$$\begin{aligned} (aX+b+I)\times(cX+d+I)\ &=\ acX^2 + adX + aXI + bcX + bd + bI + cXI + dI + I \\ &=\ acX^2 + adX + bcX + bd + I\ =\ acX^2 + (ad+bc)X + bd + I \\ &=\ acX^2 + (ad+bc)X + bd - ac(X^2+1) + I\ =\ (ad+bc)X + (bd-ac) + I. \end{aligned}$$

On reconnaît les propriétés analogues à l'addition et la multiplication pour les nombres complexes.
On pose alors

$$\begin{aligned} \varphi\ :\ \mathbb{R}[X]\ /\ \langle X^2+1\rangle\ &\longrightarrow\ \mathbb{C} \\ aX+b+I\ &\longmapsto\ ai+b, \end{aligned}$$

qui est un isomorphisme de corps. Il vient

$$\mathbb{C}\ :=\ \mathbb{R}[X]\ /\ \langle X^2+1\rangle\,.$$

2.6 Compléments : axiomes de la théorie ZFC

Dans cette sous-section, nous allons nous intéresser à certains fondements profonds des Mathématiques, plus précisément les axiome du choix, lemme de Zorn et bon ordre.

On munit un ensemble P d'une relation d'ordre partiel $\succ$.

Définition. On dit que $m \in P$ est un élément *maximal* de P si pour tout $x \in P$, $m \succ x \implies x = m$.

Définition. On dit que P est *inductif* si tout sous-ensemble totalement ordonné de P admet un majorant.

Lemme de Zorn. Tout ensemble ordonné inductif non vide admet un élément maximal.

Théorème de Zermelo (ou théorème du bon ordre). Tout ensemble peut être muni d'un ordre tel que toute partie non vide admet un plus petit élément, appelé bon ordre.

Axiome du choix. Pour tout ensemble E, il existe une application qui à chaque partie non vide de E associe un élément de cette partie.
Autrement dit, pour toute relation d'équivalence R sur E, il existe un système de représentants des classes de R, *i.e.* une partie de E qui contient exactement un représentant par classe.

Ces trois résultats sont équivalents, mais seuls les lemme de Zorn et théorème de Zermelo possèdent une démonstration (que nous admettrons ici par manque d'intérêt).
Ces trois résultats réunis sont à la base de la théorie des ensembles de Zermelo-Fraenkel, aussi appelée ZFC (le C étant l'initiale du mot "choix").

3 Propriétés de $\mathbb{R}$

Ayant maintenant construit les nombres réels, on peut finalement y établir les propriétés usuelles que nous utilisons en analyse.

3.1 Suites dans $\mathbb{R}$

Lemme. On a

$$x \neq y \iff \begin{cases} \exists N \geqslant 1,\ \forall n \in \mathbb{N},\quad x_n > y_n \\ \qquad\qquad \text{ou} \\ \exists N \geqslant 1,\ \forall n \in \mathbb{N},\quad x_n < y_n. \end{cases}$$

Dans le premier cas, on note $x > y$. Dans le second, on note $x < y$.

Démonstration. On raisonne par équivalence : $x \neq y$ si et seulement si la suite $(x_n - y_n)_{n\in\mathbb{N}}$ n'est pas négligeable si et seulement si $\exists R \geqslant 1,\ \exists (x_{n_k} - y_{n_k})_{k\in\mathbb{N}},\ |x_{n_k} - y_{n_k})| \geqslant \dfrac{1}{R}$.
Puisque $(x_n)_{n\in\mathbb{N}}$ et $(y_n)_{n\in\mathbb{N}}$ sont de Cauchy (par définition de $\mathbb{R}$),

$$\exists N \geqslant 1,\ \forall m, n \geqslant N,\quad |x_n - x_m| < \frac{1}{3R} \quad \text{et} \quad |y_n - y_m| < \frac{1}{3R}.$$

Quitte à oublier des termes (puisque l'on s'intéresse à des propriétés à partir d'un certain rang), on peut supposer que $n_k \geqslant N,\ \forall k \in \mathbb{N}$.
Supposons que $x_{n_0} > y_{n_0}$, alors $x_n > y_n,\ \forall n \in \mathbb{N}$.
On a donc montré que si $x \neq y$, alors $|x_n - y_n| = x_n - y_n > \dfrac{1}{R}$ pour tout $R > 1$, soit $x_n > y_n + \dfrac{1}{R}$ pour tout $n \geqslant N$ ou $|x_n - y_n| = y_n - x_n > \dfrac{1}{R}$ pour tout $R > 1$, soit $y_n > x_n + \dfrac{1}{R}$ pour tout $n \geqslant N$.

□

Remarque. Si $x \neq 0$, par le lemme, on a soit $\exists N, R > 1,\ x_n > \dfrac{1}{R}$ pour tout $n \geqslant N$ ou $\exists N, R > 1,\ x_n < -\dfrac{1}{R}$ pour tout $n \geqslant N$.

Inverse. En suivant le raisonnement du dessus, dans les deux cas, on pose $y = [(y_n)]$ avec

$$y_n \ = \ \begin{cases} 0 & \text{si } n < N \\ \dfrac{1}{x_n} & \text{si } n \geqslant N. \end{cases}$$

On a $xy = [(x_n y_n)]$ avec

$$(x_n y_n) \ = \ \begin{cases} (0) & \text{si } n < N \\ (1) & \text{si } n \geqslant N \end{cases} \qquad \text{donc} \qquad (1) - (x_n y_n) \ = \ \begin{cases} (1) & \text{si } n < N \\ (0) & \text{si } n \geqslant N, \end{cases}$$

qui est donc négligeable (à partir du rang N). Donc $(x_n y_n) = (1)$ soit $xy = 1$.

Théorème (Convergence monotone). Soit $x = (x_n)_{n\geqslant 1}$ une suite croissante et et majorée. Alors x converge.

Démonstration. Nous avons déjà établi l'équivalence : x est de Cauchy $\iff$ x converge. Ainsi, soit C tel que $\forall n \in \mathbb{N},\ x_n \leqslant C$. Supposons par l'absurde qu'il existe un entier $R \geqslant 1$ et une sous-suite $(x_{n_k})_{k\in\mathbb{N}}$ tel que $|x_{n_k} - x_{n_l}| > \frac{1}{R}$. Si par symétrie on suppose que $l \geqslant k$, on peut enlever les valeurs absolues : $x_{n_k} - x_{n_l} > \frac{1}{R}$. Alors :

$$C \geqslant x_{n_k} > x_{n_{k-1}} + \frac{1}{R} > x_{n_{k-2}} + \frac{2}{R} > \cdots > x_{n_0} + \frac{k}{R}$$

Autrement dit, $k > (C - x_{n_0})R \implies x_{n_k} > x_{n_0} + \frac{k}{R} > C$. Absurde ! Donc la suite est bien convergente.

□

Remarque. L'énoncé symétrique est aussi valable : si une suite est décroissante et minorée, alors elle converge. La démonstration de cet énoncé est laissée en exercice.

3.2 Ordre sur $\mathbb{R}$

Notations. Pour $x, y \in \mathbb{R}$, on note $x < y$ si $\exists N, R > 1,\ \forall n \geqslant N,\ x_n + \dfrac{1}{R} < y_n$ et $x \leqslant y$ si $x = y$ ou $x < y$. Cette ordre est total car trivialement nous pouvons comparer n'importe quels éléments de $\mathbb{R}$ deux à deux.

Définition. La <u>*valeur absolue*</u> de $x \in \mathbb{R}$ est $|x| \coloneqq \max(-x, x)$.

Lemme. Soit $x = [(x_n)]$ de Cauchy. Alors la suite $\big(|x_n|\big)$ est de Cauchy et $|x| = [(|x_n|)]$.

Démonstration. Soit $R > 1$. On a $||x_n| - |x_m|| \leqslant |x_n - x_m| < \dfrac{1}{R}$ pour un certain $N \geqslant 1$ et pour tout $n, m \geqslant N$. Alors

1. $x = -x \iff 2x = 0 \iff x = 0$ car $2 = [(2)] \neq 0$ est inversible. Donc (x_n) est négligeable et $(|x_n|)$ l'est aussi, *i.e.* $[(|x_n|)] = 0 = x = |x|$.
2. $x > -x \implies \exists N, R \geqslant 1,\ x_n > -x_n + \dfrac{1}{R}$ pour tout $n \geqslant N$. Donc $x > -x$ et $|x_n| = x$. D'où, pour $n \geqslant N$, $|x_n| = x_n$. Alors, $(|x_n| - x_n)$ est négligeable et $[(|x_n|)] = [(x_n)] = x = |x|$.
3. Le cas $x < -x$ est exactement le même. Il vient $[(|x_n|)] = |x|$.

□

Proposition. On a donc un plongement de $\mathbb{Q}$ dans $\mathbb{R}$ par l'application

$$\begin{aligned} i\ :\ \mathbb{Q} &\longrightarrow \mathbb{R} \\ \alpha &\longmapsto [\underline{\alpha}] \end{aligned}$$

où $\underline{\alpha}$ est la suite constante égale à α. On a $i(\alpha+\beta) = i(\alpha) + i(\beta)$ et $i(\alpha\beta) = i(\alpha)i(\beta)$ avec i injective et l'on identifie $i(0)$ à l'élément neutre pour la somme et $i(1)$ à l'élément neutre

pour la multiplication. Enfin, i est compatible avec l'ordre, *i.e.* $\alpha \leqslant \beta \iff i(\alpha) \leqslant i(\beta)$.

