Quelques constructions sur les naturels

Pierre Mathonet

Département de Mathématique
Faculté des Sciences

Liège, octobre 2019

Définition axiomatique, rappel

L'idée : 2 pommes, ce n'est pas deux poires. Une pomme ce n'est pas une poire, mais pas de pomme du tout, ce n'est rien, et c'est aussi pas de poire du tout...
Donc on part du nombre 0 (qui correspond au vide), et on explique que pour tout nombre, il y a un suivant.

Définition 2.1.1

L'ensemble $\mathbb{N}$ est défini par les conditions suivantes :

1. Il existe un nombre, noté 0, appartenant à $\mathbb{N}$;
2. Tout nombre $n \in \mathbb{N}$ admet un successeur unique, noté $s(n)$. Deux nombres distincts ont des successeurs distincts.
3. Le nombre 0 n'est le successeur d'aucun nombre ; $(0 \notin im(s))$
4. Si K est un ensemble tel que
   - on a $0 \in K$
   - pour tout $n \in \mathbb{N}$, si $n \in K$, alors $s(n) \in K$,

   alors K contient $\mathbb{N}$.

Question : Pourquoi n'ai-je pas écrit $n+1$ au lieu de $s(n)$?

Le quatrième axiome et les récurrences

On se donne une proposition $P(n)$ pour tout $n \in \mathbb{N}$.

Proposition (Récurrence classique, Prop. 3.1.1)

Si on les les propriétés suivantes :

1. $P(0)$ *est vraie ;*
2. *Pour tout* $n \in \mathbb{N}$*, si* $P(n)$ *est vraie, alors* $P(s(n))$ *est vrai ;*

alors $P(n)$ *est vraie pour tout* $n \in \mathbb{N}$*.*

Preuve : Soit $K = \{n : P(n) \text{ est vrai}\}$.

Prop. 3.1.1, Récurrence classique, bis

Soit $n_0 \in \mathbb{N}$. Si pour tout $n \geqslant n_0$, on se donne une assertion $P(n)$, et si les conditions suivantes sont satisfaites :

1. L'assertion $P(n_0)$ est vraie ;
2. Pour tout $n \geqslant n_0$, si $P(n)$ est vrai alors $P(s(n))$ est vrai ;

alors l'assertion $P(n)$ est vraie pour tout $n \geqslant n_0$.

Remarque : L'ordre sera reconstruit d'ici peu (sans cette proposition).
Preuve : Définir $Q(n)$ comme "$P(n)$ ou $n < n_0$".

Récurrence forte et récurrence classique

Proposition 3.1.2 (Récurrence forte)

Si pour tout $n \in \mathbb{N}$, on se donne une assertion $P(n)$, et si les conditions suivantes sont satisfaites :

1. $P(0)$ est vrai ;
2. Pour tout n, si $P(0), \ldots, P(n)$ sont vrais, alors $P(s(n))$ est vrai ;

alors la propriété $P(n)$ est vraie pour tout $n \in \mathbb{N}$.

Preuve : Considérer la proposition $P'(n) = P(0) \wedge \cdots \wedge P(n)$, et la récurrence classique.

Remarques :

1. On a encore utilisé l'ordre, implicitement. On va le définir.
2. On peut démontrer des propriétés vraies pour tout $n \geqslant n_0$.
3. Pourquoi "récurrence forte" ?
4. Oui, mais...les deux propositions sont équivalentes
5. Ils sont aussi équivalents au fait que $\mathbb{N}$ soit bien ordonné (voir plus tard).

L'addition

Idée : additionner 0, c'est ne rien faire. Définir l'ajout de $s(b)$ à partir de l'ajout de b.

Définition 3.2.1

L'addition est définie récursivement comme suit. Pour tout $a \in \mathbb{N}$,

1. on pose $a + 0 = a$.
2. pour tout $b \in \mathbb{N}$, $a + s(b) = s(a + b)$

A-t-on défini quelque chose ? Poser $K_a = \{b \in \mathbb{N} : a + b \text{ est défini}\}$.
Attention : On ne sait pas encore que $+$ est commutatif.
Cette définition est indépendante de la représentation des nombres.

