Lycée Condorcet
PCSI

Mars 2025

Sous-ensembles de $\mathbb{R}$ et rudiment d'arithmétique

Table des matières

1 Nombres entiers, décimaux, rationnels

Définition 1.

- On apelle ensemble des **entiers naturels**, l'ensemble $\mathbb{N} = \{0; 1; 2; \ldots\}$.
- On appelle ensemble des **entiers relatifs** l'ensemble $\mathbb{Z}$ constitué des entiers naturels et de leurs opposés.
- On appelle **nombre décimal** un nombre de la forme $\frac{p}{10^n}$, où p et n un entier relatif et n un entier naturel. L'ensemble des nombres décimaux est noté $\mathbb{D}$.
- On appelle **nombre rationnel** un quotient d'entiers relatifs, c'est à dire un nombre de la forme $\frac{p}{q}$, où $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$. On note $\mathbb{Q}$ l'ensemble des nombres rationnels.

Remarque.

— On a les inclusions $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{D} \subset \mathbb{Q} \subset \mathbb{R}$. Ces inclusions sont strictes.
— On appelle un nombre réel qui n'est pas un rationnel, un irrationnel.

1.1 Nombres décimaux

Proposition 2.

Soit $x \in \mathbb{R}$ et $n \in \mathbb{N}$. Le nombre décimal $d_n(x) = \dfrac{\lfloor 10^n x \rfloor}{10^n}$ satisfait l'encadrement

$$d_n(x) \leq x \leq d_n(x) + 10^{-n}$$

Les nombres $d_n(x)$ et $d_n(x) + 10^{-n}$ sont appelés respectivement **valeur décimale** par défaut (resp. par excès) de x à la précision 10^{-n}.

Corollaire 3 ($\mathbb{D}$ est dense dans $\mathbb{R}$.)**.**

Entre deux réels distincts, il existe toujours un nombre décimal.
Autrement dit, tout intervalle ouvert non vide contient un élément de $\mathbb{D}$:

$$\forall (a,b) \in \mathbb{R}^2, a < b, \quad \mathbb{D} \cap]a,b[\neq \emptyset$$

Démonstration

Procédons par disjonction de cas.

- Supposons que $b \in \mathbb{D}$.
  Comme $10^{-n} \underset{n\to+\infty}{\longrightarrow} 0$, il existe $N \in \mathbb{N}$ tel que

  $$0 < 10^{-N} < b - a$$

  On a alors

  $$a < b - 10^{-N} < b$$

  Mais comme $b \in \mathbb{D}$ alors $b + 10^{-N} \in D$ et ainsi

  $$\mathbb{D} \cap]a,b[\neq \emptyset$$

- Supposons maintenant que $b \notin \mathbb{D}$. On a alors, pour tout $n \in \mathbb{N}$, $d_n(b) \neq b$ d'où

  $$\forall n \in \mathbb{N}, \quad d_n(b) < b$$

  et comme $d_n(b) \underset{n\to\infty}{\longrightarrow} b$, il existe $N \in \mathbb{N}$ et que

  $$|d_N(b) - b| \leq \frac{b-a}{2}$$

  On a alors, comme $d_N(b) \leq b$,

  $$0 \leq b - d_N(b) \leq \frac{b-a}{2} \iff a < \frac{a+b}{2} \leq d_N(b) \leq b$$

  D'où comme $d_N(b) \neq 0$ on a bien :

  $$a < d_N(b) < b$$

  Or $d_N(b) \in \mathbb{D}$ d'où

  $$]a, b \cap \mathbb{D} \neq \emptyset$$

1.2 Nombres rationnels

Proposition 4.

Le nombre $\sqrt{2}$ est irrationnel.

Remarque.
Les nombres e et π sont aussi irrationnel.

Proposition 5.

L'ensemble des nombres rationnels est stable par somme, produit et passage à l'inverse.

Remarque.
On ne peut pas en dire autant de l'ensemble des irrationnels (sauf pour l'inverse).

Proposition 6 ($\mathbb{Q}$ et $\mathbb{R}\backslash\mathbb{Q}$ sont denses dans $\mathbb{R}$.).

Entre deux réels distincts, il existe toujours un nombre rationnel et un irrationnel.
Autrement dit, pour tous réels a, b tels que $a < b$,

$$]a,b[\cap \mathbb{Q} \neq \emptyset, \qquad]a,b[\cap (\mathbb{R}\backslash\mathbb{Q}) \neq \emptyset$$

2 Multiples et diviseurs

2.1 Définition et premières propriétés

Définition 7.

Soit $(a,b) \in \mathbb{Z}^2$, on dit que b divise a (ou est un diviseur de a) s'il existe un entier $c \in \mathbb{Z}$ tel que

$$a = bc$$

On le note $b|a$. On dit encore que a est un multiple de b.

Proposition 8.

