Chapitre 7. Ensembles $\mathbb{Z}$ et $\mathbb{R}$: ce qu'il faut savoir.

Introduction : les ensembles de nombres à connaître

- $\mathbb{N}$ l'ensemble des entiers naturels : 0, 1, 2, 3, ...
- $\mathbb{Z}$ l'ensemble des entiers relatifs, constitué des entiers naturels et de leurs opposés.
- $\mathbb{Q}$ l'ensemble des nombres rationnels, c'est-à-dire les nombres s'écrivant $\frac{p}{q}$ avec p et q entiers, q non nul (on peut même supposer $q \in \mathbb{N}^*$).
- $\mathbb{D}$ l'ensemble des nombres décimaux, c'est-à-dire les nombres s'écrivant

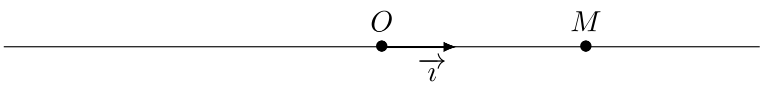
Insuffisance de $\mathbb{Q}$:

— Nous avons vu au chapitre 2 qu'il n'existait pas de $r \in \mathbb{Q}$ tel que $r^2 = 2$...

— D'autres nombres ayant une signification physique simple comme π ne sont pas rationnels...

- $\mathbb{R}$ l'ensemble des réel, a été construit pour palier à ces problèmes.
  La construction rigoureuse de $\mathbb{R}$ est difficile, hors programme.

$\mathbb{R}$ est muni d'une relation d'ordre $\leq$, ce qui permet de représenter géométriquement l'ensemble des réels par la droite numérique, qui est un axe muni d'une origine O et dirigé par un vecteur $\overrightarrow{i}$ unitaire. Pour tout réel x, on identifie x au point M d'abscisse x (i.e. le point qui vérifie $\overrightarrow{OM} = x\,\overrightarrow{i}$).



On a les inclusions suivantes :

Mentionnons aussi $\mathbb{C} = \{a + ib \ / \ a, b \text{ réels}\}$ qui vérifie $\mathbb{R} \subset \mathbb{C}$.
Mais sur $\mathbb{C}$, il n'y a pas de relation d'ordre $\leq$.

Un réel qui n'est pas rationnel, comme $\sqrt{2}$, s'appelle un irrationnel.
L'ensemble des irrationnels est donc $\mathbb{R} \backslash \mathbb{Q}$.

1 Dans $\mathbb{Z}$: un peu d'arithmétique

1.a Divisibilité dans $\mathbb{Z}$

Définition :

Soient $(a, b) \in \mathbb{Z}^2$. On dit que a divise b si

On dit aussi :
b est divisible par a ;
a est un diviseur de b ;
b est un multiple de a.
On note alors $a|b$.

Exemples :

- $3|12$ et $4|12$; les diviseurs positifs de 12 sont
- 1 et -1 divisent
- Soit a un entier ; a divise toujours
- 0 divise seulement

Remarque : Si $a|b$, peut-on dire que $a \leq b$?

Proposition :

- $\forall (a, b) \in \mathbb{Z}^2,\ a|b$ et $b|a \Longrightarrow |a| = |b|$
- $\forall (a, b, c) \in \mathbb{Z}^3,\ a|b$ et $b|c \Longrightarrow a|c$
- $\forall (a, b, c) \in \mathbb{Z}^3,\ a|b$ et $a|c \Longrightarrow a|(b + c)$
- $\forall (a, b, c, d) \in \mathbb{Z}^4,\ a|b$ et $c|d \Longrightarrow ac|bd$

1.b Division euclidienne dans $\mathbb{N}^*$

Théorème :

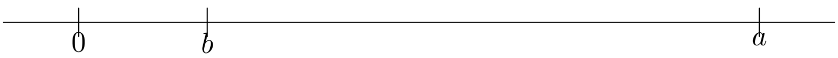
(Division euclidienne)
Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$.

Démonstration 1

Remarques : avec les notations précédentes,

- $\boxed{b|a \iff \quad r = 0}$
- q s'obtient avec une partie entière :
  On a $\dfrac{a}{b} = q + \dfrac{r}{b}$.
  Comme $0 \leq r < b$ et $b > 0$, on a $0 \leq \dfrac{r}{b} < 1$.
  Ainsi, $\dfrac{a}{b}$ est égal à l'entier q plus un nombre de $[0, 1[$: $q = \lfloor \dfrac{a}{b} \rfloor$

En Python :
Le reste dans la division euclidienne de a par b s'obtient avec : `a % b`
Le quotient dans la division euclidienne de a par b s'obtient avec : `a // b`.



