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

I Ce qui est admis ou supposé connu

- $\mathbb{N} = \{0,1,2,3,...\}$

- $+$ 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 $\times$

- $\leq$ constitue une relation d'ordre total sur $\mathbb{N}$.

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 $m \geq 1$ (sinon on aurait $\forall x \in A, x < 0$, ce qui est impossible car $A \neq \varnothing$) et que $\forall x \in A, x \leq m-1$. 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 $x+1$).

- Les calculs dans $\mathbb{N}$ sont supposés connus.
- Pour l'arithmétique, voir plus tard.

II Principe de récurrence

Théorème :
Soit P une propriété définie sur $\mathbb{N}$. Si on a :
(1) P(0) (est vraie)
(2) $\forall n \in \mathbb{N}, (\mathrm{P}(n) \Rightarrow \mathrm{P}(n+1))$ (est vrai)
Alors $\forall n \in \mathbb{N}, \mathrm{P}(n)$ (est vraie).

Démonstration :
Supposons (1) et (2).
Soit E l'ensemble des éléments de $\mathbb{N}$ tels que $\text{non}(\mathrm{P}(n))$. Montrons que E est vide.
Supposons E non vide. Alors E admet un plus petit élément m.
$m \neq 0$ car $\mathrm{P}(0)$ est vraie.
On introduit donc $m-1$. $m-1 \notin E$ car m en est le plus petit élément. Donc $\mathrm{P}(m-1)$ est vraie. Or, $\mathrm{P}(m-1) \Rightarrow \mathrm{P}(m)$. Donc $\mathrm{P}(m)$ est vraie. Donc $m \notin E$. On a donc une contradiction. Donc E est vide. Donc $\forall n \in \mathbb{N}, \mathrm{P}(n)$.

Exemples :

- Montrons par récurrence que $\forall n \in \mathbb{N}, \underbrace{\sum_{k=1}^{n} k = \frac{n(n+1)}{2}}_{\mathrm{P}(n)}$
  - Déjà, on a bien $\mathrm{P}(0)$ car $0 = 0$
  - Montrons que $\forall n \in \mathbb{N}, (\mathrm{P}(n) \Rightarrow \mathrm{P}(n+1))$

  Soit $n \in \mathbb{N}$. Supposons $\mathrm{P}(n)$, montrons $\mathrm{P}(n+1)$
  $$\sum_{k=1}^{n+1} k = \sum_{k=1}^{n} k + n + 1 = \frac{n(n+1)}{2} + n + 1 = \frac{n+1}{2} \times (n+2) = \frac{(n+1)(n+2)}{2}$$
  On a montré que si on a $\mathrm{P}(n)$, alors on a $\mathrm{P}(n+1)$. Or, on l'a fait pour n quelconque. Donc $\forall n \in \mathbb{N}, (\mathrm{P}(n) \Rightarrow \mathrm{P}(n+1))$
  - On en déduit donc selon le principe de récurrence que $\forall n \in \mathbb{N}, \mathrm{P}(n)$

  (On peut remplacer ces trois dernières lignes par « ce qui achève la récurrence »)
- Montrons par récurrence que $\forall n \in \mathbb{N}, \mathrm{P}(n)$, où $\mathrm{P}(n)$ signifie : « pour tout ensemble E de cardinal n, $P(E)$ est de cardinal 2^n »
  - $\mathrm{P}(0)$ est vraie car $\varnothing$ a une seule partie, à savoir $\varnothing$.

  C'est-à-dire que $P(\varnothing)$ a un élément, $\varnothing$, ou encore $P(\varnothing) = \{\varnothing\}$, de cardinal 1.
  - Montrons que $\forall n \in \mathbb{N}, (\mathrm{P}(n) \Rightarrow \mathrm{P}(n+1))$

  Soit $n \in \mathbb{N}$. Supposons $\mathrm{P}(n)$. Soit E un ensemble de cardinal $n+1$.
  Soit $a \in E$ (il en existe car $\text{card}(E) > 0$)
  On note $A = E \setminus \{a\}$. 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 $\text{card}(P(E)) = 2^n + 2^n = 2^{n+1}$
  Ce qui achève la récurrence.

