Chapitre 4 : L'ensemble $\mathbb{N}$

I Ce qui est admis ou supposé connu

- $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.
- $+$ et $\times$ constituent des l.c.i sur $\mathbb{N}$ avec les propriétés suivantes :
  - ◇ $+$ et $\times$ sont associatives et commutatives.
  - ◇ $\times$ est distributive sur $+$.
  - ◇ 0 est neutre pour $+$.
  - ◇ 1 est neutre pour $\times$.
- $\leqslant$ constitue une relation d'ordre total sur $\mathbb{N}$.
- Les calculs dans $\mathbb{N}$ sont supposés connus.
- Pour l'arithmétique, voir plus tard.

Théorème :
Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

Théorème :
$\mathbb{N}$ n'a pas de maximum, mais toute partie non vide majorée de $\mathbb{N}$ admet un plus grand élément.

Démonstration :
Soit A une partie non vide majorée de $\mathbb{N}$. Soit B l'ensemble des majorants de A. $B \neq \varnothing$ car A est majorée. Donc B admet un plus petit élément, disons m. Montrons que $m \in A$. Supposons que $m \notin A$. Comme m est un majorant de A, on a donc $\forall x \in A, x < m$. Cela impose que $m \geqslant 1$ (sinon on aurait $\forall x \in A, x < 0$, ce qui est impossible car $A \neq \varnothing$), et que $\forall x \in A, x \leqslant m - 1$. Donc $m - 1$ est un majorant de A. Or, m est le plus petit élément de B. On a donc une contradiction. Donc $m \in A$ et m majore A. Donc m est le plus grand élément de A. (On utilise le fait que pour tout $x \in \mathbb{N}$, l'ensemble des $y \in \mathbb{N}$ tels que $x < y$ admet un plus petit élément qui n'est autre que $x + 1$.)

II Principe de récurrence

Théorème :
Soit $\mathcal{P}$ une propriété définie sur $\mathbb{N}$. Si on a :

- $\mathcal{P}(0)$ (est vraie)

- $\forall n \in \mathbb{N}, (\mathcal{P}(n) \implies \mathcal{P}(n+1))$ (est vrai)

Alors $\forall n \in \mathbb{N}, \mathcal{P}(n)$ (est vraie)

Démonstration :
Soit E l'ensemble des éléments de $\mathbb{N}$ tels que non$(\mathcal{P}(n))$. Montrons que E est vide. Supposons E non vide. Alors E admet un plus petit élément m. $m \neq 0$ car $\mathcal{P}(0)$ est vraie. On introduit donc $m-1$. $m-1 \notin E$ car m en est le plus petit élément. Donc $\mathcal{P}(m-1)$ est vraie. Or, $\mathcal{P}(m-1) \implies \mathcal{P}(m)$. Donc $\mathcal{P}(m)$ est vraie. Donc $m \notin E$. On a donc une contradiction. Donc E est vide. Donc $\forall n \in \mathbb{N}, \mathcal{P}(n)$.

Exemple :

- Montrons par récurrence que $\forall n \in \mathbb{N}, \underbrace{\sum_{k=1}^{n} k = \frac{n(n+1)}{2}}_{\mathcal{P}(n)}$:
  - Déjà, on a bien $\mathcal{P}(0)$ car $0 = 0$.
  - Montrons que $\forall n \in \mathbb{N}, (\mathcal{P}(n) \implies \mathcal{P}(n+1))$.
    Soit $n \in \mathbb{N}$. Supposons $\mathcal{P}(n)$, montrons $\mathcal{P}(n+1)$:
    $$\sum_{k=1}^{n+1} k = \left(\sum_{k=1}^{n} k\right) + n + 1 = \frac{n(n+1)}{2} + n + 1 = \frac{n+1}{2} \times (n+2) = \frac{(n+1)(n+2)}{2} \tag{4.1}$$
  - On a montré que si on a $\mathcal{P}(n)$, alors on a $\mathcal{P}(n+1)$. Or, on l'a fait pour n quelconque. Donc $\forall n \in \mathbb{N}, (P(n) \implies P(n+1))$. On en déduit donc selon le principe de récurrence que $\forall n \in \mathbb{N}, \mathcal{P}(n)$.

