Logique et vocabulaire ensembliste

Table des matières

1 Fondations

1.1 Ensembles et éléments

Définition. Sur le plan intuitif, un ensemble E est une "collection" d'objets que l'on appelle les élements de E, telle que l'on peut "décider" si un élément donné appartient ou non à E.
On écrit "$x \in E$" si et seulement si x est un élément de E. Sinon, on écrit "$x \notin E$".

Axiome d'extensionnalité : Si E et F sont deux ensembles, alors
$E = F$ si et seulement si pour tout $x \in E$, $x \in F$ et pour tout $x \in F$, $x \in E$.

Remarque. Cet axiome décrit une technique très utilisée pour montrer l'égalité entre deux ensembles E et F :
On écrit "soit $x \in E$" et l'on montre qu'alors $x \in F$, puis on écrit "soit $x \in F$" et l'on montre qu'alors $x \in E$.

Exemple. Montrer (de manière élémentaire) que $\mathbb{R}_+ = \{x \in \mathbb{R} / \forall \varepsilon > 0, x > -\varepsilon\}$.
Si $x \in \mathbb{R}_+$, pour tout $\varepsilon > 0$, on a $x \geq 0 > -\varepsilon$, donc $x > -\varepsilon$.
Réciproquement, soit $x \in \mathbb{R}$ tel que, pour tout $\varepsilon > 0$, $x > -\varepsilon$. Supposons que $x \notin \mathbb{R}_+$. Alors $-\frac{x}{2} > 0$, donc avec $\varepsilon = -\frac{x}{2}$, on obtient $x > -\varepsilon = \frac{x}{2}$, puis $1 < \frac{1}{2}$ car $x < 0$, ce qui est faux. Ainsi $x \in \mathbb{R}_+$.

Propriété. Il existe un unique ensemble ne contenant aucun élément, il est noté $\emptyset$ [1].

Démonstration.
L'ensemble des x tels que $x \neq x$ ne possède aucun élément, d'où l'existence.
Soit E et F deux ensembles ne contenant aucun élément.
La propriété "pour tout $x \in E$, ..." est toujours vraie, donc l'après l'axiome d'extensionnalité, $E = F$. □

Propriété. Si a est un objet, l'unique ensemble dont a est le seul élément est noté $\{a\}$. C'est un singleton.
De même, lorsque $a \neq b$, $\{a, b\}$ est appelé une paire.

1. L'invention de l'ensemble vide, c'est-à-dire du zéro a constitué un pas décisif dans l'histoire des mathématiques. C'est un concept fondamental de la théorie des ensembles et, en tant qu'élément neutre, de l'algèbre.

Le zéro a été inventé beaucoup plus tard que les entiers naturels supérieurs à un. En particulier, les mathématiciens grecs (Thalès, Pythagore, Euclide, etc.) n'en disposaient pas.

Le zéro apparaît chez les Babyloniens au IIIe siècle avant notre ère, mais seulement sous la forme d'un symbole (en forme de double chevron) pour désigner l'absence d'unité d'un certain rang dans l'écriture d'un nombre (en base 60). C'était alors un chiffre, mais pas un nombre que l'on pouvait utiliser seul.

Un tel usage intrinsèque du zéro n'est apparu que vers le Vème siècle, en Inde : ce nombre est défini par le mathématicien indien Brahmagupta comme la soustraction d'un nombre par lui-même ($x - x = 0$). Il était représenté par un cercle et était appelé "sunya", le mot qui signifie "vide" en sanskrit. La notion et la notation indiennes du zéro ont été empruntées à l'Inde par les mathématiciens arabes au IXème siècle. Le mot "sunya" a été traduit en arabe par sifr, lequel est d'ailleurs la racine des mots "chiffre" et "zéro" en français.

Définition. Sur le plan intuitif, si E et F sont deux ensembles, une application f de E dans F associe à tout élément x de E un unique élément $f(x)$ de F.

Définition. "vrai" et "faux" sont appelés les deux valeurs booléennes, en mémoire de George Boole.[2] On les notera également V et F.

Définition. Un prédicat P sur un ensemble E est une application de E dans $\{V, F\}$. Dans ce cas, pour tout $x \in E$, $P(x)$ est vrai ou faux.

Exemple. L'assertion $P(x)$: [$x^2 > 4$] est un prédicat sur $\mathbb{R}$. $P(\pi)$ est vrai, $P(0)$ est fausse.

Il existe plusieurs manières de définir un ensemble :

- **Définition par énumération** : on donne tout simplement la liste de ses éléments. Par exemple $E = \{-1, 0, 1\}$,
  ou bien $F = \{\emptyset, \{0\}, \{-1, 1\}, truc\}$; on voit qu'un élément d'un ensemble peut lui-même être un ensemble.
  On peut répéter plusieurs fois le même élément, et l'ordre d'apparition des éléments n'a pas d'importance : $\{-1, 0, 1, -1, 0, 0\} = \{0, 1, -1\}$.
- **Définition par construction** : L'ensemble est donné à partir d'ensembles déjà définis et d'opérateurs sur les ensembles, que nous étudierons plus loin. Par exemple $E \cap F$ et $E \cup F$.
- **Définition en compréhension** : Si l'on dispose d'un ensemble E déjà défni et d'un *prédicat* P sur E, alors $\{x \in E / P(x)\}$ représente l'ensemble des éléments x de E tels que $P(x)$ est vrai.
  Par exemple $\mathbb{R}_+ = \{x \in \mathbb{R} / x \geq 0\}$.
  Il est important de bien maîtriser cette syntaxe.
  Si $F = \{x \in E / P(x)\}$, alors pour tout $x \in E$,
  on a l'équivalence : $x \in F$ si et seulement si $P(x)$.
- **Définition axiomatique** : on admet l'existence d'un ensemble satisfaisant certains axiomes. Par exemple l'axiome de l'infini affirme qu'il existe un ensemble A tel que, $\emptyset \in A$ et pour tout $y \in A$, $y \cup \{y\} \in A$.[3]
  On peut s'en servir pour construire $\mathbb{N}$, en posant $0 = \emptyset$, $1 = \emptyset \cup \{\emptyset\} = \{0\}$, $2 = 1 \cup \{1\} = \{0, 1\}$, ..., $n + 1 = n \cup \{n\} = \{0, 1, \ldots, n\}$ ...
- **Définition par induction structurelle** : informellement, pour définir un ensemble E par induction, on fournit un procédé de construction de nouveaux éléments de E à partir d'éléments de E déjà obtenus. On part de la donnée de quelques éléments initiaux de E, et on applique le procédé de construction étape par étape pour obtenir de plus en plus d'éléments. On obtient finalement E.

2. George Boole (1815-1864) est un logicien, mathématicien et philosophe britannique. Il est notamment à l'origine de la logique moderne. Autodidacte, il publia ses premiers travaux tout en exerçant son métier d'instituteur et de directeur d'école dans la région de Lincoln.

3. En théorie formelle des ensembles, tout objet mathématique est un ensemble

Par exemple, nous définirons par induction l'ensemble des formules propositionnelles au chapitre 2.1.

Le paradoxe de Russell (1901) [4] :
Notons A l'ensemble de tous les ensembles et posons $B = \{x \in A / x \notin x\}$. Alors $B \in B$ si et seulement si $B \notin B$, ce qui est impossible. Cela signifie que A n'est pas un ensemble ! Ainsi, notre définition d'un ensemble est seulement intuitive, non mathématique, mais elle fut utilisée telle quelle par les mathématiciens jusqu'au début du vingtième siècle. A cette époque, la logique est devenue une branche à part entière des mathématiques. Elle permet notamment de donner une définition rigoureuse de la notion d'ensemble qui évite ce type de paradoxe. Il s'agit des axiomes de Zermelo [5]-Fraenkel [6], qui sortent du programme de MPSI.

1.2 Quantificateurs

Définition du quantificateur universel :
Soit E un ensemble et P un prédicat sur E. La propriété "$\forall x \in E,\ P(x)$" signifie que pour tous les éléments x de E, $P(x)$ est vraie,
c'est-à-dire que $\{x \in E / P(x)\}$ est égal à E.

Définition du quantificateur existentiel :
Avec les mêmes notations, la propriété "$\exists x \in E,\ P(x)$" signifie qu'il existe au moins un $x \in E$ tel que $P(x)$ est vraie, c'est-à-dire que $\{x \in E / P(x)\} \neq \emptyset$.

Existence et unicité : La propriété "$\exists ! x \in E,\ P(x)$" signifie qu'il existe un unique $x \in E$ tel que $P(x)$ est vraie, c'est-à-dire que $\{x \in E / P(x)\}$ est un singleton.

Remarque. Par exemple, l'axiome d'extensionnalité s'écrit :
$E = F$ si et seulement si $[\forall x \in E,\ x \in F]$ et $[\forall x \in F,\ x \in E]$.

Remarque. L'emploi des quantificateurs en guise d'abréviations est exclu : l'usage d'un "$\forall x$" est toujours suivi d'un "$\in E,\ P(x)$" (ou plus rarement d'un ", $P(x)$"), où P est un prédicat sur E.

Exemple. Si l'on reprend la preuve de $\mathbb{R}_+ = \{x \in \mathbb{R} / \forall \varepsilon > 0, x > -\varepsilon\}$,
il serait incorrect de commencer par :
"Si $x \in \mathbb{R}_+$, $\forall \varepsilon > 0$ on a $x \geq 0 > -\varepsilon$, donc $x > -\varepsilon$".
Cependant, on pourrait continuer par :
"Réciproquement, soit $x \in \mathbb{R}$ tel que $\forall \varepsilon > 0,\ x > -\varepsilon$".

Remarque. Soit P un prédicat sur un ensemble E. Alors dans les phrases "$\forall x \in E,\ P(x)$" et "$\exists x \in E,\ P(x)$", on peut remplacer la variable x par y, ou n'importe quel autre symbole. On dit que, dans les phrases "$\forall x \in E,\ P(x)$" et

4. Bertrand Russell, 1872-1970, 3e comte Russell, est un mathématicien, logicien, philosophe, épistémologue, homme politique et moraliste britannique.
5. Ernst Zermelo,1871-1953, est un mathématicien allemand.
6. Abraham Fraenkel, 1891-1965, est un mathématicien d'abord allemand puis israélien.

"$\exists x \in E,\ P(x)$", x est une variable muette. On dit aussi que x est une variable liée. Dans la propriété "$\exists y \in \mathbb{R},\ x = y^2$", y est une variable liée, et par opposition, on dit que x est une variable libre.

1.3 Parties d'un ensemble

Définition. Soit E et F deux ensembles.
On dit que F est inclus dans E et l'on note $F \subset E$ si et seulement si tout élément de F est un élément de E, c'est-à-dire si et seulement si $\forall x \in F,\ x \in E$.
Lorsque $F \subset E$, on dit que F est une partie de E ou encore un sous-ensemble de E.

Remarque. L'axiome d'extensionnalité peut donc s'écrire :
$E = F$ si et seulement si $E \subset F$ et $F \subset E$.

Remarque. Il faut éviter de confondre les symboles $\in$ et $\subset$.
Ainsi, $1 \in \{1, 2\}$ mais $1 \not\subset \{1, 2\}$, et $\{0\} \subset \{0, 2\}$, mais $\{0\} \notin \{0, 2\}$.
Informellement, lorsqu'on écrit $A \subset B$, A et B sont des ensembles de même niveau. Au contraire, lorsqu'on écrit $a \in B$, a et B peuvent être des ensembles, mais ils ne sont pas du même type : a est hiérarchiquement inférieur à B.

Transitivité de l'inclusion : Si $A \subset B$ et $B \subset C$, alors $A \subset C$.

Définition. Si E est un ensemble, on note $\mathcal{P}(E)$ l'ensemble de ses parties.

Exemple. $\mathcal{P}(\{0, 1\}) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$.
$\mathcal{P}(\emptyset) = \{\emptyset\}$.

Remarque. $A \subset B \iff A \in \mathcal{P}(B)$.

1.4 Opérateurs sur les ensembles

Définition. Soit E et F deux ensembles :
- **Intersection :** $x \in E \cap F$ si et seulement si ($x \in E$ et $x \in F$).
- **Réunion :** $x \in E \cup F$ si et seulement si ($x \in E$ ou $x \in F$).
- **Différence ensembliste :** $E \setminus F = \{x \in E / x \notin F\}$.
- **Différence symétrique :** $E \Delta F = (E \setminus F) \cup (F \setminus E)$.
- **Complémentaire de F dans E :** Si F est une partie de E, le complémentaire de F dans E est $\overline{F} = E \setminus F$, que l'on note plus rarement $\complement_E^F$.

Propriété. Si F et G sont deux parties d'un ensemble E, alors $F \setminus G = F \cap \overline{G}$.

Remarque. $E \Delta F = F \Delta E = (E \cup F) \setminus (E \cap F)$.
On peut le démontrer par double inclusion en passant aux éléments.
Ainsi, les éléments de $E \Delta F$ sont les éléments qui sont exclusivement ou bien dans E, ou bien dans F, mais pas dans E et F en même temps.

Propriété. ***Commutativité de l'intersection et de la réunion*** :
Soit A et B deux ensembles. Alors, $A \cap B = B \cap A$ et $A \cup B = B \cup A$.

Propriété. ***Associativité de l'intersection et de la réunion*** : Soit A, B, C trois ensembles. Alors, $A \cap (B \cap C) = (A \cap B) \cap C$ et $A \cup (B \cup C) = (A \cup B) \cup C$.

Définition. Plus généralement, si I est un ensemble et si $(E_i)_{i\in I}$ est une famille d'ensembles (c'est-à-dire que pour chaque $i \in I$, "on se donne" un ensemble E_i), alors on peut définir $\bigcup_{i\in I} E_i$ et $\bigcap_{i\in I} E_i$ par :

$x \in \bigcup_{i\in I} E_i \iff (\exists i \in I,\ \ x \in E_i)$ et

$x \in \bigcap_{i\in I} E_i \iff (\forall i \in I,\ \ x \in E_i)$.

Cette dernière définition n'est pas correcte lorsque $I = \emptyset$, car tout x serait élément de l'intersection vide, donc d'après le paradoxe de Russell, l'intersection vide n'est pas un ensemble.

Exemple. On a vu que $\mathbb{R}_+ = \{x \in \mathbb{R} \ / \ \forall \varepsilon > 0,\ \ x > -\varepsilon\}$, donc $\mathbb{R}_+ = \bigcap_{\varepsilon>0}]-\varepsilon, +\infty[$.

De même, on peut montrer que $\mathbb{R}_+^* = \bigcup_{\varepsilon>0}]\varepsilon, +\infty[$.

Propriété. A, B et C sont trois ensembles. $(E_i)_{i\in I}$ est une famille d'ensembles.
Distributivité de l'intersection par rapport à la réunion :
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. $\qquad A \cap \bigcup_{i\in I} B_i = \bigcup_{i\in I} (A \cap B_i)$.
Distributivité de la réunion par rapport à l'intersection :
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. $\qquad A \cup \bigcap_{i\in I} B_i = \bigcap_{i\in I} (A \cup B_i)$ (avec $I \neq \emptyset$).

Notation. Soit $(E_i)_{i\in I}$ une famille d'ensembles deux à deux disjoints, c'est-à-dire telle que, pour tout $i, j \in I$ avec $i \neq j$, $E_i \cap E_j = \emptyset$. Alors $\bigcup_{i\in I} E_i$ est appelée une réunion disjointe et elle est notée $\bigsqcup_{i\in I} E_i$.

Remarque. Si A, B, C sont trois ensembles, la quantité $A \sqcup B \sqcup C$ désigne $A \cup B \cup C$, mais le fait d'utiliser le symbole $\sqcup$ au lieu du symbole $\cup$ indique que A, B et C sont deux à deux disjoints.

1.5 L'ensemble $\mathbb{N}$ des entiers naturels

On admet qu'il existe un ensemble, noté $\mathbb{N}$, satisfaisant les axiomes de Peano [7] suivants :

— $\mathbb{N}$ est muni d'un élément particulier noté 0 et d'une application "successeur", notée s de $\mathbb{N}$ dans $\mathbb{N}$.

7. Giuseppe Peano, 1858-1932, mathématicien et linguiste italien, inventeur d'une langue auxiliaire internationale, le Latino sine flexione (LsF). Ses qualités d'enseignant ont parfois souffert d'un excès de détails concernant les notations utilisées et les concepts de base, au détriment de l'ensemble du programme qu'il devait traiter.

— 0 n'est le successeur d'aucun entier : $\forall n \in \mathbb{N},\ \ s(n) \neq 0$.
— s est une application injective : pour tout $n, m \in \mathbb{N}$, si $s(n) = s(m)$, alors $n = m$.
— Pour toute partie F de $\mathbb{N}$, si $0 \in F$ et si pour tout $n \in F$, $s(n) \in F$, alors $F = \mathbb{N}$.

Remarques :
◇ Le dernier axiome commence par "pour toute partie de $\mathbb{N}$". L'utilisation d'une telle quantification est caractéristique de la logique du second ordre. Pour se limiter à une logique du premier ordre, où les quantificateurs ne portent que sur des éléments de $\mathbb{N}$, il est nécessaire de compliquer les énoncés des axiomes de Peano, ce qui sort du programme.
◇ Informellement, d'après le dernier axiome, $\mathbb{N} = \{0, s(0), s(s(0)), s(s(s(0))), \ldots\}$. On convient de poser $1 = s(0)$, $2 = s(1)$, $3 = s(2)$, etc.

Principe de récurrence : Soit $R(n)$ un prédicat sur $\mathbb{N}$.
Si $R(0)$ est vraie et si pour tout $n \in \mathbb{N}$, $R(n)$ implique $R(s(n))$,
alors pour tout $n \in \mathbb{N}$, $R(n)$ est vraie.

Démonstration.
On applique le dernier axiome avec $F = \{n \in \mathbb{N} / R(n)\}$. □

Addition entre entiers : Pour tout $m \in \mathbb{N}$, on pose
$0 + m = m$ et
$\forall n \in \mathbb{N},\ \ s(n) + m = s(n + m)$.
Ces conditions définissent l'addition entre entiers.

Démonstration.
Fixons $m \in \mathbb{N}$. Notons F_m l'ensemble des entiers n pour lesquels $n + m$ est défini.
$0 \in F_m$ et, pour tout $n \in \mathbb{N}$, si $n \in F_m$, alors $s(n) \in F_m$, donc $F_m = \mathbb{N}$. □

Exemple. $1 + n = s(0) + n = s(0 + n) = s(n)$, $2 + n = s(1) + n = s(1 + n) = s(s(n))$.

Propriétés de l'addition :
— 0 est neutre : $\forall m \in \mathbb{N},\ \ m + 0 = 0 + m = m$.
— Associativité : $\forall n, m, k \in \mathbb{N},\ \ (n + m) + k = n + (m + k)$.
— Commutativité : $\forall n, m \in \mathbb{N},\ \ n + m = m + n$.

Démonstration.
◇ Elément neutre : Soit $m \in \mathbb{N}$. Par définition, $0 + m = m$.
Montrons par récurrence $R(m) : m + 0 = m$.
On a bien $0 + 0 = 0$, d'où $R(0)$.
Pour $m \in \mathbb{N}$, supposons $R(m)$.
Alors $s(m) + 0 = s(m + 0) = s(m)$, d'où $R(s(m))$.
D'après le principe de récurrence, on a bien montré que $\forall m \in \mathbb{N},\ \ m + 0 = m$.
◇ Associativité : Fixons $m, k \in \mathbb{N}$.
Pour tout $n \in \mathbb{N}$, notons $R(n) : (n + m) + k = n + (m + k)$.
Lorsque $n = 0$, $(0 + m) + k = m + k = 0 + (m + k)$, d'où $R(0)$.
Pour $m \in \mathbb{N}$, supposons $R(n)$. Alors,

$(s(n)+m)+k = s(n+m)+k = s((n+m)+k)$ et $s(n)+(m+k) = s(n+(m+k))$, donc d'après $R(n)$, $R(s(n))$ est aussi vraie.
$\diamond$ Commutativité : On sait déjà que $n+0 = 0+n$ pour tout $n \in \mathbb{N}$.
Montrons que pour tout $n \in \mathbb{N}$, $n+1 = 1+n$.
En effet, c'est vrai pour $n=0$ et si $n+1 = 1+n$, alors
$s(n)+1 = s(n+1) = s(1+n) = s(s(0)+n) = s(s(0+n)) = s(s(n)) = 1+s(n)$.
Fixons enfin $m \in \mathbb{N}$ et montrons, toujours par récurrence, que $n+m = m+n$.
C'est vrai pour $n=0$ et si $n+m = m+n$, alors
$s(n)+m = s(n+m) = 1+(n+m) = (m+n)+1$, puis d'après l'associativité,
$s(n)+m = m+(n+1) = m+(1+n) = m+s(n)$. □

1.6 Produit cartésien

Définition. Si a et b sont deux objets, posons $(a,b) = \{\{a\},\{a,b\}\}$.
(a,b) est appelé le couple de composantes a et b.

Propriété. $(a,b) = (c,d)$ si et seulement si $a=c$ et $b=d$.

Remarque. En particulier, lorsque $a \neq b$, $(a,b) \neq (b,a)$, alors que $\{a,b\} = \{b,a\}$.

Démonstration.
On suppose que $\{\{a\},\{a,b\}\} = \{\{c\},\{c,d\}\}$.
Supposons que $a \neq c$. Alors $\{a\} \neq \{c\}$, donc $\{a\} = \{c,d\}$, puis $a=c=d$, ce qui est contradictoire.
Ainsi, $a=c$ et $\{\{a\},\{a,b\}\} = \{\{a\},\{a,d\}\}$.
Premier cas : Si $\{a,b\} = \{a\}$, alors $a=b=d$.
Second cas : Si $\{a,b\} \neq \{a\}$, alors $\{a,b\} = \{a,d\}$. Alors $b=a$ ou $b=d$, mais si $b=a$, alors $\{a\} = \{a,d\}$, donc $a=d=b$.
Ainsi dans tous les cas, $b=d$.
La réciproque est évidente. □

Définition. Si A et B sont deux ensembles, on pose $A \times B = \{(a,b)/a \in A \text{ et } b \in B\}$.
$A \times B$ s'appelle le produit cartésien de A et B.

Exemple. $\mathbb{R}^2$ est l'ensemble des couples de nombres réels. On peut l'assimiler à un plan muni d'un repère cartésien en confondant chaque couple (x,y) avec le point de coordonnées (x,y).

Définition.
- Si a,b,c sont trois objets, le triplet de composantes a,b et c est défini par $(a,b,c) = ((a,b),c)$.
- Si a,b,c,d sont quatre objets, le quadruplet de composantes a,b,c et d est défini par $(a,b,c,d) = ((a,b,c),d)$.
- Soit $n \geq 2$. Supposons définie la notion de n-uplet $(a_1,\ldots,a_n)$. On pose alors $(a_1,\ldots,a_{n+1}) = ((a_1,\ldots,a_n),a_{n+1})$, quels que soient les $n+1$ objets $a_1,\ldots,a_{n+1}$.

Propriété. Soit $n \geq 3$. Soit $a_1, \ldots, a_n$ et $b_1, \ldots, b_n$ $2n$ objets.
Alors $(a_1, \ldots, a_n) = (b_1, \ldots, b_n)$ si et seulement si $\forall i \in \{1, \ldots, n\},\ a_i = b_i$.

Démonstration.
Pour tout $n \in \mathbb{N}$, on note $R(n)$ l'assertion suivante : si $a_1, \ldots, a_{n+2}$ sont $n+2$ objets, si $b_1, \ldots, b_{n+2}$ sont aussi $n+2$ objets, alors $(a_1, \ldots, a_{n+2}) = (b_1, \ldots, b_{n+2})$ si et seulement si $\forall i \in \{1, \ldots, n+2\},\ a_i = b_i$.
On a déjà démontré $R(0)$ et, pour tout $n \in \mathbb{N}$, il est simple de montrer que $R(n)$ implique $R(n+1)$. □

Notation. $\mathbb{N}^*$ désigne $\mathbb{N} \setminus \{0\}$.

Définition. Soit $n \in \mathbb{N}^*$. Si $A_1, \ldots, A_n$ sont n ensembles, on pose
$A_1 \times \cdots \times A_n = \{(a_1, \ldots, a_n) / \forall i \in \{1, \ldots, n\},\ a_i \in A_i\}$.
Si E est un ensemble, on note $E^n = \underbrace{E \times \cdots \times E}_{n fois}$.
Les élements de E^n s'appellent des n-uplets ou encore des n-listes de E.

Remarque. Avec notre construction, lorsque $n \geq 2$,
$A_1 \times \cdots \times A_n = (A_1 \times \cdots \times A_{n-1}) \times A_n$.

Remarque. Convention, lorsque $n = 1$, le "1-uplet" (a) est égal à a.
Avec cette convention, $E^1 = E$.

Commutativité de deux quantificateurs universels :
Soit E et F deux ensembles. Notons $P(x, y)$ un prédicat défini sur $E \times F$. L'affirmation "$\forall (x, y) \in E \times F,\ P(x, y)$" est équivalente [8] à l'affirmation "$\forall x \in E,\ \forall y \in F,\ P(x, y)$", car elles signifient toutes les deux que "pour tout x dans E et y dans F, $P(x, y)$ est vrai", ou bien encore que "pour tout y dans F et x dans E, $P(x, y)$ est vrai".
Ainsi, l'affirmation "$\forall x \in E,\ \forall y \in F,\ P(x, y)$" est
équivalente à "$\forall y \in F,\ \forall x \in E,\ P(x, y)$".

Commutativité de deux quantificateurs existentiels :
On peut de même se convaincre que les deux affirmations
"$\exists x \in E,\ \exists y \in F,\ P(x, y)$" et "$\exists y \in F,\ \exists x \in E,\ P(x, y)$" sont équivalentes.

ATTENTION :
Un quantificateur universel ne commute pas avec un quantificateur existentiel.
En effet l'affirmation "$\forall x \in E,\ \exists y \in F,\ P(x, y)$" signifie que pour tout $x \in E$, il existe un y, qui dépend a priori de x tel que $P(x, y)$, c'est-à-dire qu'il existe une application $x \longmapsto y(x)$ de E dans F telle que, pour tout $x \in E$, $P(x, y(x))$.
Quant à l'affirmation "$\exists y \in F,\ \forall x \in E,\ P(x, y)$", elle signifie qu'il existe $y \in F$ tel que, pour tout $x \in E$, $P(x, y)$. Ici, y ne dépend pas de x.
En résumé, "$\forall x \in E,\ \exists y \in F,\ P(x, y)$" si et seulement si il existe une application $x \longmapsto y(x)$ de E dans F tel que, pour tout $x \in E$, $P(x, y(x))$,
et "$\exists y \in F,\ \forall x \in E,\ P(x, y)$" si et seulement si il existe une application **constante** $x \longmapsto y_0$ de E dans F, telle que pour tout $x \in E$, $P(x, y_0)$.

8. Exercice

On voit qu'en général, la seconde affirmation implique la première mais que la réciproque est fausse.

Exemple. $\forall x \in \mathbb{Q},\ \exists d \in \mathbb{N}^*,\ dx \in \mathbb{Z}$. En effet, tout rationnel x possède au moins une écriture fractionnelle avec un dénominateur $d \in \mathbb{N}^*$ (on le verra lors de la construction de $\mathbb{Q}$). Cependant, si on intervertit les deux quantificateurs, la phrase
$\exists d \in \mathbb{N}^*,\ \forall x \in \mathbb{Q},\ dx \in \mathbb{Z}$ est fausse.

2 Formules propositionnelles

On souhaite construire des propositions logiques structurées à partir de propositions plus simples. Outre les quantificateurs, nous allons définir dans ce but des connecteurs logiques puis définir leur sens : $\vee$ pour "ou non exclusif", $\wedge$ pour "et", $\Longrightarrow$ pour l'implication, $\Longleftrightarrow$ pour l'équivalence, $\neg$ pour la négation.

2.1 Syntaxe

Définition par induction des formules propositionnelles : on part d'un ensemble $\mathcal{V}$ dont les éléments sont appelés des variables propositionnelles. On utilise également les "connecteurs logiques" suivants : $\wedge, \vee, \Longrightarrow, \Longleftrightarrow, \neg$.
L'ensemble F des formules propositionnelles est défini par induction structurelle :

- Les variables propositionnelles sont des formules propositionnelles.
- si $P, Q \in F$, alors $(P \wedge Q), (P \vee Q), (P \Longrightarrow Q), (P \Longleftrightarrow Q)$ et $\neg P$ sont aussi des formules propositionnelles.

Plus précisément, si l'on note $F_0 = \mathcal{V}$, et pour tout $n \in \mathbb{N}$,
$F_{n+1} = F_n \cup \{\neg P / P \in F_n\} \cup \{(P \alpha Q) / P, Q \in F_n \text{ et } \alpha \in \{\wedge, \vee, \Longrightarrow, \Longleftrightarrow\}\}$,
alors $F = \bigcup_{n \in \mathbb{N}} F_n$.

Remarque. L'écriture "$F = \bigcup_{n \in \mathbb{N}} F_n$" définit bien F car on peut montrer par récurrence que F_n est défini pour tout $n \in \mathbb{N}$; en effet, si l'on note $R(n)$ la propriété "F_n est défini", alors on a $R(0)$ et pour tout $n \in \mathbb{N}$, $R(n)$ implique $R(n+1)$.

Remarque. Une formule propositionnelle s'appelle aussi une proposition, une assertion, une formule, un énoncé, une expression booléenne, etc.

Exemple. Si A, B et C sont des variables propositionnelles, alors
$(A \Longrightarrow (B \Longleftrightarrow A))$ et $(((A \wedge (\neg B \Longrightarrow \neg A)) \wedge (\neg B \vee \neg C)) \Longrightarrow (C \Longrightarrow \neg A))$ sont des formules propositionnelles.
$A \Longrightarrow (B \vee C)$ n'est pas une formule car elle n'est pas correctement parenthésée, mais on relâche en général les règles syntaxiques pour accepter ce type de formule.
$A \Longrightarrow BC\neg$ n'est pas une formule, en aucun cas.

Exemple. On obtient des "formules" plus habituelles en mathématiques par substitution : par exemple, si l'on part de la formule propositionnelle $(A \wedge B) \Longrightarrow C$, en

substituant A, B et C respectivement par $x \geq 0$, $y \geq 0$ et $x + y \geq 0$, on obtient la formule mathématique suivante : $((x \geq 0) \wedge (y \geq 0)) \Longrightarrow (x + y \geq 0)$.

Remarque. Autre exemple, la formule d'extensionnalité s'écrit :
$(E = F) \Longleftrightarrow \{[\forall x \in E,\ \ x \in F] \wedge [\forall x \in F,\ \ x \in E]\}$.

Exemple. L'axiome de l'infini s'écrit : il existe un ensemble A tel que
$(\emptyset \in A) \wedge (\forall y(y \in A \Longrightarrow y \cup \{y\} \in A))$.

Définition. Si P et Q sont deux formules propositionnelles, $P \wedge Q$ (prononcer "P et Q") s'appelle la conjonction de P et de Q,
$P \vee Q$ (prononcer "P ou Q") s'appelle la disjonction de P et de Q,
$P \Longrightarrow Q$ s'appelle une implication,
$P \Longleftrightarrow Q$ est une équivalence,
et $\neg P$ est la négation de la proposition P.

2.2 Sémantique

Définition. Une distribution de valeurs de vérité sur l'ensemble $\mathcal{V}$ des variables propositionnelles est une application de $\mathcal{V}$ dans l'ensemble $\{V, F\}$. La donnée d'une telle distribution attribue donc à chaque variable propositionnelle l'une des deux valeurs booléennes V ou F.

Définition. Soit v une distribution de valeurs de vérité sur l'ensemble $\mathcal{V}$. On prolonge v sur l'ensemble des formules propositionnelles construites à partir de $\mathcal{V}$ de la manière suivante : pour toutes formules propositionnelles P et Q,

- $v(P \wedge Q) = 1$ si et seulement si $v(P) = v(Q) = 1$ (on dira aussi que $P \wedge Q$ est vraie si et seulement si P et Q sont toutes deux vraies).
- $v(P \vee Q) = 1$ si et seulement si $v(P) = 1$ ou $v(Q) = 1$.
  Il convient de noter qu'en mathématiques, le "ou" est par défaut un "ou non exclusif".
- $v(P \Longrightarrow Q) = 0$ si et seulement si $v(P) = 1$ et $v(Q) = 0$.
  Cela signifie que l'implication $P \Longrightarrow Q$ est fausse si et seulement si P est vraie alors que Q est fausse.
  Ainsi l'implication $P \Longrightarrow Q$ est vraie si et seulement si P est fausse ou bien Q est vraie.
  C'est assez peu intuitif, mais "faux" $\Longrightarrow$ "n'importe quoi".
- $v(P \Longleftrightarrow Q) = 1$ si et seulement si $v(P) = v(Q)$.
- $v(\neg P) = 1$ si et seulement si $v(P) = 0$.

Définition. La définition précédente est équivalente à la donnée des "tables de vérité" des connecteurs logiques $\wedge$, $\vee$, $\Longrightarrow$, $\Longleftrightarrow$ et $\neg$:

P	Q	$P \wedge Q$	$P \vee Q$	$P \Longrightarrow Q$
V	V	V	V	V
V	F	F	V	F
F	V	F	V	V
F	F	F	F	V

Remarque. Les symboles $\Longrightarrow$ et $\Longleftrightarrow$ ne doivent pas être utilisés comme des abréviations, tout au moins en mathématiques. Notamment, écrire "P, donc Q" signifie que P est vraie, ce qui permet d'en déduire que Q est vraie. Au contraire, écrire "$P \Longrightarrow Q$" ne préjuge pas de la valeur booléenne de P.
Le symbole $\Longleftrightarrow$ est à réserver pour la résolution d'équations ou d'inéquations :

Exemple. Pour déterminer les couples d'entiers naturels non nuls dont le produit est égal à la somme, fixons $n, m \in \mathbb{N}^*$.
(C) : $nm = n+m \Longleftrightarrow n(m-1)-m = 0 \Longleftrightarrow n(m-1)-(m-1)-1 = 0$: astucieux !
Ensuite, $(C) \Longleftrightarrow (n-1)(m-1) = 1 \Longleftrightarrow n-1 = m-1 = 1$, car $n-1$ et $m-1$ sont des entiers naturels (cf page 20). On peut conclure : $(C) \Longleftrightarrow n = m = 2$.
L'astuce utilisée, assez fréquente, consiste à ajouter et à retrancher la même quantité, ou bien à multplier et diviser par la même quantité non nulle.
Mais pourquoi remplacer ici m par $m-1+1$?
C'est afin de faire apparaître la différence de deux termes semblables :
$n(m-1)$ et $1.(m-1)$.
Lorsqu'on retranche (resp : divise) deux termes, il est souvent intéressant de les mettre sous la même forme.

Définition. Supposons que $P \Longrightarrow Q$.
- On dit alors que P est une *condition suffisante* pour Q, car il *suffit* que P soit vérifiée pour que Q le soit.
- On dit aussi que Q est une *condition nécessaire* pour P, car lorsque P est vérifiée, alors Q est *nécessairement* vérifiée.

Lorsque $P \Longleftrightarrow Q$, on dit que P est une *condition nécessaire et suffisante* pour Q.

Remarque. On rencontre souvent des énoncés de la forme "donnez une condition C pour que P". Par exemple, donner une condition portant sur deux ensembles A et B pour que $A \cap B = A \cup B$.
De tels énoncés sont ambigus car ils ne précisent pas si l'on doit chercher une condition suffisante (i.e : trouver C telle que $C \Longrightarrow P$) ou bien une condition nécessaire (i.e : trouver C telle que $P \Longrightarrow C$). Le mieux dans cette situation est de déterminer une condition nécessaire et suffisante (CNS).

Exemple. Etudions l'exemple précédent.
Analyse : Supposons que $A \cap B = A \cup B$. Alors $A \subset A \cup B = A \cap B \subset B$ et de même, $B \subset A$, donc $A = B$.
Ainsi, une condition nécessaire est : $A = B$.
Synthèse : Réciproquement, si $A = B$, alors $A \cap B = A = A \cup B$, donc la condition $A = B$ est une CNS pour que $A \cap B = A \cup B$.

Définition. Une tautologie est une formule propositionnelle qui est toujours vraie, quelle que soit la distribution de valeurs de vérité des variables propositionnelles qui interviennent dans la formule.

Exemple. Voici quelques exemples fondamentaux de tautologies, où A, B, C sont des formules propositionnelles quelconques :

1. $A \vee \neg A$: principe du tiers-exclus,
2. $(A \vee A) \Longrightarrow A$: idempotence de $\vee$ (on a aussi l'idempotence de $\wedge$),
3. $(A \wedge B) \Longleftrightarrow (B \wedge A)$: commutativité de $\wedge$ ($\vee$ est également commutatif),
4. $(A \vee (B \vee C)) \Longleftrightarrow ((A \vee B) \vee C)$: associativité de $\vee$ ($\wedge$ est aussi associatif),
5. $(A \wedge (B \vee C)) \Longleftrightarrow ((A \wedge B) \vee (A \wedge C))$: distributivité de $\wedge$ par rapport à $\vee$,
6. $(A \vee (B \wedge C)) \Longleftrightarrow ((A \vee B) \wedge (A \vee C))$: distributivité de $\vee$ par rapport à $\wedge$,
7. $(A \wedge (A \vee B)) \Longleftrightarrow A$: première loi d'absorption,
8. $((A \vee (A \wedge B)) \Longleftrightarrow A$: seconde loi d'absorption,
9. $(\neg(A \vee B)) \Longleftrightarrow (\neg A \wedge \neg B)$: loi de Morgan [9],
10. $(\neg(A \wedge B)) \Longleftrightarrow (\neg A \vee \neg B)$: loi de Morgan,
11. $(A \Longrightarrow B) \Longleftrightarrow (\neg B \Longrightarrow \neg A)$: contraposition.
12. $(A \Longrightarrow B) \Longleftrightarrow A \vee (\neg B)$: une définition de l'implication.
13. $\neg(A \Longrightarrow B) \Longleftrightarrow (\neg A) \wedge B$.

Remarque. Les 4 premières tautologies ne sont pas à apprendre car on les utilise en pratique sans même y réfléchir.

Démonstration.
Une méthode systématique de démonstration de telles formules consiste à utiliser les tables de vérité.
À titre d'exemple, démontrons la seconde loi de Morgan :

A	B	$A \vee B$	$\neg(A \vee B)$	$\neg A \wedge \neg B$
V	V	V	F	F
V	F	V	F	F
F	V	V	F	F
F	F	F	V	V

On peut aussi construire des démonstrations qui font appel à . . .la logique.
Démontrons ainsi la première loi d'absorption :
Si A est vraie, alors $A \vee B$ puis $A \wedge (A \vee B)$ sont aussi vraies.
Si A est fausse, a fortiori, $A \wedge (A \vee B)$ est fausse. □

Autres exemples de tautologies :(inutile de les apprendre)
— $((A \Longrightarrow B) \wedge A) \Longrightarrow B$,

9. Auguste De Morgan (1806-1871), mathématicien et logicien britannique.

— $(\neg A \Longrightarrow A) \Longrightarrow A$,
— $(A \Longrightarrow B) \vee (C \Longrightarrow A)$,
— $((A \Longrightarrow B) \wedge (B \Longrightarrow C)) \Longrightarrow (A \Longrightarrow C)$ (règle du modus ponens).

Démonstration.
◇ Montrons le modus ponens.

Première méthode : Supposons que $(A \Longrightarrow B) \wedge (B \Longrightarrow C)$.
On veut montrer que $A \Longrightarrow C$. Pour cela, supposons A et montrons C.
A et $A \Longrightarrow B$ étant vraies, B est vraie.
De même, B et $B \Longrightarrow C$ étant vraies, C est vraie.

Avec les tables de vérité :

A	B	C	$A \Longrightarrow B$	$B \Longrightarrow C$	$(A \Longrightarrow B) \wedge (B \Longrightarrow C)$	$A \Longrightarrow C$	$((A \Longrightarrow B) \wedge (B \Longrightarrow C)) \Longrightarrow (A \Longrightarrow C)$
V	V	V	V	V	V	V	V
V	V	F	V	F	F	F	V
V	F	V	F	V	F	V	V
V	F	F	F	V	F	F	V
F	V	V	V	V	V	V	V
F	V	F	V	F	F	V	V
F	F	V	V	V	V	V	V
F	F	F	V	V	V	V	V

◇ $(A \Longrightarrow B) \vee (C \Longrightarrow A)$ est une tautologie, car lorsque A est fausse, $A \Longrightarrow B$ est vraie, et lorsque A est vraie, $C \Longrightarrow A$ est vraie. □

Définition. On dit que deux propositions P et Q sont logiquement équivalentes si et seulement si la proposition $P \Longleftrightarrow Q$ est une tautologie. On note alors $P \equiv Q$.
Ainsi, lorsque l'on ne s'intéresse qu'à la valeur booléenne des propositions, on peut remplacer toute proposition par une proposition qui lui est logiquement équivalente.

Exemple. La distributivité de $\wedge$ par rapport à $\vee$ signifie que les formules $(A \wedge (B \vee C))$ et $((A \wedge B) \vee (A \wedge C))$ sont logiquement équivalentes.

Définition. La contraposée de l'implication $A \Longrightarrow B$ est égale à $\neg B \Longrightarrow \neg A$.
Toute implication est logiquement équivalente à sa contraposée.

Démonstration.
D'après la tautologie 12, $(A \Longrightarrow B) \equiv A \vee (\neg B)$ et
$(\neg B \Longrightarrow \neg A) \equiv (\neg B) \vee (\neg\neg A) \equiv A \vee (\neg B)$. □

Remarque. Les tautologies 3 à 13 sont des $\Longleftrightarrow$, donc elles énoncent que deux propositions sont logiquement équivalentes. Elles permettent d'écrire une succession d'expressions connectéees par le symbole $\equiv$, c'est-à-dire de faire du *calcul booléen*.

2.3 Négation d'une proposition

◇ Les lois de Morgan permettent de nier une conjonction ou une disjonction :
$\neg(A \vee B)$ est logiquement équivalente à $(\neg A) \wedge (\neg B)$,

$\neg(A \wedge B)$ est logiquement équivalente à $(\neg A) \vee (\neg B)$.
$\diamond$ La négation d'une négation redonne la propriété initiale :
$\neg(\neg A)$ est logiquement équivalente à A.
$\diamond$ La négation d'une implication est plus délicate. Informellement, $A \Longrightarrow B$ est fausse si et seulement si A est vraie alors que B est fausse. Ainsi, lorsque A est fausse, il n'y a pas de problème, $A \Longrightarrow B$ est vraie.
Formellement, $\neg(A \Longrightarrow B)$ est logiquement équivalente à $A \wedge (\neg B)$.
$\diamond$ Une équivalence est la conjonction de deux implications, donc
$\neg(A \Longleftrightarrow B)$ est logiquement équivalente à $[\neg(A \Longrightarrow B)] \vee [\neg(B \Longrightarrow A)]$.

Propriété. Soit P un prédicat sur un ensemble E.
L'assertion "$\forall x \in E,\ P(x)$" est fausse si et seulement si il existe $x \in E$ tel que $\neg P(x)$.
Ainsi, $\neg[\forall x \in E,\ P(x)] \Longleftrightarrow [\exists x \in E,\ \neg P(x)]$.
De même, $\neg[\exists x \in E,\ P(x)] \Longleftrightarrow [\forall x \in E,\ \neg P(x)]$.

Exemple. On dispose maintenant de toutes les propriétés nécessaires pour nier n'importe quelle formule mathématique. Par exemple :

- Un ensemble A est inclus dans un ensemble B si et seulement si : $\forall x \in A,\ x \in B$.
  On en déduit que A n'est pas inclus dans B si et seulement si : $\exists x \in A,\ x \notin B$.
- Une fonction f de $\mathbb{R}$ dans $\mathbb{R}$ est croissante si et seulement si :
  $\forall x, y \in \mathbb{R},\ x \leq y \Longrightarrow f(x) \leq f(y)$.
  Ainsi, f n'est pas croissante si et seulement si :
  $\exists x, y \in \mathbb{R},\ (x \leq y) \wedge (f(x) > f(y))$: peu de rapport avec la décroissance de f.
- Une suite $(x_n)_{n\in\mathbb{N}}$ de réels converge vers 0 si et seulement si :
  $\forall \varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall n \in \mathbb{N},\ [n \geq N \Longrightarrow |x_n| \leq \varepsilon]$. Ainsi, une suite $(x_n)_{n\in\mathbb{N}}$ de réels ne converge pas vers 0 si et seulement si :
  $\exists \varepsilon > 0,\ \forall N \in \mathbb{N},\ \exists n \in \mathbb{N},\ (n \geq N) \wedge (|x_n| > \varepsilon)$.

Propriété. Soit A et B deux ensembles de E.
Soit $(E_i)_{i\in I}$ une famille de parties de E, avec $I \neq \emptyset$. Alors,

- $\overline{\overline{A}} = A$, $\quad \overline{A \cup B} = \overline{A} \cap \overline{B}$, $\quad \overline{A \cap B} = \overline{A} \cup \overline{B}$,
- $A \subset B \Longleftrightarrow \overline{B} \subset \overline{A}$,
- $\overline{\bigcap_{i\in I} E_i} = \bigcup_{i\in I} \overline{E_i}$, , $\qquad \overline{\bigcup_{i\in I} E_i} = \bigcap_{i\in I} \overline{E_i}$.

3 Relations binaires

3.1 Définitions

Définition. Soit E et F deux ensembles.
Une relation binaire R sur $E \times F$ est une partie de $E \times F$.
Lorsque la partie R est appelée une relation binaire, on convient,
pour tout $(x, y) \in E \times F$, de noter "xRy" au lieu de "$(x, y) \in R$".

Le graphe de la relation binaire R est $\{(x,y) \in E \times F / xRy\}$, donc le graphe de R est ... égal à R.

Remarque. Il s'agit donc juste d'un changement de notations et de vocabulaire. Sans cela, la définition donnée ci-dessous de la transitivité d'une relation binaire serait peu intuitive.
Le fait de changer de langage n'est pas anodin en mathématiques. Une même propriété se traduit différemment selon le langage utilisé. Elle peut être plus facile à démontrer dans un langage plutôt qu'un autre.

Exemple. Prenons pour E l'ensemble des êtres humains, et pour F l'ensemble de tous les prénoms. Lorque $(x,y) \in E \times F$, on convient que xRy si et seulement si le prénom y est l'un des prénoms de l'être humain x.
R est une relation binaire sur $E \times F$.

Remarque. Lorsque E et F sont finis, il existe plusieurs manières de représenter une relation R sur $E \times F$:

- Par un tableau : on dispose les éléments de E sur la première colonne, ceux de F sur la première ligne. On place une croix dans les cases correspondant à la ligne $x \in E$ et à la colonne $y \in F$ si et seulement si xRy.
- Avec des patates : on représente les ensembles E et F par des formes patatoïdales. On dessine une flèche d'un élément x de E vers un élément y de F si et seulement si xRy.
- Lorsque $E = F$, la représentation précédente devient un graphe orienté dont les sommets sont les éléments de E.

Définition. Lorsque $E = F$, on dit que R est une relation binaire sur E (plutôt que sur E^2). Dans ce cas,

- R est réflexive si et seulement si $\forall x \in E,\ \ xRx$,
- R est symétrique si et seulement si $\forall x, y \in E,\ \ (xRy) \Longrightarrow (yRx)$,
- R est antisymétrique si et seulement si $\forall x, y \in E,\ \ [(xRy) \wedge (yRx) \Longrightarrow x = y]$,
- et R est transitive si et seulement si $\forall x, y, z \in E,\ \ [(xRy) \wedge (yRz) \Longrightarrow (xRz)]$.

Exemple. L'égalité est une relation binaire sur tout ensemble E. Elle est réflexive, symétrique, antisymétrique et transitive.

Exemple. Si E est l'ensemble des droites de l'espace usuel (de dimension 3), la relation d'orthogonalité est symétrique, mais elle n'est ni réflexive, ni antisymétrique, ni transitive.

3.2 Relations d'ordre

Définition. Une relation binaire R sur un ensemble E est appelée une relation d'ordre si et seulement si R est réflexive, antisymétrique et transitive.

Exemple. Si A est un ensemble, la relation d'inclusion est une relation d'ordre sur $\mathcal{P}(A)$.

Définition. Une relation d'ordre R sur un ensemble E est totale si et seulement si pour tout couple (x, y) de E^2, x et y sont comparables, c'est-à-dire $(xRy) \vee (yRx)$.
Sinon, on dit que R est un ordre partiel.

Exemple. La relation d'inclusion sur $\mathcal{P}(A)$ n'est pas totale dès que A possède plus de deux éléments.
En effet, si a et b sont deux éléments distincts de A, $\{a\}$ et $\{b\}$ ne sont pas comparables.

Exemple. Prenons $E = \mathcal{F}([0, 1], \mathbb{R})$. Si $f, g \in E$, on convient que $f \leq g$ si et seulement si pour tout $t \in [0, 1]$, $f(t) \leq g(t)$. On définit ainsi une relation d'ordre sur E. C'est un ordre partiel, car en posant par exemple $f(x) = x$ et $g(x) = 1 - x$, on a $\neg(f \leq g)$ et $\neg(g \leq f)$.

Notation. Pour la suite de ce paragraphe, on fixe une relation d'ordre sur un ensemble E, que l'on note "$\preceq$".
Pour tout $x, y \in E$, on convient de noter $x \prec y$ si et seulement si $x \preceq y$ et $x \neq y$ et on convient que $x \succeq y$ si et seulement si $y \preceq x$.
La relation $\succeq$ est aussi une relation d'ordre (appelée l'ordre réciproque de $\preceq$), mais la relation d'*ordre strict* $\prec$ n'est pas réflexive, donc ce n'est pas une relation d'ordre.
Attention : lorsque l'ordre n'est pas total, $\neg(x \preceq y)$ n'est pas équivalent à $x \succ y$.