III Variantes de récurrence

Théorème :
Soit P une propriété définie sur $\mathbb{N}^*$. Si :
(1) $\mathrm{P}(1)$
(2) $\forall n \in \mathbb{N}^*, (\mathrm{P}(n) \Rightarrow \mathrm{P}(n+1))$
Alors $\forall n \in \mathbb{N}^*, \mathrm{P}(n)$.

Démonstration :

Soit P une propriété définie sur $\mathbb{N}^*$, supposons P(1) et que $\forall n \in \mathbb{N}^*, (\mathrm{P}(n) \Rightarrow \mathrm{P}(n+1))$

Soit Q la propriété définie sur $\mathbb{N}$ par $\forall n \in \mathbb{N}, (\mathrm{Q}(n) \Leftrightarrow \mathrm{P}(n+1))$

Alors Q(0) est vraie, car P(1) est vraie.

Soit $n \in \mathbb{N}$, supposons $\mathrm{Q}(n)$. Alors $\mathrm{P}(n+1)$. Donc $\mathrm{P}(n+2)$. Donc $\mathrm{Q}(n+1)$

Donc $\forall n \in \mathbb{N}, (\mathrm{Q}(n) \Rightarrow \mathrm{Q}(n+1))$

Donc, selon le principe de base de récurrence, $\forall n \in \mathbb{N}, \mathrm{Q}(n)$

Donc $\forall n \in \mathbb{N}, \mathrm{P}(n+1)$. Donc $\forall m \in \mathbb{N}^*, \mathrm{P}(m)$

Théorème (récurrence double) :

Soit P une propriété définie sur $\mathbb{N}$. Si :

(1) P(0) et P(1)

(2) $\forall n \in \mathbb{N}, (\mathrm{P}(n) \Rightarrow \mathrm{P}(n+2))$

Alors $\forall n \in \mathbb{N}, \mathrm{P}(n)$.

Démonstration :

On fait de la même façon que pour le théorème précédent avec Q définie par :

$\forall n \in \mathbb{N}, (\mathrm{Q}(n) \Leftrightarrow \mathrm{P}(n) \text{ et } \mathrm{P}(n+1))$

En prenant les hypothèses du théorème, on a :

Q(0) est vraie car P(0) et P(1) le sont

Soit $n \in \mathbb{N}$, supposons $\mathrm{Q}(n)$. Alors $\mathrm{P}(n)$ et $\mathrm{P}(n+1)$ donc $\mathrm{P}(n+2)$ et $\mathrm{P}(n+1)$

Donc $\mathrm{Q}(n+1)$.

Donc $\forall n \in \mathbb{N}, (\mathrm{Q}(n) \Rightarrow \mathrm{Q}(n+1))$

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

Théorème (récurrence forte) :

Soit P une propriété définie sur $\mathbb{N}$. Si :

(1) P(0)

(2) $\forall n \in \mathbb{N}, \left[\forall k \in [\![0,n]\!], \mathrm{P}(k)\right] \Rightarrow \mathrm{P}(n+1)$ (les $[\![\,,]\!]$ s'utilisent pour les entiers)

Alors $\forall n \in \mathbb{N}, \mathrm{P}(n)$.

(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 Q par :

$\forall n \in \mathbb{N}, (\mathrm{Q}(n) \Leftrightarrow [\forall k \in [\![0,n]\!], \mathrm{P}(k)])$

Alors Q(0) est vraie car P(0) l'est, donc $\forall k \in [\![0,0]\!], \mathrm{P}(k)$.

Soit $n \in \mathbb{N}$, supposons $\mathrm{Q}(n)$, alors $\forall k \in [\![0,n]\!], \mathrm{P}(k)$, donc $\mathrm{P}(n+1)$,

donc $\forall k \in [\![0,n+1]\!], \mathrm{P}(k)$, donc $\mathrm{Q}(n+1)$

Donc $\forall n \in \mathbb{N}, (\mathrm{Q}(n) \Rightarrow \mathrm{Q}(n+1))$

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

Théorème (récurrence finie) :
Soit m un entier naturel non nul
Soit P une propriété définie sur $[\![0,m]\!]$. Si :
(1) $P(0)$
(2) $\forall n\in [\![0,m-1]\!], (P(n)\Rightarrow P(n+1))$
Alors $\forall n\in [\![0,m]\!], P(n)$.