Définition 3.2.2

On note 1 le successeur de 0.

Alors $s(a) = a + 1$. On peut maintenant l'utiliser !

Quelques propriétés bien connues

Proposition 3.2.1

L'addition a les propriétés suivantes :

1. Elle est associative : on a $(a+b)+c = a+(b+c)$, pour tous $a, b, c \in \mathbb{N}$;
2. Elle admet 0 pour neutre : on a $a+0 = 0+a = a$ pour tout $a \in \mathbb{N}$;
3. Elle est commutative : on a $a+b = b+a$ pour tous $a, b \in \mathbb{N}$.

Définition : On dit que $(\mathbb{N}, +, 0)$ un monoïde commutatif.
Preuve pour l'associativité : Fixer a, b et faire une récurrence sur c.
Preuve pour le neutre :

1. 0 est neutre à droite par défintion.
2. 0 est neutre à gauche $0 + a = a$: récurrence directe sur a.

Preuve pour la commutativité : Fixer a et faire une récurrence sur b.

1. Le cas de base est clair.
2. On a $a + s(b) = s(a+b) = s(b+a)$. Est-ce $s(b) + a$?
3. On a bien $s(b+a) = s(b) + a$: récurrence sur a.

La multiplication

Définition 3.2.3

La multiplication est définie récursivement comme suit. Pour tout $a \in \mathbb{N}$,

1. on pose $a.0 = 0$.
2. pour tout $b \in \mathbb{N}$, on pose $a.s(b) = a.b + a$.

Note : La multiplication est bien définie

Proposition (monoïde)

La structure $(\mathbb{N}, ., 1)$ est un monoïde commutatif.

Preuve : Exercice.

Proposition 3.2.2

La multiplication distribue l'addition : on a $a.(b + c) = a.b + a.c$ et $(b + c).a = b.a + c.a$ pour tous $a, b, c \in \mathbb{N}$. De plus la structure $(\mathbb{N}, ., 1)$ est un monoïde commutatif.

Preuve : A faire comme exercice. Récurrence sur c, par exemple pour la 1ere égalité.

L'ordre usuel sur $\mathbb{N}$

But : définir l'ordre usuel. Pourquoi a-t-on $3 \leqslant 6$?

Définition 3.3.2

L'ordre usuel sur $\mathbb{N}$ est la relation $\leqslant$ définie par

$$a \leqslant b \quad \text{si, et seulement si} \quad \exists c \in \mathbb{N} : b = a + c.$$

Question : Qu'est-ce qu'un ordre ?

Définition 3.3.1

Une relation $\mathcal{R}$ de A dans A est une relation d'ordre si elle satisfait les conditions suivantes :

1. Elle est réflexive : on a $a\mathcal{R}a$ pour tout $a \in A$;
2. Elle est antisymétrique : pour tous $a, b \in A$, si $a\mathcal{R}b$ et $b\mathcal{R}a$, alors on a $a = b$;
3. Elle est transitive : pour tous $a, b, c \in A$, si $a\mathcal{R}b$ et $b\mathcal{R}c$, alors on a $a\mathcal{R}c$.

Quelques exemples d'ordres, et un résultat

1. Soit A un ensemble quelconque. L'égalité sur A est une relation d'ordre.
2. Soit X un ensemble. Notons $A = \mathcal{P}(X)$. La relation d'inclusion est un ordre sur A.
3. Soit $A = \mathbb{R}^2$ et définissons

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mathcal{R} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \Leftrightarrow x_1 \leqslant y_1 \quad \text{et} \quad x_2 \leqslant y_2.$$

C'est un ordre sur $\mathbb{R}^2$. Il n'est pas total.

Définitions et notations

1. Un ordre $\mathcal{R}$ sur un ensemble A est total si pour tous $a, b \in A$, on a $a\mathcal{R}b$ ou $b\mathcal{R}a$.
2. Etant donné un ordre $\mathcal{R}$, on peut définir un autre ordre $\mathcal{R}'$ par $a\mathcal{R}'b \Leftrightarrow b\mathcal{R}a$. Si on note l'ordre $\mathcal{R}$ par $\leqslant$, on obtient ainsi $\geqslant$.
3. Dans ce cas, on a aussi $>$ et $<$, qui sont des relations, mais pas des ordres.