Remarque. Pour la relation d'inclusion, l'usage est d'utiliser le symbole $\subset$ pour désigner la relation d'ordre d'inclusion, et non $\subseteq$.

Exemple. On définit sur E^2 la relation binaire $\mathcal{L}$ par :
$\forall (x, y), (a, b) \in E^2,\ \ (x, y)\mathcal{L}(a, b) \iff [(x \prec a) \vee ((x = a) \wedge (y \preceq b))]$.
Vérifier que $\mathcal{L}$ est une relation d'ordre.
Montrer que $\mathcal{L}$ est totale si et seulement si $\preceq$ est totale.
Lorsque E est l'ensemble des lettres de l'alphabet et que $\preceq$ est l'ordre usuel a, b, c, …, z, on vient de définir l'ordre lexicographique entre mots de deux lettres.
Généraliser aux mots de n lettres. On définit ainsi une relation binaire $\mathcal{L}_n$ sur E^n.
Montrer que c'est un ordre et qu'il est total si et seulement si $\preceq$ est total.

Définition. Soit F une partie de E et $m \in E$. On dit que m est un majorant de F si et seulement si pour tout $a \in F$, $a \preceq m$. On définit de même la notion de minorant d'une partie de E.
On dit qu'une partie est majorée si et seulement si elle possède au moins un majorant.
On dit qu'une partie est minorée si et seulement si elle possède au moins un minorant.
On dit qu'une partie est bornée si et seulement si elle est majorée et minorée.

Exemple. Posons $\mathcal{P}(A) = E$, muni de la relation d'inclusion.
Toute partie F de E est minorée par $\emptyset$ et majorée par A.
Si F est une partie de E et si $B \in E$, B est un majorant de F si et seulement si $B \supset \bigcup_{D \in F} D$, et B est un minorant de F si et seulement si $B \subset \bigcap_{D \in F} D$.
Dans ce contexte, on peut convenir que l'intersection vide est égale à A.

Définition. Si F est une partie de E et $m \in E$, on dit que m est le maximum de F si et seulement si m majore F et $m \in F$. On défnit de même le minimum de F.
Ainsi que cette définition le sous-entend, si une partie possède un maximum (resp : un minimum), il est unique. Il est noté $\max(E)$ (resp : $\min(E)$).

Exemple. Reprenons l'exemple précédent. Alors $\emptyset = \min(E)$ et $A = \max(E)$.
Si $F = \{\{a\}, \{b\}\}$ avec $a \neq b$, F ne possède ni maximum, ni minimum.
Si F est une partie quelconque de E, l'ensemble des majorants de F possède un minimum, égal à $\bigcup_{D \in F} D$. De même, l'ensemble des minorants de F possède un maximum, égal à $\bigcap_{D \in F} D$.

Définition. Si F est une partie de E, un élément m de F est dit maximal si et seulement si $\forall x \in F(x \succeq m \Longrightarrow x = m)$, i.e si et seulement si $\forall x \in F \ \neg(m \prec x)$.
Il est minimal si et seulement si $\forall x \in F(x \preceq m \Longrightarrow x = m)$, i.e si et seulement si $\forall m \in F \ \neg(m \succ x)$.

Démonstration.
Soit $x \in F$: $(x \succeq m \Longrightarrow x = m) \equiv \neg(x \succeq m) \vee (x = m)$ et
$\neg(m \prec x) \equiv \neg(m \preceq x \wedge m \neq x) \equiv \neg(x \succeq m) \vee (x = m)$. □

Exemple. Toujours avec le même exemple, Si $F = \mathcal{P}(A) \setminus \{\emptyset\}$, les éléments minimaux de F sont exactement les singletons.

Propriété. Lorsque la relation d'ordre est totale, toute partie F de E possède au plus un élément maximal et dans ce cas, c'est le maximum de F. Idem avec minimal et minimum.

Remarque. Ainsi, pour une relation d'ordre totale, les notions d'éléments minimaux et maximaux sont inutiles.

Remarque. La réciproque de la propriété précédente est vraie. En effet, supposons que E est muni d'une relation d'ordre partiel. Alors il existe deux éléments a et b de E qui ne sont pas comparables. L'ensemble $\{a, b\}$ admet a et b comme éléments maximaux.

> **Exercice.** Si E est un ensemble fini et non vide, pour tout ordre défini sur E, montrer que E possède au moins un élément minimal.
>
> **Solution :** Considérons un ordre $\leq$ sur E et supposons que E ne possède aucun élément minimal pour cet ordre.
> E étant non vide, il existe $a_0 \in E$.
> a_0 n'est pas un élément minimal de E, donc il existe $a_1 \in E$ avec $a_1 < a_0$.
> a_1 n'est pas un élément minimal de E, donc il existe $a_2 \in E$ avec $a_2 < a_1$.
> Soit $n \in \mathbb{N}$. Supposons construits $a_0, \ldots, a_n$ E tels que,
> pour tout $i \in \{0, \ldots, n-1\}$, $a_{i+1} < a_i$.
> a_n n'est pas un élément minimal de E, donc il existe $a_{n+1} \in E$ avec $a_{n+1} < a_n$.

On a ainsi fourni un procédé de construction par récurrence d'une suite (a_k) strictement décroissante d'éléments de E.
Pour tout $i < j$, $a_j < a_i$, donc $\{a_i \ / \ i \in \mathbb{N}\}$ est infini, ce qu'il fallait démontrer.

3.3 L'ordre naturel et la soustraction

L'ordre naturel : Pour tout $n, m \in \mathbb{N}$,
on convient que $n \leq m$ si et seulement si $\exists k \in \mathbb{N},\ \ m = n + k$.
Dans ce cas, k est unique. On le note $k = m - n$.

Démonstration.
Pour l'unicité, il faut montrer que, si $n + k = n + h$, alors $k = h$.
Fixons $h, k \in \mathbb{N}$. Notons $R(n)$: si $n + k = n + h$, alors $k = h$.
$R(0)$ est vraie. Pour $n \in \mathbb{N}$, supposons $R(n)$.
Supposons que $s(n)+k = s(n)+h$. Alors $s(n+k) = s(n+h)$, donc d'après le troisième axiome de Peano, $n + k = n + h$. D'après $R(n)$, $h = k$. □

Définition. On vient de montrer que, si n est un entier naturel,
pour tout $h, k \in \mathbb{N}$, $n + h = n + k$ implique $h = k$.
On dit que n est régulier.

Remarque. Par définition de l'opérateur "$-$", on a :
pour tout $m, n \in \mathbb{N}$ tel que $n \leq m$, $n + (m - n) = m$.
Pour tout $n \in \mathbb{N}$, $n \leq n$ et $n - n = 0$.
Pour tout $n \in \mathbb{N}$, $0 \leq n$ et $n - 0 = n$.

Propriété. Sous condition d'existence des différences, on a, pour tout $n, m, k \in \mathbb{N}$:
$(n - m) - k = n - (m + k)$ et $n - (m - k) = (n - m) + k = (n + k) - m$.
En particulier l'opérateur "$-$" n'est pas associatif.

Démonstration.
◇ On suppose que $m \leq n$: il existe $a \in \mathbb{N}$ tel que $n = m + a$. Alors $a = n - m$.
On suppose de plus que $k \leq a$: il existe $b \in \mathbb{N}$ tel que $a = k + b$.
Alors $(n - m) - k = a - k = b$. De plus $n = m + a = m + k + b$, donc $m + k \leq n$ et $n - (m + k) = b$. On a bien montré que $(n - m) - k = n - (m + k)$
◇ On suppose que $k \leq m$: il existe $a \in \mathbb{N}$ tel que $m = k + a$. Alors $m - k = a$.
On suppose de plus que $a \leq n$: il existe $b \in \mathbb{N}$ tel que $n = a + b$.
Alors $n - (m - k) = n - a = b$. Or $n + k = (k + a) + b = m + b$,
donc $m \leq n + k$ et $(n + k) - m = b$.
On suppose de plus que $m \leq n$: il existe $c \in \mathbb{N}$ tel que $n = m + c$.
$n = a + b = m + c = k + a + c$, donc par régularité de a, $b = k + c$.
Ainsi $(n - m) + k = c + k = b$. □

Lemme : 0 est l'unique élément de $\mathbb{N}$ qui n'est pas le successeur d'un autre entier.
Il est équivalent de dire que, pour tout $n \in \mathbb{N}$, $n \neq 0$ si et seulement si il existe $k \in \mathbb{N}$ tel que $n = s(k)$.

Démonstration.
Notons $F = \{0\} \cup \{s(k)/k \in \mathbb{N}\}$. D'après le dernier axiome de Peano, $F = \mathbb{N}$. Ainsi chaque élément non nul de $\mathbb{N}$ est le successeur d'un entier, mais d'après le second axiome de Peanon, ce n'est pas le cas de 0. □

Propriétés de l'ordre naturel :
- Réflexivité : $\forall n \in \mathbb{N},\ n \leq n$.
- Antisymétrie : Pour tout $n, m \in \mathbb{N}$, si $n \leq m$ et $m \leq n$, alors $n = m$.
- Transitivité : Pour tout $n, m, p \in \mathbb{N}$, si $n \leq m$ et $m \leq p$, alors $n \leq p$.

Ainsi, l'ordre naturel est bien une relation d'ordre sur $\mathbb{N}$.

Démonstration.
◇ $n = n + 0$, donc $n \leq n$.
◇ Supposons que $n \leq m$ et $m \leq n$. Il existe $a, b \in \mathbb{N}$ tels que $m = n + a$ et $n = m + b$.
Alors $m = m + b + a$, or m est régulier, donc $b + a = 0$.
Si $a \neq 0$, d'après le lemme, il existe $c \in \mathbb{N}$ tel que $a = s(c)$, donc $0 = s(c) + b = s(c + b)$, ce qui est impossible. Ainsi $a = 0$ puis $m = n$.
◇ Supposons que $n \leq m$ et $m \leq p$. Il existe $a, b \in \mathbb{N}$ tels que $m = n + a$ et $p = m + b$.
Alors $p = n + (a + b)$, donc $n \leq p$. □

Propriété. Soit $m, n \in \mathbb{N}$. On note $m < n$ lorsque $m \leq n$ et $m \neq n$.
Si $m < n$, alors $m + 1 \leq n$.

Démonstration.
Supposons que $m < n$. Il existe $a \in \mathbb{N}$ tel que $n = m + a$ et $a \neq 0$.
D'après le lemme, il existe $b \in \mathbb{N}$ tel que $a = s(b)$, donc $n = m + b + 1$ et $n \geq m + 1$. □

Propriété. L'ordre naturel est un ordre total sur $\mathbb{N}$.

Démonstration.
Soit $N \in \mathbb{N}$. Notons $R(N)$: pour tout $n, m \in \mathbb{N}$ tels que $n \leq N$ et $m \leq N$, n et m sont comparables.
$R(0)$ est vraie.
Supposons $R(N)$. Soit $n, m \in \mathbb{N}$ tels que $n \leq N + 1$ et $m \leq N + 1$.
Si $n \leq N$ et $m \leq N$, n et m sont comparables d'après $R(N)$.
Sinon, on a par exemple $n > N$, donc $n \geq N + 1$, puis $n = N + 1$. Alors $m \leq n$.
On a prouvé $R(N + 1)$. □

La relation d'ordre est compatible avec l'addition :
Pour tout $a, b, c, d \in \mathbb{N}$, si $a \leq b$ et $c \leq d$, alors $a + c \leq b + d$.

Démonstration.
Supposons que $a \leq b$ et $c \leq d$. Il existe $e, f \in \mathbb{N}$ tels que $b = a + e$ et $d = c + f$. Alors $b + d = (a + c) + (e + f)$, donc $a + c \leq b + d$. □

3.4 Multiplication dans $\mathbb{N}$ et relation de divisibilité

Multiplication entre entiers :
Pour tout $m \in \mathbb{N}$, on pose

$0 \times m = 0$ et
$\forall n \in \mathbb{N},\ \ s(n) \times m = n \times m + m$.
Ces conditions définissent la multiplication entre entiers.

Démonstration.
Exercice. □

Remarque. On note souvent nm au lieu de $n \times m$.

Exemple. $3m = s(s(s(0))) \times m = s(s(0)) \times m + m = s(0) \times m + m + m = m + m + m$.
Ainsi, nm est défini, moins formellement, par la propriété $nm = \underbrace{m + \cdots + m}_{n fois}$.

Propriétés de la multiplication :
- 0 est absorbant : $\forall m \in \mathbb{N},\ \ m \times 0 = 0 \times m = 0$.
- 1 est neutre : $\forall m \in \mathbb{N},\ \ m \times 1 = 1 \times m = m$.
- Distributivité de la multiplication par rapport à l'addition :
  $\forall n, m, p \in \mathbb{N},\ \ n(m+p) = (nm)+(np) = nm+np$: les dernières parenthèses sont inutiles si l'on convient que la multiplication est prioritaire devant l'addition.
- Associativité : $\forall n, m, k \in \mathbb{N},\ \ (n \times m) \times k = n \times (m \times k)$.
- Commutativité : $\forall n, m \in \mathbb{N},\ \ n \times m = m \times n$.

Démonstration.
Exercice. □

Propriété. Pour tout $a, b, c \in \mathbb{N}$, si $a \leq b$, alors $c(b-a) = cb - ca$.

Démonstration.
Posons $r = b - a$. On sait que $b = a + r$, donc $cb = ca + cr$. Ainsi, $ca \leq cb$ et $cb - ca = cr = c(b-a)$. □

La relation d'ordre est compatible avec la multiplication :
Pour tout $a, b, c, d \in \mathbb{N}$, si $a \leq b$ et $c \leq d$, alors $ac \leq bd$.

Démonstration.
Supposons que $a \leq b$ et $c \leq d$. Il existe $e \in \mathbb{N}$ tels que $b = a+e$. Alors $bc = ac+ec \geq ac$.
De même, on montre que $db \geq cb$ et on conclut par transitivité. □

Propriété. Soit $n, k \in \mathbb{N}$.
Si $nk = 0$, alors $n = 0$ ou $k = 0$.
Si $nk = 1$, alors $n = k = 1$.

Démonstration.
◇ Raisonnons par contraposition : supposons que $n \neq 0$ et $k \neq 0$.
Alors $n > 0$, donc $n \geq 1$. De même $k \geq 1$, puis $kn \geq 1 \times 1 = 1$ et $kn \neq 0$.
◇ Supposons que $nk = 1$.
$n \neq 0$ et $k \neq 0$, donc $n \geq 1$ et $k \geq 1$.
Si $n \neq 1$, alors $n \geq 2$ puis $nk \geq 2 > 1$. C'est impossible. □

Définition. Soit $n, m \in \mathbb{N}$. On dit que n divise m, que n est un diviseur de m, ou encore que m est un multiple de n si et seulement si il existe $k \in \mathbb{N}$ tel que $m = kn$. On note $n|m$.

Remarque. Tout entier divise 0 mais 0 ne divise que lui-même.

Définition. On appelle nombre premier tout entier n supérieur à 2 dont les seuls diviseurs sont 1 et n.

Propriété. La relation de divisibilité est une relation d'ordre partielle sur $\mathbb{N}$.

Démonstration.
Exercice. □

3.5 Maximum et minimum dans $\mathbb{N}$

Propriété. Toute partie non vide et majorée de $\mathbb{N}$ possède un maximum.

Démonstration.
Notons $R(n)$ la propriété suivante : toute partie non vide de $\mathbb{N}$ majorée par n possède un plus grand élément.
◇ Pour $n = 0$, l'unique partie non vide de $\mathbb{N}$ majorée par 0 est $\{0\}$. Elle possède bien un plus grand élément.
◇ Soit $n \geq 1$. Supposons $R(n-1)$.
Soit A une partie non vide de $\mathbb{N}$ majorée par n.
Premier cas : Si $n \notin A$, alors A est majorée par $n-1$ et on utilise $R(n-1)$.
Deuxième cas : Si $n \in A$, n est le plus grand élément de A. □

Remarques :
- La réciproque est vraie.
- $\mathbb{N}$ n'est pas majoré.

Propriété. Soit $a, b \in \mathbb{N}$ avec $b \neq 0$. Il existe un unique couple $(q, r) \in \mathbb{N}^2$ tel que $a = bq + r$ et $0 \leq r < b$. On dit que q et r sont le quotient et le reste de la division euclidienne de a par b.

Exemple. $27 = 6 \times 4 + 3 = 6 \times 3 + 9 = 6 \times 5 - 3$, mais seul 3 est le reste de la division euclidienne de 27 par 6.
$31 = 10 \times 3 + 1$ et $-31 = (-11) \times 3 + 2$, donc, une fois que nous aurons prolongé la division euclidienne sur $\mathbb{Z}$, le reste de la division euclidienne de -31 par 10 n'est pas l'opposé du reste de 31 par 10.

Démonstration.
◇ Posons $A = \{k \in \mathbb{N} / bk \leq a\}$.
$b \geq 1$, donc pour tout $k \in A$, $k \leq bk \leq a$. Ainsi, A est majorée, or elle est non vide car $0 \in A$, donc A possède un maximum noté q. Par construction, $bq \leq a < b(q+1)$.
Ainsi, il existe $r \in \mathbb{N}$ tel que $a = bq + r$ et $r = a - bq < b$. Ceci prouve l'existence.
◇ Pour montrer l'unicité, supposons de plus que $a = bq' + r'$ avec $q', r' \in \mathbb{N}$ et $0 \leq r' < b$.
Supposons que $r \geq r'$ (la démonstration s'adapte lorsque $r' \geq r$).
Il existe $r'' \in \mathbb{N}$ tel que $r = r' + r''$. $r = r' + r''$, donc $bq' + r' = a = bq + r = bq + r' + r''$.
Par régularité de r', $bq' = bq + r''$, donc $bq' \geq bq$.
$b \geq 1$, donc $q' \geq q$. Ainsi, $r'' = bq' - bq = b(q' - q)$.

Supposons que $q \neq q'$. Alors $q' - q \geq 1$, donc $r'' \geq b$ puis $r \geq b + r' \geq b$ ce qui est faux. Ainsi, $q = q'$, puis $r = r'$. □

Exercice. Diviser 3378 par 53.
Solution : $53 \times 6 = 318$, donc $337 = 53 \times 6 + 19$. Ainsi, $3378 = 53 \times 60 + 198$. Mais $198 = 3 \times 53 + 39$, donc $3378 = 53 \times 63 + 39$.
On présente en général ce calcul sous la forme suivante :

$$\begin{array}{rcccc|cc} & 3 & 3 & 7 & 8 & 5 & 3 \\ - & 3 & 1 & 8 & & \multicolumn{2}{l}{6} \\ \cline{1-4} & & 1 & 9 & & & \end{array}$$

$$\begin{array}{rcccc|cc} & 3 & 3 & 7 & 8 & 5 & 3 \\ - & 3 & 1 & 8 & & 6 & 3 \\ \cline{1-4} & & 1 & 9 & 8 & & \\ - & & 1 & 5 & 9 & & \\ \cline{2-5} & & & 3 & 9 & & \end{array}$$

Propriété. Toute partie non vide de $\mathbb{N}$ possède un minimum.

Démonstration.
Soit A une partie non vide de $\mathbb{N}$.
Notons M l'ensemble des minorants de A.
$0 \in M$, donc M est non vide. Elle est majorée par n'importe quel élément de A.
D'après la propriété précédente, M possède un plus grand élément, que l'on notera m.
Si $m \notin A$, pour tout $n \in A$, $n > m$, donc $n \geq m + 1$. Alors $m + 1$ est encore un minorant de A, donc il est plus petit que m, ce qui est faux. Ainsi $m \in A$. C'est le plus petit élément de A. □

Remarque. Un ensemble ordonné dont toute partie non vide possède un plus petit élément est appelé un ensemble bien ordonné.

Paradoxe de Berry[10] : Notons n le plus petit entier qui n'est pas définissable en moins de 100 mots.
L'ensemble des entiers définissables en moins de 100 mots est une partie finie de $\mathbb{N}$, car le nombre de mots de la langue française est fini, donc son complémentaire dans $\mathbb{N}$ est une partie non vide de $\mathbb{N}$, qui possède bien un plus petit élément. Ainsi, la définition de n est correcte.
Cependant c'est une définition de n utilisant strictement moins de 100 mots, alors que par définition, n n'est pas définissable en moins de 100 mots !
Les logiciens du début du vingtième siècle ont compris que la solution de ce paradoxe nécessite de distinguer le langage utilisé au sein d'une théorie du métalangage utilisé pour parler de cette théorie. Ainsi, dans la première phrase, "définissable" signifie "que l'on peut définir dans le cadre du langage de l'arithmétique". Cette même phrase définit bien l'entier n, mais cette définition utilise un métalangage décrivant des phrases du langage arithmétique. Le paradoxe est ainsi levé ; la phrase "notons n le plus petit

10. Personnage fictif inventé par Russell.

entier qui n'est pas définissable en moins de 100 mots selon le langage de la théorie arithmétique" est une définition de n selon le métalangage de cette même théorie.

Remarque. Le fait que $\mathbb{N}$ est bien ordonné se démontre essentiellement à partir du principe de récurrence, c'est-à-dire à partir du dernier axiome de Peano. Mais on peut également démontrer la réciproque : remplaçons le dernier axiome de Peano par le fait que $\mathbb{N}$ est bien ordonné et démontrons le principe de récurrence.
Soit F une partie de $\mathbb{N}$ contenant 0 et telle que pour tout $n \in F$, $s(n) \in F$. Il faut montrer que $F = \mathbb{N}$.
Sinon, $\mathbb{N} \setminus F$ est une partie non vide de $\mathbb{N}$, donc elle possède un plus petit élément que l'on notera m. $m \neq 0$ car $0 \in F$.
Il faut de plus remplacer le second axiome par l'énoncé plus fort du lemme de la page 18. Ainsi il existe $n \in \mathbb{N}$ tel que $m = s(n)$.
$n < m$ donc par définition de m, $n \in F$. Mais alors $m = s(n) \in F$, ce qui est faux.
Ainsi, le principe de récurrence est équivalent au fait que $\mathbb{N}$ est bien ordonné.
Il importe de retenir de cette remarque que lorsqu'une démonstration par récurrence semble délicate, il peut être plus simple d'utiliser directement que $\mathbb{N}$ est bien ordonné.

> **Exercice.** En adaptant cette démonstration, montrer le principe de récurrence finie.

Principe de la descente infinie : plus précisément, pour montrer que "$\forall n \in \mathbb{N},\ \ R(n)$", une alternative à la récurrence est de raisonner par l'absurde en supposant qu'il existe $n \in \mathbb{N}$ tel que $\neg[R(n)]$ et d'en déduire l'existence d'un entier naturel m tel que $m < n$ et tel que $\neg[R(m)]$. Cela permet de construire une suite strictement décroissante d'entiers naturels n_k vérifiant $\neg[R(n_k)]$, ce qui est absurde. Mais pourquoi au fait ?
Il est préférable de remplacer cet argument de descente infinie par le suivant :
On note $F = \{n \in \mathbb{N} / \neg R(n)\}$. Il est non vide par hypothèse, donc il possède un minimum n_0, mais il existe alors $m < n_0$ tel que $m \in F$, ce qui est impossible.

Exemple. C'est ainsi que Gauss[11] démontre le lemme d'Euclide[12](dans le cours d'arithmétique, on démontrera autrement un théorème plus général, appelé le lemme de ... Gauss) :
Soit $a, b, p \in \mathbb{N}$ tels que p est premier et $p|ab$. Il s'agit de montrer que $[p|a] \vee [p|b]$.
Pour cela, fixons p premier et $a \in \mathbb{N}$ tel que $p \not| a$.

11. Johann Carl Friedrich Gauss, 1777-1855, est un mathématicien, astronome et physicien allemand. Il a apporté de très importantes contributions à ces trois domaines. Surnommé "le prince des mathématiciens", il est considéré comme l'un des plus grands mathématiciens de tous les temps.

Refusant de publier un travail qu'il ne considérait pas au-dessus de toute critique, son journal montre qu'il avait fait plusieurs importantes découvertes mathématiques des années, voire des décennies, avant qu'elles ne soient publiées par ses contemporains.

Il rechignait à présenter l'intuition derrière ses très élégantes démonstrations. Il préférait qu'elles apparaissent comme sorties de nulle part et effaçait toute trace du processus de sa découverte, "de même qu'un architecte ne laisse pas l'échafaudage une fois l'édifice achevé".

12. Euclide est un mathématicien de la Grèce antique. Il est vraisemblable qu'il ait vécu vers 300 avant notre ère. Son ouvrage principal, "les Éléments" aborde la géométrie (euclidienne) et l'arithmétique selon une démarche axiomatique et déductive.

Il s'agit alors de montrer que pour tout $b \in \mathbb{N}$, si $p|ab$, alors $p|b$.
Pour cela, raisonnons par l'absurde en supposant que l'ensemble
$B = \{b \in \mathbb{N}/p|ab \text{ et } p \not| b\}$ est non vide. Alors il possède un minimum noté b_0.
Si $b_0 \geq p$, alors $b_0 - p \in B$ ce qui contredit la minimalité de b_0, donc $0 < b_0 < p$.
On peut écrire la division eucldienne de p par b_0 : il existe $q, b_1 \in \mathbb{N}$ tels que $p = qb_0 + b_1$ avec $0 \leq b_1 < b_0$.
Si $b_1 = 0$, alors $p = qb_0$, mais p est premier, donc $b_0 = 1$, or $p|ab_0$, donc $p|a$ ce qui est faux. Ainsi, $b_1 \neq 0$, donc $1 \leq b_1 < p$ puis $p \not| b_1$.
$ab_1 = ap - aqb_0$, donc $p|ab_1$. Ainsi $b_1 \in B$ et $b_1 < b_0$, ce qui est faux.

Remarque. Pour démontrer une propriété de la forme "$\forall n \in \mathbb{N},\ R(n)$", on ne raisonne cependant pas a priori par récurrence. C'est seulement lorsqu'on peut relier $R(n+1)$ à $R(n)$ que c'est une méthode envisageable.

3.6 Relations d'équivalence

Définition. Une relation binaire sur un ensemble E est une relation d'équivalence si et seulement si R est réflexive, symétrique et transitive.

Exemple. Les entiers divisibles par 2 sont dits pairs et les autres impairs.
On note P la relation binaire sur $\mathbb{N}$ définie par : nPm si et seulement si n et m ont la même parité. P est une relation d'équivalence.

Définition. Soit R une relation d'équivalence sur E.
Si $x \in E$, on note $\overline{x}$ l'ensemble des $y \in E$ tels que xRy.
$\overline{x}$ s'appelle la classe d'équivalence de x.
On désigne par E/R l'ensemble des classes d'équivalence : $E/R = \{\overline{x}/x \in E\}$.
E/R s'appelle l'ensemble quotient de E par R.

Exemple fondamental : Soit f une application de E dans F. En convenant, pour tout $x, y \in E$, que $x\ R\ y \iff f(x) = f(y)$, on définit sur E une relation d'équivalence.

Exemples :
- La relation d'égalité est l'unique relation d'équivalence dont les classes d'équivalence sont toutes des singletons. On a $(E/=) = \{\{x\}/x \in E\}$.
- La relation de parité P possède deux classes d'équivalence : $\overline{0}$ est l'ensemble des entiers pairs et $\overline{1}$ est l'ensemble des entiers impairs. Ainsi, $\mathbb{N}/P = \{\overline{0}, \overline{1}\}$.
- Sur l'ensemble des formules propositionnelles, la relation "être logiquement équivalente à " est une relation d'équivalence.
- Si E est l'ensemble des droites du plan, la relation de parallélisme est une relation d'équivalence dont les classes d'équivalence sont les directions du plan.

Propriété. Avec les hypothèses et notations précédentes,
pour tout $x, y \in E$, $xRy \iff \overline{x} = \overline{y}$.

Démonstration.
Supposons que xRy. Soit $z \in \overline{x}$. On a xRz, donc yRz puis $z \in \overline{y}$.
Ainsi, $\overline{x} \subset \overline{y}$. Par symétrie, $\overline{y} \subset \overline{x}$, donc $\overline{x} = \overline{y}$.
Réciproquement, supposons que $\overline{x} = \overline{y}$. xRx, donc $x \in \overline{x}$. Ainsi $x \in \overline{y}$ et xRy. □

Définition. Une partition $\mathcal{P}$ de E est une partie de $\mathcal{P}(E)$ telle que :
- pour tout $A, B \in \mathcal{P}$, $A \neq B \Longrightarrow A \cap B = \emptyset$,
- pour tout $A \in \mathcal{P}$, $A \neq \emptyset$,
- et $\bigcup_{A \in \mathcal{P}} A = E$.

Exemple. Si $E = \{1, \dots, 10\}$, un exemple de partition de E est
$\mathcal{P} = \{\{1\}, \{2, 3, 7, 10\}, \{4, 9\}, \{5, 6, 8\}\}$.

Théorème. Si R est une relation d'équivalence sur E, son ensemble quotient E/R est une partition de E.
Réciproquement, si $\mathcal{P}$ est une partition de E, il existe une unique relation d'équivalence R sur E telle que $\mathcal{P} = E/R$.
Elle est définie par : $\forall x, y \in E,\ \ [xRy \iff (\exists C \in \mathcal{P},\ \ x, y \in C)]$.
En résumé, la donnée d'une relation d'équivalence sur E est équivalente à la donnée d'une partition de E.

Remarque. On peut formaliser un peu plus : si l'on note $\mathcal{R}$ l'ensemble des relations d'équivalence sur E et $\mathbb{P}$ l'ensemble des partitions de E, alors le théorème précédent énonce que l'application $\begin{array}{ccc} \mathcal{R} & \longrightarrow & \mathbb{P} \\ R & \longmapsto & E/R \end{array}$ est une bijection.

Démonstration.
- Supposons que R est une relation d'équivalence.
  - Pour tout $x \in E$, $x \in \overline{x}$, donc $\overline{x} \neq \emptyset$.
  - Soit $x, y \in E$ tels que $\overline{x} \cap \overline{y} \neq \emptyset$. Il existe $z \in E$ tel que $z \in \overline{x} \cap \overline{y}$. On a xRz et zRy, donc xRy puis $\overline{x} = \overline{y}$.
  - Pour tout $x \in E$, $x \in \overline{x} \subset \bigcup_{x \in E} \overline{x}$, donc $E \subset \bigcup_{x \in E} \overline{x}$. L'inclusion réciproque est claire car, pour tout $x \in E$, $\overline{x} \subset E$.

Ainsi E/R est bien une partition de E.
- Réciproquement, soit $\mathcal{P}$ une partition de E. Raisonnons par analyse-synthèse.

Analyse : Supposons qu'il existe une relation d'équivalence R telle que $E/R = \mathcal{P}$.
Soit $x, y \in E$. Si xRy, alors $x, y \in \overline{x}$, donc il existe $C \in \mathcal{P}$ tel que $x, y \in C$.
Réciproquement, supposons qu'il existe $C \in \mathcal{P}$ tel que $x, y \in C$. Sachant que $E/R = \mathcal{P}$, il existe $z \in E$ tel que $C = \overline{z}$.
Alors $\overline{x} = \overline{z} = \overline{y}$, donc xRy. On a donc montré que
(1) : $\forall x, y \in E,\ \ [xRy \iff (\exists C \in \mathcal{P},\ \ x, y \in C)]$.
Ainsi, sous condition d'existence, il existe une unique relation d'équivalence R telle que $E/R = \mathcal{P}$. Elle est définie par (1).
Synthèse : Notons R la relation binaire définie par (1). Elle est clairement symétrique.

Soit $x \in E$. $E = \bigcup_{C \in \mathcal{P}} C$, donc il existe $C \in \mathcal{P}$ tel que $x \in C$. Ainsi, xRx. R est donc réflexive.
Soit $x, y, z \in E$ tels que xRy et yRz. Il existe $C, D \in \mathcal{P}$ tels que $x, y \in C$ et $y, z \in D$. En particulier $y \in C \cap D$, donc $C \cap D \neq \emptyset$, donc $C = D$. Alors $x, z \in C$, donc xRz. On a montré que R est transitive.
Ainsi R est une relation d'équivalence. Pour terminer, il reste à montrer que $E/R = \mathcal{P}$.
$\diamond$ Commençons par montrer que, si $x \in C \in \mathcal{P}$, alors $\overline{x} = C$:
Si $y \in \overline{x}$, il existe $D \in \mathcal{P}$ tel que $x, y \in D$. Alors $x \in C \cap D \neq \emptyset$, donc $C = D$ et $y \in C$. Ainsi $\overline{x} \subset C$. Réciproquement, si $y \in C$, alors $x, y \in C$, donc xRy puis $y \in \overline{x}$. On a bien montré que $\overline{x} = C$.
$\diamond$ Soit $x \in E$. Il existe $C \in \mathcal{P}$ tel que $x \in C$. On a $x \in C \in \mathcal{P}$, donc $\overline{x} = C \in \mathcal{P}$. DONC $E/R \subset \mathcal{P}$.
$\diamond$ Réciproquement, soit $C \in \mathcal{P}$. $C \neq \emptyset$, donc il existe $x \in E$ tel que $x \in C$.
On a encore $x \in C \in \mathcal{P}$, donc $C = \overline{x} \in E/R$. DONC $\mathcal{P} \subset E/R$.
Finalement $E/R = \mathcal{P}$, ce qui clôt la démonstration. □

Remarque. Informellement, les éléments de E/R sont les éléments de E, mais en acceptant d'identifier deux éléments x et y de E lorsque xRy, c'est-à-dire en faisant abstraction [13] de certaines caractéristiques des éléments de E.
Nous allons voir que c'est un procédé puissant pour élaborer des constructions mathématiques.

4 La logique mathématique

Ce chapitre est informel, il est seulement destiné à votre culture personnelle [14].

Définition. Un langage (du premier ordre) est un ensemble de mots (appelés des formules), se conformant à des règles syntaxiques non précisées ici, dont les lettres appartiennent à l'alphabet $\{(,), \neg, \wedge, \vee, \Longrightarrow, \Longleftrightarrow, \forall, \exists\} \cup C \cup V \cup F \cup R$, où

- C est un ensemble de constantes.
- V est l'ensemble des variables : x, y, z etc.
- F est un ensemble de fonctions : si $f \in F$ et si f possède n arguments (on dit que f est d'arité n), on peut par exemple considérer $f(x_1, \ldots, x_n)$ où les x_i sont dans V, mais aussi $f(g(x_1), h(x_2, \ldots, x_n))$ où g et h sont d'autres fonctions d'arités convenables.
- R est un ensemble de relations : si $r \in R$, r est un prédicat dépendant d'un nombre variable d'arguments.

13. Voici la défnition du mot "abstraction" proposée par le Larousse : Opération intellectuelle qui consiste à isoler par la pensée l'un des caractères de quelque chose et à le considérer indépendamment des autres caractères de l'objet.

14. Pour plus de détails, on pourra consulter *Logique mathématique*, Tome 1, de René Cori et Daniel Lascar

Exemple. Le langage de l'arithmétique est donné (par exemple) par $C = \{0\}$, $F = \{s, +, \times\}$, $R = \{=, \leq\}$.
Voici un élément de ce langage, en posant pour simplifier $1 = s(0)$ et $2 = s(1)$:
$(2 \leq p) \wedge (\forall k, \forall h((\neg(h = 1) \wedge \neg(k = 1)) \Longrightarrow \neg(h \times k = p)))$.
Cette formule exprime que p est un nombre premier. Dans cette formule, p est une variable libre alors que k et h sont des variables liées.

Définition. Une formule est close lorsqu'elle ne contient aucune variable libre.
- Une théorie T d'un langage L est un ensemble de formules closes de L.
- Les axiomes logiques de L sont des formules de L qui sont "logiquement vraies", comme toutes les tautologies (par exemple en arithmétique $(0 \leq k) \Longleftrightarrow (0 \leq k)$), la loi de Morgan (pour toute formule F, $\exists v F \Longleftrightarrow \neg\forall v \neg F$), etc. (il s'agit d'une présentation informelle).
- On utilise deux règles de déduction :
  - Le modus ponens : à partir des deux formules F et $F \Longrightarrow G$, on peut déduire la formule G.
  - La règle de généralisation : à partir de la formule F et d'une variable $v \in V$, on peut déduire la formule $\forall v F$.
- Une démonstration formelle d'une formule F de L dans une théorie T est une suite finie de formules $F_0, \ldots, F_n$ telle que $F_n = F$, et pour tout $i \in \{0, \ldots, n\}$,
  - $F_i \in T$, ou bien
  - F_i est un axiome logique, ou bien
  - F_i se déduit d'une ou de deux formules F_k avec $k < i$ par l'une des deux règles de déduction.

Exemple de la théorie des ensembles [15] ***:***
Le langage correspondant est défini par : $C = \{\emptyset\}$, $F = \emptyset$, $R = \{=, \in, \subset\}$.
La théorie ZF de Zermelo-Fraenkel est constituée des axiomes suivants
- L'axiome d'extensionnalité : $\forall x \forall y[\forall z(z \in x \Longleftrightarrow z \in y) \Longrightarrow x = y]$.
- L'axiome de la réunion, affirmant que pour tout ensemble x, il existe un ensemble y dont les éléments sont les éléments des éléments de x :
  $\forall x \exists y \forall z[z \in y \Longleftrightarrow \exists t(t \in x \wedge z \in t)]$.
- L'axiome de l'ensemble des parties, qui affirme que pour tout ensemble a, il existe un ensemble b dont les éléments sont les parties de a.
- L'axiome de l'infini, cf page 2.
- L'axiome de substitution, qui donne un procédé de construction d'ensembles, similaire mais plus précis que la "définition par compréhension", vue page 2, et qui évite l'apparition du paradoxe de Russell et de ses variantes.

Définition. Une théorie T d'un langage L est non contradictoire (on dit aussi consistante ou cohérente) si et seulement si il n'existe aucune formule F telle que F et $\neg F$ soient toutes deux démontrables à partir de T.
Une théorie T d'un langage L est complète si et seulement si pour toute formule F de L, F ou $\neg F$ est démontrable à partir de T.

15. Pour plus de détails, on pourra consulter *Théorie des ensembles*, de Jean-Louis Krivine.

Théorème d'incomplétude de Gödel[16] **:** Soit T une théorie d'un langage L. On suppose que T "contient ZF".
Si T est non contradictoire, alors la propriété "T est non contradictoire" peut être écrite comme une formule du langage L, et cette formule, qui est vraie, n'est pas démontrable à partir de T.
En résumé, une théorie ne peut pas démontrer sa propre consistance.
En particulier, toute théorie non contradictoire contenant ZF n'est pas complète.

Remarque. Le fait de supposer que T est non contradictoire est indispensable. En effet, une théorie contradictoire serait tout à fait capable de démontrer qu'elle ne l'est pas, car une théorie contradictoire permet de montrer $F \wedge (\neg F)$ pour une certaine formule, mais comme $Faux \implies G$ pour toute formule G, une théorie contradictoire est capable de démontrer que toute formule de son langage est vraie (et fausse).

Axiome du choix : en voici deux énoncés équivalents.

- Pour tout ensemble I, pour toute famille $(E_i)_{i\in I}$ d'ensembles tous non vides, il existe une famille $(x_i)_{i\in I}$ telle que, pour tout $i \in I$, $x_i \in E_i$.
- Pour tout ensemble E, pour toute relation d'équivalence sur E, il existe un ensemble R tel que l'intersection de R avec chaque classe d'équivalence est un singleton. Cela signifie qu'on peut choisir dans chaque classe d'équivalence un représentant et considérer l'ensemble de ces représentants.

Théorème d'indépendance de l'axiome du choix :
Notons AC l'axiome du choix.
Si ZF est consistante, alors ZF+AC est aussi consistante (Gôdel, 1938).
Si ZF est consistante, alors ZF+non(AC) est aussi consistante (Cohen[17], 1963).

On a donc le *choix* d'accepter ou de réfuter l'axiome du *choix*.
Par défaut, en mathématiques modernes, on travaille avec ZF+AC, même si cela conduit à quelques résultats étranges :

Paradoxe de Banach-Tarski (1924) :
Notons S la boule unité de l'espace usuel : $S = \{(x, y, z) \in \mathbb{R}^3 / x^2 + y^2 + z^2 \leq 1\}$.
Il existe une partition de S en un nombre fini de parties $D_1, \ldots, D_n$ telles que, en soumettant chaque partie à un déplacement (composition d'une rotation et d'une translation) approprié dans l'espace, leur réunion après déplacements est égale à la réunion disjointe de *deux* sphères de rayon 1.
Les parties D_i ne sont pas "mesurables", ce qui résout le paradoxe.

Propriété. (admise) : Sous l'hypothèse ZF, l'axiome du choix est équivalent à l'axiome de Zermelo ainsi qu'à celui de Zorn, où :

- Axiome de Zermelo : Tout ensemble E peut-être muni d'un bon ordre.

16. Kurt Gödel, 1906-1978, logicien et mathématicien autrichien naturalisé américain. Enfant, sa famille l'avait surnommé "monsieur Pourquoi".

17. Paul Cohen, 1934-2007, est un mathématicien américain, médaille Fields 1966

— Axiome de Zorn : Un ensemble ordonné $(E, \leq)$ possède un élément maximal dès que toutes ses chaînes sont majorées, en convenant qu'une chaîne de E désigne une partie de E totalement ordonnée par $\leq$.

5 L'art de la démonstration

La structure d'une démonstration se construit avant tout en fonction de la structure de la propriété à démontrer. En conséquence, on regarde d'abord la cible à atteindre et seulement lorsque c'est nécessaire les hypothèses dont on dispose pour y parvenir. On ne sait pas a priori sous quelles formes ces hypothèses seront utilisées.
Lorsqu'une telle démarche n'aboutit pas, on essaie plus généralement de décomposer le résultat à atteindre et de traduire les hypothèses pour les rapprocher, par exemple en essayant de les écrire dans un langage commun.
Dans ce chapitre, on notera R le résultat à démontrer.

5.1 Conjonction et disjonction

◇ Lorsque $R = P \wedge Q$, bien entendu, on montre le plus souvent P et Q.
Dans ce cas, il importe de commencer par la propriété qui semble la plus simple, afin de se familiariser en douceur avec le problème à résoudre.

◇ Lorsque $R = P \vee Q$, on peut supposer que P est fausse et démontrer Q, ou bien supposer que Q est fausse et montrer P.
On ajoute ainsi une hypothèse. Il importe de bien choisir parmi ces deux possibilités.

5.2 Démonstration par disjonction de cas

Pour démontrer une propriété dépendant de certains paramètres, on peut être amené à étudier plusieurs cas selon les valeurs de ces paramètres. Il importe que la réunion des différents cas étudiés recouvre tout l'ensemble des valeurs des paramètres.

Exemple. Soit $a, b \in \mathbb{R}$. Résoudre le système (S) : $\begin{cases} x + (4-a)y &= 0 \\ (1-a)x - 2y &= b \end{cases}$.
Ici, la question est ouverte en ce sens que le résultat à obtenir n'est pas explicitement donné. On recherche l'ensemble des couples (x, y) de $\mathbb{R}^2$ (a priori) vérifiant les deux égalités de (S).
Solution :
$(S) \iff \begin{cases} x = (a-4)y \\ (1-a)(a-4)y - 2y = b \end{cases} \iff \begin{cases} x = (a-4)y \\ (-a^2+5a-6)y = b \end{cases}$.
Le discriminant de l'équation $t^2 - 5t + 6 = 0$ vaut $\Delta = 25 - 24 = 1$, donc les racines sont $\dfrac{5 \pm 1}{2}$, soit 2 et 3.
◇ *Premier cas :* on suppose que $a \notin \{2, 3\}$.

$(S) \iff \begin{cases} y &= \dfrac{b}{-a^2+5a-6} \\ x &= \dfrac{b(a-4)}{-a^2+5a-6} \end{cases}$. Ce système possède alors une unique solution dans $\mathbb{R}^2$.
Le fait d'avoir raisonné par équivalence nous affranchit de vérifier que le couple obtenu est bien solution.

◇ *Second cas :* on suppose que $a \in \{2, 3\}$.
Alors $(S) \iff \begin{cases} x = (a-4)y \\ b = 0 \end{cases}$.

— *Premier sous-cas :* si $b \neq 0$, alors (S) ne possède aucune solution.
— *Second sous-cas :* on suppose que $b = 0$. Alors $(S) \iff x = (a-4)y$. L'ensemble des solutions est une droite de $\mathbb{R}^2$, d'équation $x+2y = 0$ lorsque $a = 2$ et $x+y = 0$ lorsque $a = 1$.

5.3 Résoudre une équation

On vient de résoudre un système d'équations. C'est un cas particulier d'équation, dont voici la définition la plus générale possible :

Définition. Si P est un prédicat sur un ensemble E, "résoudre l'équation $P(x)$, en l'inconnue $x \in E$", c'est calculer $\{x \in E / P(x)\}$ qu'on appelle alors l'ensemble des solutions de l'équation.
"calculer" signifie "donner l'ensemble des solutions sous la forme la plus simple possible".

Remarque. La plupart des équations sont de la forme "$f(x) = g(x)$", où f et g sont deux applications de E dans un autre ensemble F.
Lorsque $F = \mathbb{R}$, on rencontre parfois des équations de la forme "$f(x) \leq g(x)$", ou "$f(x) < g(x)$". Dans ce cas, on parle plutôt d'*inéquations*.

Méthode :
— Précisez d'abord pour quelles valeurs $x \in E$ l'équation a bien un sens. Par exemple, pour une équation de la forme "$f(x) = g(x)$", il faudra d'abord rechercher les domaines de définition de f et de g.
— Autant que possible, raisonnez par équivalence comme dans l'exemple précédent. Cependant le fait de raisonner par équivalence impose parfois trop de lourdeur à la rédaction. Lorsqu'on choisit de raisonner par implications, après avoir montré que $P(x) \implies x \in S$, pour un certaine partie S de E, il restera à rechercher quels sont les éléments de S qui sont effectivement solutions.

Exemple. Résoudre dans $\mathbb{R}$ l'équation du second degré générale (E) : $x^2+ax+b = 0$.
Solution : Soit $x \in \mathbb{R}$.
$(E) \iff (x + \dfrac{a}{2})^2 + b - \dfrac{a^2}{4} = 0 \iff (x + \dfrac{a}{2})^2 = \dfrac{a^2-4b}{4}$.
Posons $\Delta = a^2 - 4b$: c'est le discriminant.
Premier cas : Si $\Delta < 0$, l'ensemble des solutions est vide.

Second cas : On suppose que $\Delta \geq 0$. La fonction racine carrée est ici supposée connue. On pose $\delta = \sqrt{\Delta}$. Alors $(E) \iff \exists \varepsilon \in \{-1, 1\},\ \ x + \dfrac{a}{2} = \varepsilon \dfrac{\delta}{2}$, donc les solutions de (E) sont exactement $\dfrac{-a \pm \sqrt{\Delta}}{2}$.

5.4 Implication

$\diamond$ Lorsque $R = [P \Longrightarrow Q]$, on suppose que P est vraie (hypothèse supplémentaire) et on démontre Q.

Raisonnement par contraposition : l'implication $P \Longrightarrow Q$ est logiquement équivalente à $(\neg Q) \Longrightarrow (\neg P)$, qui est appelée sa contraposée. Ainsi,
pour démontrer $P \Longrightarrow Q$, on peut raisonner par contraposition, c'est-à-dire démontrer $(\neg Q) \Longrightarrow (\neg P)$: on suppose que Q est fausse et on démontre que P est fausse.

Exemple. Montrer que pour tout entier $n \in \mathbb{N}$, si n^2 est pair, alors n est aussi pair.
Solution : Soit $n \in \mathbb{N}$. Raisonnons par contraposition en supposant que n est impair. Il existe $k \in \mathbb{N}$ tel que $n = 2k + 1$. Alors $n^2 = 4k^2 + 4k + 1$ est impair.

Le raisonnement par l'absurde : cela consiste à supposer que R est fausse et à aboutir à une contradiction, souvent de la forme $S \wedge (\neg S)$.
Le raisonnement par l'absurde repose sur le postulat que la théorie dans laquelle on travaille est consistante. Il est donc impossible d'aboutir à une contradiction ce qui prouve que R est vraie.

Remarque. Les raisonnements par contraposition et par l'absurde sont très voisins.
D'une part, si l'on parvient à montrer R par l'absurde, on a montré que
$\neg R \Longrightarrow S \wedge (\neg S)$, dont la contraposée est $S \vee (\neg S) \Longrightarrow R$, mais $S \vee (\neg S)$ est vraie, donc R est prouvée. Ainsi, démontrer R par l'absurde revient à démontrer $S \vee (\neg S) \Longrightarrow R$ par contraposition.
D'autre part, en notant H l'ensemble des hypothèses, on souhaite démontrer $H \Longrightarrow R$. Le raisonnement par contraposition consiste à montrer $\neg R \Longrightarrow \neg H$, mais on peut le maquiller en un raisonnement par l'absurde : on suppose H et on veut démontrer R. Pour cela on raisonne par l'absurde en supposant $\neg R$ et on en déduit $\neg H$. On a donc $H \wedge (\neg H)$ ce qui est contradictoire, donc R est vraie.
Un tel maquillage est maladroit, il produit une démonstration inutilement alambiquée. Il y a cependant une réelle différence entre ces deux raisonnements ; lorsqu'on raisonne vraiment par l'absurde, la propriété S est quelconque, on en cherche seulement une qui convient. Lorsqu'on raisonne par contraposition, la propriété H est donnée.

