Ensembles

Cours de É. Bouchet – PCSI

14 septembre 2023

Table des matières

1 Généralités sur les ensembles

1.1 Définitions et notations

Définition 1.1 (Ensemble)

Un **ensemble** E est un groupement d'objets distincts, appelés **éléments** de l'ensemble.
Si x est un élément de E, on note $x \in E$.
Il existe un ensemble qui n'a pas d'éléments, il est unique, c'est l'**ensemble vide**, noté $\emptyset$.

Remarque. Deux familles d'ensembles sont d'intérêt particulier :
- Les **ensembles finis**, qui ont un nombre d'éléments fini. On appelle **cardinal** ce nombre.
- Les **ensembles dénombrables**, dont on peut numéroter les éléments.

Exemple. Parmi les ensembles usuels,
- $[\![0, n]\!]$ est l'ensemble des entiers compris entre 0 et n. C'est un ensemble fini de cardinal $(n+1)$.
- $\mathbb{N}$, $\mathbb{N}^*$, $\mathbb{Z}$, $\mathbb{N}^2$, $\mathbb{Q}$ sont des ensembles dénombrables.
- $\mathbb{R}$ n'est ni dénombrable, ni fini, car on ne peut pas numéroter ses éléments.

Remarque. Pour décrire ou lister les éléments d'un ensemble, on utilise souvent des notations du type :

$$\{\text{éléments considérés}|\text{condition à vérifier}\}.$$

Exercice 1. Écrire avec des accolades les ensembles suivants :

1. L'ensemble A des réels x qui vérifient $x^2 + e^x = 12$.
2. L'ensemble B des entiers naturels du type $3m^2 + n^3$ où $(m, n) \in \mathbb{N}^2$.
3. Soit $n \in \mathbb{N}^*$. L'ensemble C des fractions de numérateur entier compris entre 1 et n et de dénominateur n.

Solution :

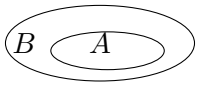
1. $A = \left\{x \in \mathbb{R} | x^2 + e^x = 12\right\}$.
2. $B = \left\{3m^2 + n^3 | (m, n) \in \mathbb{N}^2\right\} = \left\{p \in \mathbb{N} | \exists (m, n) \in \mathbb{N}^2 \text{ tels que } p = 3m^2 + n^3\right\}$.
3. $C = \left\{\dfrac{k}{n} \middle| k \in [\![1, n]\!]\right\} = \left\{x \in \mathbb{Q} \middle| \exists k \in [\![1, n]\!] \text{ tel que } x = \dfrac{k}{n}\right\}$.

1.2 Inclusion

Définition 1.2 (Inclusion, égalité)

Soient A et B deux ensembles.
- On dit que A est **inclus** dans B si tout élément de A est aussi un élément de B. On note alors $A \subset B$.
  On dit aussi que A est une **partie** (ou un **sous-ensemble**) de B.
- On dit que A et B sont **égaux** si $A \subset B$ et $B \subset A$. On note alors $A = B$.

Exemple. Représentation graphique de $A \subset B$:



Remarque. Cela donne en termes de quantificateurs :
- $A \subset B \iff \forall x \in A, x \in B$.
- $A \not\subset B \iff \exists x \in A$ tel que $x \notin B$.

Exercice 2. Montrer que $\mathbb{R}_- = \{x \in \mathbb{R} | \forall y > 0, x \leqslant y\}$.
Solution :
- Soit $x \in \mathbb{R}_-$. Alors $\forall y > 0$, $x \leqslant 0 < y$, donc $x \in \{x \in \mathbb{R} | \forall y > 0, x \leqslant y\}$. Donc $\mathbb{R}_- \subset \{x \in \mathbb{R} | \forall y > 0, x \leqslant y\}$.

— Soit $x \in \{x \in \mathbb{R} | \forall y > 0, x \leqslant y\}$. Alors $\forall y > 0$, $x \leqslant y$. En faisant tendre y vers 0, l'inégalité devient $x \leqslant 0$. Donc $x \in \mathbb{R}_-$. Donc $\{x \in \mathbb{R} | \forall y > 0, x \leqslant y\} \subset \mathbb{R}_-$.

On en déduit par double inclusion que $\mathbb{R}_- = \{x \in \mathbb{R} | \forall y > 0, x \leqslant y\}$.