L'ordre usuel est un ordre

Lemme

Tout nombre naturel est soit nul, soit un successeur.

Preuve : Récurrence.

Lemme 3.3.1

Si $a, b, c \in \mathbb{N}$ sont tels que $a + b = a + c$, alors $b = c$. Si $a, b \in \mathbb{N}$ sont tels que $a + b = 0$, alors $a = b = 0$.

Preuve de la première partie : Récurrence sur a.
Preuve de la deuxième partie : Contraposée. Si $a \neq 0$ ou $b \neq 0$, alors $a + b$ est un successeur.

Proposition 3.3.1

La relation $\leqslant$ introduite à la définition 3.3.2 est un ordre.

Preuve : Il suffit de l'écrire.

Ordre et opérations, ordre total

Proposition 3.3.2

Soient $a, b, c \in \mathbb{N}$. Si $a \leqslant b$, alors $a + c \leqslant b + c$ et $a.c \leqslant b.c$.

Preuve : Utiliser les définitions.
Remarque : Les réciproques sont vraies (si $c \neq 0$ pour la multiplication).

Proposition 3.3.3

L'ensemble ordonné $(\mathbb{N}, \leqslant)$ est totalement ordonné.

Preuve : Pour $m \in \mathbb{N}$, fixer

$$K_m = \{n \in \mathbb{N} : n \leqslant m \quad \text{ou} \quad m \leqslant n\}$$

Montrer que c'est $\mathbb{N}$.
Ou alors faire une simple récurrence.

Element minimal et minimum

Définition 3.3.4

Soit $(E, \leqslant)$ un ensemble ordonné et $A \subset E$. Un élément m est un minimum de A si

1. On a $m \in A$
2. Pour tout $a \in A$, on a $m \leqslant a$.

Définition 2.3.5

Soit $(E, \leqslant)$ un ensemble ordonné et $A \subset E$. Un élément m est minimal dans A si

1. On a $m \in A$
2. Pour tout $a \in A$, $a \leqslant m$ implique $a = m$.

Exemple : $A = \mathcal{P}(\{1,2,3\}) \setminus \{\varnothing\}$ et $\{1\}$.

Remarques :

1. Tout minimum est minimal ;
2. Dans un ensemble totalement ordonné, les deux notions coïncident.

L'ensemble des naturels est bien ordonné

Définition 3.3.6

Un ensemble ordonné $(E, \leqslant)$ est *bien ordonné* si tout sous-ensemble non vide A de E admet un minimum.

Remarque : Pour tout ensemble bien ordonné, l'ordre est nécessairement total.

Lemme 3.3.2

Pour tout $k \in \mathbb{N}$, l'ensemble $A_k = \{n \in \mathbb{N} : k < n < k+1\}$ est vide.

Preuve : Par l'absurde.

Proposition 3.3.4

L'ensemble ordonné $(\mathbb{N}, \leqslant)$ est bien ordonné.

Preuve :

1. Contraposée : si $E \subset \mathbb{N}$ n'admet pas de minimum, alors E est vide.
2. Récurrence pour la propriété $P(n)$: pour tout $i \leqslant n$, $i \notin E$. Cas de base simple, induction par l'absurde.

Soustraction et division

Définition 3.4.1

Si $a, b \in \mathbb{N}$ sont tels qu'il existe $c \in \mathbb{N}$ satisfaisant $b = a + c$, alors le nombre c est appelé la différence de b et a et on note $c = b - a$.

Remarques :

1. $b - a$ est donc défini si $a \leqslant b$;
2. Il est bien défini : le nombre c dans la définition est unique ;
3. La multiplication distribue la soustraction.