$\diamond$ Lorsque $R = [P \iff Q]$, on regarde souvent R comme la conjonction
$[P \Longrightarrow Q] \wedge [Q \Longrightarrow P]$ à laquelle on applique les méthodes précédentes.
$\diamond$ Lorsque R est "montrer que les propriétés $P_1, \ldots, P_k$ sont équivalentes", on peut se contenter de montrer le cycle d'implications $P_1 \Longrightarrow P_2 \Longrightarrow \cdots \Longrightarrow P_k \Longrightarrow P_1$. Mais la liste $P_1, \ldots, P_k$ n'est pas toujours donnée dans l'ordre idéal. Il convient donc parfois de la réordonner.

5.5 Quantificateurs

◇ Lorsque $R = [\forall x \in E,\ P(x)]$, le plus souvent, on prend x quelconque dans E, en écrivant "soit $x \in E$", puis on démontre $P(x)$.
La portion de phrase "soit $x \in E$" ne doit pas être sous-entendue. Il ne faut pas démontrer d'emblée $P(x)$ en considérant que tout le monde comprendra que x est un élément quelconque de E. D'une manière générale, toutes les variables que vous utilisez au cours d'une démonstration doivent préalablement avoir été définies sans ambiguïté.

Exemple. Soit $f : \mathbb{R} \longrightarrow \mathbb{R}$ une fonction telle que, pour tout $x, y \in \mathbb{R}$, $f(x+y) = f(x)f(y)$. Montrer que $\forall x \in \mathbb{R},\ f(x) \geq 0$.
Solution : Soit $x \in \mathbb{R}$. $f(x) = f(\frac{x}{2} + \frac{x}{2}) = f(\frac{x}{2})^2 \geq 0$.

◇ Lorsque $R = [\exists x \in E,\ P(x)]$, la méthode directe consiste à construire un élément x de E satisfaisant $P(x)$. Cela nécessite de l'imagination et de la créativité. C'est souvent un passage délicat dans une démonstration, mais cela participe à la "beauté" des mathématiques. Dans ce contexte, on procède souvent par analyse-synthèse (cf ci-dessous).
On peut aussi raisonner par l'absurde, en supposant $\forall x \in E,\ \neg(P(x))$ et en recherchant une contradiction. Il faut cependant que cette nouvelle hypothèse se marie bien avec les autres hypothèses.

Exemple. Soit $x_1, x_3 \in Qe$ avec $x_1 < x_3$.
Montrer qu'il existe $x_2 \in \mathbb{Q}$ tel que $x_1 < x_2 < x_3$.
Solution : $x_2 = \dfrac{x_1 + x_3}{2}$ convient.

◇ Lorsque $R = \neg(\forall x \in E,\ P(x))$, on a vu que R est logiquement équivalente à $[\exists x \in E,\ \neg(P(x))]$, donc pour montrer R, on peut rechercher un x dans E tel que $P(x)$ est fausse. Dans ce contexte, x est appelé un contre-exemple du prédicat $P(x)$.
Par exemple pour montrer que $\mathbb{R} \neq \mathbb{Q}$, c'est-à-dire $\neg(\forall x \in \mathbb{R},\ x \in \mathbb{Q})$, il suffit de contruire un réel non rationnel. On verra que $\sqrt{2}$ est un contre-exemple.

5.6 Existence et unicité

On suppose que R est de la forme $R = [\exists! x \in E,\ P(x)]$.
Dans de nombreux exercices et problèmes, l'énoncé d'une telle propriété se présente sous la forme : "montrer qu'il existe $x \in E$ tel que $P(x)$, puis montrer que x est unique".
Sur le plan ontologique, tout objet mathématique est unique, mais ce n'est pas du tout ce qui est demandé par l'énoncé. La propriété "x est unique" dépend de P.
En mathématiques, l'unicité est toujours prononcée relativement à un prédicat. Par exemple, 2 est l'unique entier premier et pair, mais 2 n'est pas l'unique entier pair inférieur à 10.

◇ Pour montrer qu'il existe un unique $x \in E$ tel que $P(x)$, il est souvent préférable de séparer l'existence et l'unicité. Pour l'existence, on en a déjà parlé, pour l'unicité, il

faut montrer que $\{x \in E/P(x)\}$ ne possède pas deux éléments distincts, par exemple en supposant qu'il existe $x, y \in E$ vérifiant $P(x)$ et $P(y)$ et en prouvant que $x = y$.

Mais il y a d'autres méthodes :
- On peut montrer que $\{x \in E/P(x)\}$ est un singleton.
- On peut résoudre l'équation "$P(x)$" en l'inconnue x pour montrer qu'elle admet une seule solution.
- On peut raisonner par analyse-synthèse :

5.7 Démonstration par analyse-synthèse

On a déjà rencontré un tel raisonnement page 25, pour montrer que si $\mathcal{P}$ est une partition d'un ensemble E, alors il existe une unique relation d'équivalence R sur E telle que $\mathcal{P} = E/R$.
Ce mode de raisonnement est envisageable lorsque R est de la forme $[\exists x \in E,\ P(x)]$.
Il se décompose en deux parties :
◇ **L'analyse :** on suppose qu'il existe $x \in E$ tel que $P(x)$.
C'est a priori très étrange, car on suppose justement ce qu'il faut démontrer !
A partir du fait que x vérifie $x \in E$ et $P(x)$, on cherche à préciser x, en montrant que x est nécessairement de la forme $y(t)$, où t est un paramètre et où pour tout t, $y(t)$ est parfaitement définie.
Il est fréquent que l'analyse conduise à une seule valeur possible pour x.
◇ **La synthèse :** On cherche pour quel(s) t la quantité $y(t)$ vérifie $P(y(t))$.

Remarque. Le raisonnement par analyse-synthèse est bien adapté pour démontrer une propriété d'existence et d'unicité de la forme $[\exists! x \in E,\ P(x)]$: la partie analyse doit mener à une unique solution y possible, ce qui prouve l'unicité *sous condition d'existence* puis la partie synthèse prouve que y est bien solution, donc elle établit l'existence.

Exemple. Montrer que toute fonction de $\mathbb{R}$ dans $\mathbb{R}$ se décompose de manière unique en la somme d'une fonction paire et d'une fonction impaire.
Solution :
Soit f une fonction de $\mathbb{R}$ dans $\mathbb{R}$.
Analyse : Supposons qu'il existe deux applications p et i de $\mathbb{R}$ dans $\mathbb{R}$, respectivement paire et impaire, telles que $f = p + i$.
Pour tout $x \in \mathbb{R}$, $f(x) = p(x) + i(x)$ et $f(-x) = p(x) - i(x)$, en sommant et en retranchant ces deux égalités, $p(x) = \frac{1}{2}(f(x) + f(-x))$ et $i(x) = \frac{1}{2}(f(x) - f(-x))$.
Ainsi, sous condition d'existence, il y a unicité de l'écriture de f comme somme d'une fonction paire et d'une fonction impaire.
Synthèse : Posons pour tout $x \in \mathbb{R}$, $p(x) = \frac{1}{2}(f(x)+f(-x))$ et $i(x) = \frac{1}{2}(f(x)-f(-x))$. p et i sont des applications de $\mathbb{R}$ dans $\mathbb{R}$. On vérifie qu'elles sont respectivement paire et impaire et que, pour tout $x \in \mathbb{R}$, $p(x) + i(x) = f(x)$.

5.8 Inclusion entre ensembles

$\diamond$ Pour montrer que $A \subset B$, on peut "passer aux éléments", c'est-à-dire montrer que $\forall x \in A,\ x \in B$. On commence donc par écrire "soit $x \in A$", puis on cherche à démontrer que $x \in B$.

Exemple. On pose $A = \{\frac{k(k+1)}{2}/k \in \mathbb{N}\}$. Montrer que $A \subset \mathbb{N}$.
$\diamond$ Lorsque $R \iff [A = B]$, où A et B sont deux ensembles, on peut regarder R comme la conjonction de $A \subset B$ et $B \subset A$.

5.9 Démonstrations par récurrence

On a vu précédemment que :
Principe de récurrence 1 : Soit $R(n)$ un prédicat sur $\mathbb{N}$.
Si $R(0)$ est vraie et si pour tout $n \in \mathbb{N}$, $R(n)$ implique $R(n+1)$,
alors pour tout $n \in \mathbb{N}$, $R(n)$ est vraie.

Remarque. On montre ainsi que : $\forall n \in \mathbb{N},\ R(n)$. Mais bien entendu, l'assertion $R(n)$ ne commence pas par $\forall n$.

Il arrive que le prédicat $R(n)$ ne soit défini que pour $n \geq n_0$, où $n_0 \in \mathbb{N}^*$, ou bien qu'il soit faux pour des valeurs inférieures. On peut généraliser le principe de récurrence à cette situation :
Principe de récurrence 2 :
Soit $n_0 \in \mathbb{N}^*$. Soit $R(n)$ un prédicat défini pour tout entier $n \geq n_0$.
Si $R(n_0)$ est vraie et si pour tout $n \geq n_0$, $R(n)$ implique $R(n+1)$,
alors pour tout $n \in \mathbb{N}$ tel que $n \geq n_0$, $R(n)$ est vraie.

Démonstration.
On pose $S(n) = R(n+n_0)$ et on applique le principe de récurrence 1 au prédicat $S(n)$. □

Exemple. Pour $n \in \mathbb{N}$, comparer n^2 et 2^n.
On peut aussi énoncer des principes de récurrence sur $[\![n, m]\!]$:
Principe de récurrence ascendante finie : Soit $n, m \in \mathbb{N}$ avec $n \leq m$.
Soit $R(k)$ un prédicat défini pour $k \in [\![n, m]\!]$.
Si $R(n)$ est vraie et si pour tout $k \in [\![n, m-1]\!]$, $R(k)$ implique $R(k+1)$,
alors $R(k)$ est vraie pour tout $k \in [\![n, m]\!]$.

Démonstration.
Raisonnons par l'absurde en supposant que $\{k \in [\![n, m]\!]/\neg(R(k))\}$ est non vide. Alors cet ensemble d'entiers possède un plus petit élément, noté k_0.
$k_0 > n$, car $R(n)$ est vrai, donc $k_0 - 1 \in [\![n, m-1]\!]$ et $R(k_0 - 1)$ est vraie. Alors d'après les hypothèses, $R(k_0)$ est également vraie, ce qui est faux. □
Principe de récurrence descendante finie : Soit $n, m \in \mathbb{N}$ avec $n \leq m$.
Soit $R(k)$ un prédicat défini pour $k \in [\![n, m]\!]$.
Si $R(m)$ est vraie et si pour tout $k \in [\![n+1, m]\!]$, $R(k)$ implique $R(k-1)$,

alors $R(k)$ est vraie pour tout $k \in [\![n, m]\!]$.

Démonstration.
Adapter la démonstration précédente. □

Principe de récurrence forte :
Soit $n_0 \in \mathbb{N}$. Soit $R(n)$ un prédicat défini pour tout entier $n \geq n_0$.
Si $R(n_0)$ est vraie et si pour tout $n \geq n_0$, $[\forall k \in \{n_0, \dots, n\}, R(k)]$ implique $R(n+1)$, alors pour tout $n \in \mathbb{N}$ tel que $n \geq n_0$, $R(n)$ est vraie.

Démonstration.
On pose $S(n) = [\forall k \in \{n_0, \dots, n\}, R(k)]$ et on utilise le principe de récurrence 2. □

Exemple. Tout entier naturel $n \geq 2$ se décompose sous la forme d'un produit de nombres premiers.
En effet, notons $R(n)$ cette propriété et montrons-la par récurrence forte.
$R(2)$ est évidente car 2 est premier.
Soit $n \geq 2$. On suppose $R(k)$ pour tout $k \in \{2, \dots, n\}$.
Si $n+1$ est premier, c'est bien un produit de nombres premiers.
Sinon, il existe $d \notin \{1, n+1\}$ tel que $d | n+1$. Il existe donc $d' \in \mathbb{N}$ tel que $n+1 = dd'$.
$d \neq 0$ et $d' \neq 0$. Alors $d > 1$, donc $d' < dd' = n+1$.
De plus, $d \leq dd' = n+1$ et $d \neq n+1$, donc $d \leq n$. On peut donc utiliser $R(d)$ et $R(d')$ ce qui permet de conclure.
On démontrera dans le cours d'arithmétique que cette décompostion est unique.

Exemple. Le raisonnement suivant comporte heureusement une erreur. Laquelle ?
Pour $n \in \mathbb{N}^*$, notons $R(n)$ la propriété suivante : n droites quelconques du plan sont toujours deux à deux parallèles.
Initialisation : Pour $n = 1$, on a bien $R(1)$.
Hérédité : Soit $n \geq 1$ tel que $R(n)$.
Considérons $n+1$ droites du plan, notées $D_1, \dots, D_{n+1}$.
D'après $R(n)$, les droites $D_1, \dots, D_n$ sont deux à deux parallèles.
Toujours d'après $R(n)$, les droites $D_2, \dots, D_{n+1}$ sont deux à deux parallèles.
On en déduit $R(n+1)$.
D'après le principe de récurrence, pour tout $n \in \mathbb{N}^*$, n droites du plan sont toujours 2 à 2 parallèles.
Solution : $R(1)$ est vraie et le raisonnement utilisé pour montrer que $R(n) \Longrightarrow R(n+1)$ est vrai, mais seulement lorsque $n \geq 2$, par transitivité de la relation de parallélisme.
Cependant, on n'a jamais démontré $R(2)$, qui bien sûr est fausse. C'est donc l'initialisation de la récurrence qui est incorrecte.
Ceci montre combien l'initialisation est importante. Pour éviter ce type d'erreur, il est bienvenu de vérifier qu'à partir de l'initialisation, on peut effectivement faire fonctionner l'itération pour montrer la propriété sur les premières valeurs de l'entier n.

Principe de récurrence double :
Soit $n_0 \in \mathbb{N}$. Soit $R(n)$ un prédicat défini pour tout entier $n \geq n_0$.

Si $R(n_0)$ et $R(n_0+1)$ sont vraies et si
pour tout $n \geq n_0$, $[R(n) \ \wedge \ R(n+1)]$ implique $R(n+2)$,
alors pour tout $n \in \mathbb{N}$ tel que $n \geq n_0$, $R(n)$ est vraie.

Démonstration.
On pose $S(n) = [R(n) \ \wedge \ R(n+1)]$ et on utilise le principe de récurrence 2. □

Exemple. Considérons la suite $(u_n)_{n\in\mathbb{N}}$ définie par : $u_0 = 2$, $u_1 = 5$ et, pour tout $n \in \mathbb{N}$, $u_{n+2} = 5u_{n+1} - 6u_n$.
Montrer que, pour tout $n \in \mathbb{N}$, $u_n = 2^n + 3^n$.
Solution : Pour tout $n \in \mathbb{N}$, posons $R(n) \ : \ u_n = 2^n + 3^n$.
Initialisation : On vérifie $R(0)$ et $R(1)$.
Hérédité : Soit $n \in \mathbb{N}$. On suppose $R(n)$ et $R(n+1)$.
Ainsi, $u_n = 2^n + 3^n$ et $u_{n+1} = 2^{n+1} + 3^{n+1}$.
Alors $u_{n+2} = 5(2^{n+1} + 3^{n+1}) - 6(2^n + 3^n) = 2^n(10-6) + 3^n(15-6)$, d'où $R(n+2)$.

Principe de la descente infinie : cf page 23.

6 Résoudre et rédiger un problème

Bien que les correcteurs de concours soient relativement indulgents, il y a un minimum de règles à respecter et quelques conseils à suivre.

6.1 Les préalables

- Pour appliquer correctement le cours, il est indispensable de connaître précisément les énoncés des résultats du cours, et d'en maîtriser le vocabulaire.
- Il faut bien sûr dormir suffisamment **avant** les épreuves.
- Prenez de quoi vous alimenter pendant les épreuves (du sucre notamment).
- Une montre est indispensable pendant les devoirs surveillés (l'usage des smartphones est interdit).

6.2 Règles typographiques

- Écrivez à l'encre noire ou bleue.
- Laissez une marge à gauche d'au moins 4 cm.
- N'utilisez pas l'effaceur ou le correcteur blanc sur de trop grande surface.
- Faites figurer clairement les références des questions traitées.
- Sautez une ligne entre deux questions.
- Sautez une page (voire changez de feuille) entre deux exercices, entre deux parties d'un problème.
- Respectez les notations de l'énoncé même si ce ne sont pas celles auxquelles vous êtes habitué. N'hésitez pas, en revanche, à introduire des notations supplémentaires, en les définissant clairement.

6.3 Une rédaction claire

- Ecrivez lisiblement. Encadrez vos résultats.
- Une rédaction mathématique est d'abord un texte en français ; chaque phrase doit posséder un sujet (clairement identifié), un verbe etc. Il faut faire des phrases en bon français, simples et claires.
- N'hésitez pas à faire figurer de nombreux dessins, même s'ils ne sont pas demandés, à condition toutefois qu'ils soient en rapport avec la question posée.
- Au cours des calculs, différenciez nettement les différents symboles utilisés ; par exemple une écriture hâtive confond souvent "n" et "x".
  Lorsque le calcul est terminé, simplifiez au maximum le résultat obtenu, puis encadrez-le.
  Ne trichez pas dans un calcul ; il est préférable de donner son résultat, même s'il n'est pas correct et d'indiquer ce que *devrait* donner le calcul.
- Dans vos démonstrations, on doit pouvoir distinguer du premier coup d'oeil :
  - un résultat connu auquel vous faites référence, indiqué par "d'après le cours", "d'après le théorème <nom>", "on sait que" etc.
  - l'utilisation du résultat d'une question précédente, référencée par "d'après la question <numéro>", etc.
  - un résultat déduit de vos raisonnements, qui doit être précédé d'un "donc", d'un "d'où", d'un "par conséquent", d'un "il s'ensuit que", etc ;
  - Une hypothèse intermédiaire, repérée par "supposons que" etc.
  - un résultat que vous allez démontrer, qui doit être annoncé par un "Démontrons que" , un "Il faut établir que" , etc.
  - La conclusion d'une question, ou bien une conclusion intermédiaire, repérée par "j'ai prouvé que", "nous venons de montrer que " etc.
- Il faut justifier chaque étape d'un raisonnement :
  - en utilisant une hypothèse de l'énoncé ;
  - en citant un résultat obtenu dans les questions précédentes (même si l'on n'est pas parvenu à le démontrer) ;
  - en faisant explicitement référence à un résultat du cours dont il faut alors vérifier soigneusement toutes les hypothèses.
- Lorsque vous venez de trouver une solution, mais qu'elle vous paraît très compliquée, perdez encore une ou deux minutes à essayer de la simplifier.

6.4 Un peu de stratégie

- Il est fréquent qu'un problème soit trop long dans le temps imparti. Il ne faut donc pas chercher à traiter *toutes* les questions le plus vite possible. L'objectif est de traiter *des* questions avec précision, clarté et rigueur. Ensuite bien sûr, ce niveau de qualité étant compris, il faut en faire le plus possible.
- Commencer par lire l'énoncé en diagonale : quelques minutes, pour prendre connaissance des objets mathématiques manipulés par l'énoncé.

Si vous détectez une question que vous connaissez, il faudra aussi lui accorder du temps.
Notez au brouillon les contraintes horaires que ceci impose.

— Avant d'aborder une nouvelle partie, refaîtes une lecture en diagonale de cette partie.
Avant d'aborder le 2.a.1, il faut lire en détail l'énoncé de la question 2 et tenter de comprendre ce qu'elle démontre.

— Pour une bonne utilisation des feuilles de brouillon, éviter bien sûr de tout écrire directement au propre et éviter également d'écrire tous les détails sur une feuille de brouillon puis de les recopier. Le bon usage du brouillon se situe entre les deux attitudes précédentes.

— Distinguer les questions fermées des questions ouvertes.
Pour les premières, comme la question posée donne précisément le résultat à atteindre, c'est la justification de la réponse qui est importante et qui vous apportera des points. Votre rédaction ne peut se limiter à "je suis d'accord avec l'énoncé", aussi triviale que soit la question.
Pour les questions ouvertes, il faut bien sûr conserver une rédaction précise et claire, mais avec un peu moins d'exigence, car dans ce cas, les points seront surtout décernés en fonction de la justesse de la réponse.

— Lorsque vous remarquez que vous êtes en train de faire une erreur de calcul ou de raisonnement, corrigez bien sûr, mais ayez le réflexe de rechercher dans les questions déjà traitées si vous n'avez pas commis la même erreur : il est en effet très fréquent de répéter plusieurs fois la même erreur.

— Cherchez chaque question en tenant compte des questions précédentes.
Lorsque la question posée vous résiste, consultez votre montre et accordez-vous 10 minutes de recherche. En cas d'échec, passez aux questions suivantes : les 10 minutes ne sont pas une perte pure, car elles vous auront permis de mieux vous imprégner du sujet.
Si vous parvenez à résoudre les 2 questions suivantes, pensez à revenir quelques secondes sur la question qui vous a résisté : vous aurez peut-être alors la solution, soit parce que les méthodes que vous avez utilisées pour les questions suivantes s'adaptent, soit parce que les questions suivantes donnent des informations supplémentaires, soit enfin parce que votre cerveau a inconsciemment continué à travailler sur la question résistante.
Pendant les 10 minutes de recherche, consultez l'énoncé des questions suivantes. Cela peut vous donner des informations très pertinentes pour avancer.
En résumé, les questions sont à chercher dans l'ordre, mais devant une question résistante, il ne faut pas hésiter à regarder plus loin, et/ou à revenir dessus plus tard.

— Chaque partie d'un problème est souvent largement indépendante des précédentes. Les questions faciles se trouvent en général au début de chaque partie et les questions difficiles à la fin. Si vous séchez sur les dernières questions d'une partie, passez donc à la partie suivante, après avoir pris connaissance

des résultats démontrés dans les questions que vous ne traitez pas.

7 Les nombres

7.1 $\mathbb{Z}$

7.1.1 Construction de $\mathbb{Z}$

L'idée de départ pour construire $\mathbb{Z}$ est de dire qu'un entier relatif est une différence de deux entiers naturels. Bien sûr, si $a, b \in \mathbb{N}$, lorsque $a < b$, $a - b$ n'est pas définie. Aussi, pour $a, b \in \mathbb{N}^2$ quelconques, l'idée est de définir $a - b$ sous la forme suivante : $a - b$ est égal au couple (a, b), mais en décidant d'identifier deux couples (a, b) et (c, d) lorsque $a - b = c - d$. Pour le moment, cette définition est circulaire : elle définit $a - b$ en utilisant $a - b$. Mais $a - b = c - d \iff a + d = c + b$ (une fois $\mathbb{Z}$ construit), donc on va dire que $a - b$ est égal au couple (a, b), mais en décidant d'identifier deux couples (a, b) et (c, d) lorsque $a + d = c + b$.

Définition. On définit la relation binaire R sur $\mathbb{N}^2$ par :

$$\forall a, b, c, d \in \mathbb{N},\ \ (a, b)R(c, d) \iff a + d = b + c.$$

Ainsi deux couples (a, b) et (c, d) sont en relation si et seulement si la somme des "externes" a et d est égale à la somme des internes b et c.

Propriété. R est une relation d'équivalence.

Démonstration.
La réflexivité et la symétrie sont laissés en exercice.
Si $(a, b)R(c, d)$ et $(c, d)R(e, f)$, alors $a + d = b + c$ et $c + f = d + e$, donc
$a + f + d = f + b + c = b + d + e$, or d est régulier donc $a + f = b + e$. Ainsi, $(a, b)R(e, f)$.
□

Remarque. Soit $(a, b) \in \mathbb{N}^2$. Si l'on suppose $\mathbb{Z}$ construit, la classe d'équivalence de (a, b) est l'ensemble des couples $(c, d) \in \mathbb{N}^2$ tels que $c - d = a - b$, donc c'est la trace sur $\mathbb{N}^2$ de la droite d'équation $x - y = a - b$ (cf figure). La relation d'équivalence R partitionne donc $\mathbb{N}^2$ selon des demi-droites de pente 1.

Définition. On pose $\mathbb{Z} = \mathbb{N}^2/R$.
Si $\overline{(a, b)}, \overline{(c, d)} \in \mathbb{Z}$, on pose $\overline{(a, b)} + \overline{(c, d)} \stackrel{\Delta}{=} \overline{(a + c, b + d)}$
et $\overline{(a, b)} \times \overline{(c, d)} \stackrel{\Delta}{=} \overline{(ac + bd, ad + bc)}$.
On définit ainsi une addition et une multiplication sur $\mathbb{Z}$.

Remarques
◇ Le symbole $\stackrel{\Delta}{=}$ est utilisé lorsque l'égalité est une définition, du terme de gauche par le terme de droite.

◇ Une fois $\mathbb{Z}$ entièrement construit, on se doute que $\overline{(a,b)} = a-b$. C'est ainsi que l'on devine les définitions de l'addition et de la multiplication :
$\overline{(a,b)} + \overline{(c,d)} = a-b+c-d = (a+c)-(b+d) = \overline{(a+c,b+d)}$ et
$\overline{(a,b)} \times \overline{(c,d)} = (a-b)(c-d) = (ac+bd)-(ad+bc) = \overline{(ac+bd,ad+bc)}$.

Démonstration.
◇ A priori, ces définitions ne sont pas recevables ; pour l'addition par exemple, la définition de $\overline{(a,b)} + \overline{(c,d)}$ ne peut dépendre que de $\overline{(a,b)}$ et $\overline{(c,d)}$, c'est-à-dire que $\overline{(a,b)} + \overline{(c,d)}$ doit être une fonction f de $\overline{(a,b)}$ et $\overline{(c,d)}$.
Il faut donc montrer qu'il existe une fonction f telle que, pour tout $a,b,c,d \in \mathbb{N}$, $\overline{(a+c,b+d)} = f(\overline{(a,b)},\overline{(c,d)})$.
Supposons que f existe. Elle vérifie :
pour tout $x,y \in \mathbb{Z}$, $f(x,y) = \overline{(a+c,b+d)}$ dès que $x = \overline{(a,b)}$ et $y = \overline{(c,d)}$.
Donc si $\overline{(a,b)} = \overline{(a',b')}$ et $\overline{(c,d)} = \overline{(c',d')}$, on doit avoir
$\overline{(a+c,b+d)} = f(x,y) = \overline{(a'+c',b'+d')}$.
Réciproquement, supposons que (H) : $\forall a,b,c,d,a',b',c',d' \in \mathbb{N}$,
$[\overline{(a,b)} = \overline{(a',b')}] \wedge [\overline{(c,d)} = \overline{(c',d')}] \Longrightarrow \overline{(a+c,b+d)} = \overline{(a'+c',b'+d')}$.
Alors on peut définir f par $f(x,y) = \overline{(a+c,b+d)}$ pour n'importe quels $a,b,c,d \in \mathbb{N}$ vérifiant $x = \overline{(a,b)}$ et $y = \overline{(c,d)}$.
En résumé, la définition de l'addition est correcte si et seulement si (H) est vérifiée.
Ici, il est simple de vérifier (H).
◇ On doit faire de même pour la multiplication : on suppose que $\overline{(a,b)} = \overline{(a',b')}$ et $\overline{(c,d)} = \overline{(c',d')}$, c'est-à-dire que (1) : $a+b' = a'+b$ et (2) : $c+d' = d+c'$ et on doit montrer que $\overline{(ac+bd,ad+bc)} = \overline{(a'c'+b'd',a'd'+b'c')}$,
c'est-à-dire que $ac+bd+a'd'+b'c' = ad+bc+a'c'+b'd'$.
On multiplie (1) par c et d respectivement : $ac+b'c = a'c+bc$ et $a'd+bd = ad+b'd$.
On mutiplie (2) par a' et b' : $a'c+a'd' = a'd+a'c'$ et $b'd+b'c' = b'c+b'd'$.
On fait la somme de ces 4 égalités et on simplifie. □

7.1.2 L'anneau $\mathbb{Z}$

Propriété. L'addition sur $\mathbb{Z}$ vérifie les propriétés suivantes :
- $0 \triangleq \overline{(0,0)}$ est neutre : $\forall m \in \mathbb{Z},\ m+0 = 0+m = m$.
- Associativité : $\forall n,m,k \in \mathbb{Z},\ (n+m)+k = n+(m+k)$.
- Commutativité : $\forall n,m \in \mathbb{Z},\ n+m = m+n$.
- Tout élément possède un symétrique : $\forall n \in \mathbb{Z},\ \exists m \in \mathbb{Z},\ n+m = 0$.

On résume ces propriétés en disant que $(\mathbb{Z},+)$ est un groupe commutatif.
Il y a unicité du symétrique d'un élément $n \in \mathbb{Z}$. Il est noté $-n$.
Le symétrique de $-n$ est n, i.e : $-(-n) = n$.

Démonstration.
Etudions seulement le symétrique : soit $\overline{(a,b)} \in \mathbb{Z}$.
On a $\overline{(a,b)} + \overline{(b,a)} = \overline{(a+b,a+b)} = \overline{(0,0)} = 0$, donc un symétrique de $\overline{(a,b)}$ est $\overline{(b,a)}$.

Unicité du symétrique : soit $n \in \mathbb{Z}$. Supposons que m et m' sont deux symétriques de n. Ainsi, $m+n = m'+n = 0$. Alors $m = m+0 = m+(m'+n) = (m+n)+m' = 0+m' = m'$. □

Propriété. La multiplication sur $\mathbb{Z}$ vérifie les propriétés suivantes :
- $1 \stackrel{\Delta}{=} \overline{(1,0)}$ est neutre : $\forall m \in \mathbb{Z},\ \ m \times 1 = 1 \times m = m$.
- Distributivité de la multiplication par rapport à l'addition : $\forall n, m, p \in \mathbb{Z},\ \ n(m+p) = nm + np$.
- Associativité : $\forall n, m, k \in \mathbb{Z},\ \ (n \times m) \times k = n \times (m \times k)$.
- Commutativité : $\forall n, m \in \mathbb{Z},\ \ n \times m = m \times n$.

On résume ces propriétés et le fait que $(\mathbb{Z}, +)$ est un groupe commutatif en disant que $(\mathbb{Z}, +, \times)$ est un anneau commutatif.

Démonstration.
Exercice. □

Propriété. $\forall n \in \mathbb{Z}$, $-n = (-1) \times n$.
$\forall n, m \in \mathbb{Z}$, $(-n) \times (-m) = n \times m$.

Démonstration.
Soit $n \in \mathbb{Z}$. Posons $n = \overline{(a,b)}$. On sait que $1 = \overline{(1,0)}$,
donc $(-1) \times n = \overline{(0,1)} \times \overline{(a,b)} = \overline{(b,a)} = -n$.
En particulier, avec $n = -1$, on obtient $(-1) \times (-1) = -(-1) = 1$.
Soit $n, m \in \mathbb{Z}$: $(-n) \times (-m) = (-1) \times (-1) \times n \times m = n \times m$. □

7.1.3 L'ordre de $\mathbb{Z}$

Ordre sur $\mathbb{Z}$: On définit sur $\mathbb{Z}$ une relation d'ordre total en posant :
$\forall a, b, c, d \in \mathbb{N},\ \ \overline{(a,b)} \leq \overline{(c,d)} \iff a + d \leq b + c$.

Démonstration.
◇ Il faut d'abord démontrer que la condition $a + d \leq b + c$ ne dépend que de $\overline{(a,b)}$ et $\overline{(c,d)}$, que c'est une fonction de $(\overline{(a,b)}, \overline{(c,d)})$ à valeurs dans $\{V, F\}$.
Supposons que $(a,b)R(a',b')$ et $(c,d)R(c',d')$. Ainsi, $a+b' = b+a'$ et $c+d' = c'+d$. Si $a+d \leq b+c$, alors $a+d+b'+c' \leq b+c+b'+c'$, donc $b+a'+d'+c \leq b+c+b'+c'$: il existe $\alpha \in \mathbb{N}$ tel que $b+c+b'+c' = \alpha+b+a'+d'+c$. Par régularité de $b+c$, on en déduit que $a'+d' \leq b'+c'$.
Par symétrie des rôles joués par a, b, c, d et a', b', c', d',
on en déduit que $a+d \leq b+c \iff a'+d' \leq b'+c'$.
◇ Il faut ensuite montrer que "$\leq$" est bien une relation d'ordre : exercice. □

Compatibilité de la relation d'ordre avec l'addition :
$\forall x, y, x', y' \in \mathbb{Z},\ \ [x \leq y] \wedge [x' \leq y'] \Longrightarrow x + x' \leq y + y'$.

Démonstration.
Exercice. □

Identification de $\mathbb{N}$ avec une partie de $\mathbb{Z}$:
Notons f l'application de $\mathbb{N}$ dans $\mathbb{Z}$ définie par : $\forall n \in \mathbb{N},\ \ f(n) = \overline{(n,0)}$.

On vérifie que
- f est croissante : $\forall n, m \in \mathbb{N},\ (n \leq m \Longrightarrow f(n) \leq f(m))$.
- f est injective : $\forall n, m \in \mathbb{N},\ (n \neq m \Longrightarrow f(n) \neq f(m))$.
- $f(0) = 0$ et $f(1) = 1$.
- $\forall m, n \in \mathbb{N},\ f(m+n) = f(m) + f(n)$.
- $\forall m, n \in \mathbb{N},\ f(mn) = f(m)f(n)$.

Pour la suite, on identifiera tout entier $n \in \mathbb{N}$ avec l'élément $f(n)$ de $\mathbb{Z}$. Ce "renommage" des entiers naturels est compatible avec l'ordre naturel, ainsi qu'avec l'addition et la multiplication de $\mathbb{N}$.
Les éléments de $\mathbb{Z}$ s'appellent les entiers relatifs.

Démonstration.
Soit $n, m \in \mathbb{N}$: $f(n) \leq f(m) \Longleftrightarrow \overline{(n,0)} \leq \overline{(m,0)} \Longleftrightarrow n \leq m$, donc f est croissante.
Si $f(n) = f(m)$, alors $f(n) \leq f(m)$ et $f(m) \leq f(n)$, donc $n \leq m$ et $m \leq n$, donc $n = m$. Ainsi f est injective.
Les autres propriétés sont simples à vérifier. □

Propriété. Si $m, n \in \mathbb{N}$ avec $n \leq m$, alors $f(m-n) = f(m) + (-f(n))$, donc après identification, $m - n = m + (-n)$.

Démonstration.
Dans $\mathbb{N}$, posons $a = m - n$. On sait que $m = n + a$.
$f(m) + (-f(n)) = \overline{(m,0)} + \overline{(0,n)} = \overline{(m,n)}$, mais $(m,n)R(a,0)$,
donc $f(m) + (-f(n)) = \overline{(a,0)} = f(m-n)$. □

Règle des signes :
- $\forall n \in \mathbb{Z},\ n \geq 0 \Longleftrightarrow n \in \mathbb{N}$.
- $\forall n, m \in \mathbb{Z},\ ([n \geq 0] \wedge [m \geq 0]) \Longrightarrow nm \geq 0$.
- $\forall n \in \mathbb{Z},\ n \geq 0 \Longleftrightarrow -n \leq 0$.
- $\forall x, y, a \in \mathbb{Z},\ \begin{cases} \text{si } a \geq 0,\ x \leq y \Longrightarrow ax \leq ay, \\ \text{si } a \leq 0,\ x \leq y \Longrightarrow ax \geq ay. \end{cases}$

Démonstration.
◇ Soit $n \in \mathbb{Z}$.
Si $n \in \mathbb{N}$, alors $n = f(n) = \overline{(n,0)} \geq \overline{(0,0)} = 0$, car dans $\mathbb{N}$, $0 \leq n$.
Posons $n = \overline{(a,b)}$ et supposons que $0 \leq n$.
Alors $b \leq a$, donc $n = \overline{(a-b,0)} = f(a-b) \in \mathbb{N}$.
Ainsi, $n \geq 0 \Longleftrightarrow n \in \mathbb{N}$.
◇ Soit $n, m \in \mathbb{Z}$.
Si $n \geq 0$ et $m \geq 0$, $n, m \in \mathbb{N}$. Plus précisément, il existe $h, k \in \mathbb{N}$ tels que $n = f(k)$ et $m = f(h)$. Alors $nm = f(hk) \in \mathbb{N}$, donc $mn \geq 0$.
◇ Soit $n = \overline{(a,b)} \in \mathbb{Z}$. $n \geq 0 \Longleftrightarrow b \leq a$.
Par ailleurs, $-n = \overline{(b,a)}$ donc $-n \leq 0 \Longleftrightarrow b \leq a$. Ainsi, $n \geq 0 \Longleftrightarrow -n \leq 0$.
◇ Soit $x, y, a \in \mathbb{Z}$.
Supposons d'abord que $a \geq 0$ et $x \leq y$.
Alors $0 \leq a$ et $0 = x - x = x + (-x) \leq y + (-x)$ d'après la compatibilité de la relation d'ordre avec l'addition,

donc $0 \leq a(y+(-x)) = ay + (-1)ax$ puis $ax = 0 + ax \leq ax + ay - ax = ay$.
Supposons maintenant que $a \leq 0$ et $x \leq y$.
Alors $-a \geq 0$ et $y - x \geq 0$, donc $(-a) \times (y - x) \geq 0$. On en déduit que $ax \geq ay$. □

Propriété. Toute partie non vide majorée de $\mathbb{Z}$ possède un maximum.
Toute partie non vide minorée de $\mathbb{Z}$ possède un minimum.

Démonstration.
◇ Soit A une partie non vide majorée.
Si $A \cap \mathbb{N} \neq \emptyset$, alors $A \cap \mathbb{N}$ possède un maximum dans $\mathbb{N}$: c'est le maximum de A.
Si $A \cap \mathbb{N} = \emptyset$, posons $-A = \{-n/n \in A\}$. C'est une partie non vide de $\mathbb{N}$, donc elle possède un minimum. On montre alors que $-\min(-A)$ est le maximum de A.
◇ Si maintenant A est une partie non vide minorée de $\mathbb{Z}$, alors $-A$ est non vide majorée, donc elle possède un maximum. On vérifie ensuite que $-\max(-A)$ est le minimum de A. □

Définition. Soit $n \in \mathbb{Z}$.
Le signe de n au sens large est
— 1 ou bien "positif" lorsque $n \geq 0$,
— -1 ou bien "négatif" lorsque $n \leq 0$.
Le signe de n au sens strict est
— 1 ou bien "strictement positif" lorsque $n > 0$,
— 0 ou bien "nul" lorsque $n = 0$,
— -1 ou bien "strictement négatif" lorsque $n < 0$.

Définition. Pour tout $n \in \mathbb{Z}$, on note $|n| = \max\{-n, n\}$.
C'est la valeur absolue de n. $|n| \in \mathbb{N}$.

Propriété. Pour tout $n \in \mathbb{Z}$, $n \leq |n|$, avec égalité si et seulement si $n \geq 0$.
De plus $|n|^2 = n^2$.

Propriété. $\forall n, m \in \mathbb{Z},\ |nm| = |n||m|$.

Démonstration.
Considérer les quatre cas selon les signes de n et de m au sens large. □

Propriété. $\mathbb{Z}$ est un anneau intègre, c'est-à-dire que, pour tout $n, m \in \mathbb{Z}$,
$nm = 0 \Longrightarrow [(n = 0) \vee (m = 0)]$.

Démonstration.
Supposons que $nm = 0$. Alors $0 = |nm| = |n| \times |m|$, mais $|n|, |m| \in \mathbb{N}$, donc $|n| = 0$ ou $|m| = 0$, puis $n = 0$ ou $m = 0$. □

Remarque. Soit D une partie de $\mathbb{R}$.
L'ensemble des applications de D dans $\mathbb{R}$, noté $\mathcal{F}(D, \mathbb{R})$, muni de l'addition et du produit entre fonctions, est un anneau. Les éléments neutres sont respectivement l'application identiquement nulle et l'application constante égale à 1.
Cependant cet anneau n'est pas intègre car on peut avoir $fg = 0$ alors que $f \neq 0$ et $g \neq 0$.

Propriété. Soit $n, m \in \mathbb{Z}^2$. $nm \geq 0$ si et seulement si n et m sont de même signe au sens large.

Démonstration.
$\Longleftarrow$ résulte de la règle des signes.
Pour la réciproque, démontrons la contraposée : supposons que n et m n'ont pas le même signe au sens large. Par exemple, $n > 0$ et $m < 0$. Alors $nm \leq 0$ d'après la règle des signes et $nm \neq 0$ car $\mathbb{Z}$ est intègre. Ainsi, $\neg(nm \geq 0)$. □

Propriété. Soit $a, b, n \in \mathbb{Z}$ tels que $an \leq bn$.
Si $n > 0$ alors $a \leq b$ et si $n < 0$, alors $a \geq b$.

Démonstration.
Soit $a, b, n \in \mathbb{Z}$ tel que $an \leq bn$. Alors $0 \leq (b-a)n$, donc n et $b-a$ ont le même signe.
□

Inégalité triangulaire : $\forall n, m \in \mathbb{Z},\ |n+m| \leq |n|+|m|$, avec égalité si et seulement si n et m sont de même signe.

Démonstration.
Nous présentons une démonstration très détaillée qui pourra ainsi s'adapter sans modification aux inégalités triangulaires dans $\mathbb{Q}$ et $\mathbb{R}$.
◇ *Lemme :* Soit $x, y \in \mathbb{Z}$ tels que $x \geq 0$, $y \geq 0$ et $x^2 \leq y^2$. Alors $x \leq y$.
En effet, raisonnons par l'absurde en supposant que $x > y$. Ainsi $y \leq x$ et $x \neq y$.
Alors $y.x \leq x.x$ et $y.y \leq y.x$, donc $y^2 \leq x^2$, or $x^2 \leq y^2$, donc $x^2 = y^2$.
Ainsi $(x+y)(x-y) = 0$, mais $\mathbb{Z}$ est intègre et $x \neq y$, donc $x + y = 0$.
Alors $0 \leq x \leq x + y = 0$, donc $x = 0$. De même $y = 0$, donc $x = y$ ce qui est faux.
◇ *Preuve :* Soit $n, m \in \mathbb{Z}$.
$|n+m|^2 = (n+m)^2 = n^2 + m^2 + 2nm \leq n^2 + m^2 + 2|n||m| = (|n| + |m|)^2$.
Le lemme permet de conclure.
Il y a égalité si et seulement si $nm = |nm|$, c'est-à-dire si et seulement si $nm \geq 0$, donc il y a égalité si et seulement si n et m sont de même signe. □

7.1.4 Les sous-groupes de $\mathbb{Z}$

Division euclidienne dans $\mathbb{Z}$: Pour tout $a, b \in \mathbb{Z}$ avec $b \neq 0$, il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que $a = bq + r$ et $0 \leq r < |b|$. q et r sont appelés les quotient et reste de la division euclidienne de a par b.

Démonstration.

$\diamond$ Pour l'existence, on utilise la division euclidienne sur $\mathbb{N}$: Soit $a, b \in \mathbb{Z}$ avec $b \neq 0$.
Premier cas : si $a, b \in \mathbb{N}$, c'est connu.
Second cas : supposons que $b \geq 1$ et $a < 0$. On sait alors qu'il existe $q, r \in \mathbb{N}$ tels que $-a = bq + r$ et $0 \leq r < b$. Ainsi, $a = b(-q) - r$.
Si $r = 0$, on a l'existence. Si $r > 0$, alors $a = b(-q - 1) + (b - r)$ et $0 < b - r < b$.
Troisième cas : il reste le cas où $b \leq -1$: On applique les cas précédents en remplaçant a, b par $a, -b$: il existe q, r tels que $a = (-b)q + r = b(-q) + r$ et $0 \leq r < -b = |b|$.
On a prouvé l'existence dans tous les cas.
$\diamond$ Pour l'unicité, on adapte la démonstration de la division euclidienne dans $\mathbb{N}$:
Supposons qu'il existe q, r et q', r' des entiers relatifs tels que $a = bq + r = bq' + r'$ avec $0 \leq r < |b|$ et $0 \leq r' < |b|$.
Alors $|r - r'| = |b||q - q'|$. Si $q \neq q'$, $|q - q'| \geq 1$ donc $|r - r'| \geq |b|$, ce qui est impossible car $-|b| + 1 \leq r - r' \leq |b| - 1$. □

Définition. Une partie G de $\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ si et seulement si
- $G \neq \emptyset$,
- $\forall (x, y) \in G^2,\ \ x + y \in G$,
- $\forall x \in G,\ \ -x \in G$.

Exemples. Pour tout $n \in \mathbb{Z}$, $n\mathbb{Z} \triangleq \{nx / x \in \mathbb{Z}\}$ est un sous-groupe de $\mathbb{Z}$.

Propriété. Soit G un sous-groupe de $\mathbb{Z}$.
Pour tout $n \in \mathbb{Z}$ et $g \in G$, $ng \in G$.
Pour tout $n \in \mathbb{Z}$, $n\mathbb{Z} \subset G$.

Démonstration.

Soit $g \in G$. On montre par récurrence sur n que, pour tout $n \in \mathbb{N}$, $ng \in G$.
De plus, pour tout $n \in \mathbb{N}$, $(-n)g = -(ng)$, or $ng \in G$ et G est un sous-groupe, donc $(-n)g \in G$. □

Corollaire. Soit G un sous-groupe de $\mathbb{Z}$. Alors $\boxed{1 \in G \Longleftrightarrow G = \mathbb{Z}}$.

Démonstration.

Si $1 \in G$, pour tout $n \in \mathbb{Z}$, $n = n \times 1 \in G$, donc $G = \mathbb{Z}$. La réciproque est claire. □

Théorème. Les sous-groupes de $(\mathbb{Z}, +)$ sont exactement les $n\mathbb{Z}$, où $n \in \mathbb{N}$.

Démonstration.

On a déjà vu que les $n\mathbb{Z}$ sont des sous-groupes. Il s'agit de montrer que ce sont les seuls : Soit G un sous-groupe de $(\mathbb{Z}, +)$. Si $G = \{0\}$, alors $G = 0.\mathbb{Z}$.
On peut donc supposer que $G \neq \{0\}$. Ainsi, il existe $x \in G$ avec $x \neq 0$. Alors x et $-x$ sont tous deux dans G, donc $G \cap \mathbb{N}^*$ est une partie non vide de $\mathbb{N}$. Elle possède donc un minimum noté a.

$a \in G$, donc $a\mathbb{Z} \subset G$.
Réciproquement, soit $k \in G$. Écrivons la division euclidienne de k par a : il existe $q, r \in \mathbb{Z}$ tels que $k = qa + r$ avec $0 \leq r < a$.
$-qa \in G$, $k \in G$ et G est un sous-groupe, donc $r = k - qa \in G$,
mais $0 \leq r < a = \min(G \cap \mathbb{N}^*)$, donc $r = 0$, puis $k = qa \in a\mathbb{Z}$.
Ainsi, $G = a\mathbb{Z}$. □

Propriété. Une intersection de sous-groupes de $\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

Démonstration.
Soit $(G_k)_{k\in K}$ une famille de sous-groupes de $\mathbb{Z}$ (K peut être de cardinal infini).
Montrons que $G = \bigcap_{k\in K} G_k$ est un sous-groupe de $\mathbb{Z}$.
◇ D'après le théorème précédent, tout sous-groupe de $\mathbb{Z}$ contient 0,
donc $0 \in G$ et $G \neq \emptyset$.
◇ Soit $g, h \in G$. Soit $k \in K$: g et h sont dans G_k et G_k est un sous-groupe donc $g + h \in G_k$ et $-g \in G_k$. Ainsi, $g + h \in G$ et $-g \in G$. □

Définition. Soit B une partie de $\mathbb{Z}$. Le groupe engendré par B est l'intersection des sous-groupes de $\mathbb{Z}$ contenant B. C'est le plus petit sous-groupe (au sens de l'inclusion) contenant B. On le note $Gr(B)$.

Propriété. Soient B et C deux parties de $\mathbb{Z}$ telles que $C \subset B$. Alors $Gr(C) \subset Gr(B)$.

Propriété. Si B est une partie de $\mathbb{Z}$,

$$\boxed{Gr(B) = \Big\{ \sum_{i=1}^{n} a_i b_i / n \in \mathbb{N}, (a_1, \ldots, a_n) \in \mathbb{Z}^n, (b_1, \ldots, b_n) \in B^n \Big\}.}$$

Démonstration.
Notons temporairement $B' = \{\sum_{i=1}^{n} a_i b_i / n \in \mathbb{N}, (a_1, \ldots, a_n) \in \mathbb{Z}^n, (b_1, \ldots, b_n) \in B^n\}$.
Avec $n = 0$, par convention, $\sum_{i=1}^{n} a_i b_i = 0$, donc $B' \neq \emptyset$. De plus, on vérifie que B' est stable pour l'addition et pour le passage à l'opposé, donc B' est un sous-groupe de $\mathbb{Z}$, qui contient clairement B.
Enfin, si G est un sous-groupe de $\mathbb{Z}$ contenant B, il contient B' car pour tout $a \in \mathbb{Z}$ et $b \in G$, $ab \in G$ et car G est stable pour l'addition. □

7.1.5 Divisibilité

Définition. Soit $n, m \in \mathbb{Z}$. On dit que n divise m, que n est un diviseur de m, ou encore que m est un multiple de n si et seulement si il existe $k \in \mathbb{Z}$ tel que $m = kn$. On note encore $n|m$ car c'est compatible avec la relation de divisibilité définie sur $\mathbb{N}$.

Propriété. Soit $a, b \in \mathbb{Z}$ avec $b \neq 0$. Alors b divise a si et seulement si le reste de la division euclidienne de a par b vaut 0.

Remarque. Tout entier relatif divise 0 mais 0 ne divise que lui-même.

