Chapitre 5 : Ensembles de nombres

Table des matières

1 Nombres réels et inégalités **2**
1.1 Inégalités dans $\mathbb{R}$ . . . 2
1.2 Majorant et minorant . . . 2
1.3 Maximum et minimum . . . 3
1.4 Borne supérieure et inférieure d'une partie de $\mathbb{R}$ . . . 3
1.5 Intervalles de $\mathbb{R}$ . . . 4
1.6 Valeur absolue . . . 5
1.7 Partie entière . . . 6

2 Nombres entiers et arithmétique **7**
2.1 Axiomatique des entiers . . . 7
2.2 Relation de divisibilité . . . 7
2.3 Division euclidienne . . . 7
2.4 Nombres premiers . . . 8
2.5 PGCD de deux entiers . . . 9
2.6 Calcul du PGCD de deux entiers . . . 10
2.7 PPCM . . . 10

L'étude et surtout l'utilisation des nombres ont jalonné l'histoire de l'humanité. Les premières traces de manipulation d'entiers ont été retrouvé sur les os d'Ishango datant de plus de 20000 ans ; alors que la construction des réels a été élaborée simultanément par Méray et Dedekin au XIXe siècle. Ce chapitre est composé de deux parties distinctes, la première porte sur les nombres réels alors que la seconde traite les nombres entiers.
La partie sur l'arithmétique des nombres entiers s'inspire fidèlement des livres VII et IX du plus connus des recueils en mathématiques : *Les Éléments*. Ce dernier est un traité mathématique et géométrique, constitué de 13 livres organisés thématiquement, probablement écrit par le mathématicien grec Euclide. Les Éléments furent l'un des premiers ouvrages imprimés (Venise, 1482) et n'est surpassé que par la Bible pour le nombre d'éditions publiées.

Euclide
IIIe siècle av. J.-C.

1 Nombres réels et inégalités

On admet l'existence de l'ensemble des nombres réels, que l'on note $\mathbb{R}$. On rappelle que $\mathbb{R}$ est muni d'une addition et d'une multiplication vérifiant des propriétés particulières (on dit que $(\mathbb{R}, +, \times)$ est un corps).

1.1 Inégalités dans $\mathbb{R}$

Définition 1.1 (relation de comparaison $\leqslant$)

Soient des réels x et y. La relation $\leqslant$ sur $\mathbb{R}$ est définie par $x \leqslant y \iff y - x \in \mathbb{R}_+$.

Remarque : Les relations $<$, $\geqslant$ et $>$ sont définies de manière analogue.

Proposition 1.2 (propriétés élémentaires des relations de comparaison)

Soient des réels x, y et a.

1. Si $x \leqslant y$, alors $x + a \leqslant y + a$.
   Si $x < y$, alors $x + a < y + a$.
2. Si $x \leqslant y$ et $a \geqslant 0$, alors $ax \leqslant ay$. Si $x \leqslant y$ et $a \leqslant 0$, alors $ax \geqslant ay$.
   Si $x < y$ et $a > 0$, alors $ax < ay$. Si $x < y$ et $a < 0$, alors $ax > ay$.

Corollaire 1.3 (compatibilité de la relation d'ordre avec les opérations)

Soient des réels x_1, x_2, y_1 et y_2.

1. Si $x_1 \leqslant y_1$ et $x_2 \leqslant y_2$, alors $x_1 + x_2 \leqslant y_1 + y_2$.
   Si $x_1 < y_1$ et $x_2 \leqslant y_2$, alors $x_1 + x_2 < y_1 + y_2$.
2. Si $0 \leqslant x_1 \leqslant y_1$ et $0 \leqslant x_2 \leqslant y_2$, alors $x_1 x_2 \leqslant y_1 y_2$.
   Si $0 < x_1 < y_1$ et $0 < x_2 \leqslant y_2$, alors $x_1 x_2 < y_1 y_2$.

