Chapitre 10

Nombre $\mathbb{N}$

Hugo Salou MP2I

Dernière mise à jour le 14 juin 2022

TABLE DES MATIÈRES

Première partie

Axiomatique de $\mathbb{N}$

Axiome: $(\mathbb{N}, \leqslant)$ est un ensemble non vide totalement ordonné vérifiant
- Toute partie non vide de $\mathbb{N}$ a un plus petit élément ;
- Toute partie non vide majorée de $\mathbb{N}$ a un plus grand élément ;
- $\mathbb{N}$ n'est pas majoré.

Définition:
- 0 est le plus petit élément de $\mathbb{N}$: $0 = \min(\mathbb{N})$.
- $1 = \min(\mathbb{N}^*) = \min\big(\mathbb{N} \setminus \{0\}\big)$.
- Soit $n \in \mathbb{N}$. On pose $n+1 = \min\big(\{k \in \mathbb{N} \mid k > n\}\big)$. On dit que $n+1$ est le successeur de n.
- Soit $n \in \mathbb{N}^*$. On pose $n-1 = \max\big(\{k \in \mathbb{N} \mid k < n\}\big)$. On dit que $n-1$ est le prédécesseur de n.

Proposition:

$$\begin{cases} \forall n \in \mathbb{N},\ (n+1) - 1 = n; \\ \forall n \in \mathbb{N}^*,\ (n-1) + 1 = n. \end{cases}$$

■

Proposition: Pour tout $n \in \mathbb{N}$, $\mathbb{N} \cap]n, n+1[= \varnothing$.

■

Théorème (récurrence)**:** Soit P un prédicat sur $\mathbb{N}$ et $n_0 \in \mathbb{N}$. Si

$$\begin{cases} P(n_0) \text{ est vrai }, \\ \forall n \geqslant n_0,\ P(n) \implies P(n+1), \end{cases}$$

alors

$$\forall n \geqslant n_0,\ P(n) \text{ est vrai.}$$

■

Deuxième partie

Récurrence

Proposition (récurrence double)**:** Soit P un prédicat sur $\mathbb{N}$ et $n_0 \in \mathbb{N}$. Si

$$\begin{cases} P(n_0) \text{ vraie} \\ P(n_0+1) \text{ vraie} \\ \forall n \in \mathbb{N} \text{ avec } n \geqslant n_0,\ P(n) \text{ et } P(n+1) \implies P(n+2) \end{cases}$$

Alors

$$\forall n \in \mathbb{N} \text{ avec } n \geqslant n_0,\ P(n) \text{ vraie.}$$

■

Proposition: Soit P un prédicat, $p \in \mathbb{N}^*$ et $n_0 \in \mathbb{N}$. Si

$$\begin{cases} \forall k \in [\![0, p-1]\!],\ P(n_0+k) \text{ vraie;} \\ \forall n \geqslant n_0,\ \big(P(n) \text{ et } P(n+1) \text{ et } \cdots \text{ et } P(n+p-1)\big) \implies P(n+p). \end{cases}$$

Alors,

$$\forall n \geqslant n_0, P(n) \text{ vraie.}$$

□

Proposition (récurrence forte)**:** Soit P un prédicat sur $\mathbb{N}$ et $n_0 \in \mathbb{N}$. Si $P(n_0)$ est vrai et

$$\forall n \geqslant n_0, \big(P(n_0) \text{ et } \ldots \text{ et } P(n-1) \text{ et } P(n)\big) \implies P(n+1).$$

Alors,

$$\forall n \geqslant n_0,\ P(n) \text{ est vraie.}$$

■

Troisième partie

Divisibilité

Définition: Soient $a, b \in \mathbb{Z}$. On dit que a divise b s'il existe $k \in \mathbb{Z}$ tel que $b = k \times a$. Dans ce cas, on écrit $a \mid b$. On dit aussi que a est un diviseur de b ; et que b est un multiple de a.

Proposition: " $\mid$ " est une relation d'ordre sur $\mathbb{Z}$. □

Proposition: Soient $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$.

$$a \mid b \implies |a| \leqslant |b|\,.$$

□

Proposition: Soient $a, b, c \in \mathbb{Z}$.

$$\left.\begin{matrix} a \mid b \\ a \mid c \end{matrix}\right\} \implies \big(\forall (k, \ell) \in \mathbb{Z}^2,\ a \mid (kb + \ell c)\big).$$

■

Définition: Soient $a, b \in \mathbb{Z}$. On dit que a et b sont associés si

$$a = b \text{ ou } a = -b.$$

Proposition: Soient $a, b \in \mathbb{Z}$.

$$a \mid b \iff -a \mid b \iff a \mid -b.$$

Proposition (division euclidienne dans $\mathbb{N}$)**:** Soient $(a, b) \in \mathbb{N} \times \mathbb{N}^*$.

$$\exists!\,(q, r) \in \mathbb{N}^2,\ \begin{cases} a = bq + r, \\ 0 \leqslant r < q. \end{cases}$$

$$\begin{array}{r|l} a & b \\ \hline & q \\ r & \end{array}$$

■

Proposition (division euclidienne dans $\mathbb{Z}$)**:** Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$.

$$\exists!\,(q, r) \in \mathbb{Z}^2,\ \begin{cases} a = bq + r, \\ 0 \leqslant r \leqslant |b|\,. \end{cases}$$

■

Définition: Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. D'après le théorème précédent, il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que

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

On dit que r est le quotient, et r le reste dans la division (euclidienne) de a par b.

Proposition: Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. On note r le reste de la division euclidienne de a par b.

$$r = 0 \iff a \mid b.$$

■

Quatrième partie

Arithmétique modulaire

Définition: Soient $a, b \in \mathbb{Z}$ et $c \in \mathbb{N}^*$. On dit que a est congrus à b modulo c si a et b ont le même reste dans la division euclidienne par c. Dans ce cas, on écrit $a \equiv b \ [c]$.

Proposition: La congruence modulo c est une relation d'équivalence. □

Remarque (Notation):
On note $\mathbb{Z}/c\mathbb{Z}$ l'ensemble des classes d'équivalences modulo c.

Par exemple, $\mathbb{Z}/5\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$.

Proposition: Soient $a, b \in \mathbb{Z}$ et $c \in \mathbb{N}^*$.

$$a \equiv b \ [c] \iff c \mid (b - a).$$

■