Démonstration. Montrons que i est injective, et même que $\alpha = \beta \iff i(\alpha) = i(\beta)$. On peut supposer $\alpha \neq \beta$. Alors

1. Si $\alpha < \beta$, on prend $R > 1$ tel que $\beta - \alpha > \dfrac{1}{R}$ et donc $\beta > \alpha + \dfrac{1}{R}$ pour tout $n \in \mathbb{N}$ d'où $i(\alpha) < i(\beta)$.
2. On peut supposer $i(\alpha) < i(\beta)$. Alors $\exists N, R \geqslant 1$ tels que $\alpha + \dfrac{1}{R} < \beta$ pour tout $n \geqslant N$. Alors $\alpha < \beta$.

□

Définition. Une *suite de Cauchy* est une suite $x = (x_n)_{n\in\mathbb{N}}$ telle que

$$\exists N, R \geqslant 1,\ \forall n, m \geqslant N,\quad |x_n - x_m| < i\left(\frac{1}{R}\right).$$

Définition. Une suite $(x_n)_{n\in\mathbb{N}}$ *converge* vers $l \in \mathbb{R}$ si

$$\forall R \geqslant 1,\ \exists N \geqslant 1,\ \forall n \geqslant N,\quad |x_n - x_m| < i\left(\frac{1}{R}\right).$$

Théorème. $\mathbb{Q}$ s'accumule en 0, *i.e.*

$$\forall x \in \mathbb{R}_+^*,\ \exists N \geqslant 1,\quad 0 < \frac{1}{N} < x.$$

Démonstration. Par équivalence, il nous faut montrer que $\mathbb{R}$ est archimédien, *i.e.* $\forall x \in \mathbb{R},\ \exists N \geqslant 1,\ x \leqslant N$.
Soit $x = [(x_n)]$, alors $\exists M \in \mathbb{N},\ |x_n - x_m| < 1$ pour tous $m, n \geqslant M$. On sait qu'il existe $N \geqslant 1,\ x_n + 1 \leqslant N$ pour tout $0 \leqslant n \leqslant M$. Si $n \geqslant M$, $|x_n - x_m| < 1 \Longrightarrow x_n < x_M + 1 < N$.

□

3.3 Propriétés générales sur $\mathbb{R}$

Théorème (Borne supérieure). $\mathbb{R}$ vérifie la propriété de la borne supérieure : soit $E \subseteq \mathbb{R}$ une partie non vide et majorée de $\mathbb{R}$. Alors il *existe* un *unique* $\alpha \in \mathbb{R}$ tel que :

1. $\forall x \in E\ \alpha \geqslant E$
2. $\forall R \geqslant 1,\ \exists x \in E,\ x + \frac{1}{R} > \alpha$

Démonstration. On va définir par récurrence deux suites (α_n) et (β_n) telles que pour tout $n \in \mathbb{N}$:

— $\exists x \in E$ tel que $x \geqslant \alpha_n$
— $\beta_n \geqslant E$
— $\alpha_n \leqslant \alpha_{n+1}$ (α_n croissante)
— $\beta n \geqslant \beta n + 1$ (βn décroissante).

Formalisons la démonstration : soit $a_0 \in E$ et soit $b_0 \in \mathbb{R}$ tel que $b_0 \geqslant E$ (on sous-entend par là que pour tout $x \in E,\ b_0 \geqslant x$). On définit par récurrence :

$$\beta_{n+1} - \alpha_{n+1} \leqslant \frac{\beta_n - \alpha_n}{2} \leqslant \cdots \leqslant \frac{\beta_0 - \alpha_0}{2^{n+1}}$$

Vérifions l'hérédité : on suppose que α_n et β_n sont définis et on définit α_{n+1} et β_{n+1}. Par hypothèse de récurrence, on a

$$[\alpha_n, \frac{\alpha_n + \beta_n}{2}] \cap E \ \neq\ \emptyset.$$

Deux cas de figure sont possibles :

1. $E \cap [\frac{\alpha_n+\beta_n}{2}, \beta_n] = \emptyset$
2. $E \cap [\frac{\alpha_n+\beta_n}{2}, \beta_n] \neq \emptyset$

Pour démontrer l'hérédité, faisons une disjonction de cas sur les deux cas précédents :

1. On prend $\alpha_{n+1} = \alpha_n$ et $\beta_{n+1} = \frac{\alpha_n+\beta n}{2} \leqslant \beta_n$ où on rappelle que $E \leqslant \beta_{n+1}$. Alors $\exists x$ tel que $x \geqslant \alpha_n = \alpha_{n+1}$ et $\beta_{n+1} - \alpha_{n+1} = \frac{\alpha_n+\beta_n}{2}$
2. On prend $\alpha_{n+1} = \frac{\alpha_n+\beta_n}{2}$ et $\beta_{n+1} = \beta_n \geqslant E$ par hypothèse de récurrence. Or $\alpha_{n+1} \geqslant \alpha_n$ donc $\exists x \in E$ tel que $x \geqslant \alpha_{n+1}$. De plus, on vérifie bien que $\beta_{n+1} - \alpha_{n+1} = \frac{\beta_n - \alpha_n}{2}$

La suite (α_n) est croissante et majorée donc elle converge vers une limite qu'on appelle l.
La suite (β_n) est décroissante et minorée donc elle converge vers une limite qu'on appelle l'.
Reste à montrer que $l = l'$. Supposons par l'absurde que ce n'est pas le cas, alors si $|l - l'| \neq 0$, alors il existe $R \in \mathbb{N}^*$ tel que $\frac{1}{R} \leqslant |l - l'|$. Ainsi il existe $N \in \mathbb{N}^*$ tel que :
— $|\alpha_n - l| < \frac{1}{4R}$ pour $n \geqslant N$
— $|\beta_n - l| < \frac{1}{4R}$ pour $n \geqslant N$
— $(\beta_0 - \alpha_0) \times 4R < 2^N$ pour $n \geqslant N$.
Alors :

$$|l - l'| < |\beta_n - l'| + |\alpha_n - \beta_n| + |\alpha_n - l| < \frac{1}{4R} + \frac{\beta_0 - \alpha_0}{2^N} + \frac{1}{4R} < \frac{1}{4R} + \frac{1}{4R} + \frac{1}{4R} = \frac{3}{4R}$$

Ceci amène à une contradiction, donc on a bien que $l = l'$.

□

Lemme. Si $x \in \mathbb{R},\ \exists (x_n) \in \mathbb{Q}^{\mathbb{N}}$ de Cauchy qui converge à x et $x_n \geqslant x$.

Démonstration. Soit $R \geqslant 1$. Il existe un rang n_R tel que $|x - x_{n_R}| < \frac{1}{R}$.
— Si $x_{n_R} \geqslant x$, c'est facile : on pose $y_R \coloneqq x_{n_R}$
— Sinon, on pose $y_R \coloneqq x_{n_R} + \frac{1}{R}$.
Alors $|y_R - x| = |x - (x_{n_r} + \frac{1}{R})| = |x - x_{n_r} - \frac{1}{R}| = \frac{1}{R} - (x - x_{n_R}) < \frac{1}{R}$.
On a donc une suite $(y_R)_{R \geqslant 1}$ telle que $|x - y_R| \leqslant \frac{1}{R} \implies (y_R)$ est de Cauchy et elle converge vers x.

□

Théorème (Densité de $\mathbb{Q}$ dans $\mathbb{R}$). $\mathbb{Q}$ est dense dans $\mathbb{R}$, *i.e.* $\forall x, y \in \mathbb{R}$ avec $x < y,\ \exists \alpha \in \mathbb{Q}$ tel que $x < \alpha < y$.

Démonstration (Densité de $\mathbb{Q}$ dans $\mathbb{R}$). On dégage facilement le cas où $x \in \mathbb{Q}$ ou $y \in \mathbb{Q}$: si $x \in \mathbb{Q}$, on pose $\epsilon = y - x > 0$. Par la propriété archimédienne de $\mathbb{R}$, $\exists R \in \mathbb{N}^*$ tel que $\frac{1}{R} < \epsilon \implies x < \frac{1}{R} + x < y$. Ainsi $x \in \mathbb{Q} \implies x + \frac{1}{R} \in \mathbb{Q}$.
On fait de même si $y \in \mathbb{Q}$: $-y < -x$ (alors $-y \in \mathbb{Q}$) et on applique le cas précédent.
On suppose désormais que $x, y \in \mathbb{Q}$: d'après le lemme précédent, soit (x_n) une suite rationnelle de Cauchy qui converge vers x et telle que $x_n > x$.
$y - x > 0 \implies \exists R \in \mathbb{N}^*$ tel que $\frac{1}{R} > y - x \implies \exists n \in \mathbb{N}^*$ tel que $|x_n - x| = |x - x_n| < \frac{1}{R}$.
On prend $\alpha = x_n \implies x < \alpha < x + \frac{1}{R} < y$.