Remarque : Pour les quotients, on se ramène au produit par un inverse en utilisant la stricte décroissance de la fonction inverse sur $\mathbb{R}_+^*$: $0 < x \leqslant y \Leftrightarrow 0 < \frac{1}{y} \leqslant \frac{1}{x}$ et $0 < x < y \Leftrightarrow 0 < \frac{1}{y} < \frac{1}{x}$.

Méthode :

- *Pour majorer/minorer une somme, on peut majorer/minorer chacun des termes de la somme.*
- *Pour majorer/minorer un produit, on peut majorer/minorer chacun des termes du produit selon le signe.*
- *Pour majorer un quotient, il faut majorer le numérateur et minorer le dénominateur.*
- *Pour minorer un quotient, il faut minorer le numérateur et majorer le dénominateur.*

Exemple 1.4 : Soit $n \in \mathbb{N}^*$. Montrer que $\dfrac{1}{2} \leqslant \displaystyle\sum_{k=n+1}^{2n} \frac{1}{k} < 1$ et que $2 \leqslant \displaystyle\sum_{k=0}^{n} \frac{1}{k!} \leqslant 3$.

Exemple 1.5 : Soient x,$y \in \mathbb{R}$ tels que $-1 \leqslant x \leqslant 2$ et $1 < y \leqslant 4$, encadrer $\dfrac{x + 2y}{(x+2)y}$.

1.2 Majorant et minorant

Définition 1.6 (majorant et minorant d'une partie de $\mathbb{R}$)

Soit A une partie de $\mathbb{R}$.

- Un majorant de A est un réel M tel que : $\forall x \in A$, $x \leqslant M$.
- Un minorant de A est un réel m tel que : $\forall x \in A$, $m \leqslant x$.

Remarque : Dans cette définition, on ne demande pas que le majorant ou le minorant soit dans la partie A.

Définition 1.7 (partie majorée, minorée, bornée)

Soit A une partie de $\mathbb{R}$. On dit que A est :
- majorée s'il existe un majorant de A, *i.e.*
- minorée s'il existe un minorant de A, *i.e.*
- bornée si elle est à la fois majorée et minorée, *i.e.*

Exemple 1.8 : Soit $A = \left\{\frac{1}{n}, n \in \mathbb{N}^*\right\}$. Montrer que A est bornée.

1.3 Maximum et minimum

Définition 1.9 (minimum et maximum d'une partie de $\mathbb{R}$)

Soit A une partie de $\mathbb{R}$.
- Un maximum de A (ou plus grand élément de A) est un majorant de A qui est dans A, *i.e.* un élément $M \in A$ tel que : $\forall x \in A,\ x \leqslant M$.
- Un minimum de A (ou plus petit élément de A) est un minorant de A qui est dans A, *i.e.* un élément $m \in A$ tel que : $\forall x \in A,\ m \leqslant x$.

Remarques :
1. Une partie qui admet un maximum ou un minimum est forcément non vide.
2. Si un maximum ou un minimum existe pour une partie $A \subset \mathbb{R}$, il est unique. Le maximum de A est noté $\max(A)$; le minimum de A est noté $\min(A)$.
3. Toute partie finie et non vide de $\mathbb{R}$ admet un maximum et un minimum.
   Pour $A = \{x_1, \cdots, x_n\}$, son maximum est noté $\max(x_1, \cdots, x_n)$ ou $\max\limits_{1 \leqslant i \leqslant n}(x_i)$, et son minimum est noté $\min(x_1, \cdots, x_n)$ ou $\min\limits_{1 \leqslant i \leqslant n}(x_i)$.

Exemple 1.10 : Soit $A = \left\{\dfrac{1}{n}, n \in \mathbb{N}^*\right\}$. Alors A admet un maximum mais n'admet pas de minimum.

1.4 Borne supérieure et inférieure d'une partie de $\mathbb{R}$

Axiome 1.11 (propriété de la borne supérieure / inférieure)

1. Soit A une partie de $\mathbb{R}$ **non vide** et **majorée**.
   L'ensemble des majorants de A admet un plus petit élément M, appelé borne supérieure de A.
2. Soit A une partie de $\mathbb{R}$ **non vide** et **minorée**.
   L'ensemble des minorants de A admet un plus grand élément m, appelé borne inférieure de A.