Proposition 1.3 (Transitivité de l'inclusion)

Soit A, B et D trois ensembles,

$$(A \subset B \text{ et } B \subset D) \Longrightarrow (A \subset D).$$

Démonstration. Supposons que $A \subset B$ et $B \subset D$. Soit $x \in A$. Comme $A \subset B$, alors $x \in B$. Et comme $B \subset D$, on a aussi $x \in D$. Donc pour tout $x \in A$, on a aussi $x \in D$. Ce qui implique que $A \subset D$. □

1.3 Ensemble des parties de E

Définition 1.4 (Ensemble des parties)

Soit E un ensemble. L'ensemble des sous-ensembles de E est appelé **ensemble des parties** de E, et est noté $\mathcal{P}(E)$.

Remarque. Soit A un ensemble. La définition donne directement l'équivalence $A \in \mathcal{P}(E) \Leftrightarrow A \subset E$.

Remarque. Attention aux objets manipulés : On écrit $3 \in \mathbb{R}$, $\{3\} \subset \mathbb{R}$ et $\{3\} \in P(\mathbb{R})$.

Exercice 3. Soit $E = \{1, 2, 3, 4\}$. Déterminer $\mathcal{P}(E)$.
Solution :

$$\mathcal{P}(E) = \Big\{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}, \{1,2,3\}, \{1,2,4\}, \{1,3,4\}, \{2,3,4\}, \{1,2,3,4\}\Big\}.$$

1.4 Produit cartésien

Définition 1.5 (Produit cartésien)

Soit E et F deux ensembles. On appelle **produit cartésien** de E par F, noté $E \times F$, l'ensemble des couples ordonnés (x, y) où $x \in E$ et $y \in F$.

Remarque. On a donc :
— $E \times F = \{(x, y) | x \in E \text{ et } y \in F\}$.
— $u \in E \times F \Longleftrightarrow \exists x \in E, \exists y \in F$ tels que $u = (x, y)$.

Exemple. $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ est l'ensemble des couples de réels.

Remarque. On peut généraliser le produit cartésien à plus de deux ensembles : soit $(A_1, \ldots, A_n)$ des ensembles,

$$\prod_{i=1}^{n} A_i = A_1 \times A_2 \times \cdots \times A_n = \{(x_1, x_2, \ldots, x_n) | \forall i \in [\![1, n]\!], x_i \in A_i\}.$$

2 Opérations sur les ensembles

2.1 Complémentaire

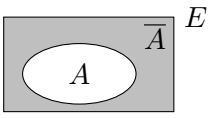
Définition 2.1 (Complémentaire)

Soit E et A deux ensembles, tels que $A \subset E$. On appelle **complémentaire** de A dans E l'ensemble des éléments de E qui ne sont pas dans A. On note

$$\overline{A} = \{x \in E | x \notin A\}.$$

Remarque. Les notations $E \setminus A$ ou A^c peuvent également être utilisées.

Exemple. Représentation graphique du complémentaire d'un ensemble A dans un ensemble E :



Remarque. En termes de quantificateurs, on a : soit $x \in E$,
- $x \in \overline{A} \iff x \notin A$.
- $x \notin \overline{A} \iff x \in A$.

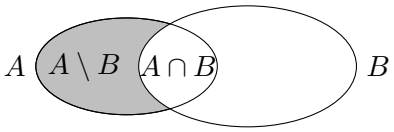
Remarque. On a également les relations suivantes :
- $\overline{E} = \emptyset$ et $\overline{\emptyset} = E$.
- $\overline{\overline{A}} = A$.
- $A \subset B \iff \overline{B} \subset \overline{A}$.

2.2 Intersection

Définition 2.2 (Intersection, différence)

Soit A et B deux ensembles.
- On appelle **intersection** de A et B et on note $A \cap B$ l'ensemble des éléments qui sont à la fois dans A et dans B.
- On appelle **différence** de A et B et on note $A \setminus B$ ou $A \cap \overline{B}$ l'ensemble des éléments de A qui ne sont pas dans B.

Exemple. Représentation graphique :



Exercice 4. On lance un dé trois fois de suite. Soit $i \in [\![1, 3]\!]$, on pose $S_i = \{$ au i-ème lancer, on tombe sur 6 $\}$. À l'aide des S_i, déterminer les ensembles $A = \{$ les trois lancers donnent 6 $\}$ et $B = \{$ aucun des lancers ne donne 6 $\}$.
Solution : On a $A = S_1 \cap S_2 \cap S_3$ et $B = \overline{S_1} \cap \overline{S_2} \cap \overline{S_3}$.