□

Proposition. Une suite de Cauchy réelle $(u_n)_{n\in\mathbb{N}}$ est bornée.

Démonstration. Fixons $\varepsilon = 1$. Soit $N \in \mathbb{N}$ tel que pour tous $p, q \geqslant N$, $|u_p - u_q| \leqslant 1$. On fixe $q = N$, et alors on a pour tout $n \geqslant N$,

$$|u_n| = |u_n - u_N + u_N| \leqslant 1 + |u_N|.$$

D'autre part, on fixe $M \coloneqq \max(|u_0| + 1, ..., |u_N| + 1)$.
Alors pour tout $n \in \mathbb{N}$ on a $|u_n| \leqslant M$.

□

Théorème (Complétude de $\mathbb{R}$). Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle. Alors (u_n) est convergente si et seulement si (u_n) est de Cauchy.

Démonstration. Soient $\varepsilon > 0$ et (u_n) une suite convergeant vers $\ell \in \mathbb{R}$. Soit $N \in \mathbb{N}$ tel que pour tout $n \geqslant N$, $|u_n - \ell| \leqslant \dfrac{\varepsilon}{2}$.
Soient $p, q \geqslant N$ entiers. Alors

$$|u_p - u_q| \leqslant |u_p - \ell| + |u_q - \ell| \leqslant \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

donc (u_n) est de Cauchy. Réciproquement, soit $\varepsilon > 0$. Alors

$$\exists N \in \mathbb{N},\ \forall p, q \geqslant N, \quad |u_p - u_q| \leqslant \varepsilon.$$

On sait que (u_n) est bornée par la proposition précédente (puisqu'elle est de Cauchy). D'après le théorème de Bolzano-Weierstrass, il existe une sous-suite $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ croissante telle que $(u_{\varphi(n)})$ converge vers ℓ. Montrons que $u_n \longrightarrow \ell$. Soit $n \geqslant N$, alors on a

$$|u_n - \ell| = \left|u_n - u_{\varphi(n)} + u_{\varphi(n)} - \ell\right| \leqslant \left|u_n - u_{\varphi(n)}\right| + \left|u_{\varphi(n)} - \ell\right| \leqslant 2\varepsilon$$

car $\varphi(n) \geqslant n \geqslant N$. Donc (u_n) est convergente.

□

4 Cardinalité

4.1 Généralités sur la cardinalité

Définition (Application injective, application bijective). Soient X et Y deux ensembles. On dit que :
- $|X| \leqslant |Y|$ s'il existe une application injective $f : X \longmapsto Y$
- $|X| = |Y|$ s'il existe une application bijective $f : X \longmapsto Y$

Définition (Ensemble fini). Un ensemble X est *fini* si $\exists n \in \mathbb{N}$ tel que $|X| = |\{x \in \mathbb{N} : x < n\}|$. Ainsi un ensemble qui n'est pas fini est dit *infini*.

Théorème de Russell. Pour tout ensemble X, $|X| \neq |\mathcal{P}(X)|$.

Démonstration. Par l'absurde, soit $f : X \longmapsto \mathcal{P}(X)$ une bijection. On définit $R \coloneqq \{x \in X \ : \ x \notin f(x)\}$. On a bien $R \subset X$. Puisque f est bijective, $\exists r \in X$ tel que $f(r) = R$. A-t-on $r \in R$?
- Si oui : $r \in R = f(r) \implies r \notin R$. Absurde !
- Si non : $r \notin R = f(R) \implies r \in R$. Absurde !

Dans les deux cas on est amené à une contradiction donc c'est l'hypothèse de bijectivité qui est elle-même absurde ! D'où le résultat voulu.

□

Pour aller plus loin, on peut démontrer qu'on a $|X| \leqslant |\mathcal{P}(X)|$, car l'application

$$\begin{aligned} X &\longrightarrow \mathcal{P}(X) \\ x &\longmapsto \{x\} \end{aligned}$$

est injective.

Théorème de Cantor-Bernstein. Soient X et Y deux ensembles. Alors

$$|X| \leqslant |Y| \quad \text{et} \quad |X| \geqslant |Y| \quad \implies \quad |X| = |Y| \,.$$

Démonstration. On suppose qu'il existe $f : X \longrightarrow Y$ et $g : Y \longrightarrow X$ injectives. Alors, $\tilde{f} : X \longrightarrow f(X)$ est bijective, de même que $\tilde{g} : Y \longrightarrow g(Y)$.
Posons

$$B \ = \ \bigcup_{k=0}^{\infty} (g \circ f)^k \big(X \setminus g(Y)\big) \qquad \text{et} \qquad R = X \setminus B.$$

On considère

$$h(x) \ = \ \begin{cases} f(x) & \text{si } x \in B \\ g^{-1}(x) & \text{si } x \in R \end{cases}$$

qui est bijective. Montrons-le.

— Injectivité : soient $x, y \in X$ tels que $h(x) = h(y)$. Montrons que $x = y$. On distingue 3 cas.

1. Si $x, y \in B$:
   alors $h(x) = f(x)$ et $h(y) = f(y)$. Or $h(x) = h(y)$ par hypothèse, soit $f(x) = f(y)$, et par injectivité de f, on en déduit $x = y$.

2. Si $x \in B$ et $y \in R$ (et symétriquement) :
   alors $\exists z \in \big(X \setminus g(Y)\big),\ \exists k \in \mathbb{N},\ x = (g \circ f)^k(z)$. Dans ce cas, on a $h(x) = f(x) = f\big((g \circ f)^k(z)\big)$ et $h(y) = g^{-1}(y)$ soit $y = g \circ h(y)$. Puisque l'on a supposé $h(x) = h(y)$, on a $f\big((g \circ f)^k(z)\big) = g^{-1}(y)$ soit $y = g \circ f\big((g \circ f)^k(z)\big) = (g \circ f)^{k+1}(z)$ d'où l'on tire $y \in B$, ce qui est contradictoire, donc $h(x) \neq h(y)$ lorsque x et y ne sont pas dans les mêmes ensembles.

3. Si $x, y \in R$:
   alors $h(x) = g^{-1}(x)$ et $h(y) = g^{-1}(y)$. De plus, on a $h(x) = h(y)$ soit $g^{-1}(x) = g^{-1}(y)$. Or g^{-1} est bijective, en particulier injective, d'où $x = y$.

— Surjectivité : soit $y \in Y$. Il faut trouver $x \in X$ tel que $h(x) = y$. On distingue 2 cas.

1. Si $g(y) \in B$:
   alors $\exists z \in \big(X \setminus g(Y)\big),\ \exists k \in \mathbb{N},\ (g \circ f)^k(z) = g(y) \in g(Y)$.
   Si $k = 0$, on aurait $g(y) = z \in X \setminus g(Y)$ ce qui est contradictoire.
   Supposons donc $k \geqslant 1$. Alors $g(y) = (g \circ f)^k(z) = g \circ f\big((g \circ f)^{k-1}(z)\big)$ soit $y = f \circ (g \circ f)^{k-1}(z)$ avec $(g \circ f)^{k-1}(z) \in B$. Ainsi, puisque $f(x) = h(x)$ (car $g(y) \in B$), $(g \circ f)^{k-1}(z)$ convient.

2. Si $g(y) \in R$:
   alors $h\big(g(y)\big) = g^{-1}\big(g(y)\big) = y$ donc $x = g(y)$ convient.

□

4.2 Cardinalité des ensembles usuels

Proposition. Soit X un ensemble infini. Alors $|\mathbb{N}| \leqslant |X|$.

Démonstration. Construisons par récurrence une injection $f : \mathbb{N} \longmapsto X$.
Pour $n = 0$: $x \neq \emptyset$ car il est non fini $\implies \exists x_0 \in X$ et on pose $f(0) \coloneqq x_0$.
On suppose $f(n)$ défini. L'application

$$\begin{aligned} \{0, \cdots, n\} &\longrightarrow X \\ i &\longmapsto f(i) \end{aligned}$$

est injective. Si elle était surjective, on aurait $|\{0, \cdots, n\}| = |X| \implies X$ est fini. Absurde !
Donc f n'est pas surjective, *i.e.* $\exists x_{n+1} \in X \setminus f(\{0, \cdots, n\})$.
On pose alors $f(n+1) \coloneqq x_{n+1}$.

□

Remarque. Nous avons en fait démontré que $\mathbb{N}$ est le plus petit ensemble de cardinal infini.

Proposition (Cardinal de $\mathbb{Z}$). On a $|\mathbb{Z}| = |\mathbb{N}|$.

Démonstration. Il suffit de construire une bijection entre les deux ensembles, comme par exemple celle-ci :

$$f(k) \;=\; \begin{cases} \dfrac{k}{2} & \text{si k pair} \\ \dfrac{-k+1}{2} & \text{si k impair.} \end{cases}$$

□

Proposition (Cardinal de $\mathbb{N} \times \mathbb{N}$***).*** On a $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$.

Démonstration. Cette proposition a une démonstration visuelle très intuitive : il suffit de se placer dans le premier quadrant de $\mathbb{R}^2$ et tracer une ligne qui relie tous les points à coordonnées entiers **sans lever le stylo**. On pourra en donner une bijection explicite, que vous pourrez vérifier par vous-même :

$$f : \mathbb{N}^2 \longrightarrow \mathbb{N}$$

$$f(i,j) = \frac{(i+j)(i+j+1)}{2} + j$$

□

Proposition (Cardinal de $\mathbb{Q}$***).*** On a $|\mathbb{Q}| \;=\; |\mathbb{N}|$.