Notation :
- La borne supérieure de A (lorsqu'elle existe) est notée $\sup(A)$, et la borne inférieure $\inf(A)$.
- Si A est une partie de $\mathbb{R}$ non majorée, on notera (par abus) $\sup(A) = +\infty$. De même, si A est une partie de $\mathbb{R}$ non minorée, on notera $\inf(A) = -\infty$.

Soit A une partie de $\mathbb{R}$ non vide et majorée.
Sa borne supérieure M est caractérisée par les deux propriétés suivantes :
1. M est un majorant de A, *i.e.* :
$$\forall x \in A,\ x \leqslant M.$$

2. M est le plus petit des majorants de A, ce qui revient à dire que si $M' < M$, alors M' n'est pas un majorant de A, *i.e.* :
$$\forall M' \in \mathbb{R},\ M' < M \implies \exists x \in A,\ x > M'.$$
On peut remplacer cette dernière propriété par :
$$\forall \varepsilon > 0,\ \exists x \in A,\ x > M - \varepsilon$$
(qui signifie : pour tout $\varepsilon > 0$, $M - \varepsilon$ n'est pas un majorant de A).

On a une caractérisation similaire pour la borne inférieure (lorsqu'elle existe).

Remarque :
1. Si $A \subset \mathbb{R}$ admet un maximum, alors elle admet aussi une borne supérieure et $\sup(A) = \max(A)$.
2. Si $A \subset \mathbb{R}$ admet un minimum, alors elle admet aussi une borne inférieure et $\inf(A) = \min(A)$.

Exemple 1.12 : Soit $A = \left\{ \dfrac{1}{n}, n \in \mathbb{N}^* \right\}$. Déterminer la borne supérieure et la borne inférieure de A.

Remarque : Nous verrons plus tard, dans le chapitre sur les suites numériques, une caractérisation qui nous permettra de déterminer plus facilement les bornes supérieures et inférieures d'une partie de $\mathbb{R}$.

1.5 Intervalles de $\mathbb{R}$

Définition 1.13 (intervalle)

Un intervalle de $\mathbb{R}$ est une partie I de $\mathbb{R}$ telle que $\forall (c,d) \in I^2$, $\forall x \in \mathbb{R}$, $c \leqslant x \leqslant d \implies x \in I$.

Cas particuliers : L'ensemble vide et les singletons de $\mathbb{R}$ sont des intervalles.
On appelle intervalle non trivial tout intervalle qui n'est ni l'ensemble vide, ni un singleton.

Théorème 1.14 (caractérisation des intervalles)

Soit I un intervalle de $\mathbb{R}$.
L'intervalle I a l'une des formes suivantes (avec a et b deux réels) :

- $[a,b] = \{x \in \mathbb{R} \ / \ a \leqslant x \leqslant b\}$
- $]a,b[= \{x \in \mathbb{R} \ / \ a < x < b\}$
- $[a,b[= \{x \in \mathbb{R} \ / \ a \leqslant x < b\}$
- $]a,b] = \{x \in \mathbb{R} \ / \ a < x \leqslant b\}$
- $[a,+\infty[= \{x \in \mathbb{R} \ / \ a \leqslant x\}$
- $]a,+\infty[= \{x \in \mathbb{R} \ / \ a < x\}$
- $]-\infty,b] = \{x \in \mathbb{R} \ / \ x \leqslant b\}$
- $]-\infty,b[= \{x \in \mathbb{R} \ / \ x < b\}$
- $]-\infty,+\infty[= \mathbb{R}$

Un intervalle du type $[a,b]$ avec $a < b$ est appelé segment.

Un intervalle du type $]a,b[$, avec $a \in \mathbb{R} \cup \{-\infty\}$ et $b \in \mathbb{R} \cup \{+\infty\}$, est appelé intervalle ouvert.