Soient $(a,b,c) \in \mathbb{Z}^3$. On a

1. $a \mid a$ (réflexivité).
2. Si $a \mid b$ et $b \mid a$ alors $|a| = |b|$.
3. Si $a \mid b$ et $b \mid c$ alors $a \mid c$ (transitivité).

Proposition 9.

Pour tout $(a,b,c) \in \mathbb{Z}^3$ si $a \mid b$ et $a \mid c$ alors pour tout $(\lambda,\mu) \in \mathbb{Z}$ $a \mid \lambda b + \mu c$.

2.2 Division euclidienne.

Théorème 10.

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il **existe un unique** couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que

$$a = bq + r \quad \text{et} \quad 0 \leq r < b$$

On appelle a le dividende de la division euclidienne, b son diviseur, q son quotient et r son reste.

Proposition 11.

Soit $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$. Alors b divise a si et seulement si le reste de la division euclidienne de a par b est nulle.

2.3 PGCD et PPCM

Notation :
Soient a et b deux entiers. On note $\mathcal{D}(a, b)$ l'ensemble des diviseurs communs de a et b.

Proposition 12.

Soient a et b deux entiers.
L'ensemble $\mathcal{D}(a, b)$ admet un plus grand élément. On l'appelle le plus grand commun diviseur (PGCD). Il est noté $\text{PGCD}(a, b)$, on trouve aussi la notation $a \wedge b$.

La démonstration de ce théorème ne donne pas de manière de calculer le PGCD de deux entiers.
La suite de ce paragraphe est consacrer à l'algorithme d'Euclide permettant de le calculer. Il est basé sur le lemme suivant.

Lemme 13.

Soit $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$. Si r désigne le reste de la division euclidienne de a par b alors :

$$\mathcal{D}(a, b) = \mathcal{D}(b, r)$$

Proposition 14.

Soit $(a, b) \in \mathbb{Z} \times \mathbb{N} \backslash \{(0, 0)\}$. Le PGCD de a et b est le dernier reste non nul quand on effectue les divisions euclidiennes successives.

Exemple 1

Calculer le PGCD de 167 et 207.

Définition 15.

On dit que deux nombres entiers non tous les deux nuls son premiers entre eux si et seulement si leur PGCD est 1.

Théorème 16 (Bezout).

Soient a et b deux entiers. Alors a et b sont premiers entre eux si et seulement si il existe $(u, v) \in \mathbb{Z}^2$ tel que

$$au + bv = 1$$

Lemme 17 (Gauss).

Soient a, b et c des entiers. Si $a \mid bc$ et $\text{PGCD}(a, b) = 1$, alors $a \mid c$.

Proposition 18.

L'ensemble des multiples non nuls et positifs de deux entiers a et b non nuls admet un plus petit élément. On appelle cet élément le **plus petit commun multiple** (PPCM) de a et b. On le note $\text{PPCM}(a, b)$ ou $a \vee b$.

Proposition 19.

Pour tout entiers positifs a et b,

$$\text{PGCD}(a, b) \times \text{PPCM}(a, b) = ab$$

3 Nombres permiers

3.1 Définitions et premières propriétés.

Définition 20.

Un entier $p \in \mathbb{N}\backslash\{0, 1\}$ est dit **premier** si et seulement si ses seuls diviseurs sont 1 et p.

Proposition 21.

Soit p un nombre permier et a, b deux entiers naturels. Si p divise ab alors il divise a ou b.

Proposition 22.

Tout entier naturel supérieur ou égal à 2 admet un diviseur premier.

On a même mieux !

Proposition 23.

Pour tout entier n non premier (et supérieur à 2), il existe un nombre premier divisant n et inférieur à $\sqrt{n}$.

Application :
Le crible d'Eratosthène. Un nombre **non** premier inférieur) 100, a d'après ce qui précède, un diviseur premier inférieur à 10. Ainsi, une fois éliminés de la grille ci-desssous tous les multiples (non triviaux) de 2, 3, 5 et 7, il ne restera que les entiers premiers inférieurs à 100.

0	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

Proposition 24 (d'Euclide).

Il existe une infinité de nombres premiers.

3.2 Décomposition en produit de facteurs premiers.

Le théorème suivant, admis, est une conséquence de la proposition 23.

Théorème 25.

Pour tout entier $n \geq 2$, il existe un entier $m \geq 1$, des nombres premiers p_1, ..., p_m et des entiers non nuls α_1, ...α_m tels que

$$n = \prod_{k=1}^{m} p_k^{\alpha_k}.$$

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

Ce théorème nous permet de décrire les diviseurs d'un entier qu'on a décomposé en facteurs premiers.

Théorème 26.

Soit $n \geq 2$. On suppose que la décomposition en facteurs premiers de n est $n = \prod_{k=1}^{m} p_k^{\alpha_k}$. Les diviseurs de n sont exactement les entiers q de la forme :

$$q = \prod_{k=1}^{m} p_k^{\beta_k} \quad \text{avec} \quad \forall k \in [\![1, m]\!] \quad 0 \leq \beta_k \leq \alpha_k.$$