Démonstration. $\mathbb{Q} \simeq \mathbb{Z} \times \mathbb{N}^* \simeq \mathbb{N} \times \mathbb{N}^* \simeq \mathbb{N}$ d'après la proposition précédente

□

Lemme (Écriture d'un nombre en base $N \geqslant 2$***).*** Nous allons utiliser cette décomposition dans la démonstration à suivre, donc démontrons-le dans le cas général pour $N \geqslant 2$. Soit $N \geqslant 2$, alors il existe une suite de nombres (a_i) telle que chaque terme appartient à $[\![0, N-1]\!]$ vérifiant aussi :

$$x = \sum_{i=1}^{\infty} \frac{a_i}{N^i}$$

Démonstration. On construit. cette suite (a_i) par récurrence avec les propriétés suivantes :

1. $x \geqslant \sum\limits_{i=1}^{n} \dfrac{a_i}{N^i}$
2. $x - \sum\limits_{i=1}^{n} \dfrac{a_i}{N^i} \leqslant \dfrac{1}{N^n}$

Prenons $a_1 \coloneqq \lfloor Nx \rfloor \implies \dfrac{a_1}{N} \leqslant x \implies x - \dfrac{a_1}{N} \leqslant \dfrac{1}{N}$.
On suppose avoir défini $a_1 \cdots a_n$ et définissions maintenant a_{n+1}. Pour satisfaire les deux conditions, on pose :

$$y \coloneqq N^n(x - \sum_{i=1}^{n} \frac{a_i}{N^i}) \in [0, 1[$$

On a bien $0 < Ny < N$. Ainsi on définit le terme de la suite comme $a_{n+1} \coloneqq \lfloor Ny \rfloor$

$$a_{n+1} \coloneqq \lfloor Ny \rfloor \implies \frac{a_{n+1}}{N^{n+1}} \leqslant \frac{y}{N^n} = x - \sum_{i=1}^{n} \frac{a_i}{N^i} \implies x \geqslant \sum_{i=1}^{n+1} \frac{a_i}{N^i}.$$

Aussi,

$$\frac{N}{N^{n+1}}(y - \frac{a_{n+1}}{N}) = \frac{Ny - \lfloor Ny \rfloor}{N^{n+1}} < \frac{1}{N^{n+1}},$$

ce qui entraîne l'inégalité suivante :

$$x - \sum_{i=1}^{n+1} \frac{a_i}{N^i} < \frac{1}{N^{n+1}}$$

Donc pour tout $n \in \mathbb{N}$,

$$x \geqslant \sum_{i=1}^{n} \frac{a_i}{N^i} \implies \forall n \in \mathbb{N},\ x - \sum_{i=1}^{n} \frac{a_i}{N^i} < \frac{1}{N^n} \implies x = \sum_{i=1}^{\infty} \frac{a_i}{N^i}.$$

On a bien démontré le résultat souhaité.

□

Théorème (Cardinal de $\mathbb{R}$). On a $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$.

Démonstration. Pour cette démonstration, on va montrer que les deux cardinaux dont il est question sont égaux chacun à $|]0,1[|$.
Montrons d'abord que $|\mathbb{R}| = |]0,1[|$. On construit une bijection entre ces deux ensembles, en se rappelant du fait que la fonction

$$\text{Arctan} : \mathbb{R} \longmapsto]\frac{-\pi}{2}, \frac{\pi}{2}[$$

est bijective. Ainsi, l'application

$$\begin{aligned} \mathbb{R} &\longrightarrow]0,1[\\ x &\longmapsto \frac{1}{2}\left(\frac{2}{\pi}\text{Arctan}(x) + 1\right) \end{aligned}$$

est elle aussi bijective, d'où le fait que $|\mathbb{R}| = |]0,1[|$.
Reste à montrer que $|\mathcal{P}(\mathbb{N})| = |]0,1[|$. Nous allons montrer cette égalité en utilisant le théorème de Cantor-Bernstein.
Montrons d'abord qu'on peut construire une injection de $]0,1[$ dans $\mathcal{P}(\mathbb{N})$:

$$\begin{aligned}]0,1[&\longrightarrow \mathcal{P}(\mathbb{N}) \\ x &\longmapsto S(x) \in \mathbb{N} \end{aligned}$$

Cherchons ce qu'on va prendre pour $S(x)$. On fixe $N \geqslant 2$, alors il existe une suite de nombres $(a_i) \in \mathbb{N}^{\mathbb{N}}$ telle que chaque terme de la suite soit un élément de $[\![0, N-1]\!]$ qui vérifie pour $x \in]0,1[$:

$$x = \sum_{i=1}^{\infty} \frac{a_i}{N^i} = \lim_{N \longrightarrow \infty} \frac{S_n}{N^n}$$

où $S_n = (\sum_{i=1}^{n} \frac{a_i}{N^i}) N^n \in \mathbb{N}$.
De plus, on a que (S_n) est croissante, c'est-à-dire $S_n \leqslant S_{n+1}$.
On peut finalement expliciter $S(x)$: $S(x) \coloneqq \{S_n : n \geqslant 1\} \subset \mathbb{N}$. On a donc bien que $|]0,1[| \leqslant |\mathcal{P}(\mathbb{N})|$.
La dernière étape consiste à construire une injection de $\mathcal{P}(\mathbb{N})$ dans $]0,1[$:
Soit S un sous-ensemble de $\mathbb{N}$. On définit :

$$x_s \coloneqq \sum_{i=0}^{\infty} \frac{\mathbb{1}_S(n)}{10^{n+1}}$$

où on rappelle que $\mathbb{1}_S(n)$ est la fonction indicatrice que vaut 1 si $n \in S$ et 0 sinon.
On remarque aussi que x_S converge. En effet :

$$x_S = \sum_{n=0}^{\infty} \frac{\mathbb{1}_S(n)}{10^{n+1}} \leqslant \sum_{n=0}^{\infty} \frac{1}{10^{n+1}} = \frac{\frac{1}{10}}{1-\frac{1}{10}} = \frac{1}{9}.$$

À présent on considère $\frac{1}{10}\lfloor 10^{n+2}x_s \rfloor - \lfloor 10^{n+1}x_s \rfloor$:

$$10^{n+1}x_s = \sum_{i=0}^{\infty} \frac{\mathbb{1}_S(i)}{10^{i+1}} 10^{n+1} = \sum_{i=0}^{n} \mathbb{1}_S(i)10^{n+1} + \sum_{i=n+1}^{\infty} \frac{\mathbb{1}_S(i)}{10^{i-n}}$$

où on remarque que la première somme de cette dernière étape est un entier naturel et que la deuxième somme est un réel positif strictement inférieur à 1. Ainsi :

$$\frac{1}{10}\lfloor 10^{n+2}x_s \rfloor - \lfloor 10^{n+1}x_s \rfloor = \frac{1}{10}\sum_{i=0}^{n+1} \mathbb{1}_S(i)10^{n+1-i} - \sum_{i=0}^{n} \mathbb{1}_s(i)10^{n-i} = \frac{\mathbb{1}_S(n+1)}{10}$$

$$\implies \mathbb{1}_S(n) = \lfloor 10^{n+1}x_S \rfloor - 10\lfloor 10^n x_S \rfloor, \quad \forall n \in \mathbb{N}$$

Nous avons alors construit une injection de $\mathcal{P}(\mathbb{N})$ dans $]0,1[$, d'où l'implication

$$|\mathcal{P}(\mathbb{N})| \leqslant |]0,1[| \implies |\mathcal{P}(\mathbb{N})| \leqslant |\mathbb{R}|.$$

On conclut alors par le théorème de Cantor-Bernstein que $|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$.

□

5 Algèbre commutative

Dans cette section, nous allons toujours prendre A un anneau commutatif et $\mathfrak{a}$, $\mathfrak{b}$ deux idéaux de A.

5.1 Définitions et théorie élémentaires

On vous renvoie aux sous-paragraphes 1.2.3 et 1.2.4 de ce polycopié pour reprendre les définitions de base sur la théorie des anneaux et sur la théorie des corps.

Définition. Un élément $a \in A$ est un *diviseur de 0* s'il existe $b \neq 0$ tel que $ab = 0$.

Définition. Un élément $a \in A$ est dit *régulier* s'il n'est pas diviseur de 0.

Proposition. Si un élément $a \in A$ est inversible, alors il est régulier.

Démonstration. On veut montrer que pour $a, b \in A$, si a est inversible alors $ab = 0 \implies b = 0$. On part de $ab = 0$. Or, a est inversible donc il existe $a^{-1} \in A$ tel que $aa^{-1} = 1$ d'où $a^{-1}(ab) = 0$. Or, dans un anneau, il y a associativité donc $(a^{-1}a)b = 0$ soit $1 \times b = 0$ donc $b = 0$ et a est régulier.

□

Définition Un anneau est *intègre* si et seulement si tout ses éléments non nuls sont réguliers.