Définition 1.15 (point intérieur d'un intervalle)

Soit I un intervalle de $\mathbb{R}$.
- On dit qu'un point $a \in I$ est un point intérieur de I s'il existe $\varepsilon > 0$ tel que $[a - \varepsilon, a + \varepsilon] \subset I$.
- L'intérieur de l'intervalle I est l'ensemble des points intérieurs de I. Il est noté $\mathring{I}$.

Exemple 1.16 : Expliciter l'intérieur de $I = [2,3[$ et de $J = [4;+\infty[$.

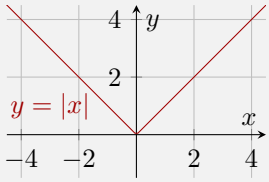
1.6 Valeur absolue

Définition 1.17 (valeur absolue d'un réel)

Soit $x \in \mathbb{R}$.
La valeur absolue de x, notée $|x|$, est définie par :

$$|x| = \max(x, -x) = \begin{cases} x & \text{si } x \geqslant 0 \\ -x & \text{si } x < 0 \end{cases}$$

On appelle valeur absolue la fonction $\begin{cases} \mathbb{R} \to \mathbb{R}_+ \\ x \mapsto |x| \end{cases}$.



Propriétés de la valeur absolue : Soient x et y deux réels.

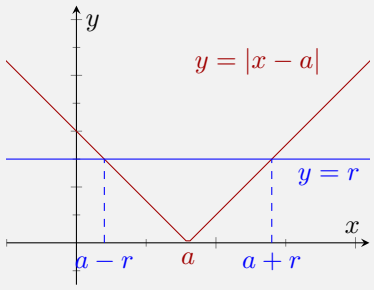
- $|-x| = |x|$
- $|x-y| = |y-x|$ (ce nombre est appelé distance de x à y)
- $x = 0 \Leftrightarrow |x| = 0$
- $x \geqslant 0 \Leftrightarrow |x| = x$; $x \leqslant 0 \Leftrightarrow |x| = -x$
- $|x| = |y| \Leftrightarrow (x = y$ ou $x = -y)$
- $\sqrt{x^2} = |x|$
- $|xy| = |x| \times |y|$
- *Inégalité triangulaire :* $|x+y| \leqslant |x| + |y|$
  Cas d'égalité : $|x+y| = |x| + |y|$ si et seulement si x et y sont de même signe.
- *Inégalité triangulaire inversée :* $\big||x| - |y|\big| \leqslant |x-y|$

Proposition 1.18 (interprétation d'inégalités avec une valeur absolue)

Soient trois réels x, a et r, avec $r \geqslant 0$.

On a les équivalences suivantes :

1. $|x-a| = r \Leftrightarrow x = a - r$ ou $x = a + r$
2. $|x-a| \leqslant r \Leftrightarrow a - r \leqslant x \leqslant a + r \Leftrightarrow x \in [a-r\,, a+r]$
3. $|x-a| < r \Leftrightarrow a - r < x < a + r \Leftrightarrow x \in \,]a-r\,, a+r[$



Exemple 1.19 : Résoudre dans $\mathbb{R}$: $(E_1) : |2x-4| = -6$; $(E_2) : |x-5| < |x-1|$ et $(E_3) : 1 \leqslant |x^2 - 4x + 3|$.

Vocabulaire : L'ensemble $B(a,r) = \{x \in \mathbb{R}, |x-a| < r\}$ est l'ensemble des points dont la distance à $a \in \mathbb{R}$ est inférieure à $r \in \mathbb{R}_+^*$. On dit que $B(a,r)$ est la boule ouverte de centre a et de rayon r.

Proposition 1.20 (caractérisation des parties bornées de $\mathbb{R}$ avec la valeur absolue)

Soit A une partie de $\mathbb{R}$.
A est une partie bornée si et seulement si : $\exists M \in \mathbb{R}_+$, $\forall x \in A$, $|x| \leqslant M$.