Le reste r est le premier entier, obtenu à partir de a en soustrayant un certain nombre de fois b, qui soit strictement inférieur à b. Le quotient q est alors le nombre de fois qu'il a fallu enlever la quantité b à a pour obtenir r.
Il est donc facile d'écrire une fonction en Python réalisant la division euclidienne : en partant a, on soustrait b tant que la quantité obtenue est supérieure ou égale à b.

```
def division_euclidienne(a,b):
    r = a
    q = 0
    while r >= b:
        r = r - b
        q = q + 1
    return(q,r)
```

1.c Nombres premiers

Définition :

On dit qu'un entier p est un nombre premier s'il est supérieur ou égal à 2, et si ses seuls diviseurs positifs sont 1 et lui-même, i.e. si :

Les premiers nombres premiers :

- Pour montrer qu'un entier $p \geq 2$ est premier,

- Pour montrer qu'un entier $p \geq 2$ n'est pas premier,

Proposition :

Tout entier $n \geq 2$ admet au moins un diviseur premier.

Proposition :

Il y a une infinité de nombres premiers.

Démonstration 2

Proposition :

(Décomposition en facteurs premiers) Tout entier $n \geq 2$ s'écrit sous la forme :

La décomposition est unique à l'ordre des facteurs près.

Exemple : $1980 =$

1.d pgcd, ppcm, algorithme d'Euclide

Définition :

Soient a et b des entiers naturels non nuls.
Le PGCD de a et b est le plus grand des diviseurs positifs communs à a et à b.
On le note $\text{pgcd}(a, b)$ ou $a \wedge b$.
Le PPCM de a et b est le plus petit des multiples strictement positifs communs à a et à b.
On le note $\text{ppcm}(a, b)$ ou $a \vee b$.

Quand l'un des entiers est nul, on peut étendre la définition : lorsque $a \neq 0$, $\text{pgcd}(a, 0) = a$. En effet, a est le plus grand diviseur de a, et c'est un diviseur de 0.

Exemples :

$\text{pgcd}(6, 9) =$ $\text{pgcd}(12, 8) =$ $\text{pgcd}(25, 12) =$

$\text{ppcm}(6, 9) =$ $\text{ppcm}(12, 8) =$ $\text{ppcm}(5, 3) =$

De manière générale, on peut montrer que $\text{pgcd}(a, b) \times \text{ppcm}(a, b) =$

C'est une conséquence du résultat général suivant :

Proposition :

Soit a et b des entiers supérieurs ou égaux à 2.
On les décompose en facteurs premiers ; plus précisément, on identifie les nombres premiers p_1, ... , p_n qui interviennent dans les décompositions de a et b :

$$a = p_1^{\alpha_1} \dots p_n^{\alpha_n} \quad \text{et} \quad b = p_1^{\beta_1} \dots p_n^{\beta_n}$$

avec α_1, β_1, ... , α_n, β_n des éléments de $\mathbb{N}$
(on peut par exemple avoir $\alpha_i = 0$ si p_i n'est pas un facteur premier de a).

Le PGCD de a et b sera :

Le PPCM de a et b sera :

Calculons par exemple les PGCD et PPCM de 24 et 32, puis de 1980 et 75 :

C'est le PPCM qui sert dans la mise au même dénominateur. Par exemple :

$$\frac{5}{24} + \frac{11}{32} =$$

Algorithme d'Euclide

Il permet de trouver le PGCD de a et b en calculant des restes successifs, et à l'aide du résultat suivant :

Proposition :

> Soit $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$. Notons r le reste dans la division euclidienne de a par b.
> On a : $\operatorname{pgcd}(a, b) = \operatorname{pgcd}(b, r)$.

Démonstration 3

On en tire l'algorithme :

Posons $r_0 = a$ et $r_1 = b$. On cherche $\operatorname{pgcd}(r_0, r_1)$.

En notant r_2 le reste dans la division euclidienne de r_0 par r_1, on a donc $\operatorname{pgcd}(r_0, r_1) = \operatorname{pgcd}(r_1, r_2)$.

- Si $r_2 = 0$, $\operatorname{pgcd}(r_1, r_2) = r_1$, on a réussi ;
- Sinon, on calcule le reste r_3 dans la division euclidienne de r_1 par r_2 :
  on a $\operatorname{pgcd}(r_1, r_2) = \operatorname{pgcd}(r_2, r_3)$...

Et ainsi de suite, jusqu'à obtenir un reste nul.

Calculons par exemple $207 \wedge 162$:

2 Dans $\mathbb{R}$: borne supérieure et borne inférieure

2.a Définitions

Rappels du chapitre 1 :

Définition :

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

- On dit que A est majorée si : $\exists\, M \in \mathbb{R}$ tel que $\forall\, x \in A$, $x \leq M$.
  Dans ce cas, on dit que M est un majorant de A.
- On dit qu'un réel M est un maximum de A si $\boxed{\text{c'est un élément de } A}$ et si c'est un majorant de A.
  Autrement dit si : $M \in A$ et $\forall\, x \in A, \quad x \leq M$.
  Un maximum, s'il existe, est unique ; on le note $\max(A)$, et on l'appelle aussi le plus grand élément de A.