  (On peut remplacer ce dernier paragraphe par « ce qui achève la récurrence »).
- Montrons par récurrence que $\forall n \in \mathbb{N}, \mathcal{Q}(n)$, où $\mathcal{Q}(n)$ signifie : « pour tout ensemble E de cardinal n, l'ensemble $\mathscr{P}(E)$ des parties de E est de cardinal 2^n » :
  - $\mathcal{Q}(0)$ est vraie car $\varnothing$ a une seule partie, à savoir $\varnothing$. C'est-à-dire que $\mathscr{P}(\varnothing)$ a un élément, $\varnothing$, ou encore $\mathscr{P}(\varnothing) = \{\varnothing\}$, de cardinal 1.
  - Montrons que $\forall n \in \mathbb{N}, (\mathcal{Q}(n) \implies Q(n+1))$: soit $n \in \mathbb{N}$. Supposons $\mathcal{Q}(n)$. Soit E un ensemble de cardinal $n+1$. Soit $a \in E$ (il en existe car card$(E) > 0$). On note $A = E \backslash \{a\}$. Alors les parties de E se répartissent en deux catégories : celles qui n'ont pas a et celles qui l'ont. Celles qui ne contiennent pas a, il y en a 2^n (ce sont les parties de A). Celles qui contiennent pas a, il y en a autant (ce sont les parties de A auxquelles on ajoute a). Il en résulte que card$(\mathscr{P}(E)) = 2^n + 2^n = 2^{n+1}$, ce qui achève la récurrence.

III Variantes de récurrence

Théorème :
Soit $\mathcal{P}$ une propriété définie sur $\mathbb{N}^*$. Si :

- $\mathcal{P}(1)$,
- $\forall n \in \mathbb{N}^*, (\mathcal{P}(n) \implies \mathcal{P}(n+1))$,

alors $\forall n \in \mathbb{N}^*, \mathcal{P}(n)$.

Démonstration :
Soit $\mathcal{P}$ une propriété définie sur $\mathbb{N}^*$, supposons $\mathcal{P}(1)$ et que $\forall n \in \mathbb{N}^*, (\mathcal{P}(n) \implies \mathcal{P}(n+1))$. Soit $\mathcal{Q}$ la propriété définie sur $\mathbb{N}$ par $\forall n \in \mathbb{N}, (\mathcal{Q}(n) \iff \mathcal{P}(n+1))$. Alors :

- $\mathcal{Q}(0)$ est vraie, car $\mathcal{P}(1)$ est vraie.
- Soit $n \in \mathbb{N}$, supposons $\mathcal{Q}(n)$. Alors $\mathcal{P}(n+1)$. Donc $\mathcal{P}(n+2)$. Donc $\mathcal{Q}(n+1)$. Donc $\forall n \in \mathbb{N}, (\mathcal{Q}(n) \implies \mathcal{Q}(n+1))$.

Donc, selon le principe de base de récurrence, $\forall n \in \mathbb{N}, \mathcal{Q}(n)$. Donc $\forall n \in \mathbb{N}, \mathcal{P}(n+1)$. Donc $\forall m \in \mathbb{N}^*, \mathcal{P}(m)$.

Théorème (récurrence double) :
Soit $\mathcal{P}$ une propriété définie sur $\mathbb{N}$. Si :

- $\mathcal{P}(0)$ et $\mathcal{P}(1)$,
- $\forall n \in \mathbb{N}, (\mathcal{P}(n) \implies P(n+2))$,

alors $\forall n \in \mathbb{N}, \mathcal{P}(n)$.

Démonstration :
On fait de la même façon que pour le théorème précédent avec $\mathcal{Q}$ définie par :

$$\forall n \in \mathbb{N}, (\mathcal{Q}(n) \iff P(n) \text{ et } \mathcal{P}(n+1)) \tag{4.2}$$

En prenant les hypothèses du théorème, on a :

- $\mathcal{Q}(0)$ est vraie car $\mathcal{P}(0)$ et $\mathcal{P}(1)$ le sont.
- Soit $n \in \mathbb{N}$, supposons $\mathcal{Q}(n)$. Alors $\mathcal{P}(n)$ et $\mathcal{P}(n+1)$, donc $\mathcal{P}(n+2)$ et $\mathcal{P}(n+1)$. Donc $\mathcal{Q}(n+1)$. Donc $\forall n \in \mathbb{N}, (\mathcal{Q}(n) \implies \mathcal{Q}(n+1))$.

Donc $\forall n \in \mathbb{N}, \mathcal{Q}(n)$. Donc $\forall n \in \mathbb{N}, \mathcal{P}(n)$.

Théorème (récurrence forte) :
Soit $\mathcal{P}$ une propriété définie sur $\mathbb{N}$. Si :

- $\mathcal{P}(0)$.
- $\forall n \in \mathbb{N}, (\forall k \in [\![0, n]\!], \mathcal{P}(k)) \implies \mathcal{P}(n+1)$ (les $[\![,]\!]$ s'utilisent pour les entiers).