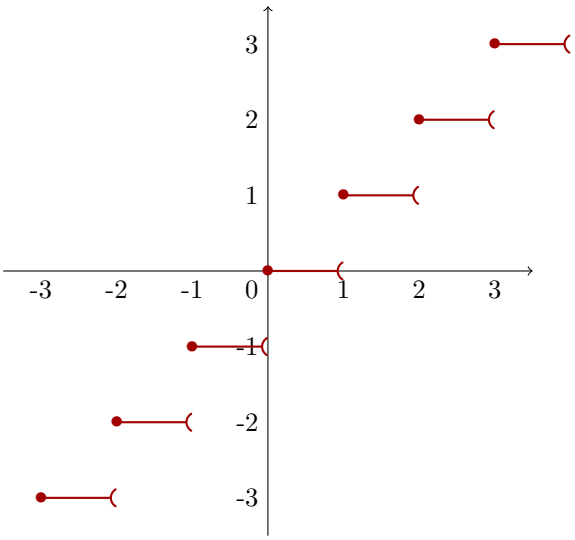
1.7 Partie entière

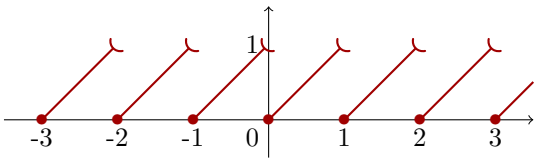
Définition 1.21 (partie entière et partie fractionnaire d'un réel)

Soit x un nombre réel.
On appelle partie entière de x le plus grand entier relatif n tel que $n \leqslant x$. On la note $\lfloor x \rfloor$.
On appelle partie fractionnaire de x la différence entre x et sa partie entière : $\{x\} = x - \lfloor x \rfloor$.
On appelle partie entière la fonction $\begin{cases} \mathbb{R} \to \mathbb{Z} \\ x \mapsto \lfloor x \rfloor \end{cases}$ et partie fractionnaire la fonction $\begin{cases} \mathbb{R} \to [0,1[\\ x \mapsto \{x\} \end{cases}$.

Remarque : Cette définition a bien un sens d'après l'axiomatique des entiers (c.f. prochaine page).

Représentation des courbes des fonctions partie entière et partie fractionnaire :





Exemple 1.22 : $\lfloor \mathbf{e} \rfloor = 2$, $\lfloor -\pi \rfloor = -4$ et $\left\{\frac{4}{3}\right\} = \frac{1}{3}$.

Proposition 1.23 (propriétés de la partie entière avec des entiers relatifs)

Soient $x \in \mathbb{R}$ et $n \in \mathbb{Z}$.

1. $x \in \mathbb{Z} \Leftrightarrow x = \lfloor x \rfloor$.
2. $\lfloor x + n \rfloor = \lfloor x \rfloor + n$.

Remarque : En général, $\lfloor x + y \rfloor \neq \lfloor x \rfloor + \lfloor y \rfloor$. Exemple : $\lfloor 5 \rfloor \neq \lfloor 2{,}5 \rfloor + \lfloor 2{,}5 \rfloor$.

Théorème 1.24 (caractérisation de la partie entière)

Soient $x \in \mathbb{R}$ et $n \in \mathbb{Z}$. On a équivalence entre :

1. $n = \lfloor x \rfloor$
2. $n \leqslant x < n + 1$
3. $x - 1 < n \leqslant x$

Remarque : En particulier, on a les inégalités suivantes $x - 1 < \lfloor x \rfloor \leqslant x < \lfloor x \rfloor + 1$ pour tout $x \in \mathbb{R}$.

Exemple 1.25 : Résoudre l'équation d'inconnue réelle x suivante $\lfloor (2x+1)^2 \rfloor = 3$.

2 Nombres entiers et arithmétique

2.1 Axiomatique des entiers

Axiome 2.1 (Construction de $\mathbb{N}$)

- Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.
- Toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément.
- $\mathbb{N}$ n'admet pas de plus grand élément.

Remarque : De manière similaire :

- Toute partie non vide et minorée de $\mathbb{Z}$ admet un plus petit élément.
- Toute partie non vide et majorée de $\mathbb{Z}$ admet un plus grand élément.

