Entiers naturels
(version chantier)

Marc SAGE

<2107

Table des matières

Transfini : au-delà du fini

ordinal et *cardinal* pas pareil : pour compter, on n'est pas obligé de faire 1, 2, 3, 4... La distinction apparaît vraiment avec les ensembles infinis, mais il faut travailler un peu pour accéder à ces notions.

Citer (Helmoltz ? ? ? ?) les entiers ne sont que la donnée de symboles dont on sait exactement qui vient après l'autre –> vision ordinale.

Card**N**>Card $\mathbb{R}$: deux démo de cantor (segemtn emboité + argument diagonal)

incrémenter / décrémenter

définir le cardinal via les bijections est une idée fin XIXe : cf Frege dans *Ecrits logiques et philosphiques* (traduit par Claude Imbert) : « [Husserl] porte le même jugement sur la définition de l'équinuméricité au moyen du concept de correspondance biunivoque »

La commutatvité n'a rien d'évident dans l'absolu : ok pour + et × mais pas ok pour l'exponentiation $a^b \neq b^a$ (sauf 2 et 4 –> exo :-))

quelques preuves par récurrences dans Henri Lombardi, *Épistémologie mathématique* (p. 41)

une preuve "élégante" de l'algo d'Euclide dans dans Henri Lombardi, *Épistémologie mathématique* (p. 28)

parler aussi d'anthyphérèse (p.19-20)

(*La création des nombres*, H ; Sinaceur, Vrin) P 178 De l'aveu de son auteur, l'axiomatique de Peano est inspirée de cette définition 71. Elle reformule, dans ce ordre, les conditions ■ [**N** est stable par successeur], ■ [le successeur est injectif], ■ [1 n'est pas successeur], et remplace la condition ■ [**N** est le plus petit ensemble contenant 1 et stable par successeur] par l'axiome d'induction compète énoncé en termes de classes, que Dedekind démontre à l'aide de ■ (Peano ne semble pas avoir saisi la généralité du concept de chaîne). Ainsi, « les axiomes de Peano » sont, en réalité, les axiomes de Dedekind-Peano.

1 Rappels de primaire : algo des 10-adiques

algo d'addition, multiplication, soustrction, division, preuve par neuf

! ! ! ! algo $2-3$ donne un 10-adique ...9999 —> on peut donc calculer dans les 10-adiques comme d'habitude

d'où ramner soustraction à addition : l'opposé d'un nombre s'obtient en complémentant tous les chiffres à 9 (et le dernier à 10). Propremnt : c'est rajouter (puis soustraire) une grande puissance de 10. Eg

$$\begin{array}{r} 18876273 \\ -10208767 \end{array} = \begin{array}{r} 18876273 \\ +\cdots 999989791233 \end{array} = \cdots 0008\ 667\ 506$$

GAffe aux diviseurs de 0 :

$$\begin{array}{r} \cdots 134033203125 \\ \times \cdots 101010010112 \end{array} = \cdots 0000$$

Les reponsable sont les divisuers propres de 10.

En base première, pas de div de 0 ! Et tout nombre sans zéro est inversible (c'est dire que $\mathbb{Z}_p^* = {}^c p\mathbb{Z}_p$). On pose alors $\frac{1}{p} = 0,1$, ce qui ouvre la porte à $\mathbb{Q}_p$.

Mais on perd l'ordre lexico (pas de premier éléments à comparer)

Desc topo ? on envoie $\mathbb{Z}_2$ dans $[0,1]$ en reversant la suite de chiffres (et en envoaynt 1 sur 2). C'est clairemen continue à valeurs dans le Cantor, pas inj (...11111 a même image que 1), mais applicaiton réciproque est bien def inj. En recollant les ambiuguités d'écriture, cela revient à "relier" ces nombrse, ce qui donne un escalier de Cantor –> on passe au réels. Ainsi, la continuité des réeles **provient** des ambiguités d'écriture (sinon on aurait un vrai Cantor !).

2 Résumé des propriétés et constructions

2.1 Propriétés

L'ensemble **N** vient avec deux objets 0 et 1, deux lois + et ×, une relation d'ordre $\leq$.

(La multiplication sera prioritaire sur l'addition, de sorte que l'expression $a \times b + c$ signifiera $(a \times b) + c$ et se notera $ab + c$.)