Théorème (récurrence finie descendante) :
Soit m un entier naturel non nul
Soit P une propriété définie sur $[\![0,m]\!]$. Si :
(3) $P(m)$
(4) $\forall n\in [\![1,m]\!], (P(n)\Rightarrow P(n-1))$
Alors $\forall n\in [\![0,m]\!], P(n)$.

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 :
$$\begin{cases} a=bq+r \\ 0\leq r<b \end{cases}$$
q est le quotient, r le reste dans la division euclidienne de a par b.

Démonstration :

- Unicité :

Supposons $\begin{cases} a=bq+r \text{ et } 0\leq r<b \\ a=bq'+r' \text{ et } 0\leq r'<b \end{cases}$

Alors $bq-bq'=r'-r$; $b(q-q')=r'-r$
Or, $-b<r'-r<b$. Supposons par exemple $r'\geq r$ (sinon on inverse les rôles)
Ainsi, $0\leq r'-r<b$
Ainsi, $q-q'=0$, car sinon $q-q'\geq 1$ et $b(q-q')\geq b$ soit $r'-r\geq b$.
Donc $(q,r)=(q',r')$

- Existence :

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

B) Numération en base quelconque

Théorème :

Soit $\beta \in \mathbb{N} \setminus \{0,1\}$

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 :

$A = a_0 \times \beta^0 + a_1 \times \beta^1 + a_2 \times \beta^2 + \ldots + a_n \times \beta^n$ (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 $\forall A \in \mathbb{N}$, $(\exists! a \in S_F, A = \sum_{k\in\mathbb{N}} a_k \beta^k)$

- 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 $\forall B \in [\![0, A-1]\!], \mathrm{P}(B)$. Montrons qu'alors $\mathrm{P}(A)$.

La division euclidienne de A par β donne :

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

Alors $Q \in [\![0, A-1]\!]$:

On a $\beta > 1$ et $Q > 0$. Donc $Q < \beta Q \leq \beta Q + r = A$, donc $Q < A$.

Donc $\mathrm{P}(Q)$: 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 $\begin{cases} a_0 = r \\ \forall k \geq 1, a_k = q_{k-1} \end{cases}$

D'où l'existence de la suite.

Si une autre suite $(a'_k)_{k\in\mathbb{N}}$ convient, alors :

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

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 :

$$2 = \overline{2}_3 = 2\times 3^0$$
$$8 = 2\times 3^1 + 2\times 3^0$$
$$74 = 2\times 3^2 + 2\times 3^1 + 0\times 3^0$$
$$222 = 2\times 3^3 + 2\times 3^2 + 0\times 3^1 + 2\times 3^0$$
$$667 = 2\times 3^4 + 2\times 3^3 + 0\times 3^2 + 2\times 3^1 + 1\times 3^0$$
$$2003 = 2\times 3^5 + 2\times 3^4 + 0\times 3^3 + 2\times 3^2 + 1\times 3^1 + 2\times 3^0$$

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

2003 en base 2 :

$$2003 = 1001\times 2 + 1$$
$$1001 = 500\times 2 + 1$$
$$500 = 250\times 2 + 0$$
$$250 = 125\times 2 + 0$$
$$125 = 62\times 2 + 1$$
$$62 = 31\times 2 + 0$$
$$31 = 15\times 2 + 1$$
$$15 = 7\times 2 + 1$$
$$7 = 3\times 2 + 1$$
$$3 = 1\times 2 + 1$$
$$1 = 0\times 2 + 1$$

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

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

$$2003 = 166\times 12 + 11$$
$$166 = 13\times 12 + 10$$
$$13 = 1\times 12 + 1$$
$$1 = 0\times 12 + 1$$

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