2.2 Relation de divisibilité

Définition 2.2 (relation de divisibilité dans $\mathbb{Z}$)

Soient a et $b \in \mathbb{Z}$.
On dit que a divise b dans $\mathbb{Z}$, ce que l'on note $a \mid b$, lorsqu'il existe $k \in \mathbb{Z}$ tel que $b = ka$.
On dit alors que a est un diviseur de b et que b est un multiple de a.
On note $\mathrm{Mul}(a)$ l'ensemble des multiples de a et $\mathrm{Div}(b)$ l'ensemble des diviseurs de b.

Exemple 2.3 : Décrire $\mathrm{Div}(4)$.

Remarques :

1. On a $\mathrm{Mul}(0) = \{0\}$, $\mathrm{Div}(0) = \mathbb{Z}$, $\mathrm{Mul}(1) = \mathbb{Z}$, $\mathrm{Div}(1) = \{1; -1\}$ et $\forall a \in \mathbb{Z}$, $1 \in \mathrm{Div}(a)$ et $0 \in \mathrm{Mul}(a)$.
2. Si $d \in \mathrm{Div}(a)$ et $d \in \mathrm{Div}(b)$, alors d divise n'importe quelle **combinaison arithmétique** de a et b, c'est-à-dire $d \in \mathrm{Div}(au + bv)$ pour tous u et v dans $\mathbb{Z}$.

2.3 Division euclidienne

Théorème 2.4 (théorème de la division euclidienne dans $\mathbb{Z}$)

Soient a et $b \in \mathbb{Z}$, avec $b \neq 0$.
Il existe un unique couple $(q,r) \in \mathbb{Z}^2$ tel que $\begin{cases} a = bq + r \\ 0 \leqslant r < |b| \end{cases}$.
Cette écriture est appelée division euclidienne de a par b.
Dans cette division euclidienne, q est appelé quotient et r est appelé reste.

Remarque : Soit $(a,b) \in \mathbb{Z}^2$ avec $b \neq 0$. $b \mid a$ si et seulement si le reste de la division euclidienne de a par b est 0.

Exemple 2.5 : Compléter les tableaux ci-dessous où q et r sont le quotient et le reste de la division euclidienne de a par b :

a	b	q	r
16	3		
12	-3		
23	-6		

a	b	q	r
5	9		
-12	5		
-7	-10		

a	b	q	r
$2^{n+1} + 1$	2		
$2^{n+1} + 3$	2		
$2^{n+1} - 1$	2		

2.4 Nombres premiers

Définition 2.6 (nombre premier)

Un nombre premier est un entier supérieur ou égal à 2 dont les seuls diviseurs positifs sont 1 et lui-même. Un entier supérieur ou égal à 2 est dit composé s'il n'est pas premier.
On note $\mathcal{P}$ l'ensemble des nombres premiers.

Autrement dit, $p \in \mathbb{N}$ est premier si et seulement si $p \geqslant 2$ et $\forall a,b \in \mathbb{N}$, $p = ab \implies a = 1$ ou $b = 1$.

Proposition 2.7 (tout entier supérieur à 2 admet au moins un diviseur premier)

Tout entier supérieur ou égal à 2 admet au moins un diviseur premier.
Plus précisément, si n est composé, alors il admet un diviseur premier p tel que $p \leqslant \sqrt{n}$.

Crible d'Eratosthène : Pour dresser la liste de tous les nombres premiers inférieurs à un entier n donné, on peut procéder de la manière suivante :

1. On écrit tous les entiers de 2 à n.
2. On entoure 2 (il est premier) et on raye tous ses multiples stricts (ils ne sont pas premiers).
3. On entoure le prochain entier p non rayé (il est premier) et on raye tous ses multiples stricts à partir de p^2 (ceux d'avant sont déjà rayés).
4. On répète l'étape précédente jusqu'à ce que l'on dépasse strictement $\sqrt{n}$.
5. À la fin de la procédure, les entiers non rayés sont les nombres premiers inférieurs à n.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Théorème 2.8 ($\mathcal{P}$ est infini)

L'ensemble des nombres premiers $\mathcal{P}$ est infini.