Exemples. $\mathbb{Z}/n\mathbb{Z}$ si n n'est pas premier n'est pas intègre car on peut trouver un couple (a, b) tel que $ab = n = \dot{0}$ alors que a et b sont non nuls. De même, on peut trouver des exemples de matrices $n \times n$ telles que leur produit vaut la matrice nulle. En revanche, l'anneau $(\mathbb{Z}, +, \times)$ est évidemment intègre.

Remarque. Une autre manière de voir l'intégrité d'un anneau est de dire que tous ses éléments non nuls sont réguliers.

Proposition (Idéaux d'un corps). $\mathbb{K}$ est un corps $\iff$ ses seuls idéaux sont $\{0\}$ et $\mathbb{K}$

Démonstration.

- Pour le sens direct, soit $\mathfrak{a} \subseteq \mathbb{K}$ un idéal non nul de $\mathbb{K}$.
  $\mathfrak{a} \neq \emptyset \implies \exists a \in \mathfrak{a}$ tel que $a \neq 0 \implies \exists a \in \mathfrak{a}$ tel que $a \in A^\times$
  $\implies 1 = a^{-1} \cdot a \in \mathfrak{a} \implies \mathfrak{a} = A$ d'après le lemme précédent.
- Pour le sens réciproque, soit $a \in A \backslash \{0\}$. Prenons $\mathfrak{a} = aA \neq 0$, en vérifiant qu'on a bien $a \in \mathfrak{a}$ car on peut décomposer a comme $a = a \cdot 1$ avec $1 \in A$. L'idéal $\mathfrak{a}$ étant non nul, alors par hypothèse $\mathfrak{a} = A$. En particulier, $1 \in \mathfrak{a}$, ainsi il existe $b \in A$ tel que $ab = 1$, *i.e.* a est inversible. Tout élément non nul étant inversible, on conclut que $\mathbb{K}$ est un corps.

□

5.2 Théorie des anneaux : approfondissements

Définition (Idéal premier). Un idéal $\mathfrak{a} \subset A$ d'un anneau est *premier* si :

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

Définition (Idéal maximal). Un idéal $\mathfrak{a} \subset A$ d'un anneau tel que $\mathfrak{a} \neq A$ est *maximal* si pour tout idéal $\mathfrak{b}$ de A :

$$\mathfrak{a} \subseteq \mathfrak{b} \subseteq A \implies \mathfrak{b} = \mathfrak{a} \text{ ou } \mathfrak{b} = A$$

Exemple. L'idéal $n\mathbb{Z}$ est maximal si et seulement si n est premier.

Définition (Opérations sur les idéaux). On définit les opérations suivants :
- $\mathfrak{a} + \mathfrak{b} = \{a + b : a \in \mathfrak{a} \text{ et } b \in \mathfrak{b}\}$
- $\mathfrak{a} \cdot \mathfrak{b} = \{a_1 b_1 + \cdots + a_n b_n : \forall i \in [\![1, n]\!]\ ,\ a_i \in \mathfrak{a} \text{ et } b_i \in \mathfrak{b}\}$
- $\mathfrak{a} \cap \mathfrak{b}$ est le plus petit idéal qui est contenu par $\mathfrak{a}$ et $\mathfrak{b}$

Exemple. Revenons au cas simple de $\mathbb{Z}$ et regardons ce que ça nous donne : soit $a, b \in \mathbb{Z}$:
- $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, où $d = \text{pgcd}(a, b)$
- $a\mathbb{Z} \cdot b\mathbb{Z} = ab\mathbb{Z}$
- $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$, où $m = \text{ppcm}(a, b)$

Définition (Idéaux étrangers). Deux idéaux $\mathfrak{a}, \mathfrak{b} \in A$ sont *étrangers* si $\mathfrak{a}+\mathfrak{b} = A$. Autrement dit, il faut que :

$$\exists a \in \mathfrak{a} \text{ et } \exists b \in \mathfrak{b} \text{ tel que } a + b = 1$$

Exemple. Les idéaux étrangers dans $\mathbb{Z}$ sont exactement $n\mathbb{Z}$ et $m\mathbb{Z}$ tels que $n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$. Ceci équivaut à dire que $\text{pgcd}(n, m) = 1$.

Exemple. Étant donné un anneau commutatif A quelconque, on peut construire des idéaux étrangers. Soient $a, c \in A$, et définissons un troisième élément $b := 1 - ac$. On prend les deux idéaux suivants : $\mathfrak{a} := aA$ et $\mathfrak{b} := bA$. Alors on vérifie facilement que $\mathfrak{a}$ et $\mathfrak{b}$ sont étrangers puisque $1 = ac + b \times 1$, où $ac \in \mathfrak{a}$ et $b \times 1 \in \mathfrak{b}$.

Définition (Divisibilité). Pour $a, b \in A$, on dit que b *divise* a et on note $b \mid a$ si et seulement si il existe $c \in A$ tel que $a = bc$.

Proposition (Unicité du quotient). Si A est intègre, alors le quotient c est unique.

Démonstration. Supposons qu'il existe deux quotients c, c' tels que $a = bc = bc'$. Alors $b(c - c') = 0$ donc par régularité de b, on a $c = c'$.

□

Proposition (Divisibilité en termes d'idéaux). Pour $a, b \in A$ anneau commutatif intègre avec $a \neq 0$, on définit les idéaux $\mathfrak{a} = aA$ et $\mathfrak{b} = bA$. Alors $b \mid a \iff \mathfrak{a} \subset \mathfrak{b}$.

Démonstration.

— $b \mid a \implies \exists c \in A$ tel que $a = bc \in \mathfrak{b} \implies \forall d \in A, ad = abc = b(ac) \in \mathfrak{b}$
$\implies aA \subset bA \implies \mathfrak{a} \subset \mathfrak{b}$.

— $aA \subset bA \implies a \in bA \implies \exists c \in A$ tel que $a = bc$.

□

Corollaire. On a de manière évidente que : $a \mid b$ et $b \mid a \iff aA = bA$.

Définition (Éléments associés). $a, b \in A$ sont *associés* si $\exists u \in A^\times$ tel que $a = ub$.

Proposition. Si A est un anneau commutatif intègre, alors a et b sont associés si et seulement si $aA = bA$.

Démonstration. Dire que a et b sont associés équivaut à dire que $a|b$ et $b|a$ puisque l'élément u est inversible d'où on peut construire une autre égalité exprimant b en fonction de a (c'est $b = u^{-1}a$). Le corollaire précédent nous donne immédiatement que ceci équivaut à $aA = bA$.

□

Définition (Élément premier). $a \in A$ est *premier* si l'idéal $\mathfrak{a} \coloneqq aA$ est premier : $a \mid bc \implies a \mid b$ ou $a \mid c$

Définition (Élément irréductible). $a \in A$ est *irréductible* si

$$a \mid bc \implies \begin{cases} b \in A^\times \\ c \in A^\times \end{cases} \quad \text{ou} \quad d \mid a \implies \begin{cases} d \in A^\times \\ d \text{ est associé à } a \end{cases}$$

Exemple. Élément irréductible et non premier :

$$A \coloneqq \mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\} \text{ et } B \coloneqq \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$$

On a $A \subset B$. L'élément 2 est irréductible mais pas premier puisque

$$2 \mid 4 = (\sqrt{5}+1) \cdot (\sqrt{5}-1)$$

A et B sont des anneaux et en plus B est principal.

Proposition. Soit A un anneau principal et $a \in A$ non nul. On pose $\mathfrak{a} = aA$. Sont équivalentes :

1. $\mathfrak{a}$ est maximal (*i.e.* si $\exists \mathfrak{b}$ un idéal tel que $\mathfrak{a} \subset \mathfrak{b} \subset A$, alors $\mathfrak{b} = \mathfrak{a}$ ou $\mathfrak{b} = A$)
2. $\mathfrak{a}$ est premier
3. a est premier
4. a est irréductible

Démonstration.

1. $1 \implies 2$: Vrai car $\begin{cases} \mathfrak{a} \text{ premier} \iff A/\mathfrak{a} \text{ intègre} \\ \mathfrak{a} \text{ maximal} \iff A/\mathfrak{a} \text{ corps} \end{cases}$
2. $2 \implies 3$: Par définition
3. $3 \implies 4$: Soit a premier, montrons que a est irréductible. Décomposons $a = bc \implies a \mid b$ ou $a \mid c$. Quitte à permuter b et c, on se réduit au cas $a \mid b$. Si $a \mid b$, alors b s'écrit $b = au$. Ainsi $a = bc = auc = a(1 - uc) = 0 \implies 1 - uc = 0$ par intégrité de A.
   Ainsi $uc = 1$ donc c est inversible.
4. $4 \implies 1$: En exercice.