Remarque. Si $n, m \in \mathbb{Z}$, n divise m si et seulement si $|n|$ divise $|m|$ dans $\mathbb{N}$.

Propriété. Soit $a, b, c \in \mathbb{Z}$.
- si $b|a$, alors pour tout $\alpha \in \mathbb{Z}$, $b|\alpha a$.
- Si $b \mid a$ et $b \mid c$, alors $b \mid (a + c)$.
- Si $b \mid a$ et $d \mid c$, alors $bd \mid ac$.
- si $b \mid a$, pour tout $p \in \mathbb{N}$, $b^p \mid a^p$.

Propriété. Soit $p \in \mathbb{N}$ et $b, a_1, \ldots, a_p, c_1, \ldots, c_p \in \mathbb{Z}$.

Si pour tout $i \in \{1, \ldots, p\}$, $b \mid a_i$, alors $b \mid \sum_{i=1}^{p} c_i a_i$.

Propriété. Pour tout $(a, b) \in \mathbb{Z}^2$,

$$\boxed{a|b \iff b\mathbb{Z} \subseteq a\mathbb{Z}.}$$

Démonstration.
Supposons que $a|b$. Il existe $m \in \mathbb{Z}$ tel que $b = ma$. Si $bx \in b\mathbb{Z}$,
$bx = max = a(mx) \in a\mathbb{Z}$, donc $b\mathbb{Z} \subseteq a\mathbb{Z}$.
Réciproquement, supposons que $b\mathbb{Z} \subseteq a\mathbb{Z}$. En particulier, $b \in a\mathbb{Z}$, donc il existe $m \in \mathbb{Z}$ tel que $b = ma$. □

Propriété. La relation de divisibilité est réflexive et transitive.

Remarque. La relation de divisibilité n'est pas un ordre sur $\mathbb{Z}$ car $-1|1$ et $1|-1$.

Définition. Soit $a, b \in \mathbb{Z}$. On dit que a et b sont premiers entre eux (ou étrangers) si et seulement si les seuls diviseurs communs de a et b sont 1 et -1.

Exemple. Deux entiers relatifs consécutifs sont toujours premiers entre eux.

Remarque. Soit $a \in \mathbb{Z}$. a est premier avec 0 si et seulement si $a = \pm 1$.

Définition. Soit $n \in \mathbb{N}$ avec $n \geq 2$ et $a_1, \ldots, a_n \in \mathbb{Z}$.
- $a_1, \ldots, a_n$ sont deux à deux premiers entre eux si et seulement si, pour tout $i, j \in \{1, \ldots, n\}$ avec $i \neq j$, a_i et a_j sont premiers entre eux.
- $a_1, \ldots, a_n$ sont globalement premiers entre eux si et seulement si les seuls diviseurs communs de $a_1, \ldots, a_n$ sont 1 et -1.

Remarque. Lorsque $a_1, \ldots, a_n$ sont deux à deux premiers entre eux, ils sont globalement premiers entre eux, mais la réciproque est fausse.
Par exemple, $6, 10$ et 15 sont globalement prermiers entre eux, mais ne sont pas deux à deux premiers entre eux.

Propriété. Soit p un nombre premier et $a \in \mathbb{Z}$.
Alors ou bien $p|a$, ou bien p et a sont premiers entre eux.

Démonstration.
Supposons que p ne divise pas a et montrons que a et p sont premiers entre eux.
Soit d un diviseur commun de p et de a. Si $|d| = p$, alors $p \mid a$ ce qui est faux, or d est un diviseur de p qui est premier, donc $|d| = 1$. Ainsi, si d est un diviseur commun de p et de a, alors $d = \pm 1$. □

Propriété. Soit $p \in \mathbb{N} \setminus \{0, 1\}$. Les propriétés suivantes sont équivalentes :

1. p est premier.
2. p est premier avec tout entier qu'il ne divise pas.
3. p est premier avec tout nombre premier contenu dans $[\![2, \sqrt{p}]\!]$.

Démonstration.
$1 \Longrightarrow 2$ résulte de la propriété précédente.
$2 \Longrightarrow 3$, car si q est un nombre premier différent de p, alors p ne divise pas q.
$3 \Longrightarrow 1$: Supposons que p n'est pas premier. Alors $\{a \in [\![2, p-1]\!] \ / \ a|p\}$ est non vide, donc il possède un minimum noté q.
Si q n'est pas premier, il existe $a \in [\![2, q-1]\!]$ tel que $a|q$. Alors a divise p, ce qui contredit la définition de q. Ainsi, q est premier.
Il existe $r \in \mathbb{N}$ tel que $qr = p$. Ainsi, $r = \frac{p}{q} \in [\![2, p-1]\!]$ et $r|p$, donc $r \geq q$. Ainsi, $p = rq \geq q^2$ ce qui prouve que $q \in [\![2, \sqrt{p}]\!]$. □

Remarque. L'équivalence $1 \Longleftrightarrow 3$ fournit un algorithme pour dresser la liste L des nombres premiers inférieurs à un entier donné n :
Initialement, $L = [\![2, n]\!]$ et on positionne un curseur sur 2. On supprime de L les multiples de 2, sauf 2, puis on déplace le curseur sur l'entier suivant de L : il s'agit de 3, car il n'a pas été supprimé. On supprime de L tous les multiples de 3, sauf 3, etc. Ainsi, à chaque itération, on déplace le curseur sur le premier entier suivant qui est encore dans L et l'on supprime de L tous les multiples du curseur, sauf le curseur. On arrête l'algorithme dès que le curseur est strictement supérieur à $\sqrt{n}$.
Cet algorithme s'appelle **le crible d'Ératosthène**.
Les nombres supprimés de la liste ne sont clairement pas premiers.
Notons p_h la h-ième position du curseur. On montre par recurrence forte sur h que $L \cap [\![2, p_h]\!] = \mathbb{P} \cap [\![2, p_h]\!]$. En effet, si p_h n'était pas un nombre premier, d'après la démonstration ci-dessus il admettrait un diviseur premier strictement inférieur, lequel serait par hypothèse de récurrence une position antérieure du curseur, donc p_h aurait été supprimé de L.
Enfin, d'après la proposition 3, les nombres situés au-delà de la dernière position du curseur sont des nombres premiers.

Théorème. $\mathbb{P}$ est de cardinal infini.

Démonstration.
Sinon, notons $\mathbb{P} = \{p_1, \ldots, p_n\}$ et posons $N = p_1 \times \cdots \times p_n + 1$. $N \geq 2$, donc en reprenant un argument de la démonstration précédente, le plus petit diviseur de N supérieur à 2 est premier. Notons-le p_i. Alors p_i divise N et p_i divise $p_1 \times \cdots \times p_n = N - 1$ donc il divise 1, ce qui est impossible. □

7.1.6 Congruence

Définition. Relation de congruence : Soit $k \in \mathbb{Z}$. On définit la relation R_k de congruence modulo k par : $\forall n, m \in \mathbb{Z},\ n\ R_k\ m \iff k|(n-m)$.
R_k est une relation d'équivalence. On note souvent "$x \equiv y\ [k]$" au lieu de $x\ R_k\ y$, et on dit que "x est congru à y modulo k".

Démonstration.
Exercice. □

Propriété. Soit $a, b \in \mathbb{Z}$ avec $b \neq 0$: il existe $r \in \{0, \dots, |b|-1\}$ tel que $a \equiv r\ [b]$.

Démonstration.
r est le reste de la division euclidienne de a par b. □

Exemple. $31 \equiv 5 \equiv -8\ [13]$.

Notation. La classe d'équivalence de n modulo k est $\overline{n} = \{n + kh / h \in \mathbb{Z}\} \stackrel{\Delta}{=} n + k\mathbb{Z}$.

En particulier, $\overline{0} = k\mathbb{Z} = \{hk / h \in \mathbb{Z}\}$.

Compatibilités de la congruence avec l'addition et la multiplication :
Pour tout $n, m, h, k \in \mathbb{Z}$,
- $n \equiv m\ [k] \Longrightarrow h + n \equiv h + m\ [k]$ et
- $n \equiv m\ [k] \Longrightarrow hn \equiv hm\ [k]$.

Corollaire : $\forall a, b, k \in \mathbb{Z},\ \forall n \in \mathbb{N},\ (a \equiv b\ [k] \Longrightarrow a^n \equiv b^n\ [k])$.

Exercice.
◇ Montrer que tout entier est congru modulo 9 à la somme des chiffres de son écriture décimale. En déduire que le produit de 859 par 4561 n'est pas égal à 3918899. Le procédé utilisé s'appelle la "preuve par 9".
◇ Imaginer une "preuve par 11".

Solution :
◇ $10 \equiv 1\ [9]$, donc pour tout $n \in \mathbb{N}$, $10^n \equiv 1^n \equiv 1\ [9]$.
$859 \equiv 4\ [9]$, $4561 \equiv 7\ [9]$, donc $859 \times 4561 \equiv 1\ [9]$, or $3918899 \equiv 2\ [9]$, donc le résultat est faux.
◇ $10^n \equiv -1\ [11]$, donc tout entier est congru modulo 11 à la somme alternée des chiffres de son écriture décimale, en commençant par le chiffre des unités, compté positivement.
$859 \equiv 1\ [11]$, $4561 \equiv -4 \equiv 7\ [11]$, donc $859 \times 4561 \equiv 7\ [11]$,
or $3918899 \equiv -5 \equiv 6\ [11]$.

Définition. Soit $x_0 \in \mathbb{R}$. Pour tout $x, y \in \mathbb{R}$, on dit que x est congru à y modulo x_0 et on note $x \equiv y\ [x_0]$ si et seulement si il existe $k \in \mathbb{Z}$ tel que $x - y = kx_0$.
La relation de congruence modulo x_0 est une relation d'équivalence sur $\mathbb{R}$, pour laquelle la classe d'équivalence de x est $x + x_0\mathbb{Z} \stackrel{\Delta}{=} \{x + kx_0 / k \in \mathbb{Z}\}$.

Cette relation est compatible avec l'addition entre réels mais pas avec la multiplication entre réels.

En trigonométrie, on utilise la relation de congruence modulo 2π ; formellement, un angle est un élément de $\mathbb{R}/(\equiv [2\pi])$.

7.1.7 PGCD

Définition. Soit $(a,b) \in \mathbb{Z}^2$. $a\mathbb{Z} + b\mathbb{Z}$ est le sous-groupe de $\mathbb{Z}$ engendré par $\{a,b\}$, donc il existe un unique $d \in \mathbb{N}$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. On dit que d est le PGCD de a et b. On note $d = \text{PGCD}(a,b) = a \wedge b$.

Propriété. Soit $(a,b) \in \mathbb{Z}^2$. $a \wedge b$ est un diviseur commun de a et b.
De plus, si d' est un autre diviseur commun de a et b, alors d' divise $a \wedge b$.
Ainsi, pour la relation d'ordre de divisibilité dans $\mathbb{N}$, $a \wedge b = \inf_{|}\{|a|, |b|\}$.
C'est la raison pour laquelle $a \wedge b$ est appelé le plus grand commun diviseur de a et b, ou, par abréviation, le ***PGCD*** de a et b.

Démonstration.
Posons $d = a \wedge b$.
$a = a.1 + b.0 \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, donc a est un multiple de d.
De même, on montre que b est un multiple de d.
Si d' est un diviseur commun de a et de b, $(a,b) \in (d'\mathbb{Z})^2$, donc $a\mathbb{Z} + b\mathbb{Z} \subset d'\mathbb{Z}$,
or $d \in a\mathbb{Z} + b\mathbb{Z}$, donc $d \in d'\mathbb{Z}$, ce qui prouve que d' divise d. □

Remarque. Lorsque a ou b est un entier relatif non nul, au sens de l'ordre naturel sur $\mathbb{N}$, $a \wedge b$ est aussi le plus grand diviseur commun de a et b.

Démonstration.
Soit $a, b \in \mathbb{Z}$ tels que a ou b est non nul. Notons $d = a \wedge b$.
Posons $\mathcal{D} = \{k \in \mathbb{N} \ / \ (k|a) \text{ et } (k|b)\}$ et $d' = \max_{\leq}(\mathcal{D})$. Il s'agit de montrer que $d' = d$.
$d \in \mathcal{D}$, donc $d \leq d'$.
$d' \in \mathcal{D}$, donc $d'|d$, or a ou b est non nul, donc $a\mathbb{Z} + b\mathbb{Z} \neq \{0\}$, donc $d \neq 0$. Ainsi il existe $k \in \mathbb{N}^*$ tel que $d = d'k$, donc $d \geq d'$. Ainsi $d = d'$. □

Exemples.
- Avec $a = 15 = 3 \times 5$ et $b = 6 = 2 \times 3$, $a \wedge b = 3$.
- $0 \wedge 0 = 0$.
- Pour tout $a \in \mathbb{Z}$, $a \wedge 0 = |a|$.
- Pour tout $a \in \mathbb{Z}$, $a \wedge 1 = 1$ et $a \wedge a = |a|$.

Propriété. a et b sont premiers entre eux si et seulement si $a \wedge b = 1$.

Définition. Plus généralement, si $k \in \mathbb{N}^*$ et si $a_1, \ldots, a_k \in \mathbb{Z}$, on dit que d est le PGCD de $a_1, \ldots, a_k$ si et seulement si $d \in \mathbb{N}$ et $d\mathbb{Z} = a_1\mathbb{Z} + \cdots + a_k\mathbb{Z} = Gr\{a_1, \ldots, a_k\}$.
Alors d est un commun diviseur de $a_1, \ldots, a_k$ et si d' est un autre commun diviseur de $a_1, \ldots, a_k$, alors d' divise d : $d = \inf_{|}\{a_1, \ldots, a_k\}$.
Si B est une partie quelconque de $\mathbb{Z}$, on dit que d est le PGCD de B si et seulement si $d \in \mathbb{N}$ et $d\mathbb{Z} = Gr(B)$. Alors d est un diviseur commun des éléments de B et si d' est un autre diviseur commun des éléments de B, alors d' divise d : $d = \inf_{|}(B)$.

Remarque. $\text{PGCD}(\emptyset) = 0 = \inf_{|}(\emptyset) = \max_{|}(\mathbb{N})$.

Propriété. Soit $k \in \mathbb{N}$, $a_1, \ldots, a_k \in \mathbb{Z}$ et $h \in \{1, \ldots, k\}$.
- Commutativité du PGCD :
  $PGCD(a_1, \ldots, a_k)$ ne dépend pas de l'ordre de $a_1, \ldots, a_k$.
- Associativité du PGCD :
  $PGCD(a_1, \ldots, a_k) = PGCD(a_1, \ldots, a_h) \ \wedge \ PGCD(a_{h+1}, \ldots, a_k)$.
- Distributivité de la multiplication par rapport au PGCD : pour tout $\alpha \in \mathbb{Z}$,
  $PGCD(\alpha a_1, \ldots, \alpha a_k) = |\alpha| PGCD(a_1, \ldots, a_k)$.

Démonstration.
$\diamond$ La commutativité est claire.
$\diamond$ Notons $d = PGCD(a_1, \ldots, a_k)$, $d' = PGCD(a_1, \ldots, a_h)$
et $d'' = PGCD(a_{h+1}, \ldots, a_k)$. Alors
$d\mathbb{Z} = a_1\mathbb{Z} + \cdots + a_k\mathbb{Z} = (a_1\mathbb{Z} + \cdots + a_h\mathbb{Z}) + (a_{h+1}\mathbb{Z} + \cdots + a_k\mathbb{Z}) = d'\mathbb{Z} + d''\mathbb{Z}$,
donc $d = d' \wedge d''$.
$\diamond$ Notons $d = PGCD(a_1, \ldots, a_k)$, $d' = PGCD(\alpha a_1, \ldots, \alpha a_k)$. Alors

$$\begin{aligned} d'\mathbb{Z} &= (\alpha a_1)\mathbb{Z} + \cdots + (\alpha a_k) \\ &= \{\sum_{i=1}^{k} \alpha a_i b_i \ / \ b_1, \ldots, b_k \in \mathbb{Z}\} \\ &= \alpha(a_1\mathbb{Z} + \cdots + a_k\mathbb{Z}) \\ &= \alpha(d\mathbb{Z}) = (\alpha d)\mathbb{Z}. \end{aligned}$$

□

7.1.8 PPCM

Définition. Soit $(a, b) \in \mathbb{Z}^2$. $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, donc il existe un unique entier naturel m tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. On dit que m est un PPCM de a et b et on note $m = a \vee b$.

Propriété. Soit $(a, b) \in \mathbb{Z}^2$. $a \vee b$ est un multiple commun de a et b, et si m' est un autre multiple commun de a et b, alors m' est un multiple de $a \vee b$.
Ainsi, pour la relation d'ordre de divisibilité dans $\mathbb{N}$, $a \wedge b = \sup_{|}\{|a|, |b|\}$.
C'est la raison pour laquelle $a \vee b$ est appelé le plus petit commun multiple de a et b, ou, par abréviation, le ***PPCM*** de a et b.

Démonstration.
Posons $m = a \vee b$. $m \in m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z} \subset a\mathbb{Z}$, donc a divise m.
De même, on montre que b divise m.
Si m' est un multiple commun de a et de b, $m' \in a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$, donc m' est un multiple de m. □

Remarque. Au sens de l'ordre naturel, le plus petit entier naturel commun multiple de a et b est toujours 0. Cependant, lorsque a et b sont des entiers relatifs non nuls, $a \vee b = \min_{\leq}\{k \in \mathbb{N}^* \ / \ a|k \text{ et } b|k\}$.

Démonstration.
Notons $m = a \vee b$.
Posons $\mathcal{M} = \{k \in \mathbb{N}^* \ / \ a|k \text{ et } b|k\}$ et $m' = \min_{\leq}(\mathcal{M})$. Il s'agit de montrer que $m' = m$.
$a \neq 0$ et $b \neq 0$, donc $m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z} \neq \{0\}$. Ainsi $m \neq 0$, donc $m \in \mathcal{M}$ puis $m' \leq m$.
$m' \in \mathcal{M}$, donc $m|m'$, or $m' \neq 0$, donc il existe $k \in \mathbb{N}^*$ tel que $m' = km$, donc $m \leq m'$.
Ainsi $m = m'$. □

Exemples.
- Avec $a = 15 = 3 \times 5$ et $b = 6 = 2 \times 3$, $a \vee b = 2 \times 3 \times 5 = 30$.
- $0 \vee 0 = 0$.
- Pour tout $a \in \mathbb{Z}$, $a \vee 0 = 0$.
- Pour tout $a \in \mathbb{Z}$, $a \vee 1 = |a|$.

Définition. Plus généralement, si $k \in \mathbb{N}^*$ et si $a_1, \ldots, a_k \in \mathbb{Z}$, on dit que m est le PPCM de $a_1, \ldots, a_k$ si et seulement si $m \in \mathbb{N}$ et $m\mathbb{Z} = a_1\mathbb{Z} \cap \cdots \cap a_k\mathbb{Z}$.
Alors m est un commun multiple de $a_1, \ldots, a_k$ et si m' est un autre commun multiple de $a_1, \ldots, a_k$, alors m' est un multiple de m : $m = \sup_{|}\{a_1, \ldots, a_k\}$.
Si B est une partie quelconque de $\mathbb{Z}$, on dit que m est le PPCM de B si et seulement si $m \in \mathbb{N}$ et $m\mathbb{Z} = \bigcap_{b \in B} b\mathbb{Z}$. Alors m est un multiple commun des éléments de B et si m' est un autre multiple commun des éléments de B, alors m' est un multiple commun de m : $m = \sup_{|}(B)$.

Remarque. Dans ce contexte, on convient que si $B = \emptyset$, $\bigcap_{b \in B} b\mathbb{Z} = \mathbb{Z}$, donc 1 est le PPCM de $\emptyset$.
Ainsi, toute partie de $\mathbb{N}$ possède une borne supérieure et une borne inférieure pour la relation d'ordre de divisibilité. On dit que l'ensemble ordonné $(\mathbb{N}, \ | \ )$ est un treillis complet.

Propriété. Soit $k \in \mathbb{N}$, $a_1, \ldots, a_k \in \mathbb{Z}$ et $h \in \{1, \ldots, k\}$.
- Commutativité du PPCM :
  $PPCM(a_1, \ldots, a_k)$ ne dépend pas de l'ordre de $a_1, \ldots, a_k$.
- Associativité du PPCM :
  $PPCM(a_1, \ldots, a_k) = PPCM(a_1, \ldots, a_h) \ \vee \ PPCM(a_{h+1}, \ldots, a_k)$.
- Distributivité de la multiplication par rapport au PPCM :
  pour tout $\alpha \in \mathbb{Z}$, $PPCM(\alpha a_1, \ldots, \alpha a_k) = |\alpha| PPCM(a_1, \ldots, a_k)$.

Démonstration.
◇ La commutativité est claire.
◇ Notons $m = PPCM(a_1, \ldots, a_k)$, $m' = PPCM(a_1, \ldots, a_h)$
et $m'' = PPCM(a_{h+1}, \ldots, a_k)$. Alors
$m\mathbb{Z} = a_1\mathbb{Z} \cap \cdots \cap a_k\mathbb{Z} = (a_1\mathbb{Z} \cap \cdots \cap a_h\mathbb{Z}) \cap (a_{h+1}\mathbb{Z} \cap \cdots \cap a_k\mathbb{Z}) = m'\mathbb{Z} \cap m''\mathbb{Z}$,
donc $m\mathbb{Z} = (m' \vee m'')\mathbb{Z}$.
◇ La dernière propriété est évidente lorsque $\alpha = 0$. Supposons maintenant que $\alpha \neq 0$.
Notons $m = PPCM(a_1, \ldots, a_k)$ et $m' = PPCM(\alpha a_1, \ldots, \alpha a_k)$. Alors

$m'\mathbb{Z} = [(\alpha a_1)\mathbb{Z}] \cap \cdots \cap [(\alpha a_k)\mathbb{Z}]$.
Soit $x \in m'\mathbb{Z}$: pour tout $i \in \{1, \ldots, k\}$, il existe $b_i \in \mathbb{Z}$ tel que $x = \alpha a_i b_i$.
Soit $i \in \{2, \ldots, k\}$: $\alpha a_1 b_1 = \alpha a_i b_i$ et $\alpha \neq 0$, donc $a_1 b_1 = a_i b_i$.
Ainsi $a_1 b_1 \in a_1\mathbb{Z} \cap \cdots \cap a_k\mathbb{Z}$, puis $x = \alpha a_1 b_1 \in \alpha(a_1\mathbb{Z} \cap \cdots \cap a_k\mathbb{Z})$, ce qui montre que $m'\mathbb{Z} \subset \alpha(a_1\mathbb{Z} \cap \cdots \cap a_k\mathbb{Z})$.
Réciproquement, si $x \in \alpha(a_1\mathbb{Z} \cap \cdots \cap a_k\mathbb{Z})$, il existe $y \in a_1\mathbb{Z} \cap \cdots \cap a_k\mathbb{Z}$ tel que $x = \alpha y$.
Pour tout $i \in \{1, \ldots, k\}$, il existe $b_i \in \mathbb{Z}$ tel que $y = a_i b_i$, donc $x = \alpha a_i b_i \in \alpha a_i\mathbb{Z}$. Ainsi $x \in [(\alpha a_1)\mathbb{Z}] \cap \cdots \cap [(\alpha a_k)\mathbb{Z}] = m'\mathbb{Z}$.
En conclusion, $m'\mathbb{Z} = \alpha(a_1\mathbb{Z} \cap \cdots \cap a_k\mathbb{Z}) = \alpha(m\mathbb{Z}) = (\alpha m)\mathbb{Z}$. □

7.1.9 Les théorèmes de l'arithmétique

Théorème de *Bézout*. Soit $(a, b) \in \mathbb{Z}^2$.
a et b sont premiers entre eux si et seulement si : $\exists (u, v) \in \mathbb{Z}^2 \;\; ua + vb = 1$.

Démonstration.
a et b sont premiers entre eux si et seulement si $a \wedge b = 1$, donc si et seulement si $\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$, or on a établi qu'un sous-groupe de $\mathbb{Z}$ contient 1 si et seulement si il est égal à $\mathbb{Z}$, donc a et b sont premiers entre aux si et seulement si $1 \in a\mathbb{Z} + b\mathbb{Z}$, ce qu'il fallait établir. □

Théorème de Bézout (généralisation). Soit $n \in \mathbb{N}$ avec $n \geq 2$ et $a_1, \ldots, a_n \in \mathbb{Z}$.
$a_1, \ldots, a_n$ sont globalement premiers entre eux si et seulement si :
$\exists u_1, \ldots, u_n \in \mathbb{Z} \;\; , \;\; u_1 a_1 + \cdots + u_n a_n = 1$.

Propriété. Soit $(a, b) \in \mathbb{Z}^2$. Posons $d = a \wedge b$.
Alors il existe $(a', b') \in \mathbb{Z}^2$, avec a' et b' premiers entre eux, tel que $a = a'd$ et $b = b'd$.

Démonstration.
d divise a et b, donc il existe $(a', b') \in \mathbb{Z}^2$ tel que $a = a'd$ et $b = b'd$.
$d \in a\mathbb{Z} + b\mathbb{Z}$, donc il existe $(a", b") \in \mathbb{Z}^2$ tel que $d = aa" + bb"$.
Premier cas. Si $d \neq 0$. Alors, en mettant en facteur d dans l'égalité précédente, $d(a'a" + b'b" - 1) = 0$, donc $a'a" + b'b" = 1$. D'après le théorème de Bézout, a' et b' sont premiers entre eux.
Deuxième cas. Si $d = 0$. Alors $a\mathbb{Z} + b\mathbb{Z} = \{0\}$, donc $a = b = 0$. Dans ce cas, $a' = b' = 1$ conviennent. □

Théorème de *Gauss*. Soit $(a, b, c) \in \mathbb{Z}^3$.
Si $a|bc$ avec a et b premiers entre eux, alors $a|c$.

Démonstration.
$(ac) \wedge (bc) = c(a \wedge b) = c$, or a est un diviseur commun de ac et de bc, donc il divise c. □

Corollaire. Soit $p, a, b \in \mathbb{Z}$.
Si $p \mid ab$ et si p est premier, alors $p \mid a$ ou $p \mid b$.

Démonstration.
p étant premier, on sait que $p \mid a$ ou bien $p \wedge a = 1$. □

Remarque. C'est faux lorsque p n'est pas premier : $6 \mid 2 \times 3$, mais 6 ne divise ni 2, ni 3.

Corollaire. Soit $(a, b, c) \in \mathbb{Z}^3$, $n \in \mathbb{N}^*$ et $a_1, \ldots, a_n \in \mathbb{Z}$.
◇ Si $a \wedge b = a \wedge c = 1$, alors $a \wedge bc = 1$.
◇ On en déduit que, si $a \wedge b = 1$, $\forall (k, l) \in (\mathbb{N}^*)^2 \;\; a^k \wedge b^l = 1$.
◇ Si $a|b$, $c|b$ et $a \wedge c = 1$ alors $ac|b$. Par récurrence, on en déduit que
si pour tout $i \in \{1, \ldots, n\}$, $a_i|b$ et si $i \neq j \Longrightarrow a_i \wedge a_j = 1$, alors $a_1 \times \cdots \times a_n \mid b$.
◇ $|ab| = (a \wedge b)(a \vee b)$. En particulier, $a \wedge b = 1 \Longrightarrow a \vee b = |ab|$.

Démonstration.
◇ Supposons que $a \wedge b = a \wedge c = 1$. Alors d'après le théorème de Bézout, il existe $u, v, u', v' \in \mathbb{Z}$ tels que $ua + vb = 1$ et $u'a + v'c = 1$. En formant le produit de ces deux égalités, on obtient $1 = vv'(bc) + a(uu'a + uv'c + vbu')$, donc $a \wedge bc = 1$.
◇ Supposons que $a|b$, $c|b$ et $a \wedge c = 1$.
$ac \mid bc$ et $ac \mid ab$, donc ac divise $(bc) \wedge (ab) = |b|(c \wedge a) = |b|$.
◇ Posons $d = a \wedge b$.
On a vu qu'il existe $a', b' \in \mathbb{Z}$ tels que $a' \wedge b' = 1$, $a = a'd$ et $b = b'd$.
a' et b' divisent $a' \vee b'$, donc d'après la propriété précédente, $a'b' \mid a' \vee b'$, mais $a'b'$ est un multiple commun de a' et b', donc c'est un multiple de $a' \vee b'$. Ainsi $|a'b'| = a' \vee b'$.
Alors, $a \vee b = (a'd) \vee (b'd) = (a' \vee b')|d| = |a'b'd|$, puis $|ab| = |d(a'b'd)| = (a \wedge b)(a \vee b)$.
□
ATTENTION : En général, $|abc| \neq (a \wedge b \wedge c)(a \vee b \vee c)$.
Par exemple, dans $\mathbb{Z}$, $6 \wedge 10 \wedge 15 = (6 \wedge 10) \wedge 15 = 1$
et $6 \vee 10 \vee 15 = (6 \vee 10) \vee 15 = 30 \vee 15 = 30$, mais $30 \times 1 \neq 6 \times 10 \times 15$.

Définition. Soit I un ensemble quelconque et $(u_i)_{i \in \mathbb{R}}$ une famille de réels. On dit qu'elle est *presque nulle* si et seulement si elle ne comporte qu'un nombre fini de composantes non nulles, c'est-à-dire si et seulement si $\{i \in I \;/\; u_i \neq 0\}$ est fini.
On note $\mathbb{R}^{(I)}$ l'ensemble des familles presques nulles de réels et pour toute partie A de $\mathbb{R}$, $A^{(I)}$ est l'ensemble des familles presque nulles d'éléments de A.

Théorème fondamental de l'arithmétique. Pour tout $a \in \mathbb{N}^*$, il existe une unique famille $(\nu_p)_{p \in \mathbb{P}} \in \mathbb{N}^{(\mathbb{P})}$ telle que

$$\boxed{a = \prod_{p \in \mathbb{P}} p^{\nu_p}.} \tag{1}$$

On dit que (1) est la décomposition de a en facteurs premiers, ou bien que c'est la décomposition primaire de a.
ν_p s'appelle la valuation p-adique de a.

Démonstration.
◇ L'existence se démontre par récurrence forte :
pour tout $n \in \mathbb{N}^*$, notons $R(n)$ l'assertion suivante : il existe une famille presque nulle d'entiers $(\nu_p)_{p\in\mathbb{P}}$ telle que $n = \prod_{p\in\mathbb{P}} p^{\nu_p}$.
Pour $n = 1$, la famille identiquement nulle convient.
Pour $n \geq 2$, supposons $R(k)$ pour tout $k \in \{1, \dots, n-1\}$.
Si n est premier, l'existence est assurée.
Sinon, il existe $p, q \in \mathbb{N}$ tels que $p \geq 2$, $q \geq 2$ et $pq = n$. Alors $p, q \in \{1, \dots, n-1\}$, donc on peut utiliser $R(p)$ et $R(q)$ pour montrer $R(n)$.
◇ Pour démontrer l'unicité, fixons $n \in \mathbb{N}^*$ et supposons qu'il existe deux familles presque nulles différentes $(\nu_p)_{p\in\mathbb{P}}$ et $(\eta_p)_{p\in\mathbb{P}}$ telles que $n = \prod_{p\in\mathbb{P}} p^{\nu_p} = \prod_{p\in\mathbb{P}} p^{\eta_p}$.
Notons $q = \max\{p \in \mathbb{P} / \nu_p \neq \eta_p\}$.
Ainsi après simplification par les p^{ν_p} tels que $p > q$, on a $q^{\nu_q} \prod_{\substack{p\in\mathbb{P}\\p<q}} p^{\nu_p} = q^{\eta_q} \prod_{\substack{p\in\mathbb{P}\\p<q}} p^{\eta_p}$.
Sans perte de généralité, on peut supposer que $\nu_q < \eta_q$, donc en posant $\alpha = \eta_q - \nu_q \in \mathbb{N}^*$, on a $\prod_{\substack{p\in\mathbb{P}\\p<q}} p^{\nu_p} = q^{\alpha} \prod_{\substack{p\in\mathbb{P}\\p<q}} p^{\eta_p}$. Alors $q \mid \prod_{\substack{p\in\mathbb{P}\\p<q}} p^{\nu_p}$, mais q est premier avec tout $p \in \mathbb{P}$ tel que $p < q$, donc q est premier avec $\prod_{\substack{p\in\mathbb{P}\\p<q}} p^{\nu_p}$, puis d'après le théorème de Gauss, $q \mid 1$, ce qui est faux. □

Propriété. Soit $a, b \in \mathbb{N}^*$. Ecrivons les décompositions de a et de b en facteurs premiers :

$$a = u \prod_{p\in\mathbb{P}} p^{\nu_p} \text{ et } b = v \prod_{p\in\mathbb{P}} p^{\mu_p}.$$

Alors $a \mid b \iff [\forall p \in \mathbb{P},\ \nu_p \leq \mu_p]$. De plus,

$$\boxed{a \wedge b = \prod_{p\in\mathbb{P}} p^{\min(\nu_p,\mu_p)} \text{ et } a \vee b = \prod_{p\in\mathbb{P}} p^{\max(\nu_p,\mu_p)}.}$$

En particulier, a et b sont premiers entre eux si et seulement si aucun élément de $\mathbb{P}$ n'intervient à la fois dans la décomposition en facteurs irréductibles de a et dans celle de b.

Démonstration.
◇ Si pour tout $p \in \mathbb{P}$, $\nu_p \leq \mu_p$, alors $b = a \times \prod_{p\in\mathbb{P}} p^{\mu_p - \nu_p}$, donc $a \mid b$.
Réciproquement, supposons que $a \mid b$. Soit $p \in \mathbb{P}$. $p^{\nu_p} \mid a$, donc $p^{\nu_p} \mid b$. Ainsi, d'après le théorème de Gauss, $p^{\nu_p} \mid p^{\mu_p}$. Si $\nu_p > \mu_p$, alors $p^{\nu_p - \mu_p} \mid 1$, ce qui est faux, donc pour tout $p \in \mathbb{P}$, $\nu_p \leq \mu_p$.

$\diamond$ Notons $d = \prod_{p\in\mathbb{P}} p^{\min(\nu_p,\mu_p)}$: d divise a et b. De plus, soit c un diviseur commun de a et b. Décomposons c en facteurs premiers : $c = \prod_{p\in\mathbb{P}} p^{\eta_p}$.
$c \mid a$, donc pour tout $p \in \mathbb{P}$, $\eta_p \leq \nu_p$.
$c \mid b$, donc pour tout $p \in \mathbb{P}$, $\eta_p \leq \mu_p$.
Ainsi, pour tout $p \in \mathbb{P}$, $\eta_p \leq \min(\nu_p, \mu_p)$. On en déduit que $c \mid d$.
Ainsi, $d = \inf_{|}\{a, b\} = a \wedge b$.
On en déduit la formule pour $a \vee b$, car on a vu que $a \vee b = \dfrac{ab}{a \wedge b}$. □

Exemple. Pour calculer les pgcd et ppcm de 1836 et 234, on peut utiliser leurs décompositions primaires : $1836 = 4 * 459 = 4 * 3 * 153 = 2^2 * 3^2 * 51 = 2^2 * 3^3 * 17$ et $234 = 2 * 117 = 2 * 3 * 39 = 2 * 3^2 * 13$, donc $1836 \wedge 234 = 2 * 3^2 = 18$ et $1836 \vee 234 = 2^2 * 3^3 * 13 * 17 = 23\,868$.

Remarque. Cet algorithme pour le calcul du PGCD de a et b n'est pas efficace, car le calcul de la décomposition de a en facteurs irréductibles est d'une grande complexité algorithmique. L'algorithme d'Euclide présenté ci-dessous est beaucoup plus efficace.

Lemme d'Euclide. Soient $(a, b) \in \mathbb{Z}^2$ avec $b \neq 0$. Notons q et r les quotient et reste de la division euclidienne de a par b. Alors $a \wedge b = b \wedge r$.

Démonstration.
$a = bq + r$, donc d est un diviseur commun de a et b si et seulement si d est un diviseur commun de b et r. Ainsi, en notant D cet ensemble de diviseurs communs, $a \wedge b = \max_{|}(D) = b \wedge r$. □

Algorithme d'Euclide. Soit $a_0, a_1 \in \mathbb{N}^*$ avec $a_0 > a_1$.
• Pour $i \geq 1$, tant que $a_i \neq 0$, on note a_{i+1} le reste de la division euclidienne de a_{i-1} par a_i. On définit ainsi une suite (strictement décroissante d'entiers naturels qui est donc nécessairement finie) $(a_i)_{0\leq i\leq N}$ telle que $a_N = 0$ et, pour tout $i \in \{0, \ldots, N-1\}$, $a_0 \wedge a_1 = a_i \wedge a_{i+1}$.
En particulier, pour $i = N - 1$, on obtient $a_0 \wedge a_1 = a_{N-1}$.
Cet algorithme, appelé algorithme d'Euclide permet donc de calculer le PGCD de deux éléments de $\mathbb{Z}$.
• Supposons maintenant que $a_0 \wedge a_1 = a_{N-1} = 1$. D'après le théorème de Bézout, il existe $(s, t) \in \mathbb{Z}^2$ tel que $sa_0 + ta_1 = 1$. La suite de l'algorithme d'Euclide permet le calcul d'un tel couple (s, t) :
Notons q_i le quotient de la division euclidienne de a_{i-1} par a_i. Ainsi, $a_{i-1} = q_i a_i + a_{i+1}$, c'est-à-dire $a_{i+1} = a_{i-1} - q_i ai$.
En particulier, avec $i = N - 2$, on obtient $1 = a_{N-3} - q_{N-2}a_{N-2}$.
Supposons que, pour un entier $i \in \{1, \ldots, N-3\}$, on dispose d'entiers s_i et t_i tels que $1 = s_i a_i + t_i a_{i+1}$. Alors $1 = s_i a_i + t_i(a_{i-1} - a_i q_i) = (s_i - t_i q_i)a_i + t_i a_{i-1}$, ce qui donne des entiers s_{i-1} et t_{i-1} tels que $1 = s_{i-1}a_{i-1} + t_{i-1}a_i$.
Par récurrence descendante, on peut donc calculer des entier s_0 et t_0
tels que $1 = s_0 a_0 + t_0 a_1$.

Exemples.

— Dans $\mathbb{Z}$, calculons le pgcd de 70 et de 6.
$70 = 6 * 11 + 4$, puis $6 = 4 + 2$ et $4 = 2 * 2 + 0$, donc $2 = 70 \wedge 6$.
De plus, $2 = 6 - 4 = 6 - (70 - 6 * 11) = -70 + 6 * 12$.

— Dans $\mathbb{Z}$, calculons le pgcd de 829 et 78.
$829 = 78 * 10 + 49$, $78 = 49 + 29$, $49 = 29 + 20$, $29 = 20 + 9$, $20 = 9 * 2 + 2$, $9 = 2 * 4 + 1$, donc $829 \wedge 78 = 1$.
Recherchons des coefficients de Bézout, $u, v \in \mathbb{Z}$ tels que $829u + 78v = 1$.

$$\begin{aligned} 1 &= 9 - 2 * 4 \\ &= 9 - (20 - 9 * 2) * 4 = -4 * 20 + 9 * 9 \\ &= -4 * 20 + 9 * (29 - 20) = 9 * 29 - 13 * 20 \\ &= 9 * 29 - 13 * (49 - 29) = -13 * 49 + 22 * 29 \\ &= -13 * 49 + 22 * (78 - 49) = 22 * 78 - 35 * 49 \\ &= 22 * 78 - 35 * (829 - 78 * 10) = -35 * 829 + 372 * 78, \end{aligned}$$

donc $u = -35$ et $v = 372$ conviennent.

Exercice. Soit $a, b, c \in \mathbb{Z}$ avec a et b non nuls.
Résoudre l'équation de Bézout (B) : $au + bv = c$ en l'inconnue $(u, v) \in \mathbb{Z}^2$.

Solution : Supposons que (B) possède au moins une solution $(u, v) \in \mathbb{Z}^2$. Alors $c \in a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$, donc c est un multiple de $a \wedge b$.
Ainsi, lorsque c n'est pas un multiple de $a \wedge b$, (B) n'admet aucune solution.
Pour la suite, on suppose que $a \wedge b \mid c$. a étant non nul, $a \wedge b \neq 0$, donc, quitte à diviser a, b et c par $a \wedge b$, on peut supposer que a et b sont premiers entre eux.
Alors grâce à l'algorithme d'Euclide, on peut déterminer un couple $(u, v) \in \mathbb{Z}^2$ tel que $ua + bv = 1$, puis en multipliant par c, on en déduit un couple $(u_0, v_0) \in \mathbb{Z}^2$ qui est une solution particulière de (B).
Soit $(u, v) \in \mathbb{Z}^2$ une solution de (B). Alors $(u - u_0)a + (v - v_0)b = 0$, donc $b \mid a(u - u_0)$ puis d'après le théorème de Gauss, $b \mid u - u_0$. Ainsi, il existe $\lambda \in \mathbb{Z}$ tel que $u = u_0 + \lambda b$. Alors $0 = (u - u_0)a + (v - v_0)b = b(\lambda a + v - v_0)$, or $b \neq 0$, donc $v = v_0 - \lambda a$. Réciproquement, s'il existe $\lambda \in \mathbb{Z}$ tel que $(u, v) = (u_0 + \lambda b, v_0 - \lambda a)$, on vériifie que $ua + vb = u_0 a + v_0 b = c$, donc l'ensemble des solutions de l'équation de Bézout est $\{(u_0 + \lambda b, v_0 - \lambda a) \ / \ \lambda \in \mathbb{Z}\}$.

Exemple. On peut adapter l'exercice pour résoudre l'équation (B) : $12x + 3y = 15$, où $x, y \in \mathbb{Z}$:
On remarque que $12 + 3 = 15$, donc $(x, y) = (1, 1)$ est une solution particulière.
Si (x, y) est solution, $4(x - 1) = 1 - y$, donc il existe $k \in \mathbb{Z}$ tel que $y = 1 - 4k$, puis $x = 1 + k$. La réciproque étant claire,
l'ensemble des solutions de (B) est $\{(1 + k, 1 - 4k) \ / \ k \in \mathbb{Z}\}$.

7.2 Construction de $\mathbb{Q}$

On peut vérifier les affirmations qui suivantes :

Définition. On définit une relation binaire R sur $\mathbb{Z} \times \mathbb{Z}^*$ par :

$$\forall (a,b),(c,d) \in \mathbb{Z} \times \mathbb{Z}^*,\ \ (a,b)R(c,d) \iff ad = bc.$$

Propriété. R est une relation d'équivalence.

Définition. On pose $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^*)/R$.
Pour tout $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$, on note $\frac{a}{b} = \overline{(a,b)}$.
Pour l'écriture $\frac{a}{b}$, on dit que a est son numérateur et que b est son dénominateur.
Pour tout $(a,b),(c,d) \in \mathbb{Z} \times \mathbb{Z}^*$, on pose $\dfrac{a}{b} \times \dfrac{c}{d} \triangleq \dfrac{ac}{bd}$ et $\dfrac{a}{b} + \dfrac{c}{d} \triangleq \dfrac{ad+cb}{bd}$.
On définit ainsi une addition et une multiplication sur $\mathbb{Q}$.

Remarque. Pour tout $a \in \mathbb{Z}$ et $b, c \in \mathbb{Z}^*$, on a bien $\dfrac{a}{b} = \dfrac{ac}{bc}$, car $(a,b)R(ac,bc)$.

Propriété. L'addition admet pour élément neutre $0 \triangleq \frac{0}{1}$, et la multplication admet pour élément neutre $1 \triangleq \frac{1}{1}$.

Propriété. $(\mathbb{Q}, +, \times)$ est un corps, c'est-à-dire que
- $(\mathbb{Q}, +, \times)$ est un anneau,
- $\mathbb{Q}$ n'est pas réduit à $\{0\}$ (on note $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$),
- $\mathbb{Q}$ est commutatif,
- tout élément non nul de $\mathbb{Q}$ est inversible : $\forall x \in \mathbb{Q}^*,\ \exists y \in \mathbb{Q}^*,\ xy = 1$.
  Dans ce cas, pour tout $x \in \mathbb{Q}^*$, l'inverse de x est unique, il est noté x^{-1}.

Propriété. Comme tout corps, $\mathbb{Q}$ est intègre, c'est-à-dire que, pour tout $x, y \in \mathbb{Q}$, $xy = 0 \Longrightarrow [(x = 0) \vee (y = 0)]$.

Démonstration.
La démonstration qui suit utilise seulement le fait que $\mathbb{Q}$ est un corps. Elle se généralise donc à tout corps. Une telle approche est caractéristique de l'algèbre : on définit des structures (groupes, anneaux, corps etc.) et on démontre des théorèmes généraux sur ces structures.
Lemme : 0 est absorbant, c'est-à-dire que, pour tout $x \in \mathbb{Q}$, $0.x = 0$.
En effet, $(0.x)+(0.x) = (0+0).x = 0.x$ donc en ajoutant de part et d'autre le symétrique (pour l'addition) de $0.x$, on obtient $0.x = 0$.
Intégrité : Soit $x, y \in \mathbb{Q}$ tels que $xy = 0$. Supposons que $x \neq 0$.
Alors $y = 1.y = (x^{-1}.x).y = x^{-1}.(x.y) = x^{-1}.0 = 0$. □

Remarque. Pour tout $x \in \mathbb{Q}$, il existe a, b tel que $x = \frac{a}{b}$, avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$: on peut imposer au dénominateur d'être strictement positif.
En effet, $\dfrac{a}{b} = \dfrac{-a}{-b}$.

Définition. Soit $x = \frac{p}{q} \in \mathbb{Q}$, avec $p \in \mathbb{Z}$ et $q \in \mathbb{Z}^*$.
On dit que x est positif si et seulement si p et q sont de même signe au sens large, c'est-à-dire si et seulement si $pq \geq 0$.

Démonstration.
Il faut prouver que cette condition ne dépend que de x et non du couple (p, q).
On suppose donc que x s'écrit également $x = \frac{p'}{q'}$ avec $p' \in \mathbb{Z}$ et $q' \in \mathbb{Z}^*$.
Supposons que $pq \geq 0$. On a $pq' = qp'$, donc $p'q'pq = (pq')^2 \geq 0$.
Si $p \neq 0$, on en déduit que $p'q' \geq 0$.
Si $p = 0$, alors $p' = 0$ donc on a encore $p'q' \geq 0$.
Ainsi $pq \geq 0 \Longrightarrow p'q' \geq 0$. □

Lemme : La somme de deux rationnels positifs est positif.

Démonstration.
Soit $x = \frac{a}{b}$ et $y = \frac{c}{d}$ deux rationnels positifs. Ainsi, $ab \geq 0$ et $cd \geq 0$.
$x + y = \dfrac{ad + bc}{bd}$ et $bd(ad + bc) = d^2ab + b^2cd \geq 0$, donc $x + y$ est positif. □

Ordre sur $\mathbb{Q}$: On définit sur $\mathbb{Q}$ une relation d'ordre total en convenant que, pour tout $x, y \in \mathbb{Q}$, $x \leq y$ si et seulement si $y - x$ est positif.

Démonstration.
◇ $x - x = 0$ est positif d'où la réflexivité.
◇ Supposons que $x \leq y$ et $y \leq x$. Alors $x - y = \frac{p}{q}$ et $y - x = \frac{-p}{q}$ sont positifs. Nécessairement, $p = 0$ donc $x = y$.
Ceci démontre l'antisymétrie.
◇ Supposons que $x \leq y$ et $y \leq z$. Ainsi, $y - x$ et $z - y$ sont positifs. D'après le lemme, $z - x = (z - y) + (y - x)$ est positif, donc $x \leq z$.
Ceci démontre la transitivité.
◇ Lorsque $x = \frac{p}{q}$ n'est pas positif, $pq < 0$, donc $-x = \frac{-p}{q}$ est positif. On en déduit que lorsque $\neg(y \leq z)$, alors $z \leq y$, donc c'est bien une relation d'ordre total. □

Compatibilité de la relation d'ordre avec l'addition :
$\forall x, y, x', y' \in \mathbb{Q},\ [x \leq y] \wedge [x' \leq y'] \Longrightarrow x + x' \leq y + y'$.

Démonstration.
Utilisez le lemme. □

Identification de $\mathbb{Z}$ avec une partie de $\mathbb{Q}$:
Notons f l'application de $\mathbb{Z}$ dans $\mathbb{Q}$ définie par : $\forall n \in \mathbb{Z},\ f(n) = \frac{n}{1}$.
On vérifie que
- f est croissante : $\forall n, m \in \mathbb{N},\ (n \leq m \Longrightarrow f(n) \leq f(m))$.
- f est injective : $\forall n, m \in \mathbb{N},\ (n \neq m \Longrightarrow f(n) \neq f(m))$.
- $f(0) = 0$ et $f(1) = 1$.
- $\forall m, n \in \mathbb{N},\ f(m + n) = f(m) + f(n)$.
- $\forall m, n \in \mathbb{N},\ f(mn) = f(m)f(n)$.

Pour la suite, on identifiera tout entier relatif $n \in \mathbb{Z}$ avec l'élément $\frac{n}{1}$ de $\mathbb{Q}$. Ce "renommage" des entiers naturels est compatible avec l'ordre naturel, ainsi qu'avec l'addition et la multiplication de $\mathbb{Z}$.
Les éléments de $\mathbb{Q}$ s'appellent les nombres rationnels.

Remarque. Soit $x \in \mathbb{Q}$. Il existe $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$ tels que $x = \frac{a}{b}$.
Avec l'identification précédente, $b = \frac{b}{1}$, donc son inverse dans $\mathbb{Q}$ est $\frac{1}{b}$.
Ainsi $x = (\frac{a}{1}) \times (\frac{1}{b})$ est le produit d'un entier relatif par l'inverse d'un entier relatif non nul. Cela justifie a posteriori la notation $\frac{a}{b}$.