Le principe fondamental est le raisonnement par récurrrence : *pour tout* 1*-prédicat* P*, on a l'implication*

$$(P_0 \wedge [\forall n \in \mathbf{N},\ P_n \implies P_{n+1}]) \implies (\forall n \in \mathbf{N},\ P_n)\,.$$

Il formalise le h-principe d'induction que je juge valide en mettant bout à bout les preuves $P_n \vdash P_{n+1}$. D'ailleurs, on montre l'équivalence avec un principe tout aussi intuitif (que la h-induction) : toute partie non vide possède un plus petit élément.

Autre formulation, dite récurrence forte (mais parfaitement équivalente)

$$[\forall n \in \mathbf{N},\ (\forall a < n,\ P_a) \implies P_n] \implies [\forall n \in \mathbf{N},\ P_n]$$

(les hypothèses et conclusions sont plus fortes, d'où plus d'hytpohèse à dispositin mais plus de choses à montrer) (appliquer à $\forall a < n,\ P_a$)

Structure additive et multiplicative.

$(\mathbf{N}, +)$ monoïde abélien de neutre 0, régulier et tel que

$$\begin{array}{rcl} a & \neq & 0 \Longrightarrow \exists b,\ a = b + 1 \\ a + b & = & 0 \implies a = 0 = b \end{array}$$

$(\mathbf{N}, \times)$ monoïde abélien de neutre 1, d'absorbant 0, tel que

$$\begin{array}{rcl} ab = 0 & \implies & a = 0 \text{ ou } b = 0 \\ \left\{ \begin{array}{c} an = bn \\ n \neq 0 \end{array} \right. & \implies & a = b \end{array}$$

La multiplication est distributive par rapport à l'addition

$$\forall a, b, c, d \in \mathbf{N},\ (a + b)\,(c + d) = ac + ad + bc + bd\,;$$

Sens des addition et multiplication.

L'addition coïncide avec l'itération de $+1$

$$a + \underline{n} = a + \overbrace{1 + 1 + \ldots + 1}^{n \text{ fois}}\ \text{(pour } n \text{ entier } \textit{primitif}\text{)}$$

La multiplication coïncide avec l'itération de l'addition

$$\underline{n} \times a = \overbrace{a + a + \ldots + a}^{n \text{ fois}}\ \text{(pour } n \text{ entier } \textit{primitif}\text{)}$$

Ordre, liens avec + et ×.

$\leq$ est un ordre total vérifiant

$$\begin{array}{rcl} \forall n & \in & \mathbf{N},\ 0 \leq n < n + 1 \\ a & \leq & b \iff \exists n,\ b = a + n \\ a & > & b \iff a \geq b + 1 \text{ çàd } \nexists n,\ a < n < a + 1 \end{array}$$

(VITAL) Toute partie non vide admet un min.

Opérations sur les comparaisons

On peut additionner les comparaisons ($\leq + \leq$ donne $\leq$, avec $<$ dès qu'une $\leq$ au début est $<$), simplifier les comparaisons (larges comme strictes).

On peut multiplier les comparaisons ($\leq \times \leq = \leq$ et $< \times < = <$, mais pas $\leq \times < = <$), multiplier les $<$ et simplifier les inégaltiés (larges comme strictes) par un entier non nul.

Constructions de suites récurrentes.

Pour tout $f : A \longrightarrow A$ et $\alpha \in A$, il y a une unique suite $(a_n) \in A^{\mathbf{N}}$ telle que $a_0 = \alpha$ et $\forall n \in \mathbf{N},\ a_{n+1} = f\,(a_n)$ (Pour toute fonctionnelle f et tout objet o, il y a un (plus petit) ensemble O contenant o et stable par f)

2.2 Quelques idées de constructions

On appelera *récurrent* un ensemble qui contient le vide et qui est stable par passage au successeur $s : a \mapsto a \cup \{a\}$. Cette propriété s'exprime au premier ordre (dans le langage ensembliste) : l'axiome de l'infini nous donne un ensemble récurrent Ω. On peut alors considérer l'ensemble $\mathcal{R}$ des ensembles récurrents inclus dans Ω et prendre son intersection que nous noterons $\mathbf{N}$.

(*Unique preuve de ce cours*) : Montrons que $\mathbf{N}$ satisfait le principe de récurrence. Soit P une propriété (exprimable au premier ordre) vraie pour $\emptyset$ et stable par passage au successeur. Alors la partie de Ω formée de éléments vérifiant P est récurrent, donc contient $\mathbf{N}$, ce qui montre que tous les éléments de $\mathbf{N}$ vérifient P.