Théorème 2.9 (lemme d'Euclide)

Soient $p \in \mathcal{P}$ et $a,b \in \mathbb{Z}$.

$$p \mid ab \Leftrightarrow (p \mid a \text{ ou } p \mid b)$$

Théorème 2.10 (théorème de décomposition en facteurs premiers)

Tout entier naturel non nul se décompose de manière unique, à l'ordre près des facteurs, comme un produit de nombres premiers.

Idée de la preuve : l'existence se démontre par récurrence forte ; l'unicité se démontre à l'aide du lemme d'Euclide.

En regroupant, dans une telle décomposition, les nombres premiers égaux entre eux, on obtient la variante suivante.

Théorème 2.11 (théorème de décomposition en facteurs premiers, variante)

Tout entier naturel non nul n se décompose de manière unique, à l'ordre près des facteurs, sous la forme

$$n = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$$

avec $r \in \mathbb{N}$, les p_i des nombres premiers distincts et les m_i des entiers naturels non nuls.

Exemple 2.12 : Décomposer 98 en facteurs premiers.

Proposition 2.13 (caractérisation de la divisibilité avec la décomposition en facteurs premiers)

Soient a et $b \in \mathbb{N}^*$.
Quitte à rajouter des facteurs ${p_i}^0$ dans les décompositions de a et b en facteurs premiers, a et b peuvent s'écrire sous la forme

$$a = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r} \quad \text{et} \quad b = p_1^{m'_1} p_2^{m'_2} \cdots p_r^{m'_r}$$

avec $r \in \mathbb{N}$, les p_i des nombres premiers distincts et les m_i et m'_i des entiers naturels.
On a alors l'équivalence suivante : $a \mid b \;\Leftrightarrow\; \forall i \in [\![1;r]\!],\ m_i \leqslant m'_i$

2.5 PGCD de deux entiers

Définition 2.14 (diviseur commun)

Soit $(a,b) \in \mathbb{Z}^2$. On dit que d est un *diviseur commun* à a et b lorsque $d|a$ et $d|b$.
On note $\mathrm{Div}(a,b) = \mathrm{Div}(a) \cap \mathrm{Div}(b)$ l'ensemble des diviseurs communs de a et b.

Définition 2.15 (PGCD de deux entiers)

Soient a et b deux entiers relatifs **dont l'un au moins est non nul**.
L'ensemble $\mathrm{Div}(a,b)$ possède un plus grand élément, qui est appelé PGCD (plus grand commun diviseur) de a et b. Il est noté $a \wedge b$ et appartient à $\mathbb{N}^*$.

Démonstration.

1. Soit $(a,b) \in \mathbb{Z}^2 \backslash \{(0,0)\}$. L'ensemble $\mathrm{Div}(a,b)$ est une partie de $\mathbb{N}$ non vide (elle contient 1) et majorée (par $|a|$ si $a \neq 0$, par $|b|$ sinon, dans tous les cas par $\max\{|a|,|b|\}$).
   Elle possède donc bien un plus grand élément, d'où l'existence de $a \wedge b$.
2. 1 étant toujours un diviseur commun à a et b, on a nécessairement $a \wedge b \in \mathbb{N}^*$.

Vocabulaire : Si $a \wedge b = 1$, on dit que a et b sont premiers entre eux. □

Exemple 2.16 : Calculer $14 \wedge 48$.

Proposition 2.17 (premières propriétés du PGCD)

Soient a et b deux entiers relatifs dont l'un au moins est non nul.

1. $a \wedge b = |a| \wedge |b|$.
2. Si $a \neq 0$, alors $a \wedge 0 = |a|$.
3. $a \wedge 1 = 1$.
4. Si $a \mid b$, alors $a \wedge b = |a|$.
5. On suppose que $b \neq 0$. Alors pour tout $q \in \mathbb{Z}$, $a \wedge b = b \wedge (a - bq)$.