□

Définition (Anneau quotient). Soit A un anneau et I un idéal. Alors :

$$A/I \coloneqq \{a + I \mid a \in A\}$$

est un anneau. On définit ainsi la classe de a comme :

$$[a] \coloneqq \{a + b \mid b \in I\}$$

Comme pour les groupes quotients, on peut y définir deux opérations :
— Une somme : $[a] + [b] = [a + b]$ qui est bien définie car I est un sous-groupe de A
— Un produit : $[a] \cdot [b] = [a \cdot b]$ qui est bien définie car I est un idéal
Finalement on peut définir un projecteur sur l'anneau quotient, dite projection canonique :

$$\begin{aligned} \pi \ : \ A &\longrightarrow A/I \\ a &\longmapsto [a] \end{aligned}$$

Exemples. Ramenons-nous comme d'habitude au cas de $\mathbb{Z}$
— $\mathbb{Z}/n\mathbb{Z}$ est un anneau fini de cardinal n
— $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre car $[2], [3] \neq 0$ alors que $[2] \cdot [3] = 0$
— $\mathbb{Z}/4\mathbb{Z}$ non plus, car $[2]^2 = 0$

Proposition (Propriétés des homomorphismes d'anneaux). Soit $f : A \longmapsto B$ un homomorphisme d'anneaux. Alors :

1. $\mathrm{Ker}(f)$ est un idéal de A
2. $\mathrm{Im}(f)$ est un sous-anneau de B
3. $A/\mathrm{Ker}(f) \simeq \mathrm{Im}(f)$

4. Il y a une bijection entre les idéaux de A contenant $\mathrm{Ker}(f)$ et les idéaux de $\mathrm{Im}(f)$.

Démonstration.

1. $\mathrm{Ker}(f)$ est un sous-groupe de A par rapport à la somme. D'où
$$\forall a \in \mathrm{Ker}(f),\ \forall b \in A,\ f(ab) = f(a)f(b) = 0 \implies f(b) = 0$$
Ainsi $ab \in \mathrm{Ker}(f)$ donc $\mathrm{Ker}(f)$ est bien un idéal de A.
2. Soient $u = f(a),\ v = f(b) \in \mathrm{Im}(f)$. On a aussi $1 = f(1) \in \mathrm{Im}(f)$. Alors :
— $u + v = f(a) + f(b) = f(a + b) \in \mathrm{Im}(f)$
— $u \cdot v = f(a) \cdot f(b) = f(ab) \in \mathrm{Im}(f)$
— $-u = -f(a) = f(-a) \in \mathrm{Im}(f)$
Donc $\mathrm{Im}(f)$ est un sous-anneau de B.
3. En notant $\pi : A \longrightarrow A/\mathrm{Ker}(\pi)$ la projection canonique, il faut montrer l'existence d'une unique fonction g telle que $\forall a \in A,\ f(a) = g \circ \pi(a)$. Or ceci a déjà faite pour les groupes. Reste à montrer que g est un morphisme d'anneaux. On pose $g([a]) \coloneqq f(a)$. Alors $g([1]) = 1$ et
$$f(ab) = g([ab]) = g([a] \cdot [b]) = f(a) \cdot f(b)$$
Ainsi $g([a] \cdot [b]) = g([a]) \cdot g([b])$ et g est donc un morphisme d'anneaux.
4. Admis.

□

Proposition. Soit $\mathfrak{a} \subset A$ un idéal. Alors

1. $\mathfrak{a}$ premier $\iff$ $A/\mathfrak{a}$ est intègre
2. $\mathfrak{a}$ maximal $\iff$ $A/\mathfrak{a}$ est un corps

En particulier, idéal maximal implique idéal premier.

Démonstration. Remarquons d'abord que pour $f : A \longrightarrow A/\mathfrak{a}$, on a $\mathrm{Ker}(f) = \mathfrak{a}$.

1. $a, b \in \mathfrak{a} \iff [ab] = 0 \iff [a] \cdot [b] = 0 \iff [a] = 0$ ou $[b] = 0$
2. Pour le sens direct, on remarque que A intègre équivaut au fait que l'idéal 0 est premier. Le sens réciproque est laissé au lecteur.

□

5.3 Polynômes : une brève introduction

Soit A un anneau. On définit $A[X] \coloneqq \{f : a_0 + a_1X + \cdots + a_nX^n : a_i \in A\}$.

> ***Définition (A-algèbre).*** Une *A-algèbre* est un anneau B muni d'un homomorphisme d'anneau $A \longrightarrow B$.

On a envie de construire le couple $(\mathcal{P}_A, X)$ des polynômes sur un anneau à une variable vérifiant pour $X \in \mathcal{P}_A$, $\forall b \in B$ avec A, B des anneaux l'existence d'une unique fonction $f : \mathcal{P}_A \longrightarrow B$ telle que $f(x) = b$. Pour ceci, on pose les définitions suivantes :
— $A^{\mathbb{N}} \coloneqq \{(a_i)_{i \geq 0}\ :\ a_i \in A\}$
— $A_0^{\mathbb{N}} \coloneqq \{(a_i) \in A^{\mathbb{N}}\ :\ \exists n \in \mathbb{N} \text{ tel que } \forall i > n,\ a_i = 0\}$
On a bien $A_0^{\mathbb{N}} \subset A^{\mathbb{N}}$. Dans $A_{\mathbb{N}}$, si $f(n) = 0$ pour tout n assez grand, alors le *support de f*, que l'on note $\mathrm{Supp}(f)$, est fini, où

$$\mathrm{Supp}(f) \coloneqq \{n \in \mathbb{N} \text{ tel que } f(n) \neq 0\}$$

Finalement, $A_0^{\mathbb{N}}$ possède une structure naturelle de groupe abélien. Notons les éléments suivants (qui vont être ceux qui forment la base canonique de notre espace) :

— $e_0 = 1 \coloneqq (1, 0, 0, \ldots)$
— $e_1 = X \coloneqq (0, 1, 0, 0, \ldots)$
— $e_2 = X^2 \coloneqq (0, 0, 1, 0, 0, \ldots)$

où plus généralement la fonction $e_n : \mathbb{N} \longrightarrow A$ est telle que :

$$\begin{cases} e_n(m) = 1 \text{ si } n = m \\ e_n(m) = 0 \text{ sinon} \end{cases}$$

Ainsi $e_n = X^n$. Tout élément $f \neq 0$ de $A_0^{\mathbb{N}}$ s'écrit de manière unique comme

$$f = a_0 e_0 + a_1 e_1 + \cdots a_n e_n$$

avec $n \coloneqq \deg(f)$ et $n, a_0, a_1, \ldots, a_n$ uniques. D'où provient l'écriture $f = a_0 + a_1 X + \cdots a_n X^n$

Soit B un A-algèbre et $b \in B$. On peut <u>évaluer</u> le polynôme en b en faisant :

$$\begin{aligned} ev_b \ : \ A[X] &\longrightarrow B \\ f &\longmapsto f(b) = a_0 + a_1 b + \cdots a_n b^n. \end{aligned}$$

En prenant $A[X] = A_0^{\mathbb{N}}$, on peut construire un homomorphisme d'anneau

$$\begin{aligned} A &\longrightarrow A[X] \\ a &\longmapsto (a, 0, 0, 0, ...) \end{aligned}$$

injectif par construction.

Définition. a_n est le <u>*coefficient dominant*</u>. Si $a_n = 1$, alors f est <u>*unitaire*</u>.

Proposition (Propriétés du degré) (admis). Soient $f, g \in A[X]$. Alors :

— $\deg(f + g) \leq \max(\deg(f), \deg(g))$
— $\deg(f + g) = \max(\deg(f), \deg(g))$ si $\deg(f) \neq \deg(g)$
— $\deg(fg) \leq \deg(f) + \deg(g)$

Proposition (Division euclidienne des polynômes). Soit A un anneau et $f, g \in A[X]$ avec $f \neq 0$ et avec un coefficient dominant inversible. Alors il existe $q, r \in A[X]$ avec $\deg(r) < \deg(f)$ tels que $g = qf + r$

Démonstration. Par récurrence sur $\deg(g)$. Supposons sans perte de généralité que $\deg(g) < \deg(f)$

— Initialisation : si $q = 0$ et $r = g$, alors $g = qf + r$
— soit $n \geq \deg(f)$. On suppose la propriété vraie pour h avec $\deg(h) < n$. Montrons que c'est vraie pour $\deg(g) = n$.

$$g = b_0 + b_1 X + \cdots + b_n X^n$$

$$f = a_0 + a_1 X + \cdots a_d X^d$$

On a $n \geq d$, et on remarque que $X^n = X^{d+n-d}$. On considère alors

$$g - a_d^{-1} b_n X^{n-d} f = b_n X^n + \cdots - b_n X^n + \cdots$$

Le degré du polynôme écrit au-dessus est de degré strictement inférieur à n, ainsi on peut l'écrire de la forme

$$g - a_d^{-1} b_n X^{n-d} f = qf + r$$

pour certains $q, r \in A[X]$. Donc $g = (q + a_d^{-1} b X^{n-d}) f + r$.

□

Proposition. Si $\mathbb{K}$ est un corps, alors $\mathbb{K}[X]$ est principal.

Démonstration. Soit $\mathbb{K}[X]$ intègre. Pour un idéal $\mathfrak{a} \subset \mathbb{K}[X]$, a-t-on que $\mathfrak{a}$ est monogène ?

— Si $\mathfrak{a} = 0$, évident

— Si $\mathfrak{a} \neq 0$, il existe $f \neq 0$ tel que $f \in \mathfrak{a}$ de degré minimal. On a facilement que $f\mathbb{K}[X] \subset \mathfrak{a}$. Montrons l'inclusion réciproque. Soit $g \in \mathfrak{a}$, alors $g = qf + r$ avec $\deg(r) < \deg(f)$. Or $r = g - qf \in \mathfrak{a}$ donc $r \neq 0$. Ceci est absurde par minimalité, donc $r = 0$.