Définition :

- On dit que A est minorée si : $\exists\, m \in \mathbb{R}$ tel que $\forall\, x \in A$, $m \leq x$.
  Dans ce cas, on dit que m est un minorant de A.
- On dit qu'un réel m est un minimum de A si $\boxed{\text{c'est un élément de } A}$ et si c'est un minorant de A.
  Autrement dit si : $m \in A$ et $\forall\, x \in A, \quad m \leq x$.
  Un minimum, s'il existe, est unique ; on le note $\min(A)$, et on l'appelle aussi le plus petit élément de A.

Définition :

On dit que A est bornée si elle est à la fois minorée et majorée.
Dire que A est bornée revient à dire : $\exists\, K \geq 0$ tel que $\forall\, x \in A$, $|x| \leq K$.

Proposition :

- Toute partie non vide et majorée de $\mathbb{Z}$ possède
- Toute partie non vide et minorée de $\mathbb{Z}$ possède
  En particulier :

Exemples :

- $[0, 1]$

- Par contre, $[0, 1[$

Pourtant, pour $[0, 1[$, 1 a un rôle particulier : non seulement c'est un majorant, mais c'est surtout le meilleur, l'optimum, car c'est

Définition :

> Soit A une partie de $\mathbb{R}$.
> On dit que A admet une <u>borne supérieure</u> si
>
> Si c'est le cas,

L'unicité vient du fait qu'un minimum (ici le minimum des majorants), s'il existe, est unique.

Dire que M est la borne supérieure de A, c'est dire que M majore A et qu'il n'y a pas de majorant de A qui soit strictement plus petit que M.

Exemples :

- $[0,+\infty[$
- $[0,1[$
- $[0,1]$
- $\mathbb{Q}_-^*$

Lien entre les notions

- Si A admet un maximum, alors A admet une borne supérieure et $\max(A)=\sup(A)$.
- Si $\sup(A)$ existe, il y a deux cas :
  — Soit $\sup(A)\in A$, alors $\max(A)$ existe et $\max(A)=\sup(A)$.
  — Soit $\sup(A)\notin A$, alors A n'a pas de maximum.

Démonstration 4

Définition :

> Soit A une partie de $\mathbb{R}$.
> On dit que A admet une <u>borne inférieure</u> si
>
> Si c'est le cas,

L'unicité vient du fait qu'un maximum (ici le maximum des minorants), s'il existe, est unique.

Dire que m est la borne inférieure de A, c'est dire que m minore A et qu'il n'y a pas de minorant de A qui soit strictement plus grand que m.

Exemples :

- $]-\infty,1]$
- $]0,1]$
- $[0,1]$

2.b Propriété de la borne supérieure

Théorème :

> **(Propriété de la borne supérieure)**
> - Toute partie non vide et majorée de $\mathbb{R}$ admet une borne supérieure.
> - Toute partie non vide et minorée de $\mathbb{R}$ admet une borne inférieure.

C'est spécifique à $\mathbb{R}$: par exemple, $\mathbb{Q}$ n'a pas cette propriété (il existe des parties A de $\mathbb{Q}$, non vides et majorées, mais qui n'ont pas de borne supérieure dans $\mathbb{Q}$).

Remarque : Lorsque A est une partie non majorée de $\mathbb{R}$, on s'autorise à écrire $\sup(A) = +\infty$.
De même, on pourra écrire $\inf(A) = -\infty$ si A n'est pas minorée.

Exercice :
Soient A et B des parties non vides de $\mathbb{R}$ telles que, pour tout $a \in A$ et tout $b \in B$, $a \leq b$.
Montrer que $\sup A$ et $\inf B$ existent et que $\sup A \leq \inf B$.

Démonstration 5

2.c Intervalles de $\mathbb{R}$

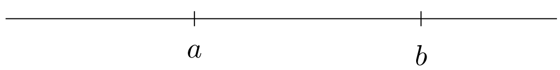
Rappel :

Définition :

> On appelle intervalle de $\mathbb{R}$ toute partie de $\mathbb{R}$ de l'une des formes suivantes (où a, b désignent des réels tels que $a \leq b$) :
>
> $\emptyset$, $\mathbb{R}$, $[a, b]$, $[a, b[$, $]a, b]$, $]a, b[$, $[a, +\infty[$, $]a, +\infty[$, $]-\infty, b]$, $]-\infty, b[$

Remarques :
- $[a, b]$ s'appelle un segment.
- On dit que l'intervalle est ouvert s'il est de l'un des types suivants :

Proposition :

> (Caractérisation des intervalles)
> Soit I une partie de $\mathbb{R}$.
> I est un intervalle de $\mathbb{R}$ si et seulement si :
>
> 
>

Démonstration 6

On pourrait utiliser cela comme définition des intervalles de $\mathbb{R}$; on dit que les intervalles de $\mathbb{R}$ sont les parties convexes de $\mathbb{R}$.