Remarque. On peut généraliser l'intersection à plus de deux ensembles : soit $(A_1, \ldots, A_n)$ des ensembles,

$$x \in \bigcap_{i=1}^{n} A_i \iff \forall i \in [\![1, n]\!], x \in A_i \quad \text{et} \quad x \in \bigcap_{i=1}^{+\infty} A_i \iff \forall i \in \mathbb{N}^*, x \in A_i.$$

Proposition 2.3 (Propriétés de l'intersection)

Soit A, B et D trois ensembles,
- $A \cap B \subset A$ et $A \cap B \subset B$,
- Si $A \subset B$, alors $A \cap B = A$,
- $A \cap (B \cap D) = (A \cap B) \cap D = A \cap B \cap D$.

Démonstration.
- $\forall x \in A \cap B$, $x \in A$. Donc $A \cap B \subset A$. De même, $A \cap B \subset B$.
- On suppose que $A \subset B$. On sait déjà que $A \cap B \subset A$. Réciproquement, soit $x \in A$. Comme $A \subset B$, alors $x \in B$, donc $x \in A \cap B$, et $A \subset A \cap B$. Par double inclusion, on obtient bien $A \cap B = A$.
- Les ensembles du troisième résultat sont tous égaux à $\{x$ tel que $x \in A, x \in B$ et $x \in D\}$, et donc égaux.

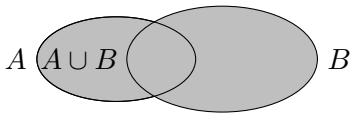
□

2.3 Réunion

Définition 2.4 (Réunion)

Soit A et B deux ensembles, on appelle **réunion** de A et B, notée $A \cup B$, l'ensemble des éléments appartenant à A ou à B.

Exemple. Représentation graphique :



Exercice 5. On lance un dé trois fois de suite. Soit $i \in [\![1, 3]\!]$, on pose $S_i = \{$ au i-ème lancer, on tombe sur 6 $\}$. À l'aide des S_i, déterminer les ensembles $C = \{$ au moins un lancer donne 6 $\}$ et $D = \{$ au plus deux lancers donnent 6 $\}$.
Solution : On a $C = S_1 \cup S_2 \cup S_3$ et $D = \overline{S_1} \cup \overline{S_2} \cup \overline{S_3}$.

Remarque. On peut généraliser la réunion à plus de deux ensembles : soit $(A_1, \ldots, A_n)$ des ensembles,

$$x \in \bigcup_{i=1}^{n} A_i \iff \exists i \in [\![1, n]\!], x \in A_i \quad \text{et} \quad x \in \bigcup_{i=1}^{+\infty} A_i \iff \exists i \in \mathbb{N}^*, x \in A_i.$$

Proposition 2.5 (Propriétés de la réunion)

Soit A, B et D trois ensembles,
- $A \subset A \cup B$ et $B \subset A \cup B$,
- Si $A \subset B$, alors $A \cup B = B$,
- $A \cup (B \cup D) = (A \cup B) \cup D = A \cup B \cup D$.

Démonstration.
- Soit $x \in A$, alors $x \in A \cup B$, donc $A \subset A \cup B$. De même, $B \subset A \cup B$.
- On suppose que $A \subset B$. On sait déjà que $B \subset A \cup B$. Soit $x \in A \cup B$. Alors $x \in B$ ou $x \in A$. Si $x \in A$, $x \in B$ car $A \subset B$. Donc $x \in B$, et $A \cup B \subset B$.
- Les ensembles du troisième résultat sont tous égaux à $\{x$ tel que $x \in A$ ou $x \in B$ ou $x \in D\}$, et donc égaux.

□

2.4 Propriétés de l'intersection et la réunion

Proposition 2.6 (Distributivité)

Soit A, B, D des ensembles,

$$A \cup (B \cap D) = (A \cup B) \cap (A \cup D) \quad \text{et} \quad A \cap (B \cup D) = (A \cap B) \cup (A \cap D).$$

Démonstration. On montre la première identité, la deuxième se montre de façon analogue.
- Soit $x \in A \cup (B \cap D)$. Alors $x \in A$ ou $x \in B \cap D$.
  - Si $x \in A$, alors $x \in (A \cup B) \cap (A \cup D)$.
  - Si $x \in B \cap D$, alors $x \in B$ et $x \in D$.
    Donc $x \in (A \cup B) \cap (A \cup D)$.