□

Proposition. Si $\mathbb{K}[X]$ est principal, alors $\mathbb{K}$ est un corps.

Démonstration. On sait déjà que $\mathbb{K}[X]$ principal $\implies$ $\mathbb{K}[X]$intègre $\implies$ $\mathbb{K}$ intègre. De plus, en considérant l'homomorphisme d'anneaux suivant :

$$\begin{aligned} ev_0 \ : \ \mathbb{K} &\longrightarrow \mathbb{K} \\ f &\longmapsto f(0). \end{aligned}$$

on déduit que $\mathbb{K} \simeq \mathbb{K}[X]/\mathrm{Ker}(f)$. Or $X \in \mathrm{Ker}(\mathrm{ev})_0$ est premier et non-nul $\implies$ $\mathrm{Ker}(\mathrm{ev}_0)$ maximal $\implies$ $\mathbb{K}[X]/\mathrm{Ker}(f)$ est un corps $\implies$ $\mathbb{K}$ est un corps.

□

On terminera ce chapitre avec une considération sur les extensions de corps. Soient K un corps et L un extension de K. En particulier, L est un $K-$espace vectoriel. Soit $x \in L$. On définit alors l'application suivante :

$$\begin{aligned} ev_n \ : \ K[X] &\longrightarrow L \\ f &\longmapsto f(x). \end{aligned}$$

Alors $\mathrm{Im}(\mathrm{ev}_n) = K[X] \subset L$ est un sous-anneau.

1. $K[X]$ est la plus petite sous-K-algèbre de L contenant x
2. $\mathrm{Ker}(\mathrm{ev}_n) = fK[X]$
   — Si $\mathrm{Ker}(\mathrm{ev}_n) \neq 0$, on dit que x est <u>algébrique</u>
   — Sinon, on dit que x est <u>transcendant</u>
3. Soit x algébrique. Alors $K[X]$ est un corps de base $(1, x, \ldots, x^{\deg(f)-1})$

Nous allons revoir les notions de nombres algébriques et transcendants dans le chapitre suivant.

Exemple (Construction de $\mathbb{C}$). Dans $\mathbb{R}[X]$, le polynôme $X^2 + 1$ est irréductible.
On pose alors $\mathbb{C} \coloneqq \mathbb{R}[X]/(X^2 + 1)\mathbb{R}[X]$. On a alors $[X] = i$ et $[X]^2 = [X^2] = [-1] = -1$. Ainsi une base de $\mathbb{C}$ est $(1, i)$.

5.4 Corps intermédiaires entre $\mathbb{Q}$ et $\mathbb{R}$

L'idée est la suivante : pour $\alpha \in \mathbb{R}$, on veut construire un corps $\mathbb{Q}[\alpha]$ tel que $\mathbb{Q} \subset \mathbb{Q}[\alpha] \subset \mathbb{R}$, c'est-à-dire le plus petit corps contenant à la fois α et $\mathbb{Q}$.
Soient L, F des corps et $K \subset L$ un sous-corps de L. Soit $\alpha \in L$. On a envie de construire $K(\alpha)$, par exemple :

$$K(\alpha) = \bigcap_{K \subset F \subset L \text{ et } \alpha \in F} F.$$

Remarque (Homomorphisme de corps). Tout homomorphisme de corps est injectif. Ceci provient du fait que le noyau d'un homomorphisme de corps est un idéal, or les seuls idéaux d'un corps sont (0) et lui-même. Le noyau doit nécessairement être égal à (0) puisque par définition le neutre multiplicatif est envoyé sur lui-même.

Reprenons dans un premier temps l'application "évaluation" de `5.4` qu'on avait noté ev_b, en remplaçant ici b par α pour être plus cohérent avec les notations.

Regardons à présent $\text{Ker}(\text{ev}_\alpha)$:
on note $\text{Ann}_K(\alpha) = \{f \in K[X] : f(\alpha) = 0\}$ les polynômes qui s'annulent en α.
Si $\text{Ann}_K(\alpha) = 0$, alors α est transcendant. Dans ce cas :

$$a_0 + a_1\alpha + \cdots a_n\alpha^n = 0 \implies a_0 = a_1 = \cdots = a_n = 0$$

Ainsi, si α est transcendant, alors $\text{Im}(\text{ev}_\alpha) \simeq K[X]$ et donc $K[\alpha]$ n'est pas un corps. Raté !

Exemple. Pour $L = \mathbb{R}$, $K = \mathbb{Q}$ et $\alpha = \pi$

On s'assure bien du fait que $\text{Ann}_{\mathbb{Q}}(\alpha) = \{f : f(\pi) = 0\}$ et on retrouve que π est transcendant.

On s'intéresse à présent au cas où $\text{Ann}_K(\alpha) \neq 0 \iff \alpha$ algébrique $\iff \exists f \in K[X]$ non nul tel que $f(\alpha) = 0$

Notation. Pour L un corps, $K \subset L$ un sous-corps et $\alpha \in L$:
— L possède une structure naturelle de $K-$espace vectoriel
— $K(\alpha)$ aussi
On note le *degré* de l'extension $\dim_K L = [L : K]$, c'est-à-dire la dimension de L comme $K-$espace vectoriel. De plus, on dit que L est une *extension finie* de K si $[L : K] < +\infty$

Supposons désormais α algébrique. Alors $\text{Ker}(\text{ev}_\alpha) = \text{Ann}_K(\alpha) \neq 0$ est un idéal de $K[X]$ qui est principal. Ainsi l'annulateur s'écrit de la forme $\text{Ann}_K(\alpha) = f \cdot K[X]$ avec $f \in K[X]$. Ce f est un générateur, et il n'en existe qu'une qui est unitaire. On l'appelle le polynôme minimal et on le note $f_{\min}$.

Exemple. Pour $\alpha = \sqrt{2}$, le polynôme minimal est $X^2 - 2$.

Regardons dans un deuxième temps $\text{Im}(\text{ev}_\alpha)$:
Considérons $K[\alpha] \subset L$ en posant

$$K[\alpha] \coloneqq \text{Im}(\text{ev}_\alpha) = \{a_0 + a_1\alpha + \ldots + a_n\alpha^n \mid n \in \mathbb{N} \text{ et } a_0, \ldots, a_n \in K\}$$

En remarquant que $K[\alpha] \subset K(\alpha)$ (tel qu'on la défini au début de cette section), on veut montrer qu'en fait $K[\alpha] = K(\alpha)$.

Théorème.

1. $f_{\min}$ est irréductible dans $K[X]$
2. $K[\alpha] = K(\alpha)$
3. En posant $d \coloneqq \deg(f_{\min})$, les éléments $1, \alpha, \dots, \alpha^{d-1}$ forment une K-base de l'espace $K(\alpha)$. Ceci implique en particulier que $[K(\alpha) : K] = \deg(f_{\min})$.

Démonstration. $\mathrm{Ann}_K(\alpha) = \mathrm{Ker}(\mathrm{ev}_\alpha) = f_{\min} \cdot K[X]$ et $\Im(\mathrm{ev}_\alpha) = K[\alpha] \subset L$. De plus, comme L est intègre, $K[\alpha]$ est aussi intègre.
Le premier théorème d'isomorphisme nous donne $K[\alpha] \simeq K[X]/\mathrm{Ann}_K(\alpha)$. Ceci implique :

$$\mathrm{Ann}_K(\alpha) \text{ est premier et non nul} \implies \mathrm{Ann}_K(\alpha) \text{ maximal} \implies K[\alpha] \text{ est un corps}$$

On déduit alors que $K[\alpha] = K(\alpha)$.
En notant $f_{\min} = a_0 + a_1 X + \cdots + a_d X^d$ avec $d = \deg(f_{\min})$ et en écrivant $\beta = u_0 + u_1\alpha + \cdots + u_n\alpha^n \in K[\alpha]$, on peut écrire $\beta = g(\alpha)$ pour g de la forme $g = u_0 + u_1 X + \cdots u_n X^n$.
On effectue la division euclidienne de g par $f_{\min}$: $g = q \cdot f_{\min} + r$, où $\deg(r) < \deg(f_{\min})$.
Alors le polynôme r s'écrit de la forme $v_0 + v_1 X + \cdots v_{d-1} X^{d-1}$.
Ainsi $\beta = g(\alpha) = q(\alpha) \cdot \underbrace{f_{\min}(\alpha)}_{=0} + r(\alpha) = v_0 + v_1\alpha + \cdots + v_{d-1}\alpha^{d-1}$.
En considérant $v_0 + v_1\alpha + \cdots + v_{d-1}\alpha^{d-1} = 0 \iff g(\alpha) = 0 \implies g \in \mathrm{Ann}_K(\alpha) \iff f_{\min} \mid g \implies \begin{cases} g = 0 \text{ ou} \\ \deg(g) \geq \deg(f_{\min}) \end{cases}$
La deuxième condition étant impossible, alors nécessairement $g = 0$.

