Les nombres

Table des matières

1 $\mathbb{Z}$

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.
$\diamond$ 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).
$\diamond$ 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) : $c+d'=d+c'$.
Alors $(ac+bd,ad+bc)\ R\ (a'c+b'd,a'd+b'c)$, car
$ac+bd+a'd+b'c=(a+b')c+(b+a')d=(a'+b)c+(a+b')d=ad+bc+a'c+b'd$,
et $(a'c+b'd,a'd+b'c)\ R\ (a'c'+b'd',a'd'+b'c')$, car
$a'c+b'd+a'd'+b'c'=a'(c+d')+b'(d+c')=a'(c'+d)+b'(d'+c)=a'd+b'c+a'c'+b'd'$,
puis l'on conclut par transitivité de R. $\square$

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 $m=m+0=m+(m'+n)=(m+n)+m'=0+m'=m'$.
$\square$

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

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 $n, m \in \mathbb{N}$: $f(n) \leq f(m) \iff \overline{(n,0)} \leq \overline{(m,0)} \iff n \leq m$, 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. □

Définition. Lorsque $n, m \in \mathbb{Z}$, on pose $n - m = n + (-m)$.

Remarque. Ainsi, pour tout $a, b \in \mathbb{N}$,
$\overline{(a,b)} = \overline{(a,0)} + \overline{(0,b)} = \overline{(a,0)} - \overline{(b,0)} = f(a) - f(b) = a - b$, après identification.
Donc $\mathbb{Z} = \{a - b \ / \ a, b \in \mathbb{N}\}$.

Compatibilité de "$-_{\mathbb{N}}$" et de "$-_{\mathbb{Z}}$" : 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 :

— $\forall n \in \mathbb{Z},\ n \geq 0 \iff n \in \mathbb{N}$.
— $\forall n, m \in \mathbb{Z},\ \ ([n \geq 0] \wedge [m \geq 0]) \implies nm \geq 0$.
— $\forall n \in \mathbb{Z},\ \ n \geq 0 \iff -n \leq 0$. Ainsi, $\mathbb{Z} = \mathbb{N} \sqcup (-\mathbb{N}^*)$.
— $\forall x, y, a \in \mathbb{Z},\ \begin{cases} \text{si } a \geq 0,\ \ x \leq y \implies ax \leq ay, \\ \text{si } a \leq 0,\ \ x \leq y \implies ax \geq ay. \end{cases}$

Démonstration.
◇ Soit $n \in \mathbb{Z}$.
Si $n \in \mathbb{N}$, alors $n = f(n) \geq f(0) = 0$, car f est croissante et 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, $n \geq 0 \iff n \in \mathbb{N}$.
◇ 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 $n = \overline{(a,b)} \in \mathbb{Z}$. $n \geq 0 \iff b \leq a$.
Par ailleurs, $-n = \overline{(b,a)}$ donc $-n \leq 0 \iff b \leq a$. Ainsi, $n \geq 0 \iff -n \leq 0$.
◇ 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. □

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 $n \in \mathbb{Z}$, $n\mathbb{Z} \stackrel{\Delta}{=} \{nx / x \in \mathbb{Z}\}$ 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 $g \in G$, $g\mathbb{Z} \subset G$.

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 non vide de sous-groupes de $\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

Démonstration.
Soit $(G_k)_{k\in K}$ une famille non vide 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. □

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.
$1 \implies 2$ résulte de la propriété précédente.
$2 \implies 3$, car si q est un nombre premier différent de p, alors p ne divise pas q.
$3 \implies 1$: 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 $1 \iff 3$ 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. □

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

Petit théorème de Fermat : (Admis pour le moment) Si $p \in \mathbb{P}$ et $a \in \mathbb{Z}$,
$(a \not\equiv 0\ [p]) \Longrightarrow a^{p-1} \equiv 1\ [p]$, donc dans tous les cas, $a^p \equiv a\ [p]$.

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 $\mathbb{R}/(\equiv [2\pi])$.

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 $\mathcal{D} = \{k \in \mathbb{N} \ / \ (k|a) \text{ et } (k|b)\}$. $\mathcal{D}$ est non vide et est majoré par $\max(a,b)$, donc on peut poser $d' = \max_{\leq}(\mathcal{D})$. 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

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

□

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 $\mathbb{N}$, $a \vee b = \sup_{|}\{|a|, |b|\}$.
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 $m\mathbb{Z} = (m' \vee m'')\mathbb{Z}$.
$\diamond$ 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, $m'\mathbb{Z} = \alpha(a_1\mathbb{Z} \cap \cdots \cap a_k\mathbb{Z}) = \alpha(m\mathbb{Z}) = (\alpha m)\mathbb{Z}$. □