Alors $\forall n \in \mathbb{N}, \mathcal{P}(n)$. (C'est-à-dire que pour tout $n \in \mathbb{N}$, si la propriété est vraie jusqu'au rang n, alors elle est vraie au rang $n+1$)

Démonstration :
On définit cette fois-ci $\mathcal{Q}$ par :

$$\forall n \in \mathbb{N}, (\mathcal{Q}(n) \iff (\forall k \in [\![0, n]\!], \mathcal{P}(k))) \tag{4.3}$$

- Alors $\mathcal{Q}(0)$ est vraie car $\mathcal{P}(0)$ l'est, donc $\forall k \in [\![0, 0]\!] \mathcal{P}(k)$.
- Soit $n \in \mathbb{N}$, supposons $\mathcal{Q}(n)$, alors $\forall k \in [\![0, n]\!], \mathcal{P}(k)$, donc $\mathcal{P}(n+1)$, donc $\forall k \in [\![0, n+1]\!], \mathcal{P}(k)$, donc $\mathcal{Q}(n+1)$. Donc $\forall n \in \mathbb{N}, (\mathcal{Q}(n) \implies \mathcal{Q}(n+1))$

Donc $\forall n \in \mathbb{N}, \mathcal{Q}(n)$, donc $\forall n \in \mathbb{N}, \mathcal{P}(n)$.

Théorème (récurrence finie) :
Soit m un entier naturel non nul. Soit $\mathcal{P}$ une propriété définie sur $[\![0, m]\!]$. Si :

- $\mathcal{P}(0)$,
- $\forall n \in [\![0, m-1]\!], (\mathcal{P}(n) \implies \mathcal{P}(n+1))$,

alors $\forall n \in [\![0, m]\!], \mathcal{P}(n)$.

Théorème (récurrence finie descendante) :
Soit m un entier naturel non nul. Soit $\mathcal{P}$ une propriété définie sur $[\![0, m]\!]$. Si :

- $\mathcal{P}(m)$,
- $\forall n \in [\![1, m]\!], (\mathcal{P}(n) \implies \mathcal{P}(n-1))$,

alors $\forall n \in [\![0, m]\!], \mathcal{P}(n)$.

IV Un peu d'arithmétique

A) Division euclidienne dans $\mathbb{N}$

Théorème :
Soient $a, b \in \mathbb{N}$, $b \neq 0$. Alors il existe un unique couple $(q, r) \in \mathbb{N} \times \mathbb{N}$ tel que :

$$\begin{cases} a = bq + r \\ 0 \leqslant r < b \end{cases} \tag{4.4}$$

q est le quotient, r le reste dans la division euclidienne de a par b.

Démonstration :

Unicité Supposons $\begin{cases} a = bq + r \quad \text{et } 0 \leqslant r < b \\ a = bq' + r' \text{ et } 0 \leqslant r' < b \end{cases}$. Alors $bq - bq' = r' - r$, soit $b(q - q') = r' - r$. Or, $-b < r' - r < b$. Supposons par exemple $r' \geqslant r$ (sinon on inverse les rôles). Alors, $0 \leqslant r' - r < b$, donc $q - q' = 0$, car sinon $q - q' \geqslant 1$ et $b(q - q') \geqslant b$ soit $r - r' \geqslant b$. Donc $(q, r) = (q', r')$.

Existence Soit $E = \{k \in \mathbb{N}, bk \leqslant a\}$. Alors $E \subset \mathbb{N}$, E est non vide, car $0 \in E$ et est majoré par a : $k \leqslant bk \leqslant a$. Donc E admet un maximum, qu'on note q. On a alors : $bq \leqslant a < b(q+1)$ (car $q \in E$ et $q + 1 \notin E$ puisque $q = \max(E)$). Donc $0 \leqslant a - bq < b(q+1) - bq$, soit $0 \leqslant a - bq < b$. On note $r = a - bq$. Alors $\begin{cases} a = bq + r \\ 0 \leqslant r < b \end{cases}$.

B) Numération en base quelconque

Théorème :
Soit $\beta \in \mathbb{N}\backslash\{0,1\}$. Soit $A \in \mathbb{N}$. Alors il existe une unique suite $(a_k)_{k\in\mathbb{N}}$ d'entiers de l'ensemble $[\![0, \beta-1]\!]$ nulle à partir d'un certain rang telle que :

$$A = a_0 \times \beta^0 + a_1 \times \beta^1 + a_2 \times \beta^2 + \ldots + a_n \times \beta^n \tag{4.5}$$

(n est tel que $\forall k > n, a_k = 0$) qu'on note $\sum_{k\in\mathbb{N}} a_k\beta^k$ (somme faussement infinie). On note alors $A = \overline{(a_n a_{n-1} \ldots a_1 a_0)}_\beta$.

Démonstration :
Notons S_F l'ensemble des suites de $\{0, \ldots \beta-1\}$ nulles à partir d'un certain rang. Pour $a \in S_F$, les termes de la suite a sont notés $a_0, a_1, a_2, \ldots$. Montrons par récurrence forte que $\forall A \in \mathbb{N}$, $(\exists! a \in S_F, A = \sum_{k\in\mathbb{N}} a_k\beta^k)$.