Propriété. Pour tout $x \in \mathbb{Q}$, il existe un unique couple (a, b) tel que $x = \frac{a}{b}$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, tels que a et b sont premiers entre eux. On dit alors que $\frac{a}{b}$ est la forme irréductible de x.

Démonstration.
Soit $x \in \mathbb{Q}$.
◇ *Existence :* il existe $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ tel que $x = \frac{p}{q}$.
En posant $d = p \wedge q$, on a vu qu'il existe $p' \in \mathbb{Z}$ et $q' \in \mathbb{N}^*$ tels que $p = dp'$, $q = dq'$ et $p' \wedge q' = 1$. Alors $x = \dfrac{dp'}{dq'} = \dfrac{p'}{q'}$, ce qui prouve l'existence.
◇ *Unicité :* Supposons que $x = \dfrac{p'}{q'} = \dfrac{p''}{q''}$ où $(p', q'), (p'', q'') \in \mathbb{Z} \times \mathbb{N}^*$, $p' \wedge q' = 1 = p'' \wedge q''$.
On a $p'q'' = q'p''$, donc $q''|q'p''$, mais $q'' \wedge p'' = 1$, donc d'après le théorème de Gauss, $q''|q'$. De même, on montre que $q'|q''$, mais $q', q'' \in \mathbb{N}^*$, donc $q' = q''$.
Or $p'q'' = q'p''$ et $q' \neq 0$, donc $p' = p''$. □

> **Exercice.** Montrer que $\sqrt{2}$ est irrationnel.
>
> **Solution :** Raisonnons par l'absurde. Supposons que $\sqrt{2} \in \mathbb{Q}$. Notons $\frac{p}{q}$ sa forme irréductible. $\frac{p}{q} = \sqrt{2}$, donc $p^2 = 2q^2$.
> Alors $q|p^2$, mais $p \wedge q = 1$, donc d'après le théorème de Gauss, $q|1$ puis $q = 1$.
> Alors $p^2 = 2$ avec p entier ce qui est impossible.

Règle des signes :
- $\forall x, y \in \mathbb{Q},\ ([x \geq 0] \wedge [y \geq 0]) \Longrightarrow xy \geq 0$.
- $\forall x \in \mathbb{Q},\ x \geq 0 \Longleftrightarrow -x \leq 0$.
- $\forall x, y, a \in \mathbb{Q},\ \begin{cases} \text{si } a \geq 0,\ x \leq y \Longrightarrow ax \leq ay, \\ \text{si } a \leq 0,\ x \leq y \Longrightarrow ax \geq ay. \end{cases}$

Démonstration.
C'est sans difficulté. Pour la dernière propriété, il suffit de reproduire la démonstration vue dans $\mathbb{Z}$. □

En adaptant la définition vue pour les entiers relatifs, on définit le signe d'un rationnel, au sens large et au sens strict.

Définition. Pour tout $x \in \mathbb{Q}$, on note $|x| = \max\{-x, x\}$.
C'est la valeur absolue de x.

Propriété. Pour tout $x \in \mathbb{Q}$, $x \leq |x|$, avec égalité si et seulement si $x \geq 0$.

De plus $|x|^2 = x^2$.

En utilisant le fait que $\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$, on montre que

Propriété. Soit $x, y \in \mathbb{Q}^2$. $xy \geq 0$ si et seulement si x et y sont de même signe au sens large.

Propriété. $\forall x, y \in \mathbb{Q},\ |xy| = |x||y|$.

Démonstration.
Si $xy \geq 0$, alors $|xy| = xy = (-x)(-y) = |x|\ |y|$, car x et y sont de même signe.
Si $xy < 0$, alors x et y sont de signes opposés,
donc $|xy| = -(xy) = (-x)y = x(-y) = |x|\ |y|$. □

Inégalité triangulaire : $\forall x, y \in \mathbb{Q},\ |x + y| \leq |x| + |y|$, avec égalité si et seulement si x et y sont de même signe.

Démonstration.
Adapter la démonstration vue dans $\mathbb{Z}$. □

Remarque. On voit ainsi que pour montrer une propriété à partir d'une propriété voisine déjà établie, il y a deux attitudes duales : on peut tenter d'appliquer la propriété voisine avec de bons paramètres, ou bien on peut tenter d'en adapter la démonstration.

Propriété. Soit x et y deux rationnels strictement positifs. Alors il existe $n \in \mathbb{N}$ tel que $x < ny$. On dit que $\mathbb{Q}$ est archimédien.

Démonstration.
Il existe $a, b, c, d \in \mathbb{N}^*$ tels que $x = \frac{a}{b}$ et $y = \frac{c}{d}$. Soit $n \in \mathbb{N}^*$. Alors
$x < ny \iff \dfrac{x}{y} < n \iff \dfrac{ad}{bc} < n.$
Prenons $n = ad + 1$: $n > ad = \dfrac{ad}{1} \geq \dfrac{ad}{bc}$, donc $x < ny$. □

7.3 L'ensemble $\mathbb{R}$ des réels

7.3.1 Corps totalement ordonnés

Définition. Soit $(K, +, \times)$ un corps muni d'une relation d'ordre $\preceq$.
On dit que $(K, +, \times, \preceq)$ est un corps ordonné si et seulement si
- *Compatibilité avec l'addition* : $\forall x, y, z \in K,\ [x \preceq y] \Longrightarrow [x + z \preceq y + z]$.
- *Compatibilité avec le produit, règle des signes* :
  $\forall x, y \in K,\ [0 \preceq x] \wedge [0 \preceq y] \Longrightarrow [0 \preceq xy]$.

Exemple. On a vu que $\mathbb{Q}$ est un corps totalement ordonné.

7.3.2 Bornes supérieures

Définition. Soit E un ensemble muni d'une relation d'ordre $\preceq$. Soit $A \subset E$.
Lorsque l'ensemble des majorants de A possède un plus petit élément, ce minimum est appelé la borne supérieure de A, et noté $\sup A$.
Lorsque l'ensemble des minorants de A possède un plus grand élément, ce maximum est appelé la borne inférieure de A, et noté $\inf A$.

Exemples :
- Prenons $E = \mathbb{Q}$ et $A = [0, 1[\cap\mathbb{Q}$.
  Lorsque $0 < a < 1$ avec $a \in \mathbb{Q}$, $\frac{a+1}{2} \in A$ et $\frac{a+1}{2} > a$, donc l'ensemble des majorants de A est $[1, +\infty[\cap\mathbb{Q}$ et $\sup(A) = 1$.
- Dans $\mathbb{N}$ muni de la relation de divisibilité, $\inf\{2, 6, 14\} = \text{pgcd}\{2, 6, 14\} = 2$ et $\sup\{2, 6, 14\} = \text{ppcm}\{2, 6, 14\} = 6 \times 7 = 42$.
  Dans ce cas, la borne inférieure est égale au minimum, mais la borne supérieure n'est pas dans l'ensemble $\{2, 6, 14\}$.
- Prenons $E = \mathcal{P}(A)$, muni de l'inclusion. Soit B une partie de E. Vérifier que B possède des bornes supérieure et inférieure que l'on précisera.

Propriété. Soit $(E, \preceq)$ un ensemble ordonné et $A \subset E$.
Si A possède un maximum, alors A possède une borne supérieure et $\sup A = \max A$.
Si A ne possède pas de maximum, mais possède une borne supérieure, alors $\sup A \notin A$.

Démonstration.
Exercice. □

Propriété. Soit $(E, \preceq)$ un ensemble ordonné et soit $A, B \in \mathcal{P}(E)$.
Si A et B possédent des bornes supérieures : si $B \subset A$, alors $\sup(B) \leq \sup(A)$.
Si A et B possédent des bornes inférieures : si $B \subset A$, alors $\inf(B) \geq \inf(A)$.

Démonstration.
$\sup(A)$ est un majorant de A, donc un majorant de B, donc il est plus grand que $\sup(B)$. □

7.3.3 Une caractérisation de $\mathbb{R}$.

Exemple. Prenons $E = \mathbb{Q}$ et $A = \{x \in \mathbb{Q} / x \geq 0 \text{ et } x^2 \leq 2\}$.
0 est le minimum de A, donc c'est aussi la borne inférieure de A.
Montrons que A ne possède pas de borne supérieure dans $\mathbb{Q}$.
Pour cela, raisonnons par l'absurde en supposant que A possède une borne supérieure dans $\mathbb{Q}$, que l'on note a. On va montrer que $a^2 = 2$. L'exercice page 60 montre alors que c'est impossible.
$\diamond$ On commence par vérifier que, pour tout $x, y \in \mathbb{Q}$ tels que $x > 0$ et $y > 0$, $x \leq y \iff x^2 \leq y^2$.
En effet, $x \leq y \implies x.x \leq y.x \leq y.y$ et $x > y \implies x.x > y.x > y.y$.
$\diamond$ Supposons que $a^2 > 2$. Soit $\varepsilon \in \mathbb{Q}_+^*$.

$$(a-\varepsilon)^2 > 2 \iff a^2 - 2a\varepsilon + \varepsilon^2 > 2 \impliedby a^2 - 2a\varepsilon > 2 \impliedby \varepsilon < \frac{a^2-2}{2a}.$$

Ainsi, si l'on pose $\varepsilon = \dfrac{a^2-2}{4a}$, on a $\varepsilon \in \mathbb{Q}_+^*$ et $(a-\varepsilon)^2 > 2$.
Alors, d'après le point précédent, $a - \varepsilon$ est un majorant de A. C'est faux par définition de a, donc $a^2 \leq 2$.
$\diamond$ Supposons que $a^2 < 2$. Soit $\varepsilon \in \mathbb{Q}_+^*$.

$$\begin{aligned}(a+\varepsilon)^2 < 2 \iff a^2 + 2a\varepsilon + \varepsilon^2 < 2 &\impliedby (\varepsilon^2 \leq \varepsilon) \wedge ((2a+1)\varepsilon < 2 - a^2) \\ &\impliedby (\varepsilon \leq 1) \wedge (\varepsilon < \frac{2-a^2}{2a+1}).\end{aligned}$$

Ainsi, si l'on pose $\varepsilon = \min(1, \dfrac{2-a^2}{2(2a+1)})$, on a $\varepsilon \in \mathbb{Q}_+^*$ et $(a+\varepsilon)^2 < 2$.
Alors, $a + \varepsilon \in A$ et a ne majore pas A, ce qui est faux. Donc $a^2 \geq 2$.
En conclusion, A ne possède pas de borne supérieure dans $\mathbb{Q}$.
Cependant A est non vide et majorée, car $x \in A \implies x \leq 2$.
L'existence de telles parties dans $\mathbb{Q}$ indique une incomplétude de ce corps. Il faut en quelque sorte ajouter toutes ces bornes supérieures pour obtenir un corps complet, le corps des réels.
Le fait que toute partie non vide majorée de $\mathbb{R}$ possède une borne supérieure est au coeur de l'analyse, tant pour démontrer des théorèmes fondamentaux (théorèmes de la limite monotone, des valeurs intermédiaires etc.) que pour définir certaines notions essentielles en analyse (intégrales, sommes infinies, convergence uniforme etc.).

Caractérisation de $\mathbb{R}$: (admise)
Il existe au moins un corps K totalement ordonné dans lequel toute partie non vide majorée admet une borne supérieure.
De plus si K' est un autre corps totalement ordonné dans lequel toute partie non vide majorée admet une borne supérieure, il existe une bijection (cf définition page 84) f de K dans K' telle que f est un morphisme de corps ordonnés, c'est-à-dire :
— $\forall x, y \in K,\ x \leq y \implies f(x) \leq f(y)$,
— $\forall x, y \in K,\ f(x+y) = f(x) + f(y)$,
— $\forall x, y \in K,\ f(xy) = f(x)f(y)$,

— $f(1_K) = 1_{K'}$.

Cela signifie que, quitte à renommer x en $f(x)$, K et K' sont égaux, tant que dans K et K' on se contente d'utiliser leurs structures de corps totalement ordonnés.
Ainsi, à un morphisme bijectif près, il existe un unique corps totalement ordonné dans lequel toute partie non vide majorée admet une borne supérieure. Il est noté $\mathbb{R}$ et ses éléments sont appelés les réels.
Il existe un morphisme injectif de corps ordonné de $\mathbb{Q}$ dans $\mathbb{R}$, qui permet d'identifier $\mathbb{Q}$ avec une partie de $\mathbb{R}$.

Propriété. Toute partie non vide minorée de $\mathbb{R}$ possède une borne inférieure.

Démonstration.
Exercice. □

Passage à la borne supérieure (resp : inférieure) : Soit $(E, \preceq)$ un ensemble ordonné et soit A une partie de E possédant une borne supérieure.
◇ Soit $e \in E$. Alors $\sup(A) \leq e \iff [\forall a \in A,\ a \leq e]$.
Le fait de passer de la propriété "$\forall a \in A,\ a \leq e$" à l'affirmation "$\sup(A) \leq e$" s'appelle le *passage à la borne supérieure*.
◇ Il faut savoir le justifier : si $[\forall a \in A,\ a \leq e]$, alors e est un majorant de A, or $\sup(A)$ est le plus petit des majorants, donc $\sup(A) \leq e$.
◇ ATTENTION, en général, $\sup(A) \notin A$, donc le passage à la borne supérieure ne se réduit pas au fait d'appliquer la propriété "$\forall a \in A,\ a \leq e$" avec $a = \sup(A)$.
◇ De même, si B est une partie de E possédant une borne inférieure, le principe du passage à la borne inférieure consiste à passer de la propriété, "$\forall a \in A,\ a \geq e$" à "$\inf(A) \geq e$".

Exemple. Soit S et T deux parties non vides majorées de $\mathbb{R}$.
On pose $S + T = \{s + t / (s, t) \in S \times T\}$. Montrer que $\sup(S + T) = \sup(S) + \sup(T)$.
Solution :
◇ Pour montrer que $\sup(S + T) \leq \sup(S) + \sup(T)$, il suffit de montrer que $\forall (s, t) \in S \times T,\ s + t \leq \sup(S) + \sup(T)$, puis de passer au sup. D'où la rédaction suivante :
◇ Soit $(s, t) \in S \times T$. $s + t \leq \sup(S) + \sup(T)$, donc $\sup(S) + \sup(T)$ est un majorant de $S + T$. Il est nécessairement plus grand que le plus petit des majorants, donc $\sup(S) + \sup(T) \geq \sup(S + T)$.
◇ $\sup(S) + \sup(T) \leq \sup(S + T) \iff \sup(S) \leq \sup(S + T) - \sup(T)$, d'où la rédaction suivante :
◇ Soit $s \in S$. Soit $t \in T$. $s + t \leq \sup(S + T)$, donc pour tout $t \in T$, $t \leq \sup(S + T) - s$. Par passage au sup, on en déduit que $\sup(T) \leq \sup(S + T) - s$.
Ainsi, pour tout $s \in S$, $s \leq \sup(S + T) - \sup(T)$, donc à nouveau par passage au sup, $\sup(S) \leq \sup(S + T) - \sup(T)$.

Compatibilité de "<" avec l'addition : $\forall x, y, z \in \mathbb{R},\ (x < y) \Longrightarrow (x + z < y + z)$.

Démonstration.
Soit $x, y, z \in \mathbb{R}$ tels que $x < y$.
Supposons que $\neg(x + z < y + z)$. Alors $x + z \geq y + z$, mais d'après la compatibilité de $\leq$ avec l'adition, $x + z \leq y + z$, donc $x + z = y + z$, puis $x = y$, ce qui est faux. □

Propriété. $\forall x, y \in \mathbb{R},\ \ x \geq y \iff -x \leq -y$.

Démonstration.
Soit $x, y \in \mathbb{R}$.
$x \geq y \iff x - x \geq y - x \iff y - x \leq 0 \iff y - x - y \leq -y$. □

Propriété. Soit A une partie non vide majorée de $\mathbb{R}$. Soit $s \in \mathbb{R}$. Alors
$s = \sup(A) \iff [\forall a \in A,\ \ a \leq s] \wedge [\forall \varepsilon > 0,\ \ \exists a \in A,\ \ s - \varepsilon < a]$.

Démonstration.
s est la borne supérieure de A si et seulement si c'est un majorant de A, ie
$[\forall a \in A,\ \ a \leq s]$ et si c'est le plus petit des majorants, i.e pour tout $\varepsilon > 0$, $s - \varepsilon$ ne majore pas A.
En effet, si $\varepsilon > 0$, $-\varepsilon < 0$, donc $s - \varepsilon < s$ et réciproquement, si $s' < s$, alors $s' = s - \varepsilon$ avec $\varepsilon = s - s' > 0$. □

> **Exercice.** Soit A une partie de $\mathbb{R}$ non vide et majorée. Montrer qu'il existe une suite $(x_n)_{n\in\mathbb{N}}$ d'éléments de A qui converge vers $\sup(A)$.
> ***Solution :*** Pour tout $n \in \mathbb{N}$, $\sup(A) - \frac{1}{n+1}$ ne majore pas A, donc il existe $x_n \in A$ tel que $x_n > \sup(A) - \frac{1}{n+1}$. Alors $0 \leq \sup(A) - x_n \leq \frac{1}{n+1}$, donc $x_n \underset{n\to+\infty}{\longrightarrow} \sup(A)$.

Propriété. Soit A une partie non vide minorée de $\mathbb{R}$. Soit $m \in \mathbb{R}$. Alors
$m = \inf(A) \iff [\forall a \in A,\ \ a \geq m] \wedge [\forall \varepsilon > 0,\ \ \exists a \in A,\ \ m + \varepsilon > a]$.

7.3.4 La droite réelle achevée

Définition. On appelle droite réelle achevée l'ensemble $\overline{\mathbb{R}} \overset{\Delta}{=} \mathbb{R} \cup \{-\infty, +\infty\}$, sur lequel l'ordre dans $\mathbb{R}$ est prolongé par les conditions : $\forall x \in \mathbb{R},\ \ -\infty < x < +\infty$.

Propriété. $(\overline{\mathbb{R}}, \leq)$ est un ensemble totalement ordonné dans lequel toute partie possède une borne inférieure et une borne supérieure.

Démonstration.
Soit A une partie de $\overline{\mathbb{R}}$.
◇ Supposons d'abord que $A \subset \mathbb{R}$.
Si A est non vide majorée dans $\mathbb{R}$, elle possède un sup dans $\mathbb{R}$. C'est encore le sup de A dans $\overline{\mathbb{R}}$.
Si A est non vide mais non majorée dans $\mathbb{R}$, son seul majorant dans $\overline{\mathbb{R}}$ est $+\infty$, donc $\sup(A) = +\infty$.
Si $A = \emptyset$, $\sup(A) = -\infty$.
◇ Supposons que $+\infty \in A$. Alors $\sup(A) = \max(A) = +\infty$.
◇ Supposons que $-\infty \in A$. Alors A possède le même ensemble de majorants que $A \setminus \{-\infty\}$, ce qui nous ramène aux cas précédents. □

Propriété. Toute partie A de $\mathbb{R}$ possède une borne supérieure dans $\overline{\mathbb{R}}$.
$\sup(A) = +\infty \iff A$ non majorée .
$\sup(A) = -\infty \iff A = \emptyset$.

7.3.5 Les intervalles

Définition.
- Pour tout $a, b \in \overline{\mathbb{R}}$, l'intervalle $]a, b[$ est défini par $]a, b[= \{x \in \mathbb{R} / a < x < b\}$.
- Pour tout $a, b \in \mathbb{R}$, l'intervalle $[a, b]$ est défini par $[a, b] = \{x \in \mathbb{R} / a \leq x \leq b\}$.
- Si $a \in \mathbb{R}$ et $b \in \overline{\mathbb{R}}$, les intervalles $[a, b[$ et $]b, a]$ sont définis par : $[a, b[= \{x \in \mathbb{R} / a \leq x < b\}$ et $]b, a] = \{x \in \mathbb{R} / b < x \leq a\}$.
- En particulier, $\mathbb{R} =]-\infty, +\infty[$ et $\emptyset =]0, -1[$ sont des intervalles.

Définition.
- Un intervalle est ouvert si et seulement si il est de la première forme $]a, b[$ avec $a, b \in \overline{\mathbb{R}}$.
- On dit qu'un intervalle est fermé si et seulement si son complémentaire est une réunion d'un ou deux d'intervalles ouverts.
- Ainsi, $[a, b]$ est fermé lorsque $a, b \in \mathbb{R}$, mais $[a, +\infty[$ est aussi fermé (avec $a \in \mathbb{R}$).
- $\emptyset$ et $\mathbb{R}$ sont à la fois ouverts et fermés.
- $[0, 1[$ n'est ni ouvert ni fermé. On dit qu'il est semi-ouvert ou semi-fermé.
- Les intervalles fermés bornés sont de la forme $[a, b]$ avec $a, b \in \mathbb{R}$. On les appelle aussi des segments.

Définition. Soit A une partie de $\mathbb{R}$.
A est convexe si et seulement si pour tout $a, b \in A$ avec $a < b$, $[a, b] \subset A$.

Théorème. Les parties convexes de $\mathbb{R}$ sont exactement ses intervalles.

Démonstration.
La propriété étant évidente lorsque $I = \emptyset$, nous supposons maintenant que $I \neq \emptyset$.
$\diamond$ Supposons que I est un intervalle. Notons $a = \text{Inf}(I) \in \mathbb{R} \cup \{-\infty\}$
et $b = \text{Sup}(I) \in \mathbb{R} \cup \{+\infty\}$. Alors pour tout $x \in \mathbb{R}$,
$a < x < b \Longrightarrow x \in I \Longrightarrow a \leq x \leq b$.
Montrons que I est convexe : Soit $x, y \in I$ avec $x < y$.
Si $t \in]x, y[$, alors $a \leq x < t < y \leq b$, donc $a < t < b$ puis $t \in I$.
Ainsi, $]x, y[\subset I$, mais $x, y \in I$, donc $[x, y] \subset I$.
Ceci démontre que I est bien convexe.
$\diamond$ Réciproquement, supposons que I est convexe et montrons que I est un intervalle.
Posons à nouveau $a = \text{Inf}(I) \in \mathbb{R} \cup \{-\infty\}$ et $b = \text{Sup}(I) \in \mathbb{R} \cup \{+\infty\}$. Il suffit de montrer que $]a, b[\subset I \subset [a, b] \cap \mathbb{R}$, mais la seconde inclusion est évidente par définition de a et b.
Soit $x \in]a, b[$. $x > a = \text{Inf}(I)$ donc il existe $i \in I$ tel que $i < x$. De même il existe $j \in I$ tel que $x < j$. Ainsi $x \in [i, j]$ avec $i, j \in I$ tels que $i < j$, mais I est convexe, donc $x \in I$. $\square$

Corollaire. Une intersection d'intervalles de $\mathbb{R}$ est un intervalle de $\mathbb{R}$.

Démonstration.
Soit $(I_k)_{k\in K}$ une famille d'intervalles. Posons $I = \bigcap_{k\in K} I_k$.
Soit $a, b \in I$ avec $a < b$.
Soit $k \in K$. $a, b \in I_k$, $a < b$ et I_k est convexe, donc $[a, b] \subset I_k$.
Ainsi $[a, b] \subset \bigcap_{k\in K} I_k = I$, donc I est convexe. □

Propriété. Si une famille d'intervalles est d'intersection non vide, l'union de ces intervalles est encore un intervalle.

Démonstration.
Soit $(I_k)_{k\in K}$ une famille d'intervalles tels qu'il existe $c \in \bigcap_{k\in K} I_k$.
Notons $J = \bigcup_{k\in K} I_k$. Il suffit de montrer que J est convexe.
Soit $a, b \in J$ avec $a < b$. Il existe $k, h \in K$ tels que $a \in I_h$ et $b \in I_k$.
$a, c \in I_h$ et I_h est un intervalle, donc $[\min(a, c), \max(a, c)] \subset I_h \subset J$.
De même, $b, c \in I_k$ et I_k est un intervalle, donc $[\min(b, c), \max(b, c)] \subset I_k \subset J$.
On en déduit que $[\min(a, c), \max(a, c)] \cup [\min(b, c), \max(b, c)] \subset J$.
Ainsi, lorsque $c < a$, $[a, b] \subset [c, b] \subset J$, lorsque $c > b$, $[a, b] \subset [a, c] \subset J$ et lorsque $a \leq c \leq b$, $[a, b] = [a, c] \cup [c, b] \subset J$. Dans tous les cas, on a montré que $[a, b] \subset J$. □

7.3.6 la valeur absolue

Définition. Soit $x \in \mathbb{R}$.
Le signe de x au sens large est
- 1 ou bien "positif" lorsque $n \geq 0$,
- -1 ou bien "négatif" lorsque $n \leq 0$.

Le signe de n au sens strict est
- 1 ou bien "strictement positif" lorsque $n > 0$,
- 0 ou bien "nul" lorsque $n = 0$,
- -1 ou bien "strictement négatif" lorsque $n < 0$.

Propriété. Le signe au sens large du produit de deux réels est égal au produit des signes de ces réels.

Démonstration.
Lorsque x et y sont des réels positifs, cela résulte de la compatibilité de $\leq$ avec le produit.
Supposons que $x \geq 0$ et $y \leq 0$. Alors $-(-y) \leq 0$, donc d'après la propriété précédente, $-y \geq 0$, puis $x(-y) \geq 0$. En utilisant à nouveau la propriété précédente, $xy \leq 0$.
On traite de même les autres cas. □

Définition. Pour tout $x \in \mathbb{R}$, on note $|x| = \max\{-x, x\}$.
C'est la valeur absolue de x.

Propriété. Soit $x \in \mathbb{R}$. Si $x \geq 0$ alors $|x| = x$ et si $x \leq 0$, alors $|x| = -x$.

Propriété. Pour tout $x \in \mathbb{R}$, $x \leq |x|$, avec égalité si et seulement si $x \geq 0$.
De plus $|x|^2 = x^2$.

Propriété. $\forall x, y \in \mathbb{R},\ |xy| = |x||y|$.

Démonstration.
Discuter selon les signes au sens large de x et y. □

Inégalité triangulaire : $\forall x, y \in \mathbb{R},\ |x + y| \leq |x| + |y|$, avec égalité si et seulement si x et y sont de même signe.

Démonstration.
Adapter la démonstration vue dans $\mathbb{Z}$. □

Corollaire de l'inégalité triangulaire : $\forall x, y \in \mathbb{R},\ ||x| - |y|| \leq |x - y|$.

Démonstration.
Soit $x, y \in \mathbb{R}$.
$|x| = |(x - y) + y| \leq |x - y| + |y|$, donc $|x| - |y| \leq |x - y|$. □

Formule : Pour tout $a, b \in \mathbb{R}$,

$$\min(a, b) = \frac{(a + b) - |a - b|}{2} \text{ et } \max(a, b) = \frac{(a + b) + |a - b|}{2}.$$

Informellement, pour atteindre $\min(a, b)$, on part du milieu de a et b, égal à $\dfrac{a + b}{2}$, et on se déplace vers la gauche selon la moitié de la distance entre a et b, égale à $|a - b|$.

Démonstration.
Discuter selon l'ordre entre a et b. □

Remarque. Cette formule est utile, notamment pour établir que $(a, b) \longmapsto \max(a, b)$ est une application continue.

Notation. Si $x \in \mathbb{R}$, on pose $x^+ = \max(x, 0)$ et $x^- = \max(-x, 0)$.
Alors $x = x^+ - x^-$ et $|x| = x^+ + x^-$.

Distance entre réels : Lorsque $x, y \in \mathbb{R}$, la quantité $d(x, y) = |x - y|$ est appelée la distance entre les deux réels x et y.
La fonction distance vérifie les propriétés suivantes : pour tout $x, y, z \in \mathbb{R}$,

- Positivité : $d(x, y) \in \mathbb{R}_+$.
- $d(x, y) = 0 \iff x = y$: d permet de *séparer* les réels.
- Symétrie : $d(x, y) = d(y, x)$.
- Inégalité triangulaire : $d(x, z) \leq d(x, y) + d(y, z)$.

Définition. Soit $\varepsilon > 0$ et $a \in \mathbb{R}$.
Pour tout $x \in \mathbb{R}$, $|x - a| \leq \varepsilon \iff x \in [a - \varepsilon, a + \varepsilon]$
Ainsi, l'intervalle $[a - \varepsilon, a + \varepsilon]$ est l'ensemble des réels qui sont à une distance de a inférieure ou égale à ε. Il est aussi appelé la boule fermée de centre a et de rayon ε, notée $B_f(a, \varepsilon)$.
L'intervalle $]a - \varepsilon, a + \varepsilon[$ est pour la même raison appelé la boule ouverte de centre a et de rayon ε, notée $B_o(a, \varepsilon)$.

7.3.7 Propriétés usuelles des réels

Propriété. $\mathbb{R}$ **est archimédien :** Pour tout $(a,b) \in {\mathbb{R}_+^*}^2$, $\exists n \in \mathbb{N},\ na > b$.

Démonstration.
Soit $a, b \in \mathbb{R}$ tels que $a > 0$ et $b > 0$. Raisonnons par l'absurde en supposant que, pour tout $n \in \mathbb{N}$, $na \leq b$. Considérons l'ensemble $A = \{na/n \in \mathbb{N}\}$. C'est une partie non vide de $\mathbb{R}$ majorée par b, donc elle possède une borne supérieure que l'on notera s.
$a > 0$, donc $s - a$ ne majore pas A : il existe $n \in \mathbb{N}$ tel que $na > s - a$.
Alors $(n+1)a > s$ ce qui est impossible. □

Remarque. Lorsque nous aurons défini la partie entière d'un réel, on pourra court-circuiter cette propriété en prenant $n = \lfloor \frac{b}{a} \rfloor + 1$.

Corollaire. Pour tout réel x, il existe un entier N tel que $N \geq x$.

Démonstration.
Si $x \leq 0$, $N = 0$ convient.
Si $x > 0$, comme $1 > 0$, le caractère archimédien de $\mathbb{R}$ prouve l'existence d'un entier naturel N tel que $N.1 > x$. □

Propriété. $\mathbb{Q}$ est dense dans $\mathbb{R}$: $\forall (x,y) \in \mathbb{R}^2,\ x < y \Longrightarrow [\exists q \in \mathbb{Q},\ x < q < y]$.

Démonstration.
Soit $x, y \in \mathbb{R}$ tels que $x < y$.
Premier cas : On suppose que $y > 0$.
Posons $\varepsilon = y - x > 0$.
D'après le caractère archimédien de $\mathbb{R}$, sachant que $\varepsilon > 0$ et $1 > 0$, il existe $N \in \mathbb{N}^*$ tel que $N\varepsilon > 1$. Ainsi $0 < \frac{1}{N} < \varepsilon$.
Notons $A = \{k \in \mathbb{N} / \frac{k}{N} < y\}$: A est une partie non vide car $y > 0$. De plus A est majorée par Ny (donc par un entier d'après le corollaire précédent), or $A \subset \mathbb{N}$, donc A possède un maximum, noté m.
On a $\frac{m}{N} < y$ et $\frac{m+1}{N} \geq y$, donc $\frac{m}{N} \geq y - \frac{1}{N} > y - \varepsilon = x$.
Ainsi, $x < \frac{m}{N} < y$ et $\frac{m}{N} \in \mathbb{Q}$.
Deuxième cas : On suppose que $y < 0$. Alors $-y < -x$ et $-x > 0$. D'après le premier cas, il existe $q \in \mathbb{Q}$ tel que $-y < q < -x$. Alors $x < -q < y$ et $-q \in \mathbb{Q}$. □

Propriété. $\mathbb{R}\backslash\mathbb{Q}$ est dense dans $\mathbb{R}$: $\forall (x,y) \in \mathbb{R}^2,\ x < y \Longrightarrow [\exists q \in \mathbb{R} \setminus \mathbb{Q},\ x < q < y]$.

Démonstration.
Adaptons l'exemple de la page 63 : on pose $A' = \{x \in \mathbb{R} / x \geq 0 \text{ et } x^2 \leq 2\}$. A' est une partie non vide de $\mathbb{R}$, majorée par 2, donc elle possède une borne supérieure $a \in \mathbb{R}$. En adaptant la preuve de l'exemple, on montre que $a^2 = 2$ et $a > 0$. On peut donc noter $a = \sqrt{2}$. D'après l'exercice page 60, $\sqrt{2}$ est irrationnel.
Soit maintenant $x, y \in \mathbb{R}$ tels que $x < y$. Alors $\dfrac{x}{\sqrt{2}} < \dfrac{y}{\sqrt{2}}$. D'après la densité de $\mathbb{Q}$ dans $\mathbb{R}$, il existe $q \in \mathbb{Q}$ tel que $\dfrac{x}{\sqrt{2}} < q < \dfrac{y}{\sqrt{2}}$.
On peut imposer $q \neq 0$. Alors $x < q\sqrt{2} < y$ et $q\sqrt{2} \notin \mathbb{Q}$. □

Définition. Soit $x \in \mathbb{R}$. On appelle partie entière de x le plus grand entier relatif inférieur ou égal à x. Elle est notée $\lfloor x \rfloor$. C'est l'unique entier n tel que $n \leq x < n+1$.
On appelle partie entière supérieure de x le plus petit entier supérieur ou égal à x. Elle est notée $\lceil x \rceil$. C'est l'unique entier n tel que $n-1 < x \leq n$.

Démonstration.
$\{k \in \mathbb{Z} / k \leq x\}$ est une partie de $\mathbb{Z}$ non vide d'après le corollaire appliqué à $-x$ et majorée dans $\mathbb{Z}$, toujours d'après le corollaire, donc elle possède bien un maximum dans $\mathbb{Z}$. Si on le note n, on a $n \leq x$ et $n+1 > x$.
Si n' est un second entier tel que $n' \leq x < n'+1$, alors $n \leq x < n'+1$, donc $n < n'+1$, puis $n \leq n'$. De même on montre que $n' \leq n$, donc $n = n'$, ce qui prouve l'unicité. □

Exemple. $\lfloor 3,3 \rfloor = 3$, $\lfloor -3,3 \rfloor = -4$.
$\lceil 3,3 \rceil = 4$ et $\lceil -3,3 \rceil = -3$.
Lorsque x est entier, $\lfloor x \rfloor = x = \lceil x \rceil$.
Lorsque x n'est pas entier, $\lfloor x \rfloor < x < \lceil x \rceil = \lfloor x \rfloor + 1$.

Une inégalité très utile : Pour tout $x, y \in \mathbb{R}$, $|xy| \leq \dfrac{x^2+y^2}{2}$.

Démonstration.
N'hésitez pas à reproduire cette démonstration sur une copie avant d'utiliser cette inégalité : soit $x, y \in \mathbb{R}$. $(|x|-|y|)^2 \geq 0$, donc $2|xy| \leq x^2+y^2$. □

Remarque. Cette inégalité est équivalente au fait que,
pour tout $x, y \in \mathbb{R}_+$, $\sqrt{xy} \leq \dfrac{x+y}{2}$, c'est-à-dire au fait que la moyenne géométrique est inférieure à la moyenne arithmétique.

7.3.8 Développement décimal d'un entier naturel

Lemme 1 : Soit (x_n) une suite strictement croissante d'entiers naturels.
Alors, pour tout $n \in \mathbb{N}$, $x_n \geq n$.

Démonstration.
Par récurrence. □

Lemme 2 : Soit $p \in \mathbb{N}$ et $(a_0, \ldots, a_{p-1}) \in \{0, \ldots, 9\}^p$. Alors $\displaystyle\sum_{k=0}^{p-1} a_k 10^k < 10^p$.

Démonstration.
Soit $p \in \mathbb{N}$.

On note $R(p)$ l'assertion : pour tout $(a_0, \ldots, a_{p-1}) \in \{0, \ldots, 9\}^p$, $\displaystyle\sum_{k=0}^{p-1} a_k 10^k < 10^p$.

Pour $p = 0$, $\displaystyle\sum_{k=0}^{p-1} a_k 10^k = 0$, car c'est une somme vide. Ceci prouve $R(0)$.

Pour $p \geq 0$, supposons $R(p)$ et montrons $R(p+1)$. Soit $(a_0, \ldots, a_p) \in \{0, \ldots, 9\}^{p+1}$.

D'après $R(p)$, $\sum_{k=0}^{p-1} a_k 10^k < 10^p$, donc $\sum_{k=0}^{p} a_k 10^k < 10^p + a_p 10^p \leq 10^p(1+9) = 10^{p+1}$.
Ceci prouve $R(p+1)$. □

Définition. Les chiffres en base 10 sont $0, 1, \ldots, 9$.

Théorème. Pour tout $n \in \mathbb{N}$, il existe un unique $p \in \mathbb{N}$ et un unique p-uplet $(a_0, \ldots, a_{p-1}) \in \{0, \ldots, 9\}^p$ tels que $n = \sum_{k=0}^{p-1} a_k 10^k$ et (si $p \geq 1$) $a_{p-1} \neq 0$.

Cette égalité s'appelle le développement décimal de l'entier n, que l'on notera sous la forme $n = a_{p-1}a_{p-2}\cdots a_0$, ou parfois $n = \overline{a_{p-1}a_{p-2}\cdots a_0}$.
Il est équivalent de dire que, pour tout $n \in \mathbb{N}$, il existe une unique suite presque nulle de chiffres $(a_k)_{k\in\mathbb{N}} \in \{0, \ldots, 9\}^{(\mathbb{N})}$ telle que $n = \sum_{k\in\mathbb{N}} a_k 10^k$.

Démonstration.
Soit $n \in \mathbb{N}$. Procédons par analyse-synthèse.

- *Analyse :* Supposons qu'il existe $(a_h)_{h\in\mathbb{N}} \in \{0, \ldots, 9\}^{(\mathbb{N})}$ telle que $n = \sum_{h\in\mathbb{N}} a_h 10^h$.

Soit $k \in \mathbb{N}$. Informellement, $\dfrac{n}{10^k}$ est un nombre décimal dont l'écriture décimale est $a_N \cdots a_k$, $a_{k-1} \cdots a_0$, donc $\left\lfloor \dfrac{n}{10^k} \right\rfloor = \overline{a_N \cdots a_k}$.
De même, $10\left\lfloor \dfrac{n}{10^{k+1}} \right\rfloor = \overline{a_N \cdots a_{k+1}0}$, donc $a_k = \left\lfloor \dfrac{n}{10^k} \right\rfloor - 10\left\lfloor \dfrac{n}{10^{k+1}} \right\rfloor$,
ce qui prouve l'unicité. Plus formellement :
$\dfrac{n}{10^k} = \sum_{h\geq k} a_h 10^{h-k} + \dfrac{1}{10^k}\sum_{h=0}^{k-1} a_h 10^h$, mais d'après le lemme 2, $0 \leq \sum_{h=0}^{k-1} a_h 10^h < 10^k$,
donc $\dfrac{1}{10^k}\sum_{h=0}^{k-1} a_h 10^h \in [0, 1[$. Ainsi, $\left\lfloor \dfrac{n}{10^k} \right\rfloor = \sum_{h\geq k} a_h 10^{h-k}$.
On a aussi $\left\lfloor \dfrac{n}{10^{k+1}} \right\rfloor = \sum_{h\geq k+1} a_h 10^{h-k-1}$, donc $10\left\lfloor \dfrac{n}{10^{k+1}} \right\rfloor = \sum_{h\geq k+1} a_h 10^{h-k}$,
puis $\left\lfloor \dfrac{n}{10^k} \right\rfloor - 10\left\lfloor \dfrac{n}{10^{k+1}} \right\rfloor = \sum_{h\geq k} a_h 10^{h-k} - \sum_{h\geq k+1} a_h 10^{h-k} = a_k$.

- *Synthèse :* Pour tout $k \in \mathbb{N}$, posons $a_k = \left\lfloor \dfrac{n}{10^k} \right\rfloor - 10\left\lfloor \dfrac{n}{10^{k+1}} \right\rfloor$. Montrons que $(a_k)_{k\in\mathbb{N}}$ est une suite presque nulle de chiffres compris entre 0 et 9 et que $n = \sum_{h\in\mathbb{N}} a_h 10^h$.

Si $n = 0$, pour tout $k \in \mathbb{N}$, $a_k = 0$, donc la propriété est démontrée. Supposons maintenant que $n \neq 0$.
◇ La suite $(10^h)_{h\in\mathbb{N}}$ est strictement croissante, donc d'après le lemme 1, pour tout $h \in \mathbb{N}$, $10^h \geq h$. Ainsi, l'ensemble $\{h \in \mathbb{N} / 10^h \leq n\}$ est non vide (il contient 0 car $n \geq 1$) et majoré par n, donc il admet un maximum noté $p \in \mathbb{N}$. Alors $10^p \leq n < 10^{p+1}$.
Ainsi, dès que $k \geq p+1$, $10^k > n$ et $\left\lfloor \dfrac{n}{10^k} \right\rfloor = 0$, donc lorsque $k \geq p+1$, $a_k = 0$.

Ceci prouve que la suite (a_k) est presque nulle.
$\diamond$ Soit $k \in \mathbb{N}$: $\frac{n}{10^k} - 1 < \left\lfloor \frac{n}{10^k} \right\rfloor \leq \frac{n}{10^k}$ et $\frac{n}{10^{k+1}} - 1 < \left\lfloor \frac{n}{10^{k+1}} \right\rfloor \leq \frac{n}{10^{k+1}}$, donc
$\left\lfloor \frac{n}{10^k} \right\rfloor - 10 \left\lfloor \frac{n}{10^{k+1}} \right\rfloor < \frac{n}{10^k} - 10(\frac{n}{10^{k+1}} - 1) = 10$
et $\left\lfloor \frac{n}{10^k} \right\rfloor - 10 \left\lfloor \frac{n}{10^{k+1}} \right\rfloor > \frac{n}{10^k} - 1 - 10\frac{n}{10^{k+1}} = -1$.
Ainsi, pour tout $k \in \mathbb{N}$, $a_k \in \{0, \dots, 9\}$.
$\diamond$ $\sum_{k\in\mathbb{N}} a_k 10^k = \sum_{k\in\mathbb{N}} \left(10^k \left\lfloor \frac{n}{10^k} \right\rfloor - 10^{k+1} \left\lfloor \frac{n}{10^{k+1}} \right\rfloor\right) = \sum_{k\in\mathbb{N}} 10^k \left\lfloor \frac{n}{10^k} \right\rfloor - \sum_{k\geq 1} 10^k \left\lfloor \frac{n}{10^k} \right\rfloor = n.$
□

Remarque. On peut généraliser et développer en base a où a est un entier supérieur ou égal à 2. Il suffit de remplacer 10 par a dans les énoncés et démonstrations précédents.

CNS de divisibilité : Soit $n \in \mathbb{N}$, dont le développement décimal est noté $n = \sum_{k\in\mathbb{N}} a_k 10^k$. On note $s = \sum_{k\in\mathbb{N}} a_k$ la somme des chiffres de n.
- n est divisible par 2 si et seulement si $a_0 \in \{0, 2, 4, 6, 8\}$.
- n est divisible par 5 si et seulement si $a_0 \in \{0, 5\}$.
- n est divisible par 10 si et seulement si $a_0 = 0$.
- n est divisible par 3 si et seulement si $s \equiv 0$ [3].
- n est divisible par 9 si et seulement si $s \equiv 0$ [9].
- n est divisible par 11 si et seulement si $\sum_{k\in\mathbb{N}} (-1)^k a_k \equiv 0$ [11].

7.3.9 L'ensemble $\mathbb{D}$ des nombres décimaux

Définition. $\mathbb{D} = \left\{ \frac{n}{10^k} / n \in \mathbb{Z} \text{ et } k \in \mathbb{N} \right\}$. C'est une partie de $\mathbb{Q}$ dont les éléments sont appelés les nombres décimaux.

Propriété. Soit $x \in \mathbb{Q}$. x est un nombre décimal si et seulement si son écriture irréductible est de la forme $x = \frac{p}{2^h 5^k}$, où $p \in \mathbb{Z}$ et $h, k \in \mathbb{N}$.

Démonstration.
S'il existe $p, h, k \in \mathbb{N}$ tels que $x = \frac{p}{2^h 5^k}$, alors en posant $m = \max\{h, k\}$,
$x = \frac{n}{10^m}$ où $n = p 2^{m-h} 5^{m-k}$, donc $x \in \mathbb{D}$.
Réciproquement, si $x \in \mathbb{D}$, il existe $n \in \mathbb{Z}$ et $k \in \mathbb{N}$ tels que $x = \frac{n}{10^k}$.
Si $n = 0$, la propriété est vraie. Sinon, la forme irréductible de x est $x = \frac{\frac{n}{d}}{\frac{10^k}{d}}$, où $d = n \wedge 10^k$. d divise 10^k, donc d est de la forme $2^a 5^b$, ce qui permet de conclure. □

Corollaire. $\mathbb{D} \neq \mathbb{Q}$. Par exemple, $\frac{1}{3} \notin \mathbb{D}$.

Propriété. $d \in \mathbb{D}$ si et seulement si il existe une famille presque nulle de chiffres indexée par $\mathbb{Z}$, $(a_k)_{k\in\mathbb{Z}} \in \{0, \dots, 9\}^{(\mathbb{Z})}$ telle que $d = \sum_{k\in\mathbb{Z}} a_k 10^k$.

Lorsque $d \neq 0$, l'ensemble $\{k \in \mathbb{Z}/a_k \neq 0\}$ est non vide et fini, donc il possède un minimum m et un maximum M. Lorsque $m < 0$, on écrit $d = a_M \cdots a_0 \ , \ \overline{a_{-1} \cdots a_m}$.

7.3.10 Approximation d'un réel

Définition. Soit $x, \alpha \in \mathbb{R}$ et $\varepsilon \in \mathbb{R}_+^*$.
- On dit que α est une valeur approchée de x à ε près si et seulement si $d(x, \alpha) \leq \varepsilon$. On note alors $x = \alpha \pm \varepsilon$.
- On dit que α est une valeur approchée de x à ε près par défaut si et seulement si $\alpha \leq x \leq \alpha + \varepsilon$,
- On dit que α est une valeur approchée de x à ε près par excès si et seulement si $\alpha - \varepsilon \leq x \leq \alpha$.

Propriété. Soit $x \in \mathbb{R}$ et $p \in \mathbb{N}$. Posons $\alpha = \dfrac{\lfloor 10^p x \rfloor}{10^p}$. $\alpha \in \mathbb{D}$.
Alors α est une valeur approchée de x par défaut à 10^{-p} près,
et $\alpha + 10^{-p}$ est une valeur approchée de x par excès à 10^{-p} près.

Démonstration.
$\lfloor 10^p x \rfloor \leq 10^p x < \lfloor 10^p x \rfloor + 1$. □

Exemple. Admettons que $e = 2,71828183\cdots$. Alors $10^3 e = 2718$,
donc $\dfrac{\lfloor 10^3 e \rfloor}{10^3} = 2,718$ est une valeur approchée de e à 10^{-3} près.

Remarque. On peut donc approcher tout réel x par un nombre décimal α à une précision ε aussi petite que l'on veut. Il en résulte que $\mathbb{D}$ est dense dans $\mathbb{R}$.

7.3.11 Développement d'un réel en base quelconque

Notation. On fixe un entier naturel a supérieur ou égal à 2. On pourra si l'on préfère remplacer a par 10 ci-dessous et se limiter aux développements en base 10.

Propriété. Soit $(v_n)_{n\geq 1}$ une suite d'entiers telle que, pour tout $n \in \mathbb{N}^*$, $0 \leq v_n \leq a-1$.
Pour tout $n \in \mathbb{N}$, posons $x_n = \displaystyle\sum_{k=1}^{n} v_k a^{-k}$.
La suite (x_n) est croissante et majorée, donc elle converge vers une limite x que l'on notera $x = \displaystyle\sum_{n=1}^{+\infty} v_n a^{-n}$. Dans ces conditions, on dit que $(v_n)_{n\geq 1}$ est un développement de x en base a (développement décimal lorsque $a = 10$, développement binaire lorsque $a = 2$) et on note $x = 0, \overline{v_1 v_2 \cdots v_n v_{n+1} \cdots}$.
De plus, $x \in [0, 1]$ et $[x = 1 \iff (\forall n \in \mathbb{N}^*, \ v_n = a - 1)]$.

Démonstration.
Soit $n \in \mathbb{N}^*$: $x_{n+1} - x_n = v_{n+1} a^{-n-1} \geq 0$, donc la suite (x_n) est croissante.
$x_n \leq \displaystyle\sum_{k=1}^{n} (a-1) a^{-k} = \sum_{k=0}^{n-1} a^{-k} - \sum_{k=1}^{n} a^{-k} = 1 - a^{-n}$.

En particulier, pour tout $n \in \mathbb{N}^*$, $x_n \leq 1$, donc la suite (x_n) est croissante et majorée. On verra plus loin qu'une telle suite est toujours convergente. Il existe donc $x \in \mathbb{R}$ tel que $x_n \underset{n\to+\infty}{\longrightarrow} x$. De plus, pour tout $n \in \mathbb{N}^*$, $0 \leq x_n \leq 1$, donc $x \in [0,1]$.