3 Partie entière et approximations décimales d'un réel

3.a Partie entière : définition, propriétés

Théorème-définition :

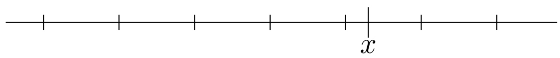
Soit $x \in \mathbb{R}$. Il existe un unique entier relatif $n \in \mathbb{Z}$ tel que

Cet entier est appelé partie entière de x, on le note $E(x)$ ou $\lfloor x \rfloor$.

Retenir :

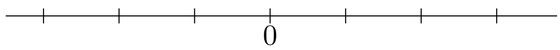
- La propriété qui caractérise $\lfloor x \rfloor$:

$$\lfloor x \rfloor \in \mathbb{Z} \quad \text{et} \quad \lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$$



C'est le plus grand entier qui soit inférieur ou égal à x.

- *Quelques exemples* :
$\lfloor 1.5 \rfloor =$
$\lfloor 0.2 \rfloor =$
$\lfloor -2.2 \rfloor =$
$\lfloor -0.8 \rfloor =$

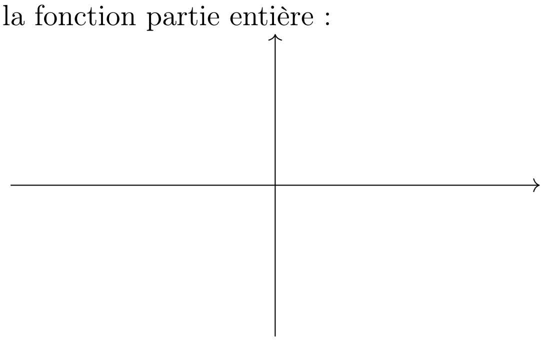


- Comment reconnaître la partie entière ?
— À l'aide d'une écriture de x :

— À l'aide d'un encadrement de x :

⚠ Si on a obtenu seulement $p \leq x \leq p+1$ avec p entier, que peut-on dire ?

- Courbe représentative de la fonction partie entière :



Proposition :

- $x = \lfloor x \rfloor \iff x \in \mathbb{Z}$.
- La fonction partie entière est croissante, c'est-à-dire que :

- Si $n \in \mathbb{Z}$, alors $\lfloor x + n \rfloor = \lfloor x \rfloor + n$

  ⚠ *En général* $\lfloor x + y \rfloor \neq \lfloor x \rfloor + \lfloor y \rfloor$*!*

Démonstration 7

Remarque : Soit $n \in \mathbb{Z}$. L'entier p tel que $n = 2p$ dans le cas où n est pair, tel que $n = 2p + 1$ dans le cas où n est impair, s'obtient par une formule unique à l'aide de la partie entière :

3.b Approximations décimales d'un réel

Partons d'un exemple : "$\sqrt{2} = 1,414213562...$" ; "$\sqrt{2} \sim 1,414213562$" (écritures à éviter en maths !)
On souhaite être précis en parlant de <u>valeur décimale approchée par défaut ou par excès</u> :

$$1,41 < \sqrt{2} < 1,42$$

$$1,414 < \sqrt{2} < 1,415$$

$$1,4142 < \sqrt{2} < 1,4143$$

Dans le dernier encadrement, on a bien des valeurs approchées de $\sqrt{2}$ à 10^{-4} près car :

On a aussi que la différence entre ces valeurs approchées est exactement 10^{-4}.

Recherche dans le cas général
Soit $x \in \mathbb{R}$, on cherche des nombres décimaux r_d et r_e :

- avec n chiffres après la virgule et tels que $r_e - r_d =$

- et qui encadrent x :

Proposition :

Soit $x \in \mathbb{R}$ et $n \in \mathbb{N}$.
Les valeurs approchées décimales de x à 10^{-n} près sont :

Autrement dit, on a l'inégalité :

Proposition :

Soit $x \in \mathbb{R}$. Les valeurs approchées décimales de x à 10^{-n} près tendent vers x lorsque n tend vers $+\infty$.

Ainsi, $\boxed{\text{pour tout } x \in \mathbb{R}\text{, il existe une suite de } \boxed{\text{rationnels}} \text{ qui converge vers } x}$.

Démonstration 8

On dit que $\mathbb{Q}$ est dense dans $\mathbb{R}$.

Plan du cours