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 $b = b'd$.
$d = a \wedge b = (a'd) \wedge (b'd) = (a' \wedge b')d$.
Si $d \neq 0$, on en déduit que $a' \wedge b' = 1$, ce qu'il fallait démontrer.
Si $d = 0$ alors $a = b = 0$ et 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 $n = \prod_{p\in\mathbb{P}} p^{\nu_p} = \prod_{p\in\mathbb{P}} p^{\eta_p}$.
Il existe $q \in \mathbb{P}$ tel que $\nu_q \neq \eta_q$. Alors $q^{\nu_q} \prod_{\substack{p\in\mathbb{P}\\p\neq q}} p^{\nu_p} = q^{\eta_q} \prod_{\substack{p\in\mathbb{P}\\p\neq q}} p^{\eta_p}$.
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 $\prod_{\substack{p\in\mathbb{P}\\p\neq q}} p^{\nu_p} = q^{\alpha} \prod_{\substack{p\in\mathbb{P}\\p\neq q}} p^{\eta_p}$. Alors $q \mid \prod_{\substack{p\in\mathbb{P}\\p\neq q}} p^{\nu_p}$, mais q est premier avec tout $p \in \mathbb{P}$ tel que $p \neq q$, donc q est premier avec $\prod_{\substack{p\in\mathbb{P}\\p\neq q}} p^{\nu_p}$, 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 :

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

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 $a \vee b = \dfrac{ab}{a \wedge b}$. $\square$

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 $(a, b) \in \mathbb{N}^2$ 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, dans $\mathbb{N}$, $a \wedge b = \max_{|}(D) = b \wedge r$. $\square$

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 $i \in \{0, \dots, N-1\}$, $a_0 \wedge a_1 = a_i \wedge a_{i+1}$.
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 $i \in \{1, \dots, N-3\}$, 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.

— 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, $2 = 6 - 4 = 6 - (70 - 6 * 11) = -70 + 6 * 12$.

— 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 vérifie 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 $\{(1 + k, 1 - 4k) \ / \ k \in \mathbb{Z}\}$.

2 Construction de $\mathbb{Q}$

On peut vérifier les affirmations qui suivent :

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 $x, y \in \mathbb{Q}$, $xy = 0 \implies [(x = 0) \vee (y = 0)]$.

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

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 $x \in \mathbb{Q}$.
$\diamond$ *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.

$\diamond$ *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 $x < ny$. □

3 L'ensemble $\mathbb{R}$ des réels

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.

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 $\sup(B)$. □

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 22 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, $x \leq y \Longrightarrow x.x \leq y.x \leq y.y$ et $x > y \Longrightarrow x.x > y.x > y.y$.
$\diamond$ Supposons que $a^2 > 2$. Soit $\varepsilon \in \mathbb{Q}_+^*$.

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

Ainsi, si l'on pose $\varepsilon = \dfrac{a^2-2}{4a}$, on a $\varepsilon \in \mathbb{Q}_+^*$ et $(a-\varepsilon)^2 > 2$ $\quad (1 \in A$, donc $a \geq 1)$.
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 $\varepsilon \in \mathbb{Q}_+^*$.

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

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 $x \in A \Longrightarrow x \leq 2$.
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 f de K dans K' telle que f est un morphisme de corps ordonnés, c'est-à-dire :
- $\forall x, y \in K,\ x \leq y \Longrightarrow f(x) \leq f(y)$,
- $\forall x, y \in K,\ f(x+y) = f(x) + f(y)$,
- $\forall x, y \in K,\ f(xy) = f(x)f(y)$,

— $f(1_K) = 1_{K'}$.

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'addition, $x + z \leq y + z$, 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
$m = \inf(A) \iff [\forall a \in A,\ \ a \geq m] \wedge [\forall \varepsilon > 0,\ \ \exists a \in A,\ \ m + \varepsilon > a]$.

3.4 La droite réelle achevée

Définition. On appelle droite réelle achevée l'ensemble $\overline{\mathbb{R}} \triangleq \mathbb{R} \cup \{-\infty, +\infty\}$, 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 $\sup(A) = \max(A) = +\infty$.

$\diamond$ Supposons que $-\infty \in A$. Si $A = \{-\infty\}$, alors $\sup(A) = -\infty$. Sinon, A possède le même ensemble de majorants que $A \setminus \{-\infty\}$, ce qui nous ramène aux cas précédents. $\square$

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

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.
Soit I une partie quelconque de $\mathbb{R}$. Il s'agit de montrer que I est convexe si et seulement si I est un intervalle. 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 $x \in I$. □

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 $[a, b] \subset J$. □

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 d'après la propriété du début de la page 27, $-y \geq 0$, puis $x(-y) \geq 0$. En utilisant à nouveau la même propriété, $xy \leq 0$.
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 $B_o(a,\varepsilon)$.