  Donc $A \cup (B \cap D) \subset (A \cup B) \cap (A \cup D)$.
- Réciproquement, soit $x \in (A \cup B) \cap (A \cup D)$.
  Alors $x \in A \cup B$ et $x \in A \cup D$.
  - Si $x \in A$, alors $x \in A \cup (B \cap D)$.
  - Si $x \notin A$, alors $x \in B$ et $x \in D$.
    Donc $x \in B \cap D$ et $x \in A \cup (B \cap D)$.

Donc $(A \cup B) \cap (A \cup D) \subset A \cup (B \cap D)$.
Par double inclusion, on obtient $A \cup (B \cap D) = (A \cup B) \cap (A \cup D)$. □

Exercice 6. Soit E un ensemble et X et Y deux sous-ensembles de E. Simplifier l'expression $(X \cap Y) \cup (X \cap \overline{Y})$.
Solution : Par distributivité,

$$(X \cap Y) \cup (X \cap \overline{Y}) = X \cap (Y \cup \overline{Y}) = X \cap E = X.$$

Proposition 2.7 (Passage au complémentaire)

Soit A, B des ensembles,

$$\overline{A \cap B} = \overline{A} \cup \overline{B} \quad \text{et} \quad \overline{A \cup B} = \overline{A} \cap \overline{B}.$$

Démonstration. On montre la première identité, la deuxième se montre de façon analogue. On commence par remarquer que :

$$x \in \overline{A \cap B} \iff x \notin A \cap B \iff x \notin A \text{ ou } x \notin B \iff x \in \overline{A} \text{ ou } x \in \overline{B} \iff x \in \overline{A} \cup \overline{B}.$$

Les implications de gauche à droite donnent $\overline{A \cap B} \subset \overline{A} \cup \overline{B}$ et les réciproques donnent $\overline{A} \cup \overline{B} \subset \overline{A \cap B}$. Donc par double inclusion, $\overline{A \cap B} = \overline{A} \cup \overline{B}$. □

2.5 Partitions

Définition 2.8 (Ensembles disjoints)

Soit A et B deux ensembles. On dit que A et B sont **disjoints** lorsque $A \cap B = \emptyset$.

Définition 2.9 (Ensembles deux à deux disjoints)

Soit A_1, A_2, …, A_n des ensembles. On dit qu'ils sont **deux à deux disjoints** lorsque $\forall i \neq j$, $A_i \cap A_j = \emptyset$.

Définition 2.10 (Partition)

Soit E un ensemble et A_1, A_2, … A_n des sous-ensembles de E. On dit que les A_i forment une **partition** ou un **recouvrement disjoint** de E lorsqu'ils sont deux à deux disjoints et qu'on a $E = \bigcup_{i=1}^{n} A_i$.

Exemple. Ajouter un exemple de représentation graphique.

Remarque. Cette notion sera très utile pour les chapitres de dénombrement et de probabilités.

Exemple. Si A est un sous-ensemble de E, alors $(A, \overline{A})$ est une partition de E.

Exemple. $[0, 1[$, $[1, 2[$ et $\{2\}$ forment une partition de $[0, 2]$.

3 Ensembles usuels

3.1 Quelques rappels

Définition 3.1 (Ensembles usuels)

On appelle 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 ensemble des **nombres décimaux** l'ensemble $\mathbb{D} = \left\{ \frac{p}{10^n} \middle| p \in \mathbb{Z}, n \in \mathbb{N} \right\}$, c'est-à-dire l'ensemble des nombres ayant un nombre fini de chiffres après la virgule.
On appelle ensemble des **nombres rationnels** l'ensemble $\mathbb{Q} = \left\{ \frac{p}{q} \middle| p \in \mathbb{Z}, q \in \mathbb{N}^* \right\}$ et ensemble des **nombres irrationnels** l'ensemble $\mathbb{R} \setminus \mathbb{Q}$.

Remarque. On a $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{D} \subset \mathbb{Q} \subset \mathbb{R}$ et ces inclusions sont strictes.

3.2 Applications à l'arithmétique

Définition 3.2 (Multiple, diviseur)

Soient $(a, b) \in \mathbb{Z}^2$. On dit que a **divise** b ou que a est **un diviseur** de b ou que b est un **multiple** de a s'il existe un entier $k \in \mathbb{Z}$ pour lequel $b = ak$.

Remarque. Si $a \in \mathbb{Z}$, les multiples de a sont l'ensemble $a\mathbb{Z} = \{ak | k \in \mathbb{Z}\}$.