Si pour tout $n \in \mathbb{N}^*$, $v_n = a-1$, alors $x_n = \sum_{k=1}^{n}(a-1)a^{-k}$ et ce qui précède montre que $x_n = 1 - a^{-n}$, donc $x_n \underset{n\to+\infty}{\longrightarrow} 1$.
Réciproquement, supposons que $x_n \underset{n\to+\infty}{\longrightarrow} 1$.
Alors $\sum_{k=1}^{+\infty} v_k a^{-k} = 1 = \sum_{k=1}^{+\infty}(a-1)a^{-k}$, donc $\sum_{k=1}^{+\infty}(a-1-v_k)a^{-k} = 0$.
Soit $N \geq 1$: $0 \leq \sum_{k=1}^{N}(a-1-v_k)a^{-k} \leq \sum_{k=1}^{+\infty}(a-1-v_k)a^{-k} = 0$,
donc pour tout $k \in \mathbb{N}^*$, $a-1-v_k = 0$. □

Remarque. $\sum_{n=1}^{+\infty}(a-1)a^{-n} = 1$, donc si $N \in \mathbb{N}$ avec $N \geq 2$,

$$\sum_{n=N+1}^{+\infty}(a-1)a^{-n} = \lim_{K\to+\infty}\sum_{n=N+1}^{K}(a-1)a^{-n} = a^{-N}\lim_{K\to+\infty}\sum_{n=1}^{K-N}(a-1)a^{-n} = a^{-N}.$$

On en déduit que si $v_N < a-1$, les suites $(v_1, v_2, \ldots, v_N, a-1, \ldots, a-1, \ldots)$ et $(v_1, v_2, \ldots, v_N+1, 0, \ldots, 0, \ldots)$ sont deux développements en base a d'un même réel.

Exemple. En base 10, $0,567999999\cdots = 0,568$.
Sans une règle supplémentaire sur les chiffres du développement décimal d'un réel, il n'y a donc pas unicité du développement décimal d'un réel.

Notation. Posons
$\mathcal{V} = \{(v_n)_{n\geq 1} / \forall n \in \mathbb{N}^*\ v_n \in \mathbb{N} \cap [0,a[\text{ et } \forall N \in \mathbb{N}^*\ \exists n \geq N\ v_n \neq a-1\}$.
Ainsi, les éléments de $\mathcal{V}$ sont les suites de chiffres qui ne sont pas tous égaux à $a-1$ à partir d'un certain rang.

Théorème. Tout réel de $[0,1[$ admet un unique développement en base a dans $\mathcal{V}$.

Démonstration.
Soit $x \in [0,1[$.
• *Unicité.*
Supposons que x admet un développement en base a dans $\mathcal{V}$, que l'on notera (v_n).
Soit $k \in \mathbb{N}^*$. $x = 0,\overline{v_1 v_2 \cdots v_n \cdots}$, donc $a^k x = v_1 v_2 \cdots v_k + 0,\overline{v_{k+1} \cdots v_N \cdots}$, où $v_1 v_2 \cdots v_k$ désigne $\sum_{h=1}^{k} v_h a^{k-h}$ (notation d'un entier en base a).
D'après une remarque précédente, si $0,\overline{v_{k+1} \cdots v_N \cdots} = 1$, alors pour tout $n \geq k+1$, $v_n = a-1$, ce qui est faux car $(v_n) \in \mathcal{V}$, donc $0,\overline{v_{k+1} \cdots v_N \cdots} \in [0,1[$.
On en déduit que $\lfloor a^k x \rfloor = v_1 v_2 \cdots v_k$ [on retrouve le fait que $a^{-k}\lfloor a^k x \rfloor$ est la valeur décimale approchée de x par défaut à a^{-k} près], puis que $v_k = \lfloor a^k x \rfloor - a\lfloor a^{k-1} x \rfloor$.

Ceci prouve l'unicité, en supposant l'existence.

• *Existence.*

Pour tout $k \in \mathbb{N}^*$, posons $v_k = \lfloor a^k x \rfloor - a\lfloor a^{k-1}x \rfloor$ et montrons que la suite (v_n) est un développement de x dans $\mathcal{V}$.

◇ Pour tout $k \in \mathbb{N}^*$, $v_k a^{-k} = a^{-k}\lfloor a^k x \rfloor - a^{-(k-1)}\lfloor a^{k-1}x \rfloor$,

donc $\displaystyle\sum_{h=1}^{k} v_h a^{-h} = a^{-k}\lfloor a^k x \rfloor$.

D'autre part, $\lfloor a^k x \rfloor \leq a^k x < \lfloor a^k x \rfloor + 1$, donc (1) : $\displaystyle\sum_{h=1}^{k} v_h a^{-h} \leq x < a^{-k} + \sum_{h=1}^{k} v_h a^{-h}$

(également vraie pour $k = 0$).

En faisant tendre k vers $+\infty$, on en déduit que $x = \displaystyle\sum_{h=1}^{+\infty} v_h a^{-h}$.

◇ $\lfloor a^{k-1}x \rfloor \leq a^{k-1}x < \lfloor a^{k-1}x \rfloor + 1$, donc $a\lfloor a^{k-1}x \rfloor \leq a^k x < a\lfloor a^{k-1}x \rfloor + a$. Ainsi, $a\lfloor a^{k-1}x \rfloor \leq \lfloor a^k x \rfloor < a\lfloor a^{k-1}x \rfloor + a$. On en déduit que $0 \leq v_k < a$.

Ainsi, (v_n) est un développement en base a de x.

◇ Il reste à montrer que $(v_n) \in \mathcal{V}$.

Supposons qu'il existe $N \in \mathbb{N}^*$ tel que, pour tout $n \geq N$, $v_n = a - 1$. Alors

$x - \displaystyle\sum_{h=1}^{N} v_h a^{-h} = \sum_{h=N+1}^{+\infty} (a-1)a^{-h} = a^{-N}$, ce qui est faux d'après l'inégalité stricte de (1). □

Remarque. Soit $x \in \mathbb{R}_+$. On peut écrire $x = \lfloor x \rfloor + \{x\}$, où $\lfloor x \rfloor \in \mathbb{N}$ et où $\{x\} = x - \lfloor x \rfloor \in [0, 1[$ est la partie fractionnaire de x.

On obtient le développement en base a du réel x en concaténant le développement en base a de l'entier$\lfloor x \rfloor$ avec celui du réel $\{x\} \in [0, 1[$.

Théorème hors programme : caractérisation d'un rationnel. Soit $x \in [0, 1[$. Notons $x = 0, \overline{v_1 \cdots v_n \cdots}$ le développement en base a de x.

x est un rationnel si et seulement si son développement en base a est périodique à partir d'un certain rang, c'est-à-dire si et seulement si il existe $N \in \mathbb{N}^*$ et $p \in \mathbb{N}^*$ tel que $\forall n > N,\ v_n = v_{n+p}$.

Démonstration.

Notons $(v_n)_{n\geq 1}$ le développement dans $\mathcal{V}$ de x.

• On suppose que ce développement est périodique à partir d'un certain rang : il existe $p \in \mathbb{N}^*$ et $N \in \mathbb{N}$ tels que, pour tout $n > N$, $v_{n+p} = v_n$.

Notons $y = a^N x - \lfloor a^N x \rfloor$ et montrons que $y \in \mathbb{Q}$, ce qui prouvera bien que $x = \dfrac{y + \lfloor a^N x \rfloor}{a^N} \in \mathbb{Q}$. Or $y = 0, \overline{v_{N+1}v_{N+2}\cdots v_{N+p-1}v_{N+p}v_{N+1}v_{N+2}\cdots v_{N+p-1}\cdots}$, donc $a^p y - \lfloor a^p y \rfloor = y$. Ainsi, $y = \dfrac{\lfloor a^p y \rfloor}{a^p - 1} \in \mathbb{Q}$.

• Réciproquement, on suppose que $x \in \mathbb{Q}$, donc il existe $(p, q) \in \mathbb{N} \times \mathbb{N}^*$ tel que $x = \frac{p}{q}$.

◇ Si $k \in \mathbb{N}$, effectuons la division euclidienne de $a^k p$ par q : il existe $(\beta_k, r_k) \in \mathbb{N}^2$ tel que $a^k p = \beta_k q + r_k$ et $0 \leq r_k < q$.
Ainsi, $a^k x = \beta_k + \dfrac{r_k}{q}$. Mais $\dfrac{r_k}{q} \in [0,1[$, donc $\beta_k = \lfloor a^k x \rfloor$ et
$\dfrac{r_k}{q} = a^k x - \lfloor a^k x \rfloor = 0, \overline{v_{k+1} v_{k+2} \cdots}$.
◇ $(r_k)_{k\in\mathbb{N}}$ est une suite à valeurs dans $\{0, \ldots, q-1\}$ qui est de cardinal fini, donc il existe $(k,h) \in \mathbb{N}^2$ tel que $k > h$ et $r_h = r_k$. On en déduit que
$0, \overline{v_{h+1} v_{h+2} \cdots} = \dfrac{r_h}{q} = \dfrac{r_k}{q} = 0, \overline{v_{k+1} v_{k+2} \cdots}$. D'après l'unicité du développement décimal d'un réel, pour tout $n \in \mathbb{N}^*$, $v_{h+n} = v_{k+n}$. Ainsi, pour tout $n > h$,
$v_n = v_{h+(n-h)} = v_{k+n-h} = v_{n+(k-h)}$, donc la suite (v_n) est périodique à partir du rang $h+1$ de période $k-h$. □

Remarque. Reprenons la seconde partie de la démonstration précédente.
L'application $\begin{array}{ccc} \{0,\ldots,q\} & \longrightarrow & \{0,\ldots,q-1\} \\ k & \longmapsto & r_k \end{array}$ n'est pas injective pour une raison de cardinal, donc il existe $(k,h) \in \{0,\ldots,q\}$ tel que $k > h$ et $r_k = r_h$. Ainsi, on peut imposer $k - h \leq q$, ce qui prouve que la plus petite période du développement décimal de $\frac{p}{q}$ est inférieure à q.

8 Applications

8.1 Généralités

Définition. Une fonction f de E dans F est un triplet $f = (E, F, \Gamma)$, où E et F sont des ensembles et où Γ est une relation binaire sur $E \times F$ telle que
$\forall x \in E,\ \forall y, z \in F,\ (x\ \Gamma\ y) \wedge (x\ \Gamma\ z) \Longrightarrow (y = z)$, c'est-à-dire telle que pour tout $x \in E$, il existe au plus un $y \in F$ en relation avec x.
On note alors "$y = f(x)$ " au lieu de $x\ \Gamma\ y$ ou bien $(x, y) \in \Gamma$.

- Le domaine de définition de f est $\{x \in E / \exists y \in F,\ x\ \Gamma\ y\}$. On le notera $\mathcal{D}_f$.
- Une application de E dans F est une fonction telle que $\mathcal{D}_f = E$.
- E s'appelle l'ensemble de départ de f et F l'ensemble d'arrivée.
- Γ s'appelle le graphe de f. $\Gamma = \{(x, y) \in E \times F / x\ \Gamma\ y\} = \{(x, f(x)) / x \in \mathcal{D}_f\}$.
- Lorsque $y = f(x)$, où $x \in E$ et $y \in F$,
  - on dit que y est l'image de x par f et
  - que x est un antécédent de y par f.

Remarque. En pratique, on confond souvent les deux notions d'application et de fonction, lorsque le domaine de définition est connu sans ambiguité. La suite de ce chapitre est essentiellement consacrée aux applications, ce qui évite d'étudier précisément les problèmes de domaines de définition.

Propriété. Soit f une fonction d'un ensemble E vers un ensemble F et soit g une fonction d'un ensemble E' vers un ensemble F'.
Alors $f = g$ si et seulement si $E = E'$, $F = F'$, $\mathcal{D}_f = \mathcal{D}_g$
et pour tout $x \in \mathcal{D}_f$, $f(x) = g(x)$.

Démonstration.
Notons $f = (E, F, \Gamma)$ et $g = (E', F', \Gamma')$. Supposons que $f = g$. Alors $E = E'$ et $F = F'$.
Soit $x \in \mathcal{D}_f$. Il existe $y \in F$ tel que $(x, y) \in \Gamma$. Alors $(x, y) \in \Gamma'$. Ainsi $x \in \mathcal{D}_g$ et $y = f(x) = g(x)$ ...
Réciproquement, supposons que $E = E'$, $F = F'$, $\mathcal{D}_f = \mathcal{D}_g$
et pour tout $x \in \mathcal{D}_f$, $f(x) = g(x)$.
Soit $(x, y) \in \Gamma$. Alors $x \in \mathcal{D}_f$, donc $x \in \mathcal{D}_g$ et $f(x) = g(x) = y$, donc $(x, y) \in \Gamma'$. □

Remarque. C'est pour garantir cette propriété qu'une fonction est définie comme un triplet (E, F, Γ). Ainsi, si deux fonctions f et g sont telles que $\mathcal{D}_f = \mathcal{D}_g$ et
$\forall x \in \mathcal{D}_f,\ f(x) = g(x)$, elles sont tout de même différentes dès lors qu'elles ont des ensembles de départ ou d'arrivée différents.

Définition. Soit E et I deux ensembles. La famille $(e_i)_{i \in I}$ d'éléments de E indexée par I est l'unique application de I dans E dont le graphe est $\{(i, e_i) / i \in I\}$. Il s'agit d'une autre façon de noter une application, parfois mieux adaptée.

Définition. Une *suite* est une famille d'éléments indexée par $\mathbb{N}$, ou éventuellement par $\{n \in \mathbb{N} / n \geq n_0\}$ (où $n_0 \in \mathbb{N}$).

Définition. Lorsque E ou F est vide, $E \times F = \emptyset$, donc il existe au plus une fonction de E dans F, c'est $f = (E, F, \emptyset)$. On vérifie qu'il s'agit bien d'une fonction, appelée la fonction vide, dont le domaine de définition est vide.
De même, lorsque $I = \emptyset$ avec E quelconque, il existe une unique famille vide d'éléments de E.

Exemple. La fonction $f : x \longmapsto \frac{1}{x}$ de $\mathbb{R}$ dans $\mathbb{R}$ a pour domaine de définition $\mathbb{R}^*$ et pour graphe $\{(x, \frac{1}{x})/x \in \mathbb{R}^*\}$.

Notation. L'application identité sur E est définie par : $\forall x \in E,\ Id_E(x) = x$.

Définition. Soit E un ensemble et A une partie de E. L'indicatrice de A dans E est l'unique application, notée $\mathbf{1}_A$, de E dans $\{0, 1\}$ telle que $\mathbf{1}_A(x) = 1$ si $x \in A$ et $\mathbf{1}_A(x) = 0$ si $x \in E \setminus A$.

Propriété. Soit E un ensemble et A et B deux parties de E. En définissant naturellement la somme, la différence et le produit de deux applications de E dans $\mathbb{R}$, on vérifie que : $\mathbf{1}_{E\setminus A} = \mathbf{1}_E - \mathbf{1}_A$, $\mathbf{1}_{A\cap B} = \mathbf{1}_A.\mathbf{1}_B$ et $\mathbf{1}_{A\cup B} = \mathbf{1}_A + \mathbf{1}_B - \mathbf{1}_A.\mathbf{1}_B$.

Remarque. Il est important de bien distinguer une fonction f, par exemple la fonction exponentielle $exp : x \longmapsto e^x$ de $\mathbb{R}$ dans $\mathbb{R}$, de la quantité $f(x)$ pour x donné. Ainsi $exp \in \mathcal{F}(\mathbb{R}, \mathbb{R})$ alors que pour $x \in \mathbb{R}$, $exp(x) = e^x$ est un réel.

Définition. Soit f une application d'un ensemble E vers un ensemble F. On suppose que F est muni d'une relation d'ordre $\preceq$. Soit A une partie de E.

- Soit $m \in F$. On dit que m est un majorant (resp : minorant) de f sur A si et seulement si m est un majorant (resp : minorant) de $f(A)$.
- On dit que f est majorée (resp : minorée, bornée) sur A si et seulement si $f(A)$ est une partie majorée (resp : minorée, bornée) de F.
- Lorsque $f(A)$ possède un maximum (resp : minimum), on dit que f possède un maximum (resp : un minimum) sur A et on note $\max\limits_{x\in A} f(x) = \max(f(A))$ (resp : ...).
- Lorsque $f(A)$ possède une borne supérieure (resp : inférieure), on dit que f possède un sup sur A (resp : un inf) et on note $\sup\limits_{x\in A} f(x) = \sup(f(A))$ (resp : ...).

Exemple. Déterminer le maximum de l'application $x \longmapsto x(1 - x)$ sur $[0, 1]$.
Solution : Notons f cette fonction. On pourrait la dériver et tracer son tableau de variations. De façon plus élémentaire, pour tout $x \in [0, 1]$,
$f(x) = x - x^2 = -(x - \frac{1}{2})^2 + \frac{1}{4} \leq \frac{1}{4}$, donc $\frac{1}{4}$ majore f sur $[0, 1]$.
De plus, $f(\frac{1}{2}) = \frac{1}{4}$, donc $\max\limits_{x\in[0,1]} f(x) = f(\dfrac{1}{2}) = \dfrac{1}{4}$.

Exemple. De manière élémentaire, déterminer la borne supérieure de $x \longmapsto \dfrac{x-1}{x+1}$ sur $[1, +\infty[$.
Solution : Notons f cette application. Pour tout $x \in [1, +\infty[$,

$0 \leq f(x) < \dfrac{x+1}{x+1} = 1$, donc 1 est un majorant de f sur $[1, +\infty[$.
Soit $a < 1$. Pour tout $x \in [1, +\infty[$, $x + 1 > 0$,
donc $f(x) > a \iff x - 1 > a(x+1) \iff x(1-a) > a+1$, or $1 - a > 0$,
donc $f(x) > a \iff x > \dfrac{a+1}{1-a}$. Cette inéquation possède des solutions, donc 1 est le plus petit des majorants. On a montré, sans recourir à des arguments d'analyse, que $\sup_{x \in [1,+\infty[} f(x)$ est défini et qu'il vaut 1.

Définition. Soit I un ensemble quelconque et soit $(f_i)_{i \in I}$ une famille d'éléments d'un ensemble F. On suppose que F est muni d'une relation d'ordre $\preceq$.

- Soit $m \in F$. On dit que m est un majorant (resp : minorant) de la famille $(f_i)_{i \in I}$ si et seulement si m est un majorant (resp : minorant) de $\{f_i / i \in I\}$.
- On dit que la famille (f_i) est majorée (resp : minorée, bornée) si et seulement si $\{f_i / i \in I\}$ est une partie majorée (resp : minorée, bornée) de F.
- Lorsque $\{f_i / i \in I\}$ possède un maximum (resp : minimum), on dit que la famille (f_i) possède un maximum (resp : un minimum)
  et on note $\max_{i \in I} f_i = \max(\{f_i / i \in I\})$ (resp : ...).
- Lorsque $\{f_i / i \in I\}$ possède une borne supérieure (resp : inférieure), on dit que la famille (f_i) possède un sup (resp : un inf)
  et on note $\sup_{i \in I} f_i = \sup(\{f_i / i \in I\})$ (resp : ...).

Exemple. Pour tout $n \in \mathbb{N}^*$, posons $x_n = \dfrac{n-1}{n+1}$. En adaptant l'exemple précédent, on peut montrer que $\sup_{n \in \mathbb{N}^*} x_n = 1$.

Notation. On note $\mathcal{F}(E, F)$ ou bien F^E l'ensemble des applications de E dans F. F^I est donc aussi l'ensemble des familles indexées par I d'éléments de l'ensemble F

Définition. Soient E et F deux ensembles, E' une partie de E et F' une partie de F.

- Soit f une application de E dans F.
  Si $E' \subset E$, la restriction de f à E' est l'unique application de E' dans F telle que $\forall x \in E',\ \ f|_{E'}(x) = f(x)$.
- Soit f une application de E' dans F. On appelle prolongement de f sur E toute application g de E dans F telle que $g|_{E'} = f$.
- Si F' est une partie de F telle que, pour tout $x \in E$, $f(x) \in F'$, la corestriction de f à F' est l'unique application de E dans F' telle que : pour tout $x \in E$, $f|^{F'}(x) = f(x)$.
- Si $E' \subset E$ et $F' \subset F$, lorsque pour tout $x \in E'$, $f(x) \in F'$, on désigne par $f|^{F'}_{E'}$ l'unique application de E' dans F' telle que, pour tout $x \in E'$, $f|^{F'}_{E'}(x) = f(x)$.

Définition. Soit f une application d'un ensemble E *dans lui-même*. Une partie A de E est stable par f si et seulement si $[\forall x \in A,\ \ f(x) \in A]$, c'est-à-dire si et seulement si $f|^A_A$ est définie.

Définition. Soit f une application de E dans F et g une application de F dans G. La composée de g et de f est l'unique application $g \circ f$ de E dans G définie par : $\forall x \in E,\ (g \circ f)(x) = g(f(x))$.

Remarque. Pour considérer $g \circ f$, on doit être dans la situation $E \xrightarrow{f} F \xrightarrow{g} G$: il y a donc inversion de l'ordre.

Exemple. Si $\begin{array}{rccc} f : & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & \sin x \end{array}$ et $\begin{array}{rccc} g : & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & x^3 \end{array}$, alors $(f \circ g)(x) = \sin(x^3)$ et $(g \circ f)(x) = \sin^3 x$.

Associativité de la composition : Soit f une application de E dans F, g une application de F dans G et h une application de G dans H. Alors $h \circ (g \circ f) = (h \circ g) \circ f$. On peut donc noter $h \circ g \circ f$ cette fonction.

Démonstration.
Pour tout $x \in E$, $[h \circ (g \circ f)](x) = h[(g \circ f)(x)] = h[g(f(x))]$
et $[(h \circ g) \circ f](x) = (h \circ g)(f(x)) = h(g(f(x)))$. □

8.2 Applications croissantes et décroissantes

Définition. Soit f une application d'un ensemble ordonné $(E, \leq_E)$ dans un ensemble ordonné $(F, \leq_F)$.

- f est croissante si et seulement si $[\forall x, y \in E,\ x \leq_E y \Longrightarrow f(x) \leq_F f(y)]$.
- f est strictement croissante si et seulement si $\forall x, y \in E,\ x <_E y \Longrightarrow f(x) <_F f(y)$.
- f est décroissante si et seulement si elle est croissante de $(E, \leq_E)$ dans $(F, \geq_F)$.
- f est strictement décroissante si et seulement si $\forall x, y \in E,\ x <_E y \Longrightarrow f(x) >_F f(y)$.
- f est monotone si et seulement si f est croissante ou décroissante.
- f est strictement monotone si et seulement si f est strictement croissante ou strictement décroissante.

Exemples :

- L'application $x \longmapsto x^2$ est croissante sur $\mathbb{R}_+$, décroissante sur $\mathbb{R}_-$, donc sur $\mathbb{R}$, elle n'est pas monotone.
- L'application partie entière est croissante sur $\mathbb{R}$.
  En effet, si $x, y \in \mathbb{R}$ avec $x < y$, alors $\{k \in \mathbb{Z} / k \leq x\} \subset \{k \in \mathbb{Z} / k \leq y\}$.
- L'application $\begin{array}{ccc} (\mathbb{N}^*, |) & \longrightarrow & (\mathbb{N}^*, |) \\ n & \longmapsto & n^2 \end{array}$ est strictement croissante.
- Si E est un ensemble, l'application $\begin{array}{ccc} (\mathcal{P}(E), \subset) & \longrightarrow & (\mathcal{P}(E), \subset) \\ A & \longmapsto & \overline{A} \end{array}$ est strictement décroissante.
- Notons $\mathbb{N}^{(\mathbb{P})}$ l'ensemble des familles $(v_p)_{p \in \mathbb{P}}$ d'entiers naturels telles que

$\{p \in \mathbb{N}/v_p \neq 0\}$ est de cardinal fini. Il s'agit des suites *presque nulles* indexées par $\mathbb{P}$. On munit $\mathbb{N}^{(\mathbb{P})}$ de l'ordre produit :

$$(v_p)_{p\in\mathbb{P}} \leq (w_p)_{p\in\mathbb{P}} \Longleftrightarrow [\forall p \in \mathbb{P},\ \ v_p \leq w_p].$$

Alors l'application $\begin{array}{ccc} \mathbb{N}^{(\mathbb{P})} & \longrightarrow & \mathbb{N}^* \\ (v_p)_{p\in\mathbb{P}} & \longmapsto & \prod_{p\in\mathbb{P}} p^{v_p} \end{array}$ est une bijection (d'après le théorème sur la décomposition primaire d'un entier) qui est strictement croissante si l'on munit $\mathbb{N}^*$ de la relation de divisiblité.

Remarque. On a vu qu'il existe des fonctions qui ne sont ni décroissantes, ni croissantes. Ainsi, si l'on suppose qu'une application f n'est pas croissante, on ne peut pas affirmer qu'elle est décroissante.

Propriété.
- La composée de deux applications croissantes est croissante.
- La composée de deux applications décroissantes est croissante.
- La composée d'une application croissante et d'une application décroissante est décroissante.

Propriété. Soit f et g deux fonctions de $\mathbb{R}$ dans $\mathbb{R}$.
- Si f et g sont croissantes, alors $f+g$ est croissante.
- Si f et g sont décroissantes, alors $f+g$ est décroissante.
- Si f est croissante, $-f$ est décroissante.
- Si f et g sont à valeurs positives et croissantes (resp : décroissantes), alors fg est croissante (resp : décroissante).
- Si f et g sont à valeurs strictement positives et sont strictement croissantes (resp : strictement décroissantes), alors fg est strictement croissante (resp : strictement décroissante).

Démonstration.
Démontrons seulement la dernière propriété dans le cas strictement décroissant.
Soit $x, y \in \mathbb{R}$ tels que $x < y$. On a $0 < f(y) < f(x)$ et $0 < g(y) < g(x)$, donc $(fg)(y) = f(y)g(y) < f(x)g(y) < f(x)g(x)$. Ainsi fg est strictement décroissante. □

Exemple. Pour tout $x \in [0, \frac{\pi}{2}]$, posons $f(x) = \cos(\sin x) + \sin(\cos x)$.
cos est une application décroissante de $[0, \frac{\pi}{2}]$ dans $[0, 1]$ et sin est croissante de $[0, \frac{\pi}{2}]$ dans $[0, 1]$. Ainsi, par composition, $x \longmapsto \cos(\sin x)$ et $x \longmapsto \sin(\cos x)$ sont décroissantes, ce qui montre, sans dériver, que f est décroissante.

Définition. Soit f et g deux applications d'un ensemble E dans un ensemble ordonné $(F, \leq)$. On écrit $f \leq g$ si et seulement si , pour tout $x \in E$, $f(x) \leq g(x)$.
On définit ainsi une relation d'ordre sur $\mathcal{F}(E, F)$.

Exemple. Sur $\mathbb{R}_+$, $\sin \leq Id_{\mathbb{R}_+}$.

8.3 Images directes et réciproques

Définition. Soit f une application de E dans F.

— Si A est une partie de E, l'image directe de A par f est $f(A) \stackrel{\Delta}{=} \{f(x)/x \in A\}$.
Ainsi, $\forall y \in F,\ \ y \in f(A) \iff [\exists x \in A,\ \ y = f(x)]$.
$f(A)$ est l'ensemble des images par f des éléments de A.

— Si B est une partie de F, l'image réciproque de B par f est
$f^{-1}(B) \stackrel{\Delta}{=} \{x \in E/f(x) \in B\}$. Ainsi, $\forall x \in E,\ \ x \in f^{-1}(B) \iff f(x) \in B$.
$f^{-1}(B)$ est l'ensemble des antécédents par f des éléments de B.

Remarque. La notation $f(A)$ est pratique, mais curieuse, car dès que f est une application de E dans F, cette notation fait également de f une application de $\mathcal{P}(E)$ dans $\mathcal{P}(F)$.

Exemple. $\exp(\mathbb{R}) = \mathbb{R}_+^*$, $\cos([0, \frac{\pi}{2}]) = [0, 1]$, $\sin(\mathbb{R}) = [-1, 1]$.
$(\mathbf{1}_A)^{-1}(\{1\}) = A$, $\exp^{-1}([1, +\infty[) = \mathbb{R}_+$, $\sin^{-1}(\{1, -1\}) = \{\frac{\pi}{2} + k\pi/k \in \mathbb{Z}\}$.
Si $f\ :\ x \longmapsto x^2$, $f^{-1}([1, 2[) =]-\sqrt{2}, -1] \cup [1, \sqrt{2}[$.

Propriétés des images directes : Soit f une application de E dans F, $(A_i)_{i\in I}$ une famille de parties de E, A et A' deux parties de E.

— $A \subset A' \Longrightarrow f(A) \subset f(A')$.
— $f\Big(\bigcup_{i\in I} A_i\Big) = \bigcup_{i\in I} f(A_i)$.
— $f\Big(\bigcap_{i\in I} A_i\Big) \subset \bigcap_{i\in I} f(A_i)$, mais l'inclusion réciproque est fausse en général.
— $f(E \setminus A) \supset f(E) \setminus f(A)$, mais l'inclusion réciproque est fausse en général.

Démonstration.

— Soit $y \in F$.
$$\begin{aligned} y \in f\Big(\bigcup_{i\in I} A_i\Big) &\iff \exists x \in \bigcup_{i\in I} A_i,\ \ y = f(x) \\ &\iff \exists x \in E, \exists i \in I,\ \ x \in A_i \wedge y = f(x) \\ &\iff \exists i \in I,\ \ \exists x \in A_i,\ \ y = f(x) \\ &\iff \exists i \in I,\ \ y \in f(A_i) \\ &\iff y \in \bigcup_{i\in I} f(A_i). \end{aligned}$$

— Soit $y \in f\Big(\bigcap_{i\in I} A_i\Big)$. Il existe $x \in \bigcap_{i\in I} A_i$ tel que $y = f(x)$.
Pour tout $i \in I$, $x \in A_i$, donc $y = f(x) \in f(A_i)$. Ainsi $y \in \bigcap_{i\in I} f(A_i)$.
DONC, $f\Big(\bigcap_{i\in I} A_i\Big) \subset \bigcap_{i\in I} f(A_i)$.
Lorsque f est l'application valeur absolue sur $\mathbb{R}$, en prenant $A_1 = \mathbb{R}_+$ et $A_2 = \mathbb{R}_-$, $f(A_1 \cap A_2) = f(\{0\}) = \{0\}$ et $f(A_1) \cap f(A_2) = \mathbb{R}_+$. Ainsi, l'inclusion réciproque peut être fausse.

— Soit $y \in f(E) \setminus f(A)$. Il existe $x \in E$ tel que $y = f(x)$. Si $x \in A$, alors $y = f(x) \in f(A)$ ce qui est faux. Ainsi $x \in E \setminus A$, donc $y \in f(E \setminus A)$.
— Toujours avec l'application valeur absolue, si $A = \mathbb{R}_+$, alors $f(\mathbb{R} \setminus A) = \mathbb{R}_+^*$ et $f(\mathbb{R}) \setminus f(A) = \emptyset$. Dans ce cas, $f(E \setminus A) \not\subset f(E) \setminus f(A)$.
□

Propriétés des images réciproques : Soit f une application de E dans F, $(B_i)_{i\in I}$ une famille de parties de F, B et B' deux parties de F.
— $B \subset B' \Longrightarrow f^{-1}(B) \subset f^{-1}(B')$.
— $f^{-1}\Big(\bigcup_{i\in I} B_i\Big) = \bigcup_{i\in I} f^{-1}(B_i)$.
— $f^{-1}\Big(\bigcap_{i\in I} B_i\Big) = \bigcap_{i\in I} f^{-1}(B_i)$.
— $f^{-1}(F \setminus B) = E \setminus f^{-1}(B)$.

Démonstration.
— Soit $x \in f^{-1}\Big(\bigcup_{i\in I} A_i\Big)$. Alors $f(x) \in \bigcup_{i\in I} A_i$, donc il existe $i_0 \in I$ tel que $f(x) \in A_{i_0}$. Alors $x \in f^{-1}(A_{i_0}) \subset \bigcup_{i\in I} f^{-1}(A_i)$.
Réciproquement, soit $x \in \bigcup_{i\in I} f^{-1}(A_i)$. Il existe $i_0 \in I$ tel que $x \in f^{-1}(A_{i_0})$. Alors $f(x) \in A_{i_0} \subset \bigcup_{i\in I} A_i$, donc $x \in f^{-1}\Big(\bigcup_{i\in I} A_i\Big)$.
— De même, on montre que $f^{-1}\Big(\bigcap_{i\in I} A_i\Big) = \bigcap_{i\in I} f^{-1}(A_i)$.
— Soit $x \in E$. $x \in f^{-1}(F \setminus B) \iff f(x) \in F \setminus B \iff \neg(f(x) \in B)$, donc $x \in f^{-1}(F \setminus B) \iff \neg(x \in f^{-1}(B)) \iff x \in E \setminus f^{-1}(B)$.
□

Propriété. Avec les notations de la propriété précédente,
$A \subset f^{-1}(f(A))$ et $f(f^{-1}(B)) \subset B$, mais les inclusions réciproques peuvent être fausses.

Démonstration.
◇ Soit $x \in A$. $f(x) \in f(A)$, or $x \in f^{-1}(f(A)) \iff f(x) \in f(A)$, donc $x \in f^{-1}(f(A))$.
◇ Soit $y \in f(f^{-1}(B))$. Il existe $x \in f^{-1}(B)$ tel que $y = f(x)$. Mais $x \in f^{-1}(B)$, donc $f(x) \in B$. On en déduit que $y \in B$.
◇ Reprenons pour f l'application valeur absolue de $\mathbb{R}$ dans $\mathbb{R}$.
Avec $A = \mathbb{R}_+$, $f(A) = \mathbb{R}_+$ donc $f^{-1}(f(A)) = \mathbb{R}$ (ensemble des antécédents de réels positifs). Avec $B = \mathbb{R}$, $f^{-1}(B) = \mathbb{R}$ puis $f(f^{-1}(B)) = \mathbb{R}_+$. □

8.4 Injectivité et surjectivité

Définition. Soit f une application de E dans F.
On dit que f est injective si et seulement si $\forall x, y \in E,\ [f(x) = f(y) \Longrightarrow x = y]$.
f est injective si et seulement si, pour tout couple d'éléments distincts de E, leurs images sont différentes.
f est injective si et seulement si tout élément de F possède au plus un antécédent.

Exemple. L'application qui à chaque individu associe son prénom n'est pas injective. Celle qui associe à tout individu ses empreintes digitales est injective.

Interprétation graphique.

Propriété. Soit f une application d'un ensemble ordonné $(E, \leq_E)$ dans un ensemble ordonné $(F, \leq_F)$.
Si $\leq_E$ est total et si f est strictement monotone, alors f est injective.

Définition. Soit f une application de E dans F.
On dit que f est surjective si et seulement si $\forall y \in F,\ \exists x \in E,\ y = f(x)$.
f est surjective si et seulement si $f(E) = F$.
f est surjective si et seulement si tout élément de F possède au moins un antécédent.

Exemple. L'application $(x, y) \longmapsto x$ de $\mathbb{R}^2$ dans $\mathbb{R}$ est surjective.

Définition. On dit que f est bijective si et seulement si f est injective et surjective, c'est-à-dire si et seulement si tout élément de l'ensemble d'arrivée possède un unique antécédent dans l'ensemble de départ.

Exemple. L'application $(x, y) \longmapsto (x+y, x-y)$ est une bijection de $\mathbb{R}^2$ dans lui-même.

Remarque. On évitera de confondre l'injectivité de f avec la pseudo-injectivité : f est pseudo-injective si et seulement si $\forall x, y \in E,\ [x = y \Longrightarrow f(x) = f(y)]$, ce qui est ...toujours vrai.
De même, on évitera de confondre la surjectivité de f avec la pseudo-surjectivité : f est pseudo-surjective si et seulement si $\forall x \in E,\ \exists y \in F,\ y = f(x)$, ce qui est ...toujours vrai.

Propriété. Si l'on considère une application quelconque, il existe une manière naturelle de lui associer une bijection : soit f une application de E dans F. C'est déjà une surjection si l'on remplace F par $f(E)$.
Sur E, on définit la relation binaire R par : $xRy \Longleftrightarrow f(x) = f(y)$. R est une relation d'équivalence. Alors l'application $\begin{array}{rccc} \overline{f} : & E/R & \longrightarrow & f(E) \\ & \overline{x} & \longmapsto & f(x) \end{array}$ est une bijection.

Démonstration.
Il faut d'abord montrer que $\overline{f}$ est correctement définie, c'est-à-dire que $f(x)$ est effectivement une fonction de $\overline{x}$, ou encore que si $\overline{x} = \overline{y}$, alors $f(x) = f(y)$, ce qui est évident.
On vérifie ensuite la surjectivité et l'injectivité. □

Propriété. La composée de deux injections est une injection.

La composée de deux surjections est une surjection.
La composée de deux bijections est une bijection.

Démonstration.
Soit f une application de E dans F et g une application de F dans G.
$\diamond$ Supposons que f et g sont injectives. Soit $x, y \in E$ tels que $(g \circ f)(x) = (g \circ f)(y)$. On a $g(f(x)) = g(f(y))$, or g est injective, donc $f(x) = f(y)$, puis $x = y$ car f est injective. Ceci démontre que $g \circ f$ est injective.
$\diamond$ Supposons que f et g sont surjectives. Soit $z \in G$. g étant surjective, il existe $y \in F$ tel que $z = g(y)$. f est aussi surjective, donc il existe $x \in E$ tel que $y = f(x)$. Alors $z = (g \circ f)(x)$. Ceci prouve la surjectivité de $g \circ f$. $\square$

Propriété. Soit f une application de E dans F et g une application de F dans G.
Si $g \circ f$ est injective, alors f est injective.
Si $g \circ f$ est surjective, alors g est surjectif.

Propriété. (hors programme) Soient E, F et G trois ensembles.
- Soit $f : F \longrightarrow G$ et g et h deux applications de E dans F.
  Si f est injective, alors $fg = fh \Longrightarrow g = h$: on dit que f est simplifiable (ou régulière) à gauche.
- Soit $f : E \longrightarrow F$ et g et h deux applications de F dans G.
  Si f est surjective, alors $gf = hf \Longrightarrow g = h$: on dit que f est simplifiable (ou régulière) à droite.

Démonstration.
$\diamond$ Supposons que f est injective et que $fg = fh$.
Soit $x \in E$. On a $f(g(x)) = f(h(x))$ et f est injective, donc $g(x) = h(x)$.
$\diamond$ Supposons que f est surjective et que $gf = hf$.
Soit $y \in F$. Il existe $x \in E$ tel que $y = f(x)$. Alors $g(y) = g(f(x)) = h(f(x)) = h(y)$.
$\square$

Définition et propriété :
$\diamond$ Soit f une bijection de E dans F.
Pour tout $y \in F$, notons $f^{-1}(y)$ l'unique antécédent de y par f.
Alors f^{-1} est une bijection de F dans E, appelée la bijection réciproque de f.
$\diamond$ On vérifie que $f \circ f^{-1} = Id_F$ et $f^{-1} \circ f = Id_E$.
$\diamond$ Réciproquement, s'il existe une application g de F dans E telle que $f \circ g = Id_F$ et $g \circ f = Id_E$, alors f et g sont des bijections et $g = f^{-1}$.
$\diamond$ $(f^{-1})^{-1} = f$.

Démonstration.
$\diamond$ Soit $y \in F$. Posons $x = f^{-1}(y)$. C'est l'unique antécédent de y par f, donc $f(x) = y$.
Ainsi $(f \circ f^{-1})(y) = y$, pour tout $y \in F$, donc $f \circ f^{-1} = Id_F$.
$\diamond$ Soit $x \in E$. Posons $y = f(x)$. x est un antécédent de y par f,
donc $x = f^{-1}(y) = f^{-1}(f(x))$. Ainsi, $f^{-1} \circ f = Id_E$.
$\diamond$ Id_E et Id_F étant bijectives, la propriété précédente permet d'en déduire que f^{-1} est une bijection de F dans E.

$\diamond$ Supposons qu'il existe une application g de F dans E telle que $f \circ g = Id_F$ et $g \circ f = Id_E$. La propriété précédente prouve à nouveau que f et g sont bijectives.
Enfin, $g = g \circ Id_F = g \circ (f \circ f^{-1}) = (g \circ f) \circ f^{-1} = Id_E \circ f^{-1} = f^{-1}$. $\square$

Exemple. La bijection réciproque de la bijection $(x, y) \longmapsto (x + y, x - y)$ de $\mathbb{R}^2$ dans lui-même est l'application $(a, b) \longmapsto (\frac{a+b}{2}, \frac{a-b}{2})$.

Remarque. La dernière partie de cette propriété fournit une méthode souvent efficace pour prouver la bijectivité d'une application : il suffit de trouver g telle que $f \circ g = Id_F$ et $g \circ f = Id_E$.
Par exemple, l'application $\begin{array}{ccc} (\mathcal{P}(E), \subset) & \longrightarrow & (\mathcal{P}(E), \subset) \\ A & \longmapsto & \overline{A} \end{array}$ est une bijection car, composée avec elle-même, elle donne l'identité.
Une application de f telle que $f \circ f = Id_E$ s'appelle une involution sur E.

Propriété. Soit f une bijection de E dans F. Soit B une partie de F. Alors l'image directe de B par f^{-1} coïncide avec l'image réciproque de B par f.
C'est heureux car ils sont tous les deux notés $f^{-1}(B)$.

Démonstration.
Notons A_1 l'image directe de B par f^{-1} et A_2 l'image réciproque de B par f.
Soit $x \in E$. $x \in A_1 \iff \exists y \in B,\ \ x = f^{-1}(y)$
et $x \in A_2 \iff f(x) \in B \iff \exists y \in B,\ \ f(x) = y$. $\square$

Propriété. Soit f une bijection de E dans F et g une bijection de F dans G.
Alors $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Démonstration.
On sait déjà que $g \circ f$ est bien une bijection.
De plus, $(g \circ f) \circ (f^{-1} \circ g^{-1}) = gff^{-1}g^{-1} = Id_G$ et $(f^{-1}g^{-1})(gf) = Id_E$. $\square$

Remarque. La notation f^{-1}, pour une application f, est utilisée selon deux sens *différents*, qu'il est important de bien distinguer :
- Lorsque f est une application *quelconque* de E dans F, si B est une partie de F, alors $f^{-1}(B) = \{x \in E / f(x) \in B\}$.
- Lorsque f est une *bijection* de E dans F, pour tout $y \in F$, $f^{-1}(y)$ est l'unique antécédent de y par f.

En particulier, dès que l'on utilise une expression de la forme $f^{-1}(y)$ où y est un *élément* de l'ensemble d'arrivée de f, on suppose nécessairement que f est une bijection.
Lorsque $y \in F$, il importe de bien distinguer $f^{-1}(y)$ qui représente, pour une bijection f, l'unique antécédent de y, et $f^{-1}(\{y\})$ qui représente, pour une application f quelconque, l'ensemble des antécédents de y. Cet ensemble peut être vide lorsque f n'est pas surjective, il peut contenir plus de deux éléments lorsque f n'est pas injective.

> **Exercice.** Soit f une application de E dans F.
> Lorsque f est surjective, montrer que, pour toute partie B de F, $f(f^{-1}(B)) = B$.
> Lorsque f est injective, montrer que, pour toute partie A de E, $f^{-1}(f(A)) = A$.

Propriété. Soit f une bijection de E dans F.

Pour toute partie B de F, $f(f^{-1}(B)) = B$.
Pour toute partie A de E, $f^{-1}(f(A)) = A$.

Propriété. (hors programme)
Soit f une application de E dans F. On suppose que $E \neq \emptyset$.
Alors f est injective si et seulement si il existe $g : F \longrightarrow E$ telle que $g \circ f = Id_E$,
et f est surjective si et seulement si il existe $g : F \longrightarrow E$ telle que $f \circ g = Id_F$.

Démonstration.
$\diamond$ Supposons qu'il existe $g : F \longrightarrow E$ telle que $g \circ f = Id_E$. Alors $g \circ f$ est injective, donc on sait que f est injective.
Réciproquement, supposons que f est injective. $E \neq \emptyset$, donc on peut choisir $e \in E$.
$f|^{f(E)} = h$ est une bijection de E dans $f(E)$, donc on peut poser, pour tout $y \in F$, $g(y) = h^{-1}(y)$ lorsque $y \in f(E)$ et $g(y) = e$ lorsque $y \in F \setminus f(E)$.
Soit $x \in E$. Alors $f(x) \in f(E)$, donc $g \circ f(x) = g(f(x)) = h^{-1}(f(x)) = x$. Ainsi, $g \circ f = Id_E$.
$\diamond$ Supposons qu'il existe $g : F \longrightarrow E$ telle que $f \circ g = Id_F$. Alors $f \circ g$ est surjective, donc on sait que f est surjective.
Réciproquement, supposons que f est surjective. Pour tout $y \in F$, choisissons (on utilise l'axiome du choix) un antécédent de y par f, que l'on notera $g(y)$: son existence est assurée car f est surjective. Par construction, pour tout $y \in F$, $f(g(y)) = y$, donc $f \circ g = Id_F$. $\square$

8.5 Lois internes

Définition. Une loi interne sur E est une application f de $E \times E$ dans E. Dans ce contexte la notation *préfixe* "$f(x, y)$" est remplacée par la notation *infixe* "$x\ f\ y$", où $x, y \in E$.
On dit que (E, f) est un magma (hors programme).

Exemple. L'addition et la multiplication sont des lois internes sur $\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{Q}$.

Définition. Soit Δ une loi interne sur E. Δ est associative si et seulement si pour tout $x, y, z \in E$, $(x\ \Delta\ y)\ \Delta\ z = x\ \Delta\ (y\ \Delta\ z)$.
Dans ce cas, pour tout $x, y, z \in E$, cette quantité est notée sans parenthèses : $x\ \Delta\ y\ \Delta z$.
On dit alors que (E, Δ) est un magma associatif.

Notation. Soit Δ une loi interne associative sur un ensemble E.
Soit $n \in \mathbb{N}^*$ et $x_1, \ldots, x_n \in E$. Pour tout $p \in \{1, \ldots, n\}$, on définit par récurrence la quantité $x_1\ \Delta\ x_2\ \Delta\ \cdots\ \Delta\ x_p = y_p$ en convenant que
$y_1 = x_1$ et pour tout $p \in \{1, \ldots, n-1\}$, $y_{p+1} = y_p\ \Delta\ x_{p+1}$.

Propriété. Avec ces notations, l'hypothèse d'associativité garantit que la quantité $x_1\ \Delta\ x_2\ \Delta\ \cdots\ \Delta\ x_p$ ne dépend pas de la façon dont elle est parenthésée.

Démonstration.
Soit $n \in \mathbb{N}^*$. Soit E un ensemble muni d'une loi Δ associative. On note $R(n)$ l'assertion suivante : pour tout $x_1, \dots, x_n \in E$, toute expression correctement parenthésée de $x_1 \Delta x_2 \Delta \cdots \Delta x_n$ donne le même résultat.
$R(n)$ est évidente pour $n = 1$ et $n = 2$, elle résulte de l'associativité pour $n = 3$.
Soit $n \geq 3$, supposons $R(k)$ pour tout $k \in \{1, \dots, n\}$.
Soit $x_1, \dots, x_{n+1} \in E$. Soit $p \in \{1, \dots, n\}$. Posons $y = x_1 \Delta \cdots \Delta x_p$ (qui ne dépend pas du choix du parenthésage d'après l'hypothèse de récurrence) et $z = x_{p+1} \Delta \cdots \Delta x_{n+1}$.
Il suffit de montrer que $y \Delta z = x_1 \Delta \cdots \Delta x_{n+1}$, car toute expression correctement parenthésée de $x_1 \Delta x_2 \Delta \cdots \Delta x_{n+1}$ peut s'écrire sous la forme $y \Delta z$ pour un certain p.
Premier cas : Supposons que $p = n$. Alors il n'y a rien à démontrer, car par définition de $x_1 \Delta x_2 \Delta \cdots \Delta x_{n+1}$, on a $y \Delta z = x_1 \Delta x_2 \Delta \cdots \Delta x_{n+1}$.
Second cas : On suppose que $p \leq n - 1$. Par définition de z,
$y \Delta z = y \Delta ((x_{p+1} \Delta \cdots \Delta x_n) \Delta x_{n+1})$, donc par associativité,
$y \Delta z = (y \Delta (x_{p+1} \Delta \cdots \Delta x_n)) \Delta x_{n+1}$. D'après l'hypothèse de récurrence,
$y \Delta z = (x_1 \Delta x_2 \Delta \cdots \Delta x_n) \Delta x_{n+1} = x_1 \Delta x_2 \Delta \cdots \Delta x_{n+1}$, ce qui prouve $R(n+1)$. □

Définition. Soit Δ une loi interne sur E et soit $e \in E$. On dit que e est un élément neutre de (E, Δ) si et seulement si, pour tout $x \in E$, $x \Delta e = e \Delta x = x$.
Si E possède un élément neutre, il est unique. On peut donc parler de *l'*élément neutre.
On dit alors que (E, Δ) est un magma unitaire, ou bien unifère.

Définition. On dit que (E, Δ) est un monoïde si et seulement si E est un ensemble et Δ est une loi interne associative sur E qui possède un élément neutre.
On dit que le monoïde est commutatif, ou abélien, si et seulement si,
pour tout $x, y \in E$, $x \Delta y = y \Delta x$.

Remarque. Un monoïde est donc un magma unitaire et associatif.

Remarque. l'usage est de confondre le monoïde (E, Δ) et l'ensemble sous-jacent E.

Exemple. Si A est un ensemble, alors $(\mathcal{P}(A), \cup)$ est un monoïde commutatif dont l'élément neutre est $\emptyset$. Qu'en est-il de $(\mathcal{P}(A), \cap)$?

Exemple. Si A est un ensemble, dont les éléments sont appelés des lettres, on note A^* l'ensemble des mots écrits avec l'alphabet A. Plus formellement, $A^* = \bigsqcup_{n \in \mathbb{N}} A^n$, en convenant que A^0 désigne le singleton contenant le mot vide.
La concaténation entre mots structure A^* comme un monoïde.