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. $\mathbb{R}\setminus\mathbb{Q}$ 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 25 : 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 22, $\sqrt{2}$ 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 A une partie de $\mathbb{R}$. On dit que A est dense dans $\mathbb{R}$ si et seulement si pour tout $x, y \in \mathbb{R}$ avec $x < y$, il existe $a \in A$ tel que $x \leq a \leq y$.

Propriété. A est dense dans $\mathbb{R}$ si et seulement si, pour tout $x \in \mathbb{R}$, il existe une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de A telle que $a_n \underset{n\to+\infty}{\longrightarrow} x$.

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.

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 $(a_0, \dots, a_{p-1}) \in \{0, \dots, 9\}^p$. Alors $\sum_{k=0}^{p-1} a_k 10^k < 10^p$.

Démonstration.
Soit $p \in \mathbb{N}$. $\sum_{k=0}^{p-1} a_k 10^k \leq \sum_{k=0}^{p-1} 9.10^k = 9\frac{10^p - 1}{10 - 1} = 10^p - 1 < 10^p$. □

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

Théorème. Pour tout $n \in \mathbb{N}$, il existe un unique $p \in \mathbb{N}$ et un unique p-uplet $(a_0, \dots, a_{p-1}) \in \{0, \dots, 9\}^p$ 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 $(a_k)_{k\in\mathbb{N}} \in \{0, \dots, 9\}^{(\mathbb{N})}$ 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 $(a_h)_{h\in\mathbb{N}} \in \{0, \dots, 9\}^{(\mathbb{N})}$ telle que $n = \sum_{h\in\mathbb{N}} a_h 10^h$.

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

• *Synthèse :* Pour tout $k \in \mathbb{N}$, posons $a_k = \left\lfloor \frac{n}{10^k} \right\rfloor - 10 \left\lfloor \frac{n}{10^{k+1}} \right\rfloor$. 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 $\left\lfloor \frac{n}{10^k} \right\rfloor = 0$, donc lorsque $k \geq p+1$, $a_k = 0$.
Ceci prouve que la suite (a_k) est presque nulle.

◇ 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 $k \in \mathbb{N}$, $a_k \in \{0, \ldots, 9\}$.

◇ $\sum_{k\in\mathbb{N}} a_k 10^k = \sum_{k\in\mathbb{N}} \left(10^k \left\lfloor \frac{n}{10^k} \right\rfloor - 10^{k+1} \left\lfloor \frac{n}{10^{k+1}} \right\rfloor \right) = \sum_{k\in\mathbb{N}} 10^k \left\lfloor \frac{n}{10^k} \right\rfloor - \sum_{k\geq 1} 10^k \left\lfloor \frac{n}{10^k} \right\rfloor = n.$

□

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].

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 $p \in \mathbb{Z} \setminus (2\mathbb{Z} \cup 5\mathbb{Z})$ 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 $m = \max\{h, k\}$,

$x = \dfrac{n}{10^m}$ où $n = p2^{m-h}5^{m-k}$, donc $x \in \mathbb{D}$.
Réciproquement, si $x \in \mathbb{D}$, il existe $n \in \mathbb{Z}$ et $k \in \mathbb{N}$ tels que $x = \dfrac{n}{10^k}$.

Si $n = 0$, la propriété est vraie. Sinon, la forme irréductible de x est $x = \dfrac{\frac{n}{d}}{\frac{10^k}{d}}$, où $d = n \wedge 10^k$. d divise 10^k, donc d est de la forme 2^a5^b, ce qui permet de conclure. □

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

Remarque. $\mathbb{D}$ est un sous-anneau de $\mathbb{Q}$.

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 $d = \displaystyle\sum_{k\in\mathbb{Z}} a_k 10^k$.

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 $d = a_M \cdots a_0\ ,\ \overline{a_{-1}\cdots a_m}$.

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 $\mathbb{R}$.

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 $x_n = \sum_{k=1}^{n} v_k a^{-k}$.
La suite (x_n) est croissante et majorée, donc elle converge vers une limite x que l'on notera $x = \sum_{n=1}^{+\infty} v_n a^{-n}$. 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.
$x_n \leq \sum_{k=1}^{n} (a-1)a^{-k} = \sum_{k=0}^{n-1} a^{-k} - \sum_{k=1}^{n} a^{-k} = 1 - a^{-n}$.
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 $N \geq 0$,
$\sum_{n=N+1}^{+\infty} (a-1)a^{-n} = \lim_{K\to+\infty} \sum_{n=N+1}^{K} (a-1)a^{-n} = a^{-N} \lim_{K\to+\infty} \sum_{n=1}^{K-N} (a-1)a^{-n} = a^{-N}$.
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 $\displaystyle\sum_{h=1}^{k} v_h a^{k-h}$ (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 d'après le principe des tiroirs, 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.