- $\mathcal{P}(0)$ est vrai : si on prend, pour tout $k \in \mathbb{N}$, $a_k = 0$, on a bien $\sum_{k\in\mathbb{N}} a_k\beta^k = 0$, et si un des termes de a n'est pas nul, alors $\sum_{k\in\mathbb{N}} a_k\beta^k \neq 0$.
- Soit $A \in \mathbb{N}^*$, supposons que $\forall B \in [\![0, A-1]\!], \mathcal{P}(B)$. Montrons qu'alors $\mathcal{P}(A)$. La division euclidienne de A par β donne :

$$\begin{cases} A = \beta Q + r \\ r \in \{0, 1, \ldots \beta - 1\} \end{cases} \tag{4.6}$$

Alors $Q \in [\![0, A-1]\!]$: on a $\beta > 1$ et $Q > 0$. Donc $Q < \beta Q \leqslant \beta Q + r = A$, donc $Q < A$. Donc $\mathcal{P}(Q)$: il existe une unique suite $(q_k)_{k\in\mathbb{N}} \in S_F$ telle que $Q = \sum_{k\in\mathbb{N}} q_k\beta^k$. Donc $A = \left(\sum_{k\in\mathbb{N}} q_k\beta^{k+1}\right) + r = \sum_{k\in\mathbb{N}} a_k\beta^k$ avec $\begin{cases} a_0 = r \\ \forall k \geqslant 1, a_k = q_{k-1} \end{cases}$. D'où l'existence de la suite.
Si une autre suite $(a'_k)_{k\in\mathbb{N}}$ convient, alors :

$$A = \sum_{k\in\mathbb{N}} a'_k\beta^k = \sum_{k\in\mathbb{N}^*} a'_k\beta^k + a'_0 = \beta \sum_{k\in\mathbb{N}^*} a'_k\beta^{k-1} + a'_0 \tag{4.7}$$

Comme $a'_0 \in [\![0, \beta-1]\!]$, on a alors $a'_0 = r$ et $\sum_{k\in\mathbb{N}^*} a'_k\beta^{k-1} = Q$ (par unicité du couple (Q, r)). Donc $a'_0 = a_0$, et $\forall k \in \mathbb{N}^*, a'_k = q_{k-1} = a_k$ par hypothèse de récurrence. D'où l'unicité de la suite.

Cette démonstration donne un algorithme pour obtenir les chiffres.

Exemple :

- Donner 2003 en base 3.

  Division euclidienne de 2003 par 3 : 667 reste 2
  Division euclidienne de 667 par 3 : 222 reste 1
  Division euclidienne de 222 par 3 : 74 reste 0
  Division euclidienne de 74 par 3 : 24 reste 2
  Division euclidienne de 24 par 3 : 8 reste 0
  Division euclidienne de 8 par 3 : 2 reste 2
  Division euclidienne de 2 par 3 : 0 reste 2

Donc, en remontant :

$$\begin{aligned}
2 &= \bar{2}_3 = 2 \times 3^0 \\
8 &= 2 \times 3^1 + 2 \times 3^0 \\
74 &= 2 \times 3^2 + 2 \times 3^1 + 0 \times 3^0 \\
222 &= 2 \times 3^3 + 2 \times 3^2 + 0 \times 3^1 + 2 \times 3^0 \\
667 &= 2 \times 3^4 + 2 \times 3^3 + 0 \times 3^2 + 2 \times 3^1 + 1 \times 3^0 \\
2003 &= 2 \times 3^5 + 2 \times 3^4 + 0 \times 3^3 + 2 \times 3^2 + 1 \times 3^1 + 2 \times 3^0
\end{aligned} \tag{4.8}$$

Donc $2003 = \overline{(2202012)}_3$.

- 2003 en base 2 :

$$\begin{aligned}
2003 &= 1001 \times 2 + 1 \\
1001 &= 500 \times 2 + 1 \\
500 &= 250 \times 2 + 0 \\
250 &= 125 \times 2 + 0 \\
125 &= 62 \times 2 + 1 \\
62 &= 31 \times 2 + 0 \\
31 &= 15 \times 2 + 1 \\
15 &= 7 \times 2 + 1 \\
7 &= 3 \times 2 + 1 \\
3 &= 1 \times 2 + 1 \\
1 &= 0 \times 2 + 1
\end{aligned} \tag{4.9}$$

Donc $2003 = \overline{(11111010011)}_2$

- 2003 en base 12 : on utilise les symboles 0, 1, 2,..., A, B.

$$\begin{aligned}
2003 &= 166 \times 12 + 11 \\
166 &= 13 \times 12 + 10 \\
13 &= 1 \times 12 + 1 \\
1 &= 0 \times 12 + 1
\end{aligned} \tag{4.10}$$

Donc $2003 = \overline{(11AB)}_{12}$