Proposition 3.3 (Diviseur d'une combinaison linéaire)

Soient $(a, b, d, \lambda, \mu) \in \mathbb{Z}^5$. Si d divise a et b, alors d divise $\lambda a + \mu b$.

Démonstration. On suppose que d divise a et b, donc il existe des entiers k et k' tels que $a = kd$ et $b = k'd$. On en déduit :

$$\lambda a + \mu b = d(\lambda k + \mu k').$$

Or $\lambda k + \mu k'$ est un entier. Donc d divise $\lambda a + \mu b$. □

Proposition 3.4 (Théorème de division euclidienne)

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ pour lequel $a = bq + r$ et $0 \leqslant r < b$.
On appelle a le **dividende** de la division euclidienne, b son **diviseur**, q son **quotient** et r son **reste**.

Remarque. Il est important de remarquer que ce théorème donne à la fois l'existence et l'unicité.

Démonstration. On commence par la preuve de l'existence. Soit $\mathcal{D} = \mathbb{N} \cap \{a - bk | k \in \mathbb{Z}\}$. C'est une partie non vide de $\mathbb{N}$ (si $a \geqslant 0$, $a \in \mathcal{D}$, si $a \leqslant 0$, comme $b \geqslant 1$, on trouve $ab \leqslant a$ et donc $a - ba \in \mathcal{D}$), $\mathcal{D}$ admet donc un plus petit élément que l'on note r. Par définition de $\mathcal{D}$, il existe donc un entier $q \in \mathbb{Z}$ tel que $r = a - bq$, et donc $a = bq + r$. Reste à vérifier les hypothèses sur r. On a $r \geqslant 0$ puisque $r \in \mathcal{D}$. Supposons que $r \geqslant b$. Alors, $r - b \geqslant 0$, donc $r - b \in \mathcal{D}$, ce qui est impossible puisque r est le plus petit élément de $\mathcal{D}$. Donc $r < b$.
Montrons maintenant l'unicité. Soit $(q, r) \in \mathbb{Z} \times \mathbb{N}$ et $(q', r') \in \mathbb{Z} \times \mathbb{N}$ deux couples qui satisfont aux conditions. Alors $bq + r = a = bq' + r'$, donc :

$$b(q - q') = r' - r.$$

Par ailleurs, $0 \leqslant r < b$ et $0 \leqslant r' < b$, donc $-b < r' - r < b$. On en déduit que$-b < b(q - q') < b$. En divisant par $b > 0$, on obtient $-1 < q - q' < 1$. Puisque $q - q' \in \mathbb{Z}$, on en déduit que $q - q' = 0$. Donc $q = q'$, d'où $r' - r = 0$ et $r = r'$. Cela permet de conclure que la décomposition est unique. □

Exemple. Pour déterminer la division euclidienne dans un cas concret, il suffit de la poser :

$$\begin{array}{r|l} 264 & 5 \\ \cline{2-2} 14 & 52 \\ 4 & \end{array}$$

Ici, on a donc $264 = 52 \times 5 + 4$, avec $0 \leqslant 4 < 5$.

Définition 3.5 (PCGD)

Soit $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$. Soit $\mathcal{D}$ l'ensemble des diviseurs qui sont communs à a et b. On appelle **PGCD** (plus grand commun diviseur) de a et b le plus grand élément de $\mathcal{D}$.

Démonstration. L'ensemble $\mathcal{D}$ est un ensemble d'entiers non vide (il contient 1) et majoré (par $|a|$ ou $|b|$), il contient donc bien un plus grand élément. □

Exemple. Les diviseurs communs à 12 et à 18 sont ± 1, ± 2, ± 3, ± 6, donc le PCGD de 12 et 18 vaut 6.

Proposition 3.6 (PGCD d'un entier et de 0)

Soit $a \in \mathbb{Z}^*$, alors le PGCD de a et 0 vaut $|a|$.

Démonstration. $|a|$ est le plus grand diviseur de a. Comme tous les diviseurs de a divisent aussi 0, on en déduit le résultat annoncé. □

Proposition 3.7 (PGCD et division euclidienne)

Soit $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$, et soit r le reste de la division euclidienne de a par b. Alors le PGCD de a et b et le PGCD de b et r sont égaux.

Démonstration. On pose D_1 l'ensemble des diviseurs communs à a et b, D_2 celui des diviseurs communs à b et r. Soit q le quotient de la division euclidienne de a par b.