Notation. Soit (E, Δ) un monoïde dont l'élément neutre est noté e.
Soit $n \in \mathbb{N}^*$ et $x_1, \dots, x_n \in E$. Pour tout $p \in \{1, \dots, n\}$, on a défini par récurrence la quantité $x_1 \Delta x_2 \Delta \cdots \Delta x_p = y_p$. On convient de plus que $y_0 = e$, c'est-à-dire que

$$x_1 \Delta x_2 \Delta \cdots \Delta x_p = e, \quad \text{lorsque } p = 0.$$

Définition. Soit G un ensemble muni d'une loi interne notée "$\times$". On suppose que G est un monoïde dont l'élément neutre sera notée 1_G.
On dit que $(G, \times)$ est un groupe si et seulement si tout élément de G possède un symétrique pour la loi interne, c'est-à-dire si et seulement si, pour tout $x \in G$, il existe $y \in G$ tel que $x \times y = y \times x = 1_G$.
Dans ce cas, pour tout $x \in G$, le symétrique de x est unique, il est noté x^{-1}.

Démonstration.
Soit $x \in G$. Soit y et z deux symétriques de x. Alors
$y = y \times e = y \times (x \times z) = (y \times x) \times z = e \times z = z$. □

Remarque. On aurait très bien pu continuer à noter Δ la loi de G et e son élément neutre, avec Δ et e substituable par n'importe quel autre symbole, mais l'usage restreint la notation de la loi interne d'un groupe à seulement deux notations : la notation multiplicative, que l'on vient de voir, et la notation additive, réservée aux groupes commutatifs. Ainsi, $(G, +)$ est la notation générique d'un groupe commutatif. Son élément neutre est alors noté 0 ou 0_G et le symétrique de x est alors noté $-x$.

Remarque. On dit qu'un groupe est abélien si et seulement si il est commutatif.

Exemple. $(\mathbb{Z}, +)$ et $(\mathbb{Q}, +)$ sont des groupes commutatifs.
$(\mathbb{Q}^*, \times)$ est un groupe commutatif mais $(\mathbb{Z}^*, \times)$ n'est pas un groupe.

Définition. On appelle ***anneau*** tout triplet $(A, +, .)$, où A est un ensemble et où "+" et "." sont deux lois internes sur A telles que
- $(A, +)$ est un groupe abélien (l'élément neutre étant noté 0 ou 0_A),
- "." est une loi associative, admettant un élément neutre noté 1 ou 1_A,
- la loi "." est ***distributive*** par rapport à la loi "+", c'est-à-dire que
$\forall (x, y, z) \in A^3 \;\; x.(y + z) = (x.y) + (x.z)$ et $(x + y).z = (x.z) + (y.z)$.

9 Dénombrement

Remarque. Ce chapitre utilise seulement la théorie des ensembles et les propriétés de $\mathbb{N}$.
En effet, les autres notions utilisées sont uniquement bâties sur la théorie des ensembles et des entiers : injections, surjections et bijections, relations d'équivalence, monoïdes etc.

9.1 Cardinal d'un ensemble

Lemme : Soit $n, m \in \mathbb{N}$. S'il existe une injection de $\mathbb{N}_n$ dans $\mathbb{N}_m$, alors $n \leq m$.

Démonstration.
Pour tout $n \in \mathbb{N}$, notons $R(n)$ l'assertion : pour tout $m \in \mathbb{N}$, s'il existe une injection de $\mathbb{N}_n$ dans $\mathbb{N}_m$, alors $n \leq m$.
Si $n = 0$, pour tout $m \in \mathbb{N}$, on a bien $m \geq 0 = n$, donc $R(0)$ est vraie.
Pour $n \geq 0$, supposons $R(n)$. Soit $m \in \mathbb{N}$.
Supposons qu'il existe une injection g de $\mathbb{N}_{n+1}$ dans $\mathbb{N}_m$.
Posons $k = g(n+1)$. $k \in \mathbb{N}_m$, donc $m \geq 1$.
- Si $k < m$, on note $g' = \tau \circ g$, où τ est l'injection de $\mathbb{N}_m$ qui échange k et m.
- Si $k = m$, on pose $g' = g$.

Dans tous les cas, $g'(n+1) = m$.
De plus g' est une injection en tant que composée d'injections.
Notons h l'application de $\mathbb{N}_n$ dans $\mathbb{N}_{m-1}$ définie par restriction de g' :
$\forall a \in \mathbb{N}_n,\ \ h(a) = g'(a)$.
h est bien à valeurs dans $\mathbb{N}_{m-1}$ car pour tout $a \in \mathbb{N}_n$, $h(a) = g'(a) \in \mathbb{N}_m$ et d'après l'injectivité de g', $g'(a) \neq g'(n+1) = m$.
h est clairement injective, par restriction d'une application injective.
Alors, d'après $R(n)$, $n \leq m-1$, donc $n+1 \leq m$, ce qui prouve $R(n+1)$. □

Définition. Soit E un ensemble. S'il existe $n \in \mathbb{N}$ tel que $\mathbb{N}_n$ est en bijection avec E, alors n est unique. On dit que n est le cardinal de E. Il est noté $\text{card}(E)$ ou bien $\#E$, ou encore $|E|$.
En cas d'inexistence d'un tel entier n, on dit que E est infini.

Démonstration.
Supposons qu'il existe $n, m \in \mathbb{N}$, une bijection f de E dans $\mathbb{N}_n$ et une bijection g de E dans $\mathbb{N}_m$. Montrons que $n = m$.
L'application $f \circ g^{-1}$ est une bijection, donc une injection de $\mathbb{N}_m$ dans $\mathbb{N}_n$, donc d'après le lemme $m \leq n$. Mais $[f \circ g^{-1}]^{-1}$ est une injection de $\mathbb{N}_n$ dans $\mathbb{N}_m$, donc $n \leq m$, puis $n = m$. □

Exemple. $\emptyset = \mathbb{N}_0$ est de cardinal nul.
Pour tout $n \in \mathbb{N}$, $\mathbb{N}_n$ est de cardinal n.

Exemple. Pour tout $n, m \in \mathbb{Z}$, notons $[\![n, m]\!] = \{k \in \mathbb{N} / n \leq k \leq m\}$.

Lorsque $m < n$, $[\![n, m]\!] = \emptyset$. Supposons maintenant que $m \geq n$.
Alors l'application $\begin{array}{rccc} f : & [\![n, m]\!] & \longrightarrow & \mathbb{N}_{m-n+1} \\ & k & \longmapsto & k - n + 1 \end{array}$ est une bijection, donc

$$\mathrm{Card}([\![n, m]\!]) = m - n + 1.$$

Remarque. Lorsque A est de cardinal n, si f est une bijection de $\mathbb{N}_n$ dans A, en posant $a_i = f(i)$, on a $A = \{a_1, \ldots, a_n\}$. Ainsi une bijection de $\mathbb{N}_n$ dans A donne une manière de numéroter les éléments de A.
Mais réciproquement, lorsqu'on écrit $B = \{b_1, \ldots, b_n\}$, on n'affirme pas que les b_i sont deux à deux distincts.

Propriété. Soit A un ensemble de cardinal $n \in \mathbb{N}$ et soit B un ensemble quelconque. B est fini de cardinal n si et seulement si il existe une bijection de A sur B.

Lemme : Soit $n \in \mathbb{N}$. Soit K une partie de $\mathbb{N}_n$. Alors K est un ensemble fini et $|K| \leq n$, avec égalité si et seulement si $K = \mathbb{N}_n$.

Démonstration.
Notons $R(n)$ cette propriété.
Supposons que $n = 0$. Soit K une partie de $\mathbb{N}_0 = \emptyset$. Alors $K = \emptyset = \mathbb{N}_0$, donc $|K| = 0$. Ceci prouve $R(0)$.
Pour $n \geq 0$, supposons $R(n)$. Soit K une partie de $\mathbb{N}_{n+1}$.
Premier cas : Supposons que $n + 1 \notin K$. Alors d'après $R(n)$, K est un ensemble fini et $|K| \leq n < n + 1$. De plus $K \neq \mathbb{N}_{n+1}$.
Second cas : Supposons que $n + 1 \in K$. Posons $H = K \setminus \{n + 1\}$. H est une partie de $\mathbb{N}_n$, donc d'après $R(n)$, H est un ensemble fini et $|H| \leq n$. Posons $h = |H|$.
Par définition du cardinal, il existe une bijection f de H dans $\mathbb{N}_h$.
Posons $f(n+1) = h+1$. Alors f est prolongée en une application de K dans $\mathbb{N}_{h+1}$, pour laquelle tout élément de $\mathbb{N}_{h+1}$ possède un unique antécédent. C'est donc une bijection de K dans $\mathbb{N}_{h+1}$, ce qui prouve que K est un ensemble fini avec $|K| = h + 1 \leq n + 1$.
De plus, si $|K| = n + 1$, alors $h = n$, donc d'après $R(n)$, $H = \mathbb{N}_n$, puis $K = \mathbb{N}_{n+1}$.
Réciproquement, si $K = \mathbb{N}_{n+1}$, on a bien sûr $|K| = n + 1$, donc on a prouvé $R(n + 1)$.
□

Propriété. Soit A un ensemble fini de cardinal $n \in \mathbb{N}$. Soit B une partie de A.
Alors B est un ensemble fini et $|B| \leq |A|$, avec égalité si et seulement si $B = A$.

Démonstration.
Il existe une bijection f de A dans $\mathbb{N}_n$.
◇ $f|_B$ réalise une bijection de B dans $f(B)$. $f(B)$ est une partie de $\mathbb{N}_n$ donc d'après le lemme précédent, $f(B)$ est un ensemble fini de $\mathbb{N}_n$ et $|f(B)| \leq n$. On en déduit que B est fini et que $|B| = |f(B)| \leq n = |A|$.
◇ Supposons que $|B| = |A|$. Alors $|f(B)| = n$, donc d'après le lemme, $f(B) = \mathbb{N}_n$, puis $B = f^{-1}(f(B)) = f^{-1}(\mathbb{N}_n) = A$. □

Remarque. Ainsi, pour montrer l'égalité entre deux ensembles finis, on peut se contenter de montrer une inclusion et l'égalité des cardinaux.

Remarque. Lorsque E est un ensemble fini, aucune partie stricte de E n'est donc en bijection avec E. On peut montrer la réciproque (en TD) : si E est un ensemble infini, alors E est en bijection avec l'une de ses parties strictes. On obtient ainsi une propriété caractéristique d'un ensemble infini.
On peut même montrer que E est infini si et seulement si pour tout $x \in E$, E et $E \setminus \{x\}$ sont en bijection : le fait d'ôter un élément d'un ensemble infini n'en modifie pas le cardinal (en convenant que deux ensembles sont de même cardinal si et seulement si ils sont en bijection). Cette propriété des ensembles infinis est au coeur des mathématiques. Elle permet de remplacer l'affirmation un peu vague "si l'on enlève un élément parmi vraiment beaucoup d'éléments, il en reste à peu près toujours autant" par une propriété d'invariance fondamentale : si on enlève un élément d'un ensemble infini, il en reste toujours exactement autant.
L'existence de l'infini n'est pas démontrée en mathématiques, elle est admise dans les axiomes (axiome de l'infini ou axiomes de Peano). C'est une condition préalable pour faire des mathématiques.

Propriété. Soit A une partie de $\mathbb{N}$. A est finie si et seulement si elle est majorée.
En particulier, $\mathbb{N}$ est infini.

Démonstration.
$\diamond$ Supposons que A est majorée. Il existe $n \in \mathbb{N}$ tel que, pour tout $a \in A$, $a \leq n$. Ainsi $A \subset [\![0, n]\!]$, donc A est finie.
$\diamond$ Notons $R(n)$ l'assertion : si A est de cardinal n, alors A est majorée.
Si A est de cardinal 0, A est vide donc est majorée : $R(0)$ est vraie.
Pour $n \geq 0$, supposons $R(n)$. Soit A une partie de $\mathbb{N}$ de cardinal $n+1$. Il existe une bijection f de $\mathbb{N}_{n+1}$ dans A. Posons $a = f(n+1)$. $f|_{\mathbb{N}_n}$ est une bijection de $\mathbb{N}_n$ dans $A \setminus \{a\}$, donc $A \setminus \{a\}$ est de cardinal n. D'après $R(n)$, il existe $m \in \mathbb{N}$ tel que, pour tout $b \in A \setminus \{a\}$, $b \leq m$.
Si $a \leq m$, alors m majore A.
Si $a > m$, alors a majore A. Ceci démontre $R(n+1)$.
$\diamond$ Si $m \in \mathbb{N}$ était un majorant de $\mathbb{N}$, alors $m+1 \leq m$, ce qui est faux.
$\mathbb{N}$ n'est pas majoré, donc il est infini. $\square$

Exemple. Soit $(x_n)_{n\in\mathbb{N}}$ une suite de réels et $l \in \mathbb{R}$. Alors x_n ne tend pas vers l si et seulement si il existe $\varepsilon > 0$ tel que $\{n \in \mathbb{N} / |x_n - l| > \varepsilon\}$ est infini.

9.2 Cardinaux d'ensembles usuels

Propriété. Pour tout $n \in \mathbb{N}^*$, une réunion *disjointe* de n ensembles finis est finie et son cardinal est égal à la somme des cardinaux de ces ensembles.

Démonstration.
Il suffit d'établir la propriété pour $n = 2$, car une récurrence simple permet alors de conclure.
Soit A et B deux ensembles finis disjoints de cardinaux respectifs n et m.

Il existe des bijections f de A sur $\mathbb{N}_n$ et g de B sur $\mathbb{N}_m$.
Pour tout $x \in A \sqcup B$, posons $h(x) = f(x)$ si $x \in A$ et $h(x) = g(x) + n$ si $x \in B$.
h est ainsi une application de $A \sqcup B$ dans $\mathbb{N}_{n+m}$. On vérifie que h est surjective et injective. □

Exemple. En admettant qu'une femme a au plus 400 000 cheveux et qu'il y a au moins un million de parisiennes, montrer qu'au moins 3 parisiennes ont le même nombre de cheveux.
Solution : Notons f l'application qui à une parisienne associe son nombre de cheveux. En posant $N = 400000$, elle permet de partitionner l'ensemble des parisiennes sous la forme $P = \bigsqcup_{i=0}^{N} P_i$ où P_i est l'ensemble des parisiennes possédant exactement i cheveux.
On raisonne alors par l'absurde : si pour tout $i \in \{0, \dots, N\}$, $|P_i| \leq 2$,
alors $|P| = \sum_{i=0}^{N} |P_i| \leq 2N < 10^6$, ce qui est faux.
Principe du "ou exclusif" : Pour dénombrer un ensemble, ce principe consiste à découper celui-ci en plusieurs sous-ensembles disjoints qui sont plus faciles à dénombrer. Le cardinal de l'ensemble global est alors la somme des cardinaux des sous-ensembles.

> **Exercice.** Une urne contient 5 billes blanches et 10 billes noires. On tire *avec remise* 3 billes. Quelle est la probabilité que les 2 premières soient d'une même couleur, et que la dernière soit de l'autre couleur ?
> ***Solution :*** Les probabilités feront l'objet d'un cours ultérieur. On admet que la probabilité cherchée est $P = \dfrac{|A|}{|E|}$, où E est l'ensemble de tous les tirages possibles de 3 billes et où A est la partie de E constituée des tirages pour lesquels les 2 premières billes sont d'une même couleur alors que la dernière est de l'autre couleur.
> Numérotons les billes, $b_1, \dots, b_5$ pour les 5 billes blanches et $n_1, \dots, n_{10}$ pour les 10 billes noires. Posons $B = \{b_1, \dots, b_5\} \cup \{n_1, \dots, n_{10}\}$.
> Comme l'ordre des 3 billes importe, un tirage de trois billes sera formellement un triplet d'éléments de B, donc $E = B^3$.
> Pour construire un élément de E, on choisit d'abord le premier élément, soit 15 choix, puis le second, soit encore 15 choix, puis le dernier. Ainsi $|E| = 15^3$. On donne plus loin une démonstration plus formelle pour dénombrer plus généralement un produit cartésien.
> Pour dénombrer A, on applique le principe du "ou exclusif", car $A = A_1 \sqcup A_2$, où A_1 est l'ensemble des tirages pour lesquels les deux premières billes sont blanches et la dernière noire, et où A_2 est l'ensemble des tirages pour lesquels les deux premières billes sont noires et la dernière blanche.
> En raisonnant comme pour le dénombrement de E, on obtient $|A_1| = 5.5.10$ et $|A_2| = 10.10.5$. Ainsi, $P = \dfrac{250 + 500}{15^3} = 0,22 \pm 10^{-2}$.

Propriété. Soit E un ensemble fini et A une partie de E. Alors $|E \setminus A| = |E| - |A|$.

Démonstration.
$E = A \sqcup (E \setminus A)$. □

Principe du passage au contraire : Pour dénombrer une partie d'un ensemble, il est parfois plus simple de dénombrer son complémentaire.

Exemple. Quel est le nombre de surjections de $\mathbb{N}_n$ dans $\mathbb{N}_2$?
Lorsque $n < 2$, ce nombre est nul. Supposons que $n \geq 2$.
Appliquons le principe des contraires en dénombrant la partie A de $\mathcal{F}(\mathbb{N}_n, \mathbb{N}_2)$ constituée des fonctions qui ne sont pas surjectives : Si $f \in A$, l'une des deux valeurs de $\mathbb{N}_2$ n'est pas atteinte, donc f est constante. Ainsi $|A| = 2$.
Pour construire une fonction quelconque de $\mathbb{N}_n$ dans $\mathbb{N}_2$, on choisit pour chaque élément de $\mathbb{N}_n$ son image dans $\mathbb{N}_2$, soit 2 choix à chacune de ces n étapes.
Ainsi, $|\mathcal{F}(\mathbb{N}_n, \mathbb{N}_2)| = 2^n$. On donne plus loin une preuve plus formelle pour dénombrer plus généralement $\mathcal{F}(E, F)$.
En conclusion, le nombre de surjections demandé est $2^n - 2$.

Propriété. Soit E un ensemble fini et R une relation d'équivalence sur E.
Alors E/R est aussi de cardinal fini.

Démonstration.
On le démontre par récurrence forte sur le cardinal de E ; pour $n \in \mathbb{N}$, on note $R(n)$ l'assertion suivante : pour tout ensemble E de cardinal n, pour toute relation d'équivalence R sur E, E/R est fini.
$R(0)$ est vraie. Soit $n \in \mathbb{N}$. On suppose $R(k)$ pour tout $k \in \{0, \dots, n\}$.
Soit E un ensemble de cardinal $n+1$ et R une relation d'équivalence sur E.
Il existe $a \in E$. Notons $cl_R(a)$ sa classe d'équivalence pour R.
Sur $E' = E \setminus cl_R(a)$, on définit la relation binaire R' par : $xR'y \iff xRy$.
R' est une relation d'équivalence sur E'. $|E'| = |E| - |cl_R(a)|$, or $|cl_R(a)| \geq 1$, donc $|E'| \leq n$. On peut donc appliquer l'hypothèse de récurrence. Ainsi E'/R' est fini. On vérifie que $E/R = E'/R' \sqcup \{cl_R(a)\}$, donc E/R est fini. On a prouvé $R(n+1)$. □

Formule : Si A et B sont deux ensembles finis, alors $A \cup B$ est fini et

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Démonstration.
$A \cup B$ est la réunion disjointe de $A \setminus (A \cap B)$, $B \setminus (A \cap B)$ et $A \cap B$, donc $A \cup B$ est fini et

$$\begin{aligned} |A \cup B| &= |A \setminus (A \cap B)| + |B \setminus (A \cap B)| + |A \cap B| \\ &= (|A| - |A \cap B|) + (|B| - |A \cap B|) + |A \cap B| \\ &= |A| + |B| - |A \cap B|. \end{aligned}$$

□

Remarque. La formule du crible, hors programme, généralise la formule précédente au cas d'une réunion de n ensembles finis $E_1, \dots, E_n$:

$$\#\Big(\bigcup_{i=1}^{n} E_i\Big) = \sum_{i=1}^{n} \#E_i - \sum_{1\le i<j\le n} \#(E_i \cap E_j) + \cdots + (-1)^{k+1} \sum_{1\le i_1<i_2<\cdots<i_k\le n} \#(\bigcap_{j=1}^{k} E_{i_j}) + \cdots + (-1)^{n+1} \#(\bigcap_{i=1}^{n} E_i).$$

Elle se démontre par récurrence sur n.

Propriété. Pour tout $n \in \mathbb{N}^*$, un produit cartésien de n ensembles finis est fini et son cardinal est égal au produit des cardinaux de ces ensembles.

Démonstration.
Il suffit d'établir la propriété pour $n = 2$, puis on conclut par récurrence.
Soit A et B deux ensembles finis de cardinaux respectifs n et m.
Il existe une bijection f de $\mathbb{N}_m$ dans B. Ainsi $A \times B = \bigsqcup_{i=1}^{m} [A \times \{f(i)\}]$.
Soit $i \in \mathbb{N}_m$. Pour tout $a \in A$, notons $g(a) = (a, f(i))$. g est une bijection de A dans $A \times \{f(i)\}$, donc $A \times \{f(i)\}$ est un ensemble fini dont le cardinal vaut $|A|$.
On en déduit que $A \times B$ est fini et que $|A \times B| = \sum_{i=1}^{m} |A| = m|A|$ par définition de la multiplication (ou par récurrence sur m). □

Principe du "et" : Si le dénombrement d'un ensemble se décompose en une succession de p étapes offrant respectivement $n_1, n_2, \ldots, n_p$ possibilités, où chacun des nombres n_i ne dépend que de l'étape i, le nombre total d'issues est égal à $n_1 \times n_2 \times \cdots, \times n_p$ parce que chaque choix d'une étape doit être associé à chaque choix de tout autre étape.

Exemple. Un facteur sanguin est constitué d'un groupe sanguin dans $\{A, B, AB, O\}$ et d'un rhésus dans $\{+; -\}$. Pour constituer un facteur sanguin, il faut un groupe sanguin, ce qui laisse 4 choix, et un rhésus, ce qui laisse 2 choix. Il y a donc $4 \times 2 = 8$ facteurs sanguins distincts.

Formule : Si E et F sont des ensembles finis, alors $\mathcal{F}(E, F)$ est fini et

$$|\mathcal{F}(E, F)| = |F|^{|E|}.$$

Remarque. Cela explique la notation classique $\mathcal{F}(E, F) = F^E$.

Démonstration.
Notons n le cardinal de E. Il existe une bijection de f $\mathbb{N}_n$ dans E. Notons, pour tout $i \in \mathbb{N}_n$, $e_i = f(i)$.
Pour tout $h \in \mathcal{F}(E, F)$, notons $\varphi(h) = (h(e_1), \ldots, h(e_n))$. On définit ainsi une application φ de $\mathcal{F}(E, F)$ dans F^n.
On vérifie que φ est bijective, ce qui permet de conclure. □

Propriété. Si E est de cardinal n, alors $\mathcal{P}(E)$ est de cardinal 2^n.

Démonstration.
Notons $x_1, \dots, x_n$ les éléments deux à deux distincts de E.
Pour construire une partie quelconque F de E, on décide de prendre ou de ne pas prendre x_1 dans F (2 choix), puis on décide de prendre ou de ne pas prendre x_2 dans F (2 choix), et on procède ainsi jusqu'à x_n. Il y a donc 2^n façons de construire ainsi des parties de E. Elles sont toutes distinctes et toute partie de E est ainsi obtenue exactement une fois, donc le cardinal de $\mathcal{P}(E)$ vaut 2^n.
On peut rendre cette preuve plus formelle, en traduisant le procédé de construction mis en évidence sous la forme d'une bijection d'un ensemble d'"ingrédients" dont le cardinal est connu vers $\mathcal{P}(E)$. Ici, il est plus simple d'écrire la bijection réciproque. C'est l'application φ qui à une partie A de E associe son indicatrice.
Notons donc, pour tout $A \in \mathcal{P}(E)$, $\varphi(A)$ l'application de E dans $\{0,1\}$ définie par :
si $x \in A$, $\varphi(A)(x) = 1$ et si $x \in E \setminus A$, $\varphi(A)(x) = 0$.
Montrons que φ est une bijection de $\mathcal{P}(E)$ dans $\mathcal{F}(E, \{0,1\})$.
$\diamond$ Soit $A, B \in \mathcal{P}(E)$ tels que $\varphi(A) = \varphi(B)$.
Si $x \in A$, $\varphi(A)(x) = 1$, donc $\varphi(B)(x) = 1$, donc $x \in B$. On établit de même la réciproque, donc $A = B$. On a prouvé que φ est injective.
$\diamond$ Soit $f \in \mathcal{F}(E, \{0,1\})$. Posons $A = \{x \in E / f(x) = 1\}$. Alors $\varphi(A) = f$, donc φ est surjective.
φ étant une bijection, on en déduit que $|\mathcal{P}(E)| = |\mathcal{F}(E, \{0,1\})| = 2^n$. □

Remarque. Plus généralement, pour dénombrer un ensemble fini F, on peut rechercher un procédé de construction des éléments de F, qui fournit tous les éléments de F une seule fois. Il n'est pas toujours nécessaire de traduire ce procédé de construction sous la forme d'une bijection.

9.3 Sommes et produits finis

Notation. Lorsque $(G,+)$ est un monoïde commutatif, on a déjà défini la notation $\sum_{i=1}^{n} x_i = x_1 + \cdots + x_n$ pour tout $n \in \mathbb{N}$ et $x_1, \ldots, x_n \in G$.
En notation multiplicative, dans un monoïde commutatif $(G,\times)$, ceci devient :

$$x_1 \times \cdots \times x_n = \prod_{i=1}^{n} x_i.$$

On fixe dans tout ce paragraphe un monoïde *commutatif* $(G,+)$.
Toutes les propriétés qui suivent sont bien sûr valables indépendamment de la façon dont la loi interne est notée. Il sera notamment utile de les traduire en notation multiplicative.

Remarque. Dans l'écriture $S = \sum_{i=1}^{n} x_i$, la variable i est muette, car elle peut être remplacée par toute autre variable : $S = \sum_{j=1}^{n} x_j$.
Au contraire, n n'est pas une variable muette (c'est une variable libre) : si $m \neq n$, a priori $S \neq \sum_{i=1}^{m} x_i$.

En particulier, l'écriture $\sum_{n=1}^{n} x_n$ n'a aucun sens car la variable n devrait être à la fois muette et libre.

Exemples à connaître : (on peut les démontrer par récurrence)

- Pour tout $a \in G$ et $n \in \mathbb{N}$, $\sum_{k=1}^{n} a = na$.
- Pour tout $n \in \mathbb{N}$, $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.
- Pour tout $n \in \mathbb{N}$, $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.
- Pour tout $n \in \mathbb{N}$, $\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$.

Notation. Pour tout $n \in \mathbb{N}$, on note $\mathcal{S}_n$ l'ensemble des bijections de $\mathbb{N}_n$ dans lui-même.

Commutativité généralisée : Soit $n \in \mathbb{N}$ et $x_1, \ldots, x_n \in G$. Alors

$$\forall \sigma \in \mathcal{S}_n, \quad \sum_{i=1}^{n} x_i = \sum_{j=1}^{n} x_{\sigma(j)}.$$

Démonstration.
Admis pour le moment car la démonstration utilise des propriétés du groupe symétrique de degré n, égal à $(\mathcal{S}_n, \circ)$. □

Remarque. Nous verrons plus tard que cette propriété *n'est plus valable* dans le cadre des sommes infinies de séries semi-convergentes.

Définition. Soit A un ensemble fini et $(x_a)_{a\in A}$ une famille de G indexée par A.
Notons $n = |A|$. Il existe une bijection f de $\mathbb{N}_n$ dans A. On pose $\sum_{a\in A} x_a \stackrel{\Delta}{=} \sum_{i=1}^{n} x_{f(i)}$.
Cette quantité ne dépend pas de la bijection f.

Démonstration.
Soit g une seconde bijection de $\mathbb{N}_n$ dans A. Alors $\sum_{i=1}^{n} x_{g(i)} = \sum_{i=1}^{n} x_{f([f^{-1}\circ g](i))} = \sum_{i=1}^{n} y_{\sigma(i)}$,
en posant $\sigma = f^{-1} \circ g$ et $y_j = x_{f(j)}$ pour tout $j \in \mathbb{N}_n$.
$\sigma \in \mathcal{S}_n$, donc d'après la propriété précédente, $\sum_{i=1}^{n} y_{\sigma(i)} = \sum_{i=1}^{n} y_i = \sum_{i=1}^{n} x_{f(i)}$. □

Exemple. Si $n, m \in \mathbb{Z}$, $\sum_{k=m}^{n} x_k = \sum_{a\in[\![m,n]\!]} x_a$, où $[\![m, n]\!] = \{k \in \mathbb{Z} / m \leq k \leq n\}$.
En particulier, lorsque $n < m$, $\sum_{k=m}^{n} x_k = \sum_{k\in\emptyset} x_k = 0$.

Propriété d'additivité : Soit A un ensemble fini, $(x_a)_{a\in A}$ et $(y_a)_{a\in A}$ deux familles d'éléments de G indexées par A. Alors

$$\sum_{a\in A}(x_a + y_a) = \Big(\sum_{a\in A} x_a\Big) + \Big(\sum_{a\in A} y_a\Big).$$

Démonstration.
En utilisant une bijection de $\mathbb{N}_n$ dans A, on se ramène au cas où $A = \{1, \ldots, n\}$, que l'on démontre par récurrence sur n. □

Exemple.
$$\sum_{k=1}^{n} k(k+1) = \sum_{k=1}^{n} k^2 + \sum_{k=1}^{n} k = \frac{n(n+1)(2n+1)}{6} + \frac{n(n+1)}{2} = \frac{n(n+1)(n+2)}{3}.$$

Distributivité généralisée : Soit A un ensemble fini, $\lambda \in \mathbb{C}$ et $(x_a)_{a\in A}$une famille de *complexes* indexée par A. Alors

$$\sum_{a\in A}(\lambda x_a) = \lambda \sum_{a\in A} x_a.$$

Démonstration.
En utilisant une bijection de $\mathbb{N}_n$ dans A, on se ramène au cas où $A = \{1, \dots, n\}$, que l'on démontre par récurrence sur n. □

Remarque. Cette formule est valable dans un contexte plus général, où le produit utilisé est distributif par rapport à l'addition utilisée. C'est notamment le cas lorsque $(G, +, \times)$ est un anneau, avec $\lambda \in G$ et pour tout $a \in A$, $x_a \in G$.

Changement de variable dans une somme finie : Soit B un ensemble fini, $(x_b)_{b\in B}$ une famille d'éléments de G. Soit φ une bijection d'un ensemble A dans B. Alors

$$\sum_{b\in B} x_b = \sum_{a\in A} x_{\varphi(a)}.$$

Lorsqu'on transforme l'une des sommes en l'autre somme, on dit qu'on a posé $b = \varphi(a)$. Il importe en pratique de s'assurer que φ est bien bijective.

Démonstration.
Posons $n = |B| = |A|$. Il existe une bijection f de $\mathbb{N}_n$ dans A. Alors $\varphi \circ f$ est une bijection de $\mathbb{N}_n$ dans B, donc $\sum_{b\in B} x_b = \sum_{i=1}^{n} x_{[\varphi\circ f](i)} = \sum_{i=1}^{n} x_{\varphi(f(i))} = \sum_{a\in A} x_{\varphi(a)}$. □

Exemple. Dans la quantité $S = \sum_{k=0}^{n} k$, on pose $k = n - h$. L'application φ correspondante est la bijection $\begin{array}{rccc}\varphi : & [\![0,n]\!] & \longrightarrow & [\![0,n]\!] \\ & h & \longmapsto & n-h\end{array}$. Ainsi, $S = \sum_{h=0}^{n}(n-h) = n(n+1) - S$, ce qui permet de retrouver que $\sum_{k=0}^{n} k = \dfrac{n(n+1)}{2}$.

Décalage d'indice : Pour tout $m, n, p \in \mathbb{Z}$, $\sum_{k=m}^{n} x_k = \sum_{h=m-p}^{n-p} x_{h+p}$.

Démonstration.
On pose $k = h + p = \varphi(h)$ où φ est bien une bijection de $[\![m-p, n-p]\!]$ dans $[\![m, n]\!]$. □

Remarque. En pratique, le plus souvent, $p = \pm 1$.

Exemple. (à connaître) : calcul d'une somme géométrique .

Soit $q \in \mathbb{C}$ avec $q \neq 1$. Soit $m, n \in \mathbb{N}$ avec $m \leq n$. On souhaite calculer $S = \sum_{k=m}^{n} q^k$.

Par distributivité,

$qS = \sum_{k=m}^{n} q^{k+1} = \sum_{k=m+1}^{n+1} q^k = S - q^m + q^{n+1}$, donc $\boxed{\sum_{k=m}^{n} q^k = \dfrac{q^m - q^{n+1}}{1-q}}$.

Théorème. Soit $(G..)$ un groupe commutatif fini. Alors, pour tout $a \in G$, $a^{\#G} = 1_G$.

Démonstration.
Soit $a \in G$. Notons φ l 'application de G dans G définie par $\varphi(g) = ag$. Alors φ est une bijection dont la bijection réciproque est $g \longmapsto a^{-1}g$, donc si l'on pose $S = \prod_{g\in G} g$, on a $S = \prod_{g\in G} \varphi(g) = \prod_{g\in G} ag = a^{\#G}S$, car G est commutatif. En multipliant cette égalité par S^{-1}, on en déduit que $a^{\#G} = 1_G$. □

Lemme : Soit C un ensemble fini. On suppose que $C = A \sqcup B$. Alors, pour toute famille $(x_c)_{c\in C}$ d'éléments de C, $\sum_{c\in C} x_c = \Big(\sum_{a\in A} x_a\Big) + \Big(\sum_{b\in B} x_b\Big)$.

Démonstration.
Posons $n = |A|$ et $m = |B|$.
Il existe des bijections $f : \mathbb{N}_n \longrightarrow A$ et $g : [\![n+1, n+m]\!] \longrightarrow B$,
donc $\sum_{a\in A} x_a = \sum_{i=1}^{n} x_{f(i)}$ et, en posant $b = g(j)$, $\sum_{b\in B} x_b = \sum_{j=n+1}^{n+m} x_{g(j)}$.
En posant $h(k) = f(k)$ lorsque $k \in \mathbb{N}_n$ et $h(k) = g(k)$ lorsque $k \in [\![n+1, n+m]\!]$, on définit une bijection de $\mathbb{N}_{n+m}$ dans $A \sqcup B = C$. Ainsi,
$\Big(\sum_{a\in A} x_a\Big) + \Big(\sum_{b\in B} x_b\Big) = \Big(\sum_{i=1}^{n} x_{h(i)}\Big) + \Big(\sum_{j=n+1}^{n+m} x_{h(j)}\Big)$. On conclut par associativité. □

Sommation par paquets : Soit A un ensemble fini et $(x_a)_{a\in A}$ une famille d'éléments de G. Soit $n \in \mathbb{N}$. On suppose qu'il existe des parties $A_1, \ldots, A_n$ de A telles que $A = \bigsqcup_{i=1}^{n} A_i$. Alors

$$\sum_{a\in A} x_a = \sum_{i=1}^{n} \sum_{a\in A_i} x_a.$$

Démonstration.
A partir du lemme, par récurrence. □

Sommation par paquets, seconde formulation : Soit A un ensemble fini et $(x_a)_{a\in A}$ une famille d'éléments de G. On suppose qu'il existe un ensemble fini B et une famille $(A_b)_{b\in B}$ de parties de A telles que $A = \bigsqcup_{b\in B} A_b$. Alors

$$\sum_{a\in A} x_a = \sum_{b\in B} \sum_{a\in A_b} x_a.$$

Démonstration.
On se ramène à la première formulation en considérant une bijection $f : \mathbb{N}_n \longrightarrow B$ et en posant $A'_i = A_{f(i)}$. □

Sommation par paquets, troisième formulation : Soit A un ensemble fini et $(x_a)_{a\in A}$ une famille d'éléments de G. Soit R une relation d'équivalence sur A. Alors

$$\sum_{a\in A} x_a = \sum_{c\in A/R}\sum_{a\in c} x_a.$$

Démonstration.
On sait que dans ces conditions, A/R est fini et que $A = \bigsqcup_{c\in A/R} c$. □

Remarque. En particulier, si l'on prend $x_a = 1$ pour tout $a \in A$, on en déduit que $|A| = \sum_{a\in A} 1 = \sum_{c\in A/R} |c|$.

9.4 Applications et cardinaux

Notation. Considérons une application f de E dans F, où E est de cardinal fini.
On a vu que l'application $\begin{array}{rccc} \overline{f}: & E/R & \longrightarrow & f(E) \\ & \overline{x} & \longmapsto & f(x) \end{array}$ est une bijection, où $\overline{x}$ est la classe d'équivalence de x pour la relation d'équivalence R définie par : $xRy \iff f(x) = f(y)$.
On sait de plus que E/R est fini, donc $f(E)$ est fini et $|E/R| = |f(E)|$.
Par ailleurs, $|E| = \sum_{c\in E/R} |c|$.
Pour tout $c \in E/R$, $|c| \geq 1$, donc $|E| \geq \sum_{c\in E/R} 1 = |E/R|$.
Ainsi, dans tous les cas, $|E| \geq |f(E)|$.
De plus, $|E| = |f(E)|$ si et seulement si $0 = |E| - |f(E)| = \sum_{c\in E/R} (|c| - 1)$, donc si et seulement si pour tout $c \in E/R$, $|c| = 1$. Ainsi $|E| = |f(E)|$ si et seulement si les classes d'équivalence de R sont toutes des singletons, c'est-à-dire si et seulement si R est la relation d'égalité, ou encore si et seulement si f est injective. On peut énoncer :

Propriété. Soit E un ensemble fini et f une application de E dans un ensemble quelconque F. Alors $f(E)$ est fini. De plus,
$|f(E)| \leq |E|$, avec égalité si et seulement si f est injective, et
$|f(E)| \leq |F|$, avec égalité si et seulement si f est surjective.

Remarque. Lorsque F est de cardinal infini, on a bien sûr $|f(E)| \leq +\infty = |F|$.

Propriété. Soit E et F deux ensembles finis *de même cardinal*. Soit f une application de E dans F. Alors f injective $\iff$ f surjective $\iff$ f bijective .

Démonstration.
f injective $\iff |f(E)| = |E| \iff |f(E)| = |F| \iff f$ surjective. □

Remarque. Ainsi, lorsque E est fini, une application de E dans E injective (resp : surjective) est toujours surjective (resp : injective). C'est faux lorsque E est infini. Par

exemple l'application $\begin{array}{ccc} \mathbb{N} & \longrightarrow & \mathbb{N} \\ n & \longmapsto & n+1 \end{array}$ est injective mais 0 n'a aucun antécédent, donc elle n'est pas surjective.
De plus, l'application $f : \mathbb{N} \longrightarrow \mathbb{N}$ définie par $f(2n) = n$ et $f(2n+1) = n$ pour tout $n \in \mathbb{N}$, est surjective sans être injective.

Propriété. Soit A et B deux ensembles.
S'il existe une injection de A dans B et si B est fini, alors A est fini et $|A| \leq |B|$.
S'il existe une surjection de A dans B et si A est fini, alors B est fini et $|A| \geq |B|$.

Démonstration.
◇ Supposons qu'il existe une injection f de A dans B et que B est fini.
f est alors une bijection de A dans $f(A)$ qui est une partie de B. On en déduit que $f(A)$ est finie avec $|f(A)| \leq |B|$, puis que A est fini avec $|A| \leq |B||$.
◇ Sous ces hypothèses, on a vu que $|A| \geq |f(A)| = |B|$. □

Principe des tiroirs : Si l'on doit ranger p objets dans n tiroirs et que $p > n$, alors il existe au moins 2 objets qui seront dans le même tiroir.

Démonstration.
L'application qui à un objet associe le tiroir où il sera rangé n'est pas injective. □

Principe des bergers : Soit E et F des ensembles finis et $f : E \longrightarrow F$ une application. On suppose qu'il existe $k \in \mathbb{N}^*$ tel que, pour tout $y \in F$, $|f^{-1}(\{y\})| = k$. Cela signifie que tout élément de F possède exactement k antécédents par f.
Alors $|E| = k|F|$.

Démonstration.
Nous sommes dans la situation du début de ce paragraphe. Pour tout $x \in E$, la classe d'équivalence de x est $\overline{x} = \{y \in E / f(x) = f(y)\} = f^{-1}(\{f(x)\})$, donc par hypothèse, toutes les classes d'équivalence sont de cardinal k.
Alors $|E| = \sum_{c \in E/R} |c| = |k| \sum_{c \in E/R} 1 = k|E/R| = k|f(E)|$. Enfin, $f(E) = F$, car tout élément de F possède au moins un antécédent. □

9.5 Listes et combinaisons

Vocabulaire : Soit E un ensemble et $p \in \mathbb{N}$.
- Une p-liste (aussi appelée un p-uplet) d'éléments de E est un élément de E^p.
- Un p-arrangement d'éléments de E est une p-liste dont les éléments sont deux à deux distincts.
- Une p-combinaison de E est une partie de E de cardinal p.

Lorsque E est de cardinal fini, l'objet de ce chapitre est de dénombrer les p-listes, p-arrangements et p-combinaisons d'éléments de E.
Pour tout ce chapitre, on supposera que E est un ensemble de cardinal fini égal à n.

Propriété. Le nombre de p-listes d'éléments de E est égal à n^p (c'est $|E|^p$).

Choix (ou tirages) successifs avec répétitions éventuelles :

On utilise les p-listes dans les problèmes de choix successifs de p éléments d'un ensemble, avec d'éventuelles répétitions, ou bien de tirages successifs d'éléments d'un ensemble avec remise. Cela permet ainsi de dénombrer le nombre d'issues possibles lorsqu'on effectue p fois indépendamment une même expérience.

Exemple. Le nombre de mots de 4 lettres, ayant un sens ou non, écrits dans notre alphabet de 26 lettres est égal à 26^4 : on peut considérer qu'un tel mot est obtenu par tirages successifs avec remise de 4 lettres parmi les 26 lettres de l'alphabet.
Le nombre d'octets, c'est-à-dire de mots de 8 lettres, écrits dans l'alphabet $\{0,1\}$, est égal à $2^8 = 256$.

Propriété. Soit $p \in \mathbb{N}$. Si $a = (e_1, \ldots, e_p)$ est un p-arrangement d'éléments de E, l'application $\begin{array}{rccc} f_a : & \mathbb{N}_p & \longrightarrow & E \\ & i & \longmapsto & e_i \end{array}$ est une injection.
De plus, l'application $a \longmapsto f_a$ est une bijection de l'ensemble des p-arrangements d'éléments de E vers l'ensemble des injections de $\mathbb{N}_p$ dans E.

Démonstration.
Notons $\mathcal{A}_p$ l'ensemble des p-arrangements d'éléments de E et $\mathcal{I}_p$ l'ensemble des injections de $\mathbb{N}_p$ dans E. Notons $\begin{array}{rccc} \varphi : & \mathcal{A}_p & \longrightarrow & \mathcal{I}_p \\ & a & \longmapsto & f_a \end{array}$ et $\begin{array}{rccc} \Psi : & \mathcal{I}_p & \longrightarrow & \mathcal{A}_p \\ & f & \longmapsto & (f(1), \ldots, f(p)) \end{array}$.
On vérifie que Ψ est bien à valeurs dans $\mathcal{A}_p$, puis que $\varphi \circ \Psi = Id_{\mathcal{I}_p}$ et $\Psi \circ \varphi = Id_{\mathcal{A}_p}$. □

Remarque. Supposons que $p > n$. Alors il n'existe aucun p-arrangement dans E, ni aucune p-combinaison.
En effet, pour les p-combinaisons, on a vu que toute partie de E est de cardinal inférieur à n, et pour les p-arrangements, d'après la propriété précédente, le nombre de p-arrangements coïncide avec le nombre d'injections de $\mathbb{N}_p$ dans E, que l'on sait être nul lorsque $|\mathbb{N}_p| > |E|$.
Pour toute la suite de ce paragraphe, on suppose que p est un entier compris entre 0 et n.

Notation. Pour tout $n \in \mathbb{N}$, on appelle factorielle (de) n le produit des entiers consécutifs de 1 à n. Elle est notée $n!$. Ainsi,

$$n! = 1 \times 2 \times \cdots (n-1) \times n$$

Conformément à une convention étudiée page 88, on convient que $0! = 1$: c'est un produit vide.

Théorème. Le nombre de p-arrangements d'éléments d'un ensemble de cardinal n est

$$A_{n,p} = n(n-1)\cdots(n-p+1) = \frac{n!}{(n-p)!}.$$

C'est aussi le nombre d'injections d'un ensemble à p éléments vers un ensemble à n éléments.

Démonstration.
◇ Soit B un ensemble de cardinal p. Il existe une bijection f de $\mathbb{N}_p$ dans B.
Notons $\mathcal{I}_B$ l'ensemble des injections de B dans E.
Alors l'application $\varphi : \begin{array}{ccc} \mathcal{I}_B & \longrightarrow & \mathcal{I}_p \\ g & \longmapsto & g \circ f \end{array}$ est une bijection, dont la bijection réciproque est ...
Pour prouver le théorème, il suffit donc de montrer que $|\mathcal{I}_p| = A_{n,p}$. Notons $R(p)$ cette propriété et raisonnons par récurrence finie.
◇ Lorsque $p = 0$, $\mathbb{N}_p = \emptyset$ et on sait qu'il existe une unique application (vide) de $\mathbb{N}_p$ dans E. C'est une injection, d'où $R(0)$.
Lorsque $0 \leq p < n$, on suppose $R(p)$.
Si g est une injection de $\mathbb{N}_{p+1}$ dans E, sa restriction $g|_{\mathbb{N}_p}$ est une injection de $\mathbb{N}_p$ dans E, donc on peut définir l'application $\Psi : \begin{array}{ccc} \mathcal{I}_{p+1} & \longrightarrow & \mathcal{I}_p \\ g & \longmapsto & g|_{\mathbb{N}_p} \end{array}$.
Soit $h \in \mathcal{I}_p$. Pour tout $g \in \mathcal{I}_{p+1}$, $\Psi(g) = h \iff g|_{\mathbb{N}_p} = h$,
donc $\Psi^{-1}(\{h\}) = \{g \in \mathcal{F}(\mathbb{N}_{p+1}, E) / \forall i \in \mathbb{N}_p,\ g(i) = h(i) \text{ et } g(p+1) \in E \setminus h(\mathbb{N}_p)\}$.
On peut mettre cet ensemble en bijection avec $E \setminus h(\mathbb{N}_p)$, donc $|\Psi^{-1}(\{h\})| = n - p \in \mathbb{N}^*$.
D'après le principe des bergers, $|\mathcal{I}_{p+1}| = (n-p)|\mathcal{I}_p|$, d'où $R(p+1)$. □

Exemple. paradoxe des anniversaires : Soit C une classe d'élèves et f l'application qui à tout élément de C associe sa date d'anniversaire. La probabilité que 2 élèves au moins aient la même date d'anniversaire est égal à $p = 1 - \dfrac{N}{\#(\mathcal{F}(C, D))}$, où D est l'ensemble des dates possibles (on simplifie la situation en supposant que $\#D = 365$, c'est-à-dire en oubliant les années bissextiles) et où N est le nombre d'injections de C dans D. Ainsi, $p = 1 - \dfrac{365 \times 364 \times \cdots \times (365 - n + 1)}{365^n}$, où n est le nombre d'élèves de C. Avec $n = 47$, on obtient $p = 95,5\%$.

Corollaire. Pour tout $n \in \mathbb{N}$, $|\mathcal{S}_n| = n!$.
Plus généralement, *factorielle de n* est le nombre de bijections d'un ensemble de cardinal n dans un autre ensemble de cardinal n.

Choix successifs sans répétition, tirages sans remise :
On utilise les p-arrangements dans les problèmes de choix successifs de p éléments pris parmi n, sans répétition, ou bien de tirages successifs de p éléments dans un ensemble de n éléments sans remise. Ici, l'ordre d'apparition des différents choix ou tirages compte, c'est-à-dire que deux p-arrangements ayant les mêmes éléments dans un ordre différent sont comptabilisés tous les deux.
Cela permet ainsi de dénombrer le nombre d'issues possibles lorsqu'on effectue p fois une expérience, sans possibilité de retrouver un résultat précédemment obtenu.

Exemple. 8 sportifs se présentent pour courir un 100m. Déterminer le nombre de podiums possibles.
Un podium est un 3-arrangement de coureurs, désignant le médaillé d'or, le médaillé d'argent et le médaillé de bronze. Le nombre de podiums est donc $A_{8,3} = 8.7.6 = 336$.

Théorème. Le nombre de p-combinaisons d'éléments d'un ensemble de cardinal n, c'est-à-dire le nombre de parties de p éléments incluses dans un ensemble de cardinal n est égal à

$$\binom{n}{p} \triangleq \frac{A_{n,p}}{p!} = \frac{n!}{(n-p)!p!}.$$

Cette quantité s'appelle le coefficient binomial "p parmi n".

Démonstration.

Notons $\mathcal{C}_p$ l'ensemble des p-combinaisons d'éléments de E et $\begin{array}{rccc}\varphi : & \mathcal{I}_p & \longrightarrow & \mathcal{C}_p \\ & f & \longmapsto & f(\mathbb{N}_p)\end{array}$.