Définition 3.4.2

Soient $a, b \in \mathbb{N}$, si il existe $c \in \mathbb{N}$ tel que $b = a.c$, on dit que a divise b, ou que b est multiple de a. On note $a|b$ pour indiquer que a divise b.

Question : Peut-on définir le quotient ?

Proposition 3.4.2

Tout nombre divise 0. Le nombre 0 ne divise que 0, mais pas de manière unique. Si $a \neq 0$, pour tout b il existe au plus un nombre c tel que $b = a.c$.

Preuve :

1. Le cas de 0 : utiliser les définitions.
2. L'autre cas, on prouve une unicité. On montre que $ac = ac'$ implique $c = c'$ par récurrence sur $a \neq 0$.

Définition 3.4.3

Soient $a, b \in \mathbb{N}$ tels que $a \neq 0$. S'il existe $c \in \mathbb{N}$ tel que $b = a.c$, on écrit $c = b : a$ ou $c = \frac{b}{a}$. Le nombre c est appelé quotient de la division de b par a.

Proposition 3.4.3

Si $a, b \in \mathbb{N}$ satisfont $a.b = 0$, alors $b = 0$ ou $a = 0$.

Division euclidienne (avec reste)

Exemple : division de 37 par 7 : $37 = 5.7 + 2.$. Le nombre 5 est le quotient, tandis que 2 est le reste.

Proposition 3.4.4

Soient $a \in \mathbb{N}$ et $d \in \mathbb{N}_0$. Il existe des nombres q et r satisfaisant les conditions $a = qd + r$ et $0 \leqslant r < d$. De plus, le couple (q, r) est unique.

Preuve : 7

1. Existence, on fixe d, et on fait une récurrence sur a.
2. Unicité : on suppose $qd + r = q'd + r'$, où $r, r' < d$. On montre $q = q'$ par l'absurde.

Remarques :

1. Le même type de division existe dans l'anneau des polynômes à coefficients réels ou complexes, par exemple, mais aussi dans bien d'autres structures ;
2. Cette division permet de définir les systèmes de numération ;
3. On a $d|a$ si, et seulement si le reste de la division de a par d est nul ;
4. En particulier, si $a \neq 0$, si $d|a$ alors $d \leqslant a$.

Le lemme d'Euclide

Le lemme d'Euclide

Si un nombre premier p divise le produit deux nombres a et b alors il divise a ou il divise b.

Preuve : A résumer adéquatement.

1. P.A. On suppose qu'il existe p, a, b t.q. p premier, $p|ab$, $p \not| a$, $p \not| b$
2. On fixe un p et un a satisfaisant cette cond., et on regaarde l'ensemble des b :

$$E = \{b \in \mathbb{N} : p|ab, p \not| b\}.$$

3. E n'est pas vide, donc il admet un minimum b_0.
4. On montre que $1 < b_0 < p$:
   (a) $1 < b_0$ car $0 \notin E$, $1 \notin E$
   (b) $b_0 < p$: P.A. et division par p si $b_0 \geqslant p$.
5. On divise p par b_0 et on a un reste $b_1 < b_0$. Mais $b_1 \in E$.

Où utilise-t-on que p est premier ?

Le théorème fondamental de l'arithmétique

Théorème 3.4.1

Tout nombre naturel supérieur ou égal à 2 se décompose en un produit de facteur premiers (éventuellement réduit à un seul facteur). La décomposition est unique à l'ordre des facteurs près.

Preuve :

1. On a déjà fait l'existence (exemple de récurrence forte)
2. Unicité : P.A.
3. Si il existe $n \in \mathbb{N}$ qui admet deux décompositions distinctes, alors il y a un plus petit n ayant 2 décompositions.
4. On note $n = p_1 \dots p_l = q_1 \dots q_m$.
5. On montre que $p_1 \notin \{q_1, \dots, q_m\}$ et $p_1 \in \{q_1, \dots, q_m\}$.

Proposition 3.4.5

L'ensemble des nombres premiers est infini.

Preuve : P.A. Si les nombres premiers forment l'ensemble $\{p_1, \dots, p_m\}$, alors $p_1 \dots p_m + 1$ n'a as de décomposition.