□

Remarque. Pour un polynôme $f \in K[X]$, si $\deg(f) > 1$ et f irréductible, alors f n'a pas de racines dans K. Attention ! La réciproque est FAUSSE.
Par contre, en se restreignant, on a l'équivalence suivante pour $f \in K[X]$, $\deg(f) \leq 3$ et f irréductible $\iff$ f n'a pas de racines dans K

Exemple. $\mathbb{Z}$ de manière évidente, ou encore $\mathfrak{a} = a\mathbb{Z}$ pour $a \geq 0$

6 Théorie sur les polynômes

6.1 Nombres algébriques, transcendants et irrationnels

Définition. Soit $\alpha \in \mathbb{C}$. On dit que

1. α est *algébrique* s'il existe $P \in \mathbb{Q}[z]$ non nul tel que $P(\alpha) = 0$,
2. α est *transcendant* s'il n'est pas algébrique,
3. α est *irrationnel* si $\alpha \in \mathbb{R} \setminus \mathbb{Q}$.

Exemple. Pour $\sqrt{2}$, on a $f(x) \coloneqq x^2 - 2$ continue, croissante et telle que $f(0) < 0$ et $f(2) > 0$, donc d'après le théorème des valeurs intermédiaires, il existe un unique $\alpha > 0$ tel que $f(\alpha) = 0$; on l'appelle précisément $\sqrt{2}$.

Définition. Le *polynôme minimal* P_α de $\alpha \in \mathbb{C}$ algébrique est l'unique générateur de l'idéal $I_\alpha \coloneqq \{P \in \mathbb{Q}[X],\ P(\alpha) = 0\}$. De plus, on a naturellement $deg(\alpha) = deg(P_\alpha)$.

Théorème. On a $|\{\alpha \in \mathbb{C},\ \alpha \text{ algébrique}\}| = |\mathbb{N}|$.

Démonstration. Il suffit de montrer que les nombres algébriques sont dénombrables. Pour $Q \in \mathbb{Q}[X]$, on note $E_Q = \{x \in \mathbb{C} : Q(x) = 0\}$ l'ensemble des racine de ce polynôme. On pose les nombres algébriques $\mathcal{A} \coloneqq \bigcup_{Q \in \mathbb{Q}[X], Q \neq 0} E_Q$. Ensuite on décompose $\mathcal{A}$ selon le degré de Q :

$$\mathcal{A} = \bigcup_{n \in \mathbb{N}} \bigcup_{Q \in \mathbb{Q}_n[X]} E_Q$$

Dans un premier temps, on s'assure que $\forall Q \in \mathbb{Q}[X], |E_Q| \leq n$, donc E_Q est fini. Ensuite :

$$\mathbb{Q}_n[X] \simeq \mathbb{Q}^* \times \underbrace{\mathbb{Q} \times \cdots \times \mathbb{Q}}_{n \text{ fois}}$$

parce qu'un polynôme de degré n a $n+1$ coefficients, dont un qui est non nul (le coefficient dominant). Ainsi, comme $\mathbb{Q}$ et $\mathbb{Q}^*$ sont dénombrables, $\mathbb{Q}_n[X]$ est dénombrable. Comme union dénombrable d'ensembles finis, on conclut que $\mathcal{A}$ est dénombrable.

□

Théorème (admis). Soient K un corps et $F, G \in K[X]$ avec $G \neq 0$. Alors il existe un unique couple (Q, R) de polynômes de $K[X]$ tels que $F = QG + R$ où $deg(R) < deg(Q)$, avec comme convention que $deg(0) = -\infty$.

Exemple. Pour la division euclidienne de $2X^3 + +1$ par $X^2 + 1$, on écrit

$$\begin{array}{rl|l} 2X^3 & +X+1 & X^2+1 \\ \cline{3-3} -2X^3 & -2X & 2X \\ \cline{1-2} & -X+1 & \end{array}$$

donc on a $\underbrace{2X^3+X+1}_{F} = \underbrace{2X}_{Q}\underbrace{(X^2+1)}_{G} + \underbrace{(-X+1)}_{R}$.

Corollaire. Tout idéal de $K[X]$ est principal, *i.e.* pour tout idéal I, il existe $F \in K[X]$ tel que $I = \{PF,\ P \in K[X]\}$.

Démonstration. Si I est nul, c'est trivial car on prend $F = 0$. Sinon, il existe $G \in I\{0\}$ de degré minimal. Pour $F \in I$, on peut faire sa division euclidienne et alors $F = GQ + R$ avec $deg(R) < deg(G)$. On a donc $R = F - GQ \in I$ car $F, G \in I$ et $GQ \in I$ par propriété d'absorbance de l'idéal.
De plus, G est de degré minimal donc nécessairement $R = 0$.

□

Corollaire. Soient K un corps et $F \in K[X] \setminus \{0\}$ tel que $deg(F) = d$. Alors, on a $|\{\alpha \in K,\ F(\alpha) = 0\}| \leqslant d$.

Démonstration (par récurrence sur d). Si $d = 0$, on a $F = c \in K \setminus \{0\}$ donc $F(\alpha) = c \neq 0$ pour tout $\alpha \in K$. Si $d \geqslant 1$, soit $\alpha \in K$ une racine (s'il n'y en a pas, il n'y a rien à montrer) de F. Alors on peut écrire $F = Q(x-\alpha) + R$, et on a $0 = deg(R) < deg(x-\alpha) = 1$. Or, on a $0 = F(\alpha) = Q(\alpha)(\alpha - \alpha) + c$ d'où $c = 0$. Ainsi, $F = Q(x-\alpha)$ avec $deg(Q) = d-1$. Par hypothèse de récurrence, on a $|\{\beta \in K,\ Q(\beta) = 0\}| \leqslant d-1$ et alors $\{z \in \mathbb{C},\ F(z) = 0\} = \{\alpha\} \cup \{\beta \in K,\ Q(\beta) = 0\}$ soit $|\{z \in \mathbb{C},\ F(z) = 0\}| = |\{\alpha\} \cup \{\beta \in K,\ Q(\beta) = 0\}|$, *i.e.* $|\{z \in \mathbb{C},\ F(z) = 0\}| \leqslant 1 + d - 1 = d$.

□

6.2 Construction des transcendants

Théorème de Dirichlet. Soit α irrationnel. Alors il existe une infinité de $\frac{p}{q} \in \mathbb{Q}$ avec $p, q \in \mathbb{N}$ tels que $\text{pgcd}(p,q) = 1$ et $q \geqslant 1$ tels que

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Démonstration. Soit $N \geqslant 1$. On considère $\{i\alpha\} = i\alpha - [i\alpha]$ où $1 \leqslant i \leqslant N$. Il y a N intervalles. Il y a $N+1$ points rouges. Par le principe des tiroirs, il existe $i < j$ tel que $|\{j\alpha\} - \{i\alpha\}| < \frac{1}{N}$. Or

$$\{j\alpha\} - \{i\alpha\} = j\alpha - [j\alpha] - i\alpha + [i\alpha] = (j-i)\alpha - \big(\underbrace{[j\alpha] - [i\alpha]}_{p}\big)$$

avec $\{i\alpha\} \neq \{j\alpha\}$ pour tous i, j car α est irrationnel, d'où

$$|q\alpha - p| < \frac{1}{N} \implies \left|\alpha - \frac{p}{q}\right| < \frac{1}{qN}.$$

Avec N qui varie, il y a donc une infinité de $\frac{p}{q}$. De plus, pour $q < N$ on a

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{qN} < \frac{1}{q^2}.$$

□

Théorème de Liouville. Soit $\alpha \in \mathbb{R}$ algébrique de degré $d \geqslant 1$. Alors

$$\exists C > 0, \quad \forall \left(\frac{p}{q}\right) \in \mathbb{Q}, \quad \left|\alpha - \frac{p}{q}\right| \geqslant \frac{C}{q^d}.$$

Démonstration. Soit α algébrique irrationnel. Soit $P \in \mathbb{Z}[X]$ un multiple entier de P_α. Soit $\varepsilon \in]0, 1]$ tel que $\{x \in \mathbb{R},\ P(x) = 0\} \cap [\alpha - \varepsilon, \alpha + \varepsilon] = \{\alpha\}$. Soit $|\alpha - X| \leqslant \varepsilon$. On a

$$P(X) = \sum_{i=1}^{d} \frac{P^{(i)}(\alpha)}{i!}(X - \alpha)^i \implies |P(X)| \leqslant C\,|X - \alpha| \quad \text{où} \quad C \coloneqq \sum_{i=1}^{d} \frac{\left|P^{(i)}(\alpha)\right|}{i!}.$$

Si $X \coloneqq \dfrac{p}{q}$, avec $P(X) = \sum\limits_{i=0}^{d} a_i X^i$, $a_i \in \mathbb{Z}$, on a

$$P\Big(\frac{p}{q}\Big) = \frac{1}{q^d} \sum_{i=0}^{d} a_i p^i q^{d-i}$$

soit

$$C\left|\alpha - \frac{p}{q}\right| \geqslant \left|P\Big(\frac{p}{q}\Big)\right| = \frac{1}{q^d}\left|\sum_{i=0}^{d} a_i p^i q^{d-i}\right| \geqslant \frac{1}{q^d} \implies \left|\alpha - \frac{p}{q}\right| \geqslant \frac{C}{q^d} \quad \text{où} \quad C' = \frac{1}{C}.$$

□