Soit $A \in \mathcal{C}_p$. $f \in \varphi^{-1}(\{A\})$ si et seulement si $f(\mathbb{N}_p) = A$, donc si et seulement si f réalise une bijection de $\mathbb{N}_p$ dans A. Ainsi, pour tout $A \in \mathcal{C}_p$, $|\varphi^{-1}(\{A\})| = p!$ et le principe des bergers permet de conclure. □

Choix simultanés, tirages sans remise où l'ordre est indifférent :

On utilise les p-combinaisons dans les problèmes de choix simultanés de p éléments pris parmi n, ou bien de tirages successifs de p éléments dans un ensemble de n éléments sans remise lorsque l'ordre d'apparition des différents tirages n'intervient pas.

Exercice. Avec un jeu de 32 cartes, quelle est la probabilité qu'une main de 5 cartes comporte au plus 2 piques.

Solution :

◇ Rappelons qu'une carte possède une couleur (pique, coeur, carreau, trèfle) et une valeur (7,8,9,10,valet, dame, roi, as). Dans un jeu de 32 cartes, on dispose donc de 8 cartes de chaque couleur.

Dans un jeu de 52 cartes, on dispose des mêmes couleurs et des valeurs supplémentaires 2,3,4,5,6, soit 13 valeurs au total.

◇ Ici, la condition portant sur la main ne dépend pas de l'ordre des cartes, donc on peut assimiler une main de 5 cartes à une partie de 5 éléments parmi les 32 cartes. Ainsi, le nombre total de mains de 5 cartes est $\binom{32}{5}$.

◇ On applique le principe du "ou exclusif" en fonction du nombre de piques dans la main :

— Le nombre de mains de 5 cartes sans aucun pique est $\binom{24}{5}$,

— Le nombre de mains de 5 cartes comportant exactement un pique est $8 \times \binom{24}{4}$, car pour en construire une, on peut d'abord choisir un pique, soit 8 choix, puis un ensemble de 4 cartes d'une couleur différente de pique, soit $\binom{24}{4}$ choix. On a donc appliqué le principe du "et".

— De la même façon, il y a $\binom{24}{3} \times \binom{8}{2}$ mains de 5 cartes avec 2 piques exactement.

Ainsi la probabilité demandée est égale à $\dfrac{\binom{24}{5}+\binom{24}{4}\times 8+\binom{24}{3}\times\binom{8}{2}}{\binom{32}{5}}$.

Exercice. Avec un jeu de 32 cartes, quelle est la probabilité qu'une main de 5 cartes comporte au plus 4 piques.

Solution : On peut adapter la solution précédente, mais il est préférable de passer au contraire, en cherchant d'abord à dénombrer les mains comportant uniquement des piques, ce qui est plus simple, car cela revient à choisir 5 éléments parmi les 8 cartes de couleur pique. Ainsi, la probabilité cherchée est
$\dfrac{\binom{32}{5}-\binom{8}{5}}{\binom{32}{5}}$.

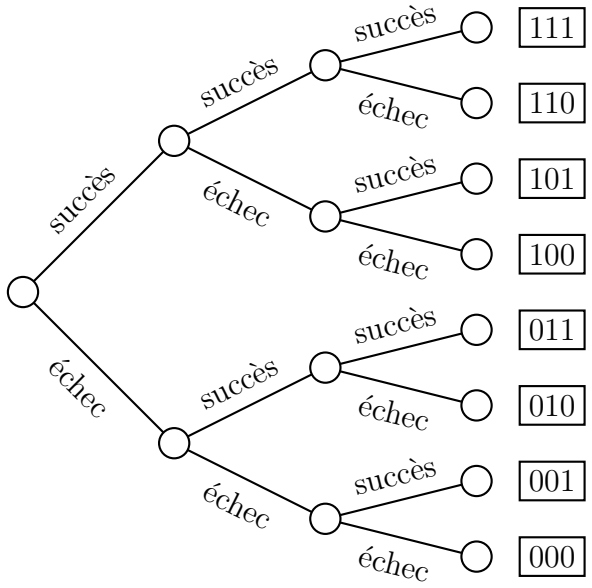
Exercice. Combien le mots MISSISSIPPI possède-t-il d'anagrammes, qu'ils aient un sens ou non ?

Solution : On cherche le nombre de mots de 11 lettres possèdant 1 M, 2 P, 4 I et 4 S.
Pour construire un tel mot, on remplit par des lettres 11 cases initialement vides. On choisit d'abord l'emplacement de la lettre M, soit 11 choix, puis les deux emplacements des lettres P parmi les 10 emplacements restants, soit $\binom{10}{2}$ choix etc. Ainsi, le nombre cherché est égal à $N = 11.\binom{10}{2}.\binom{8}{4} = 34650$.
A noter qu'on aurait pu raisonner en classant les 4 lettres M, P, I, et S dans un autre ordre.

9.6 Les coefficients binomiaux

Considérons un ensemble de n éléments, noté $E = \{e_1, \ldots, e_n\}$.
Pour démontrer que $|\mathcal{P}(E)| = 2^n$, on a mis $\mathcal{P}(E)$ en bijection avec $\mathcal{F}(E, \{0,1\})$ en associant à toute partie de E son indicatrice. Mais $\mathcal{F}(E, \{0,1\})$ est aussi l'ensemble des familles $(\varepsilon_i)_{1\leq i\leq n}$ d'éléments de $\{0,1\}$. On peut donc coder toute partie A de E par une suite binaire de longueur n.
Par exemple, avec $n = 5$, la partie $A = \{e_2, e_3, e_5\}$ de E est codée par la suite 01101.
Cette bijection envoie les parties de E à k éléments sur les suites binaires possédant exactement k "1". Ainsi $\binom{n}{k}$ est aussi le nombre de suites binaires de longueur n possèdant exactement k "1". On peut le retrouver directement en disant que pour construire une telle suite, il suffit de convenir de l'ensemble des k positions des "1" parmi les n positions.
Changeons un peu le vocabulaire, en remplaçant "0" par "échec" et "1" par "succès". On considére un test que l'on peut répéter n fois, comme le fait de lancer une pièce

de monnaie et de tester si elle tombe sur le côté "face". Alors $\binom{n}{k}$ est le nombre de réalisations de n tests comportant exactement k succès.
On peut représenter les 2^n réalisations possibles par un arbre :



Ainsi, dans un tel arbre, s'il représente la répétition de n tests, le nombre de chemins réalisant exactement k succès est égal à $\binom{n}{k}$. C'est ainsi que les coefficients binomiaux vous ont été présentés la première fois, en classe de Première.

Formule : $\forall n, p \in \mathbb{N}$ avec $0 \leq p \leq n$, $\binom{n}{p} = \binom{n}{n-p}$.

Démonstration.
C'est évident avec la formule $\binom{n}{p} = \dfrac{n!}{(n-p)!p!}$, mais on peut aussi en donner une preuve combinatoire : avec les notations de la démonstration précédente, l'application $\begin{array}{ccc} \mathcal{C}_p & \longrightarrow & \mathcal{C}_{n-p} \\ A & \longmapsto & \overline{A} \end{array}$ est une bijection (c'est une involution). □

Formule comité-président : Pour tout $n, k \in \mathbb{N}^*$ avec $k \leq n$,

$$k\binom{n}{k} = n\binom{n-1}{k-1}.$$

Démonstration.
C'est très simple par le calcul, mais on peut aussi en donner une preuve combinatoire, qui permet notamment de retenir la formule :

$k\binom{n}{k}$ est le nombre de comités à k éléments parmi n, où chaque comité est muni d'un président. Formellement, c'est le nombre de couples (a, A) où A est une partie à k éléments d'un ensemble E de cardinal n et où $a \in A$. Mais pour dénombrer ces couples, on peut d'abord choisir le président a, soit n choix, puis le président choisit la composition des autres membres du comité, soit $\binom{n-1}{k-1}$ choix.
On peut alors concevoir une formule "comité à deux présidents" : pour tout $n, k \in \mathbb{N}$ avec $2 \leq k \leq n$, $k(k-1)\binom{n}{k} = n(n-1)\binom{n-2}{k-2}$. Je vous laisse généraliser : □

Formule comité-bureau : Pour tout $p \in \mathbb{N}$, pour tout $n, k \in \mathbb{N}$ avec $p \leq k \leq n$,

$$\binom{k}{p} \times \binom{n}{k} = \binom{n}{p} \times \binom{n-p}{k-p}.$$

Formule du triangle de Pascal [18] **:** $\forall n, p \in \mathbb{N}$ avec $1 \leq p < n$,

$$\binom{n}{p} = \binom{n-1}{p} + \binom{n-1}{p-1}.$$

Remarque. Il est souvent pratique de convenir que, pour tout $n, p \in \mathbb{Z}$ tels que $\neg(0 \leq p \leq n)$, $\binom{n}{p} = 0$.
Alors la formule du triangle de Pascal est vraie pour tout $n \geq 1$ et $p \in \mathbb{Z}$ (le raisonnement combinatoire reste valable).

Démonstration.
Là aussi, on peut vérifier cette formule par le calcul : à faire.
◇ De manière combinatoire, distinguons un élément a dans E. On peut alors partitionner l'ensemble des p-combinaisons de E en deux sous-ensembles :
- les p-combinaisons ne contenant pas a, qui sont toutes les p-combinaisons de $E \setminus \{a\}$, au nombre de $\binom{n-1}{p}$,
- et les p-combinaisons contenant a, que l'on peut mettre en bijection avec les $(p-1)$-combinaisons de $E \setminus \{a\}$, au nombre de $\binom{n-1}{p-1}$.

◇ En classe de Première, sachant que $\binom{n}{p}$ est égal au nombre de chemins réalisant p succès dans un arbre représentant la répétition de n tests, on vous a aussi tenu le raisonnement suivant : ces chemins sont de deux sortes. Il y a les chemins pour lesquels les p succès se sont produits pendant les $n-1$ premiers tests, qui sont au nombre de

18. Blaise Pascal, 1623-1662, est un mathématicien, physicien, inventeur, philosophe, moraliste et théologien français. Enfant précoce, il publie un traité de géométrie projective à seize ans et il invente la première machine à calculer (la pascaline) à 19 ans. Après 1654 il se consacre à la réflexion philosophique et religieuse. Ses "pensées" seront publiées après sa mort.

$\binom{n-1}{p}$ et ceux qui correspondent à $p-1$ succès lors des $n-1$ premiers tests suivis d'un dernier succès, qui sont au nombre de $\binom{n-1}{p-1}$. Mais il s'agit en fait de la même démonstration. □

Représentation graphique du triangle de Pascal.

Remarque. On vient de voir plusieurs exemples de démontrations combinatoires de formules. Le principe général de ce type de preuve, concernant une égalité entre entiers de la forme $a = b$, consiste à interpréter a et b comme le dénombrement d'un même ensemble fini selon deux méthodes différentes.
Par exemple, la formule $\sum_{k=0}^{n} \binom{n}{k} = 2^n$ peut se démontrer en disant que, pour constuire une partie quelconque d'un ensemble à n éléments, on choisit d'abord le nombre k d'éléments de cette partie, puis on choisit k éléments parmi n qui constitueront cette partie.
Cependant cette dernière formule est un cas particulier de la formule du binôme de Newton :

Formule du binôme de Newton[19] **:** On se place dans un anneau $(A, +, \times)$. Soit a_1 et a_2 deux éléments de A qui commutent, c'est-à-dire tels que $a_1 a_2 = a_2 a_1$. Alors

$$\forall n \in \mathbb{N},\ \ (a_1 + a_2)^n = \sum_{k=0}^{n} \binom{n}{k} a_1^k\ a_2^{n-k}.$$

Démonstration.

- *Première méthode : par récurrence.*

On note $R(n)$ l'assertion $(a_1 + a_2)^n = \sum_{k=0}^{n} \binom{n}{k} a_1^k a_2^{n-k}$. $R(0)$ est vraie.

Pour $n \geq 0$, on suppose $R(n)$.

$$\begin{aligned}(a_1 + a_2)^{n+1} &= (a_1 + a_2) \sum_{k=0}^{n} \binom{n}{k} a_1^k a_2^{n-k} \\ &= a_1^{n+1} + \sum_{k=0}^{n-1} \binom{n}{k} a_1^{k+1} a_2^{n-k} + a_2^{n+1} + \sum_{k=1}^{n} \binom{n}{k} a_1^k a_2^{n-k+1}.\end{aligned}$$

Dans la première somme, posons $h = k + 1$:
l'application $k \longmapsto k+1$ est une bijection de $\{0, \ldots, n-1\}$ dans $\{1, \ldots, n\}$, donc
$\sum_{k=0}^{n-1} \binom{n}{k} a_1^{k+1} a_2^{n-k} = \sum_{k=0}^{n-1} \binom{n}{(k+1)-1} a_1^{k+1} a_2^{n+1-(k+1)} = \sum_{h=1}^{n} \binom{n}{h-1} a_1^h a_2^{n+1-h}$.
L'indice h de cette somme est une variable muette que l'on peut renommer en k, donc

19. Isaac Newton, 1642-1727 est un philosophe, mathématicien, physicien, alchimiste, astronome et théologien britannique. Il a fondé la mécanique classique, dont la théorie de la gravitation universelle. En mathématiques, il est à l'origine avec Leibniz du calcul infinitésimal.

$$\begin{aligned}(a_1+a_2)^{n+1} &= a_1^{n+1} + \sum_{k=1}^{n} \binom{n}{k-1} a_1^k a_2^{n+1-k} + a_2^{n+1} + \sum_{k=1}^{n} \binom{n}{k} a_1^k a_2^{n-k+1} \\ &= a_1^{n+1} + a_2^{n+1} + \sum_{k=1}^{n} (\binom{n}{k-1} + \binom{n}{k}) a_1^k a_2^{n+1-k} \\ &= a_1^{n+1} + a_2^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a_1^k a_2^{(n+1)-k} \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} a_1^k a_2^{(n+1)-k}.\end{aligned}$$

Ceci prouve $R(n+1)$.

• *Seconde méthode : combinatoire.* $(a_1+a_2)^n = (a_1+a_2)\times\cdots\times(a_1+a_2)$. Si l'on développe complètement ce produit de n facteurs, où chaque facteur est la somme de deux termes, on obtient une somme de termes où chaque terme est un produit de n facteurs, obtenu en choissant dans chacun des n facteurs a_1+a_2, ou bien a_1, ou bien a_2. Ainsi, (1) : $(a_1+a_2)^n = \sum_{f\in\mathcal{F}(\mathbb{N}_n,\{1,2\})} \prod_{i=1}^{n} a_{f(i)}$: chacun de ces termes est construit en choissant $a_{f(1)}$ dans le premier facteur a_1+a_2, puis $a_{f(2)}$ dans le second facteur a_1+a_2, etc. Plus rigoureusement, on peut démontrer la relation (1) par récurrence sur n, car elle entraîne

$$\begin{aligned}(a_1+a_2)^{n+1} &= a_1 \sum_{f\in\mathcal{F}(\mathbb{N}_n,\{1,2\})} \prod_{i=1}^{n} a_{f(i)} + a_2 \sum_{f\in\mathcal{F}(\mathbb{N}_n,\{1,2\})} \prod_{i=1}^{n} a_{f(i)} \\ &= \sum_{\substack{f\in\mathcal{F}(\mathbb{N}_{n+1},\{1,2\}) \\ \text{tel que } f(n+1)=1}} \prod_{i=1}^{n+1} a_{f(i)} + \sum_{\substack{f\in\mathcal{F}(\mathbb{N}_{n+1},\{1,2\}) \\ \text{tel que } f(n+1)=2}} \prod_{i=1}^{n+1} a_{f(i)} \\ &= \sum_{f\in\mathcal{F}(\mathbb{N}_{n+1},\{1,2\})} \prod_{i=1}^{n+1} a_{f(i)}.\end{aligned}$$

Pour tout $k\in\{0,\dots,n\}$, notons F_k l'ensemble des fonctions f de $\mathcal{F}(\mathbb{N}_n,\{1,2\})$ telles que 1 possède exactement k antécédents. La famille $(F_0,\dots,F_n)$ est une partition de $\mathcal{F}(\mathbb{N}_n,\{1,2\})$ donc, en sommant par paquets, $(a_1+a_2)^n = \sum_{k=0}^{n}\sum_{f\in F_k}\prod_{i=1}^{n} a_{f(i)}$.

Mais si $f\in F_k$, parmi $a_{f(1)},\dots,a_{f(n)}$, on rencontre exactement k fois a_1 et $n-k$ fois a_2, donc $\prod_{i=1}^{n} a_{f(i)} = a_1^k a_2^{n-k}$. Ainsi, $(a_1+a_2)^n = \sum_{k=0}^{n} a_1^k a_2^{n-k} \sum_{f\in F_k} 1 = \sum_{k=0}^{n} a_1^k a_2^{n-k}|F_k|$.

De plus, pour construire une application f de F_k, il suffit d'indiquer quelle est la partie à k éléments de $\mathbb{N}_n$ dont les images par f sont égales à 1, donc $|F_k| = \binom{n}{k}$. □

Formule du multinôme : (Hors programme). Soit $p,n\in\mathbb{N}^*$. Soit $a_1,\dots,a_p$ p

éléments d'un anneau A qui commutent deux à deux. Alors

$$(a_1 + \cdots + a_p)^n = \sum_{\substack{i_1,\ldots,i_p \in \mathbb{N} \\ \text{tel que } i_1+\cdots+i_p=n}} \frac{n!}{i_1! \times \cdots \times i_p!}\, a_1^{i_1} \times \cdots \times a_p^{i_p}.$$

Exemple. Avec $n = p = 3$, les triplets (i_1, i_2, i_3) d'entiers naturels tels que $i_1 + i_2 + i_3 = 3$ sont $(1,1,1), (1,2,0), (2,1,0), (1,0,2), (2,0,1), (0,1,2), (0,2,1)$, $(3,0,0), (0,3,0)$ et $(0,0,3)$, donc
$(a+b+c)^3 = 6abc + 3(ab^2 + a^2b + ac^2 + a^2c + bc^2 + b^2c) + a^3 + b^3 + c^3$.

Démonstration.
On adapte la démonstration combinatoire.
On obtient d'abord $(a_1 + \cdots + a_p)^n = \sum_{f \in \mathcal{F}(\mathbb{N}_n, \mathbb{N}_p)} \prod_{i=1}^{n} a_{f(i)}$.
Pour tout $(i_1, \ldots, i_p) \in \mathbb{N}^p$ tel que $i_1 + \cdots + i_p = n$, on note $F_{i_1,\ldots,i_p}$ l'ensemble des $f \in \mathcal{F}(\mathbb{N}_n, \mathbb{N}_p)$ telles que, pour tout $j \in \mathbb{N}_p$, le nombre d'antécédents de j par f est égal à i_j. La famille des $F_{i_1,\ldots,i_p}$, lorsque $(i_1, \ldots, i_p)$ parcourt tous les p-uplets d'entiers tels que $i_1 + \cdots + i_p = n$, est une partition de $\mathcal{F}(\mathbb{N}_n, \mathbb{N}_p)$, donc en sommant par paquets,
$(a_1 + \cdots + a_p)^n = \sum_{\substack{i_1,\ldots,i_p \in \mathbb{N} \\ \text{tel que } i_1+\cdots+i_p=n}} |F_{i_1,\ldots,i_p}| a_1^{i_1} \times \cdots \times a_p^{i_p}$.
Pour construire une fonction quelconque de $F_{i_1,\ldots,i_p}$, on choisit d'abord les i_1 antécédents de 1 parmi les n éléments de $\mathbb{N}_n$, soit $\binom{n}{i_1}$ choix, puis les i_2 antécédents de 2 parmi les $n - i_1$ éléments restants de $\mathbb{N}_n$, soit $\binom{n-i_1}{i_2}$ choix, etc., jusqu'aux choix des i_{p-1} antécédents de $p-1$ parmi les $n - i_1 - \cdots - i_{p-2}$ éléments restants. Ainsi,

$$\begin{aligned} |F_{i_1,\ldots,i_p}| &= \binom{n}{i_1}\binom{n-i_1}{i_2}\cdots\binom{n-i_1-\cdots-i_{p-2}}{i_{p-1}} \\ &= \frac{n!}{i_1!(n-i_1)!}.\frac{(n-i_1)!}{i_2!(n-i_1-i_2)!}\cdots\frac{n-i_1-\cdots-i_{p-2}}{i_{p-1}!(n-i_1-\cdots-i_{p-2}-i_{p-1})!} \\ &= \frac{n!}{i_1! \times \cdots \times i_p!}. \end{aligned}$$

□

Remarque. Associons à toute application f de $\mathbb{N}_n$ dans $\mathbb{N}_p$ la suite $(f(1), f(2), \ldots, f(n))$, que l'on peut assimiler à un mot de longueur n écrit sur l'alphabet $\{1, \ldots, p\}$, ou si l'on préfère au codage d'un mot de longueur n écrit sur l'alphabet $A = \{a_1, \ldots, a_p\}$. La fonction qui envoie f sur ce mot est une bijection de $\mathcal{F}(\mathbb{N}_n, \mathbb{N}_p)$ dans A^n, il suffit d'ailleurs de montrer l'injectivité. Donc $F_{i_1,\ldots,i_p}$ est aussi le nombre de mots de n lettres comportant i_1 lettres a_1,…,i_p lettres a_p. Cela généralise l'exercice Mississippi.

Petit théorème de Fermat : Soit $p \in \mathbb{P}$ et $n \in \mathbb{N}$. Alors $n^p \equiv n\ [p]$.
En particulier, si $n \notin p\mathbb{Z}$, alors $n^{p-1} \equiv 1\ [p]$.

Démonstration.
◇ Soit $k \in \{1, \dots, p-1\}$. $k! \binom{p}{k} = p(p-1)\cdots(p-k+1)$ est un multiple de p car $k \leq p-1$, mais p est premier, donc $p \wedge (k!) = 1$. Ainsi, d'après le théorème de Gauss, $p \mid \binom{p}{k}$.
◇ Soit $n \in \mathbb{N}$ tel que $n^p \equiv n\ [p]$. Alors, d'après la formule du binôme de Newton, $(n+1)^p = \sum_{k=0}^{p} \binom{p}{k} n^k$, donc d'après le point précédent, modulo p,
$(n+1)^p \equiv n^0 + n^p \equiv n+1$. De plus, $0^p = 0$, donc par récurrence sur n, on montre que $n^p \equiv n\ [p]$.
◇ Supposons maintenant que $n \notin p\mathbb{Z}$. On vient de montrer que $p|(n^p - n) = n(n^{p-1}-1)$, mais $n \wedge p = 1$, donc d'après le théorème de Gauss, $p|(n^{p-1}-1)$. □

La formule suivante est analogue à la formule du binôme de Newton, mais elle concerne la dérivée n-ième d'un produit de deux fonctions :
Formule de Leibniz : Soient f et g deux applications d'un intervalle I dans $\mathbb{R}$. Si f et g sont n fois dérivables sur I, alors fg est n fois dérivable sur I et

$$(fg)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} f^{(k)} g^{(n-k)}.$$

Démonstration.
Soit $n \in \mathbb{N}$. Notons $R(n)$ l'assertion suivante : si f et g sont n fois dérivables sur I, fg est n fois dérivable sur I et $(fg)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} f^{(k)} g^{(n-k)}$.
Pour $n = 0$, $R(0)$ est vraie.
Pour $n \geq 0$, supposons $R(n)$. On suppose également que f et g sont $n+1$ fois dérivables sur I. D'après $R(n)$, $(fg)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} f^{(k)} g^{(n-k)}$.
Pour tout $k \in \{0, \dots, n\}$, $f^{(k)}$ et $g^{(n-k)}$ sont dérivables sur I, donc $f^{(k)} g^{(n-k)}$ est dérivable sur I. On peut donc dériver l'égalité précédente. On obtient :

$$\begin{aligned}
(fg)^{(n+1)} &= \sum_{k=0}^{n} \binom{n}{k} (f^{(k+1)} g^{(n-k)} + f^{(k)} g^{(n-k+1)}) \\
&= \sum_{k=1}^{n+1} \binom{n}{k-1} f^{(k)} g^{(n-k+1)} + \sum_{k=0}^{n} \binom{n}{k} f^{(k)} g^{(n-k+1)} \\
&= f^{(n+1)} g^{(0)} + f^{(0)} g^{(n+1)} + \sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k} \right) f^{(k)} g^{(n-k+1)} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} f^{(k)} g^{(n-k+1)}.
\end{aligned}$$

Ceci prouve $R(n+1)$.

Ainsi, d'après le principe de récurrence, pour tout $n \in \mathbb{N}$, on a montré $R(n)$. □

Remarque. Lorsque a et b sont des réels, on peut retrouver la formule du binôme de Newton à partir de la formule de Leibniz, en l'appliquant avec $f(t) = e^{ta}$ et $g(t) = e^{tb}$, en $t = 0$. En effet, pour tout $k \in \mathbb{N}$, $\dfrac{d^k}{dt^k}(e^{ta}) = a^k e^{ta}$.

9.7 Sommes et produits : quelques techniques

9.7.1 Télescopage

Propriété. Soit $m, n \in \mathbb{Z}$ avec $m \leq n$. Soit $(u_k)_{m \leq k \leq n+1}$ une famille d'éléments d'un groupe abélien $(G, +)$. Alors $\displaystyle\sum_{k=m}^{n}(u_{k+1} - u_k) = u_{n+1} - u_m$.

De même, $\displaystyle\sum_{k=m+1}^{n+1}(u_{k-1} - u_k) = u_m - u_{n+1}$.

On dit que ces sommes sont télescopiques.

Exemple.

◇ $\displaystyle\sum_{k=1}^{n}\frac{1}{k(k+1)} = \sum_{k=1}^{n}\Big(\frac{1}{k} - \frac{1}{k+1}\Big) = 1 - \frac{1}{n+1} \underset{n\to+\infty}{\longrightarrow} 1$, donc la série $\displaystyle\sum_{k\geq 1}\frac{1}{k(k+1)}$ converge et $\displaystyle\sum_{k=1}^{+\infty}\frac{1}{k(k+1)} = 1$.

◇ $\displaystyle\sum_{k=1}^{n}\ln(1+\frac{1}{k}) = \sum_{k=1}^{n}(\ln(k+1) - \ln k) = \ln(n+1) - \ln 1 \underset{n\to+\infty}{\longrightarrow} +\infty$, donc la série $\displaystyle\sum_{k\geq 1}\ln(1+\frac{1}{k})$ diverge (alors que $\ln(1+\frac{1}{n}) \underset{n\to+\infty}{\longrightarrow} 0$).

◇ $\displaystyle\sum_{k=0}^{n}k(k!) = \sum_{k=0}^{n}((k+1)-1)(k!) = \sum_{k=0}^{n}((k+1)! - k!) = (n+1)! - 1$.

9.7.2 Séparation des indices pairs et impairs

D'après le principe de sommation par paquets, lorsque $(u_k)_{0\leq k\leq n}$ est une famille d'éléments d'un monoïde commutatif, $\displaystyle\sum_{k=0}^{n}u_k = \sum_{\substack{0\leq k\leq n\\ k \text{ pair}}}u_k + \sum_{\substack{0\leq k\leq n\\ k \text{ impair}}}u_k = \sum_{p=0}^{\lfloor\frac{n}{2}\rfloor}u_{2p} + \sum_{p=0}^{\lfloor\frac{n-1}{2}\rfloor}u_{2p+1}$.

Exemple. $\displaystyle\sum_{k=0}^{2n}(-1)^k k^2 = \sum_{k=0}^{n}(2k)^2 - \sum_{k=0}^{n-1}(2k+1)^2 = 4\sum_{k=0}^{n}k^2 - \sum_{k=0}^{n-1}(4k^2+4k+1)$, donc $\displaystyle\sum_{k=0}^{2n}(-1)^k k^2 = 4n^2 - 4\frac{n(n-1)}{2} - n = 2n^2 + n$.

9.7.3 Fonction génératrice

Soit $m, n \in \mathbb{N}$ avec $m \leq n$ et soit $(u_k)_{m \leq k \leq n}$ une famille de complexes. La fonction génératrice de cette famille est l'application polynomiale $P : x \longmapsto \sum_{k=m}^{n} u_k x^k$.

Si P est connu, on peut en déduire plusieurs sommes : $\sum_{k=m}^{n} u_k = P(1)$, $\sum_{k=m}^{n} k u_k = P'(1)$, $\sum_{k=m}^{n} k(k-1)u_k = P''(1)$, $\sum_{k=m}^{n} \frac{u_k}{k+1} = \int_0^1 P(t)dt$ etc.

Plus tard, vous étudierez la théorie des séries entières, qui sont des applications de la forme $x \longmapsto \sum_{k=m}^{+\infty} u_k x^k$. Cela permet de prolonger la méthode précédente à des calculs de sommes de séries.

Exemple.

◇ Calculer $S = \sum_{k=0}^{n} \binom{n}{k} k$.

$S = P'(1)$, où $P(x) = \sum_{k=0}^{n} \binom{n}{k} x^k = (x+1)^n$ d'après la formule du binôme de Newton, donc $S = n2^{n-1}$.

On peut aussi calculer S en utilisant la formule du comité-président :

$S = \sum_{k=1}^{n} \binom{n-1}{k-1} n = n2^{n-1}$.

◇ Calculer $S = \sum_{k=0}^{n} k2^k$.

$S = 2P'(2)$, où $P(x) = \sum_{k=0}^{n} x^k = \frac{x^{n+1}-1}{x-1}$ (pour $x \neq 1$).

$P'(x) = \frac{(n+1)x^n(x-1) - (x^{n+1}-1)}{(x-1)^2} = \frac{nx^{n+1} - (n+1)x^n + 1}{(x-1)^2}$,

donc $S = 2(n2^{n+1} - (n+1)2^n + 1) = (n-1)2^{n+1} + 2$.

9.7.4 Quelques formules

Somme arithmétique : Soit $r \in \mathbb{C}$. Une suite (u_n) de complexes est arithmétique de raison r si et seulement si elle vérifie la relation de récurrence suivante :
$\forall n \in \mathbb{N},\ u_{n+1} = u_n + r$. Par récurrence, on montre que pour tout $n \in \mathbb{N}$, $u_n = u_0 + nr$.
Soit $m, n \in \mathbb{N}$ avec $m \leq n$ et soit (u_n) une suite arithmétique de raison r. Alors

$$\sum_{k=m}^{n} u_k = \frac{u_m + u_n}{2}(n - m + 1),$$

ce que l'on retient de la manière suivante : une somme arithmétique est égale à la moyenne de ses termes extrèmes multiplié par son nombre de termes.

Démonstration.

$$\begin{aligned} 2\sum_{k=m}^{n} u_k &= u_m + u_{m+1} + \cdots + u_{n-1} + u_n \\ &\quad + u_n + u_{n-1} + \cdots + u_{m+1} + u_m \\ &= (u_m + u_n) + (u_{m+1} + u_{n-1}) + \cdots + (u_{n-1} + u_{m+1}) + (u_n + u_m). \end{aligned}$$

Or, pour tout $k \in \{0, \ldots, n-m\}$, $u_{m+k}+u_{n-k} = 2u_0+r(m+k+n-k) = 2u_0+r(m+n)$, donc il ne dépend pas de k. Ceci permet de conclure. □

Exemple. $\displaystyle\sum_{k=1}^{n}(2k-1) = \frac{(2n-1)+(2-1)}{2} \times n = n^2.$

Formule de Bernoulli : Soit $(A, +, \times)$ un anneau. Soit a et b deux éléments de A qui commutent (i.e $ab = ba$). Alors, pour tout $n \in \mathbb{N}$,

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

Démonstration.

$(a-b)\displaystyle\sum_{k=0}^{n} a^k b^{n-k} = \sum_{k=0}^{n}(a^{k+1}b^{(n+1)-(k+1)} - a^k b^{(n+1)-k})$. Il s'agit d'une somme télescopique, ce qui permet de conclure. □

Remarque. Lorque $n+1$ est impair,

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

Exemple. $a^3 - b^3 = (a-b)(a^2+ab+b^2)$.

Somme géométrique : Soit $r \in \mathbb{C}$. Une suite (u_n) de complexes est géométrique de raison r si et seulement si elle vérifie la relation de récurrence suivante :
$\forall n \in \mathbb{N},\ u_{n+1} = ru_n$. Par récurrence, on montre que pour tout $n \in \mathbb{N}$, $u_n = u_0 r^n$.
Soit $m, n \in \mathbb{N}$ avec $m \leq n$ et soit (u_n) une suite géométrique de raison r avec $r \neq 1$. Alors

$$\sum_{k=m}^{n} u_k = \frac{u_{n+1} - u_m}{r-1},$$

ce que l'on retient de la manière suivante : une somme géométrique est égale au terme suivant le dernier moins le premier terme divisé par la raison privée de 1.

Remarque. On a déjà rencontré et démontré ce résultat page 99, mais il est à ce point important qu'il mériterait d'apparaître même une dizaine de fois.

Démonstration.
C'est un cas particulier de la formule de Bernoulli :
$u_{n+1}-u_m = u_0(r^{n+1}-r^m) = u_0 r^m(r^{n+1-m}-1) = u_0 r^m(r-1)\sum_{k=0}^{n-m} r^k = (r-1)\sum_{k=0}^{n-m} u_{m+k}$.
□

Exemple. Soit $n \in \mathbb{N}^*$. Soit ω une racine n-ième différente de 1.
Alors $\sum_{k=0}^{n-1} \omega^k = \frac{\omega^n - 1}{\omega - 1} = 0$.

Ainsi, pour tout $h \in \{1, \dots, n-1\}$, $\sum_{k=0}^{n-1} e^{2i\pi\frac{hk}{n}} = 0$.

9.7.5 Sommes doubles

Soit $m, n, p, q \in \mathbb{N}$ avec $m \leq n$ et $p \leq q$.
Soit $(u_{k,\ell})_{(k,\ell)\in\{m,\dots,n\}\times\{p,\dots,q\}}$ une famille d'éléments d'un monoïde commutatif $(G, +)$.
On peut partitionner $A = \{m, \dots, n\} \times \{p, \dots, q\}$ en la famille $(A_i)_{m\leq i\leq n}$,
où $A_i = \{(i, \ell)/l \in \{p, \dots, q\}\}$. Ainsi,
$\sum_{(k,\ell)\in A} u_{k,\ell} = \sum_{i=m}^{n} \sum_{(k,\ell)\in A_i} u_{k,\ell}$. De plus , pour tout $i \in \{m, \dots, n\}$,
l'application $\begin{array}{rccc} \varphi : & \{p, \dots, q\} & \longrightarrow & A_i \\ & \ell & \longmapsto & (i, \ell) \end{array}$ est une bijection, donc on peut poser dans la somme interne, $(k, \ell) = \varphi(\ell')$. Ainsi, $\sum_{(k,\ell)\in A} u_{k,\ell} = \sum_{i=m}^{n}\sum_{\ell'=p}^{q} u_{i,\ell'} = \sum_{k=m}^{n}\sum_{\ell=p}^{q} u_{k,\ell}$, en renommant les indices.
À la place de $\sum_{(k,\ell)\in A} u_{k,\ell}$, on note souvent $\sum_{\substack{m\leq k\leq n \\ p\leq\ell\leq q}} u_{k,\ell}$.
De plus, on peut aussi considérer la partition de A selon la famille $(B_\ell)_{p\leq\ell\leq q}$,
où $B_\ell = \{(k, \ell)/m \leq k \leq n\}$. Ainsi, on a montré que

$$\sum_{\substack{m\leq k\leq n \\ p\leq\ell\leq q}} u_{k,\ell} = \sum_{k=m}^{n}\sum_{\ell=p}^{q} u_{k,\ell} = \sum_{\ell=p}^{q}\sum_{k=m}^{n} u_{k,\ell}.$$

Exemple. $\sum_{\substack{1\leq k\leq n \\ 1\leq\ell\leq q}} (k + l) = \sum_{k=1}^{n}\Big(\sum_{\ell=1}^{q} k + \sum_{\ell=1}^{q} \ell\Big) = \sum_{k=1}^{n}\Big(kq + \frac{q(q+1)}{2}\Big)$,
donc $\sum_{\substack{1\leq k\leq n \\ 1\leq\ell\leq q}} (k + l) = q\frac{n(n+1)}{2} + n\frac{q(q+1)}{2}$.

Propriété. Avec les notations précédentes, on suppose de plus que $(G,+,\times)$ est un anneau et que, pour tout $(k,\ell)\in A$, $u_{k,\ell}=v_kw_\ell$, où $v_k,w_\ell\in G$. Alors

$$\sum_{\substack{m\leq k\leq n\\ p\leq \ell\leq q}} v_kw_\ell=\Big(\sum_{k=m}^{n}v_k\Big)\Big(\sum_{\ell=p}^{q}w_\ell\Big).$$

Démonstration.
$\sum_{\substack{m\leq k\leq n\\ p\leq \ell\leq q}} v_kw_\ell=\sum_{k=m}^{n}\sum_{\ell=p}^{q}v_kw_\ell=\sum_{k=m}^{n}v_k\Big(\sum_{\ell=p}^{q}w_\ell\Big)$. Notons $S=\sum_{\ell=p}^{q}w_\ell$.
Ainsi, $\sum_{\substack{m\leq k\leq n\\ p\leq \ell\leq q}} v_kw_\ell=\sum_{k=m}^{n}(v_kS)=\Big(\sum_{k=m}^{n}v_k\Big)S$. □

9.7.6 Sommes triangulaires

Soit $m,n\in\mathbb{N}$ avec $m\leq n$. Notons $T=\{(k,\ell)/m\leq k\leq\ell\leq n\}$. Si l'on représente T dans le plan $\mathbb{R}^2$, on obtient bien un triangle.
Soit $(u_{k,\ell})_{(k,\ell)\in T}$ une famille d'éléments d'un monoïde commutatif $(G,+)$.
Notons $T'=\{m,\dots,n\}^2\setminus T$ et prolongeons la famille $(u_{k,\ell})$ sur T' en convenant que, pour tout $(k,\ell)\in T'$, $u_{k,\ell}=0_G$. $\{T,T'\}$ étant une partition de $\{m,\dots,n\}^2$, on a
$\sum_{\substack{m\leq k\leq n\\ m\leq \ell\leq n}} u_{k,\ell}=\sum_{(k,\ell)\in T}u_{k,\ell}+\sum_{(k,\ell)\in T'}u_{k,\ell}=\sum_{(k,\ell)\in T}u_{k,\ell}$.
Ainsi, la somme triangulaire $\sum_{(k,\ell)\in T}u_{k,\ell}$ peut être vue comme une somme double en ajoutant des "0". D'après le paragraphe précédent,
$\sum_{(k,\ell)\in T}u_{k,\ell}=\sum_{k=m}^{n}\sum_{\ell=m}^{n}u_{k,\ell}=\sum_{k=m}^{n}\sum_{\ell=k}^{n}u_{k,\ell}$. Le plus souvent, la somme triangulaire est notée $\sum_{m\leq k\leq\ell\leq n}u_{k,\ell}$, ce qui rend la formule précédente naturelle. De même, on peut montrer que $\sum_{m\leq k\leq\ell\leq n}u_{k,\ell}=\sum_{\ell=m}^{n}\sum_{k=m}^{\ell}u_{k,\ell}$.
De même, on a $\sum_{m\leq k<\ell\leq n}u_{k,\ell}=\sum_{k=m}^{n}\sum_{\ell=k+1}^{n}u_{k,\ell}=\sum_{\ell=m}^{n}\sum_{k=m}^{\ell-1}u_{k,\ell}$.

Exemple.
◇ Soit $n\in\mathbb{N}^*$ et $(u_k)_{1\leq k\leq n}$ une famille de réels. D'après la fin du paragraphe précédent, $\Big(\sum_{k=1}^{n}u_k\Big)^2=\sum_{\substack{1\leq k\leq n\\ 1\leq \ell\leq n}}u_ku_\ell$, donc d'après le principe de sommation par paquets,
$\Big(\sum_{k=1}^{n}u_k\Big)^2=\sum_{k=1}^{n}u_k^2+2\sum_{1\leq k<\ell\leq n}u_ku_\ell$.

◇ Notons $S = \sum_{1\leq k<\ell\leq n} \frac{k}{l}$. Ainsi, $S = \sum_{k=1}^{n} k \sum_{\ell=k+1}^{n} \frac{1}{\ell}$, mais pour simplifier S, il est indispensable d'intervertir les deux variables :
$S = \sum_{\ell=1}^{n} \frac{1}{\ell} \sum_{k=1}^{\ell-1} k = \sum_{\ell=1}^{n} \frac{1}{\ell} \frac{\ell(\ell-1)}{2} = \frac{1}{2} \sum_{\ell=1}^{n} (\ell-1) = \frac{n(n-1)}{4}$.

9.7.7 Produits

Toutes les propriétés précédentes, lorsqu'elles étaient valables dans un monoïde commutatif $(G,+)$ sont bien sûr valables en notation multiplicative dans un monoïde commutatif $(G,\times)$, car il ne s'agit que d'un changement de notation de la loi utilisée.
Par exemple, on peut énoncer une propriété de produit par paquets : Soit A un ensemble fini et $(x_a)_{a\in A}$ une famille d'éléments d'un monoïde commutatif $(G,\times)$. Soit $n \in \mathbb{N}$. On suppose qu'il existe des parties $A_1, \ldots, A_n$ de A telles que $A = \bigsqcup_{i=1}^{n} A_i$.

Alors $\prod_{a\in A} x_a = \prod_{i=1}^{n} \prod_{a\in A_i} x_a$.

Soit $m, n \in \mathbb{N}$ avec $m \leq n$ et soit $(u_k)_{m\leq k\leq n}$ une famille de réels strictement positifs. Alors $\prod_{k=m}^{n} u_k = \exp\Big(\sum_{k=m}^{n} \ln u_k\Big)$, ce qui permet dans certains cas de ramener l'étude d'un produit à celle d'une somme.

Exemple. Soit $m, n \in \mathbb{N}$ avec $m \leq n$ et soit $(u_k)_{m\leq k\leq n}$ une famille de complexes. Soit $\lambda \in \mathbb{C}$. Alors $\prod_{k=m}^{n} (\lambda u_k) = \lambda^{n-m+1} \prod_{k=m}^{n} u_k$.

Exemple. $\prod_{k=1}^{n} 2k^2(k+1) = 2^n (n!)^2 (n+1)!$.

Exemple. Calcul de $\prod_{\substack{0\leq k\leq 2n \\ k\neq n}} (-1)^k (n-k)$:

$\prod_{\substack{0\leq k\leq 2n \\ k\neq n}} (-1)^k (n-k) = \Big(\prod_{k=0}^{n-1} (-1)^k (n-k)\Big)\Big(\prod_{k=n+1}^{2n} (-1)^k (n-k)\Big)$. Dans le second produit, posons $h = 2n-k$: $\prod_{k=n+1}^{2n} (-1)^k (n-k) = \prod_{h=0}^{n-1} (-1)^h (h-n)$, donc

$\prod_{\substack{0\leq k\leq 2n \\ k\neq n}} (-1)^k (n-k) = (-1)^n \Big(\prod_{k=0}^{n-1} (-1)^k (n-k)\Big)^2 = (-1)^n \prod_{k=0}^{n-1} (n-k)^2 = (-1)^n (n!)^2$.

Exemple de produit télescopique : Soit $n \in \mathbb{N}$ avec $n \geq 2$.
$\prod_{k=2}^{n}\Big(1-\frac{1}{k}\Big) = \prod_{k=2}^{n}\frac{k-1}{k} = \frac{1}{n}$.

9.7.8 Intégration par parties itérée

Intégration par parties itérée : (Hors programme).
Soit I un intervalle de $\mathbb{R}$, $n \in \mathbb{N}$, f et g deux applications de classe C^n de I dans $\mathbb{R}$. Alors, pour tout $a, b \in I$,

$$\int_a^b f^{(n)}(t)g(t)dt = \Big[\sum_{i=0}^{n-1} f^{(n-1-i)}(t)g^{(i)}(t)(-1)^i\Big]_a^b + (-1)^n \int_a^b f(t)g^{(n)}(t)dt.$$

Formule de Taylor avec reste intégral :
Soit I un intervalle de $\mathbb{R}$, $n \in \mathbb{N}$, f une application de classe C^{n+1} de I dans $\mathbb{R}$. Alors, pour tout $a, b \in I$,

$$f(b) = f(a) + \sum_{k=1}^{n} \frac{(b-a)^k}{k!} f^{(k)}(a) + \int_a^b \frac{(b-t)^n}{n!} f^{(n+1)}(t)dt.$$

Calcul de $\lim_{x\to+\infty} \int_0^x t^n e^{-t}dt$ à l'aide de la formule de Taylor avec reste intégral :
Fixons $x \in \mathbb{R}_+^*$ et $n \in \mathbb{N}$. Notons $a_n = \int_0^x t^n e^{-t}dt$.
Le reste intégral de la formule de Taylor s'écrit $\int_a^b \frac{(b-t)^n}{n!} f^{(n+1)}(t)dt$.
On peut mettre a_n sous cette forme :
$a_n = n! \int_x^0 \frac{(0-t)^n}{n!}(-1)^{n+1}e^{-t}dt = n! \int_x^0 \frac{(0-t)^n}{n!} f^{(n+1)}(t)dt$, en posant $f(t) = e^{-t}$.
La formule de Taylor avec reste intégral donne alors :
$a_n = n!\Big(f(0) - \sum_{k=0}^{n} \frac{f^{(k)}(x)}{k!}(0-x)^k\Big) = n!\Big(1 - \sum_{k=0}^{n} \frac{x^k}{k!}e^{-x}\Big)$.
En conservant l'entier n fixé, on fait maintenant tendre x vers $+\infty$. D'après les propriétés de "croissances comparées", pour tout $k \in \{0, \ldots, n\}$, $x^k e^{-x} \underset{x\to+\infty}{\longrightarrow} 0$, donc $\int_0^x t^n e^{-t}dt \underset{x\to+\infty}{\longrightarrow} n!$.
Cela signifie que $\int_0^{+\infty} t^n e^{-t}dt$ est définie et que $\int_0^{+\infty} t^n e^{-t}dt = n!$.

Exemple d'application :
Sous les hypothèses et notations de la formule précédente, fixons $a, b \in I$ avec $a \leq b$.
Soit $m, M \in \mathbb{R}$ tels que , pour tout $t \in [a, b]$, $m \leq f^{(n+1)}(t) \leq M$.

Alors $m\frac{(b-a)^{n+1}}{(n+1)!} \leq f(b) - \sum_{k=0}^{n} \frac{(b-a)^k}{k!} f^{(k)}(a) \leq M\frac{(b-a)^{n+1}}{(n+1)!}$.

Inégalité de Taylor-Lagrange :
Soit $a, b \in \mathbb{R}$ avec $a \neq b$. On se place sur $I = [\min(a,b), \max(a,b)]$.
Soit $n \in \mathbb{N}$ et f une application de classe C^{n+1} de I dans $\mathbb{R}$.
Soit $M \in \mathbb{R}$ tel que, pour tout $t \in I$, $|f^{(n+1)}(t)| \leq M$. Alors

$$\left| f(b) - f(a) - \sum_{k=1}^{n} \frac{(b-a)^k}{k!} f^{(k)}(a) \right| \leq M\frac{|b-a|^{n+1}}{(n+1)!}.$$

Passage de la formule de Taylor-Lagrange à celle de Taylor-Young :
Ici, n est fixé dans $\mathbb{N}$.
On suppose que f est une application de classe C^{n+1} de $[a,b]$ dans $\mathbb{R}$, avec $a < 0 < b$, de sorte que f soit définie et C^{n+1} au "voisinage de 0".
On montrera plus tard que toute application continue sur un segment (i.e : un intervalle de la forme $[c,d]$ avec $c, d \in \mathbb{R}$ et $c < d$) est bornée. C'est donc le cas ici pour l'application $f^{(n+1)}$ sur le segment $[a,b]$: il existe $M \in \mathbb{R}$ tel que, pour tout $x \in [a,b]$, $|f^{(n+1)}(x)| \leq M$.
Soit $t \in [a,b]$ avec $t \neq 0$. On peut alors appliquer l'inégalité de Taylor-Lagrange à f entre 0 et t :
$\left| f(t) - \sum_{k=0}^{n} \frac{f^{(k)}(0)}{k!} t^k \right| \leq \frac{M}{(n+1)!}|t|^{n+1}$, donc si l'on pose $\varepsilon(t) = \frac{1}{t^n}\Big(f(t) - \sum_{k=0}^{n} \frac{t^k}{k!} f^{(k)}(0)\Big)$, alors $|\varepsilon(t)| \leq M\frac{|t|}{(n+1)!}$. Ceci est vrai pour tout $t \in [a,b] \setminus \{0\}$.

Faisons maintenant tendre t vers 0 : $M\frac{|t|}{(n+1)!} \underset{t\to 0}{\longrightarrow} 0$, donc d'après le principe des gendarmes, $\varepsilon(t) \underset{t\to 0}{\longrightarrow} 0$.

On a donc montré que $f(t) = \sum_{k=0}^{n} \frac{f^{(k)}(0)}{k!} t^k + t^n\varepsilon(t)$, où $\varepsilon(t) \underset{t\to 0}{\longrightarrow} 0$, ce que l'on peut écrire sous la forme $f(t) = f(0) + a_1 t + a_2 t^2 + \cdots + a_n t^n + t^n\varepsilon(t)$, en posant $a_k = \frac{f^{(k)}(0)}{k!}$.
Dans le membre de droite de cette égalité, chaque terme $a_k t^k$ est prépondérant devant le terme suivant $a_{k+1}t^{k+1}$, en ce sens que le quotient de $a_{k+1}t^{k+1}$ par t^k tend vers 0 lorsque t tend vers 0. De même, le terme $a_n t^n$ est prépondérant devant le "reste" $t^n\varepsilon(t)$.
Il s'agit d'un *développement limité* de la quantité $f(t)$ au voisinage de 0, où chaque nouveau terme apporte une précision supplémentaire à la valeur de $f(t)$.
C'est la formule de Taylor-Young.