2.6 Calcul du PGCD de deux entiers

Proposition 2.18 (expression du PGCD à l'aide de la décomposition en facteurs premiers)

Soient a et $b \in \mathbb{N}^*$.
Les entiers a et b peuvent s'écrire sous la forme

$$a = p_1^{m_1} \cdots p_r^{m_r} \quad \text{et} \quad b = p_1^{m'_1} \cdots p_r^{m'_r}$$

avec $r \in \mathbb{N}$, les p_i des nombres premiers distincts et les m_i et m'_i des entiers naturels.
On a alors l' expression suivante pour le PGCD de a et b :

$$a \wedge b = {p_1}^{\min(m_1, m'_1)} \cdots {p_r}^{\min(m_r, m'_r)}$$

Exemple 2.19 : Déterminer $84 \wedge 90$.

Remarque : Il n'est pas toujours facile de déterminer la décomposition en facteurs premiers d'un entier. Nous présentons ci-dessous une deuxième méthode de calcul de PGCD qui n'utilise pas cette décomposition.

Algorithme d'Euclide : Pour calculer le PGCD de deux entiers a et b avec b non nul :

- on effectue la division euclidienne $a = bq + r$ de a par b. On a alors : $a \wedge b = b \wedge r$.
- On recommence avec b et r, et ainsi de suite jusqu'à obtenir un reste nul.
- Le PGCD est alors le dernier reste non nul obtenu.

Exemple 2.20 : Déterminer $1234 \wedge 96$ à l'aide de l'algorithme d'Euclide.

Algorithme d'Euclide sous Python :

```
def euclide(a,b) :
        a,b=abs(a),abs(b)
        if a<b:
                a,b=b,a
        while b > 0 :
                r=a%b
                a,b=b,r
        return a
```

2.7 PPCM

Définition 2.21 (multiple commun)

Soit $(a,b) \in \mathbb{Z}^2$ et $m \in \mathbb{Z}$. On dit que m est un *multiple commun* à a et b lorsque $a|m$ et $b|m$.
On note $\mathrm{Mul}(a,b) = \mathrm{Mul}(a) \cap \mathrm{Mul}(b)$ l'ensemble des multiples communs de a et de b.

Définition 2.22 (PPCM de deux entiers)

Soient a et b deux entiers relatifs **non nuls**.
L'ensemble $\mathrm{Mul}(a,b) \cap \mathbb{N}^*$ possède un plus petit élément, qui est appelé PPCM (plus petit commun multiple) de a et b. Il est noté $a \vee b$.

Démonstration. Soit $(a,b) \in (\mathbb{Z}^*)^2$. L'ensemble $\mathrm{Mul}(a,b) \cap \mathbb{N}^*$ est une partie de $\mathbb{N}$ non vide (elle contient $|ab| \in \mathbb{N}^*$), donc elle possède bien un plus petit élément, d'où l'existence de $a \vee b$. □

Utilisation du PPCM : Pour réduire deux fractions $\frac{a}{b}$ et $\frac{c}{d}$ au même dénominateur, on prend en général comme dénominateur commun le PPCM de b et d.

Proposition 2.23 (propriétés du PPCM)

Soient a et b deux entiers relatifs non nuls.

1. $a \vee b = |a| \vee |b|$.
2. $a \vee 1 = |a|$.
3. Si $a \mid b$, alors $a \vee b = |b|$.

Proposition 2.24 (expression du PPCM à l'aide de la décomposition en facteurs premiers)

Soient a et $b \in \mathbb{N}^*$.
a et b peuvent s'écrire sous la forme

$$a = p_1^{m_1} \cdots p_r^{m_r} \quad \text{et} \quad b = p_1^{m'_1} \cdots p_r^{m'_r}$$

avec $r \in \mathbb{N}$, les p_i des nombres premiers distincts et les m_i et m'_i des entiers naturels.
On a alors l'expression suivante pour le PPCM de a et b :

$$a \vee b = {p_1}^{\max(m_1,m'_1)} \cdots {p_r}^{\max(m_r,m'_r)}$$

Théorème 2.25 (lien entre PGCD et PPCM)

Soient a et $b \in \mathbb{Z}^*$. On a la relation :

$$|ab| = (a \wedge b) \times (a \vee b)$$

Exemple 2.26 : Calculer $84 \vee 60$ de deux manières différentes.