— Soit $d \in D_1$ Alors, d divise b et divise $a - bq = r$. Donc $d \in D_2$. Donc $D_1 \subset D_2$.

— Soit $d \in D_2$. Alors d divise b et divise $bq + r = a$. Donc $d \in D_1$. Donc $D_2 \subset D_1$.

Donc $D_1 = D_2$. Donc ils ont les mêmes plus grands éléments. Donc le PGCD de a et b et le PGCD de b et r sont égaux. □

Remarque. Cette proposition est à la base de l'algorithme d'Euclide : on effectue des divisions euclidiennes successives jusqu'à obtenir un reste nul. Le PGCD recherché correspondra donc au dernier reste non nul.

Exercice 7. En utilisant l'algorithme d'Euclide, déterminer le PGCD de 12 et 18.
Solution : On procède par divisions euclidiennes successives :

$$18 = 12 \times 1 + 6 \text{ avec } 0 \leqslant 6 < 12$$
$$12 = 6 \times 2 + 0 \text{ avec } 0 \leqslant 0 < 6$$

On retrouve donc bien que le PGCD vaut 6 (le dernier reste non nul), beaucoup plus vite qu'en listant tous les diviseurs.

Définition 3.8 (PPCM)

Soit $(a, b) \in (\mathbb{Z}^*)^2$. Soit $\mathcal{M}$ l'ensemble des multiples strictement positifs qui sont communs à a et b. On appelle **PPCM** (plus petit commun multiple) de a et b le plus petit élément de $\mathcal{M}$.

Démonstration. L'ensemble $\mathcal{M}$ est un ensemble d'entiers non vide (il contient $|ab|$) et minoré (par 0), il contient donc bien un plus petit élément. □

Exemple. On cherche les multiples strictement positifs communs à 12 et 18. Ceux de 12 sont 12, 24, 36, 48... Ceux de 18 sont 18, 36, 54... Le PPCM de 12 et 18 est donc 36.

3.3 Ensemble des nombres premiers

Définition 3.9 (Nombre premier)

Soit $p \in \mathbb{N}$. On dit que p est un **nombre premier** si $p \neq 1$ et si ses seuls diviseurs positifs sont 1 et p.

Remarque. Le crible d'Ératosthène (à tracer) permet d'obtenir facilement les valeurs des petits nombres premiers : 2, 3, 5, 7, 11, 13, 17, 19...

Proposition 3.10 (Décomposition en produit de facteurs premiers)

Tout entier naturel non nul se décompose de manière unique (à l'ordre des facteurs près) comme produit de nombre premiers.

Démonstration. Hors-programme (l'existence se ferait par récurrence forte). □

Remarque. Cette décomposition en produit de facteurs premiers fournit aussi une autre méthode de calcul pour le PGCD ou le PPCM de deux entiers a et b :

- la décomposition en facteurs premiers du PGCD de a et b est constituée des facteurs qui apparaissent **à la fois dans a et dans b**, chacun affecté du **plus petit exposant** qui apparaît dans une des décompositions.
- la décomposition en facteurs premiers du PPCM de a et b est constituée des facteurs qui apparaissent **dans a ou dans b**, chacun affecté du **plus grand exposant** qui apparaît dans une des décompositions.

Exercice 8. En utilisant une décomposition en facteurs premiers, déterminer le PGCD et le PPCM de 12 et 18.
Solution : On a $12 = 2 \times 2 \times 3 = 2^2 \times 3$ et $18 = 2 \times 3 \times 3 = 2 \times 3^2$. Donc le PGCD vaut $2 \times 3 = 6$ et le PPCM $2^2 \times 3^2 = 36$.

Proposition 3.11 (Ensemble des nombres premiers)

L'ensemble des nombres premiers est infini.

Démonstration. Supposons que l'ensemble des nombres premiers est fini à $n \in \mathbb{N}^*$ éléments. On peut alors noter p_1, p_2, …, p_n la liste complète des nombres premiers.
On pose $N = p_1 \times p_2 \times \ldots \times p_n + 1$. On a $N > 1$, donc $\exists k \in [\![1, n]\!]$ tel que p_k divise N. Or p_k divise aussi $p_1 \times p_2 \times \ldots \times p_n$, donc p_k divise $N - p_1 \times p_2 \times \ldots \times p_n = 1$. Absurde, car 1 n'admet pas de diviseur premier.
L'ensemble des nombres premiers est donc infini. □