On montre qu'il y a une unique loi $+$ satisfaisant $a + 0 = a$ et $a + s(b) = s(a + b)$, définie par induction : à a fixé, déifnir $a + n := \alpha_n$ où α est l'unique suite telle que $\begin{cases} \alpha_0 = a \\ \alpha_{s(n)} = s(\alpha_n) \end{cases}$. LE reste en découle.

Rq : on doit avoir $a + 1 = a + s(0) = s(a + 0) = s(a)$. Ajouter 1 correspond donc à appliquer le successeur (ce qui définit 1 comme le successeur de 0). On définit alors les premiers entiers primitifs :

$$\begin{aligned} 2 &: = 1 + 1 \\ 3 &: = 1 + 1 + 1 \\ 4 &: = 1 + 1 + 1 + 1 \\ 5 &: = 1 + 1 + 1 + 1 + 1... \end{aligned}$$

De même que pour l'addition, on montre qu'il y a une unique loi $\times$ satisfait $a0 = 0$ et $a(b + 1) = ab + a$, définie par induction : à a fixé, déifnir $a \cdot n := \mu_n$ où μ est l'unique suite telle que $\begin{cases} \mu_0 = 0 \\ \mu_{n+1} = \mu_n + a \end{cases}$. Le reste en découle.

Rq La multiplication est l'itération de l'addition :

$$\begin{aligned} a \cdot 1 &= (a \cdot 0) + a = 0 + a = a, \text{ puis} \\ a \cdot 2 &= (a \cdot 1) + a = a + a, \text{ de même} \\ a \cdot 3 &= a + a + a, \text{ etc.} \end{aligned}$$

Il y a une unique relation d'ordre $\leq$ vérifiant

$$\forall n \in \mathbf{N},\ 0 \leq n < n + 1.$$

L'ordre est défini à l'aide de $+$. Tout en découle.

3 Quelques démo ensemblistes, ordinales

3.1 Descriptions ensembliste/ordinale

un entier n est égal à l'union de ses prédécesseurs

$$n + 1 = \{0, 1, 2, ..., n - 2, n - 1, n\}$$

(contient 0, n, pas n' et est stable par s et s^{-1})

ajouter 1 correspond à prendre le successeur

$$\forall a \in \mathbf{N},\ a + 1 = s(a)\ ;$$

tout entier non nul est successeur

$$a \neq 0 \implies \exists n,\ a = s(n)$$

retirer 1 correspond à prendre l'union

$$\forall a \in \mathbf{N}^*, \ \cup a = a - 1\,;$$

la relation d'ordre large correspond à l'inclusion

$$a \leq b \iff a \subset b\,;$$

la relation d'ordre stricte correspond à l'appartenance

$$a < b \iff a \in b\,;$$

****le max coïncide avec l'union

$$\max\{a, b\} = a \cup b\,;$$

****le min coïncide avec l'intersection

$$\min\{a, b\} = a \cap b\,;$$

3.2 $\in$ est une relation d'ordre strict dont la relation d'ordre associée est $\subset$

Par fondation, on ne peut avoir $n \in n$.

On affirme ensuite que

$$n \subset a \iff n \subsetneq s(a)$$

$\Longrightarrow$ clair car $a \subsetneq s(a)$.

$\Longleftarrow$ réc sur n. Pour $n = 0$, on a $\emptyset \subsetneq s(0) = \{\emptyset\} \implies \emptyset \subset 0$, donc $vrai \implies vrai$. Ensuite, si $s(n) \subsetneq s(a)$, on a en particulier $n \subset s(n) \subsetneq s(a)$, d'où par HR $n \subset a$. Nous voulons $s(n) \subset a$, donc il suffit de montrer que $n \in a$. Puisque $n \in s(n) \subsetneq s(a)$, on a $n \in a$ ou $n = a$. Mais ce dernier à rejeter car on a des inclusino strictes, CQFD.

Montrons par récurrence sur n que

$$a \subsetneq n \iff a \in n.$$

Pour $n = 0$, on veut $a \subsetneq \emptyset \iff a \in \emptyset$, ce qui est vrai (faux $\Longleftrightarrow$ faux).

Supposons le résultat vrai pour un $n \geq 0$. Alors on a les équivalences

$$a \in s(n) \iff (a \in n \text{ ou } a = n) \overset{\text{HR}}{\iff} (a \subsetneq n \text{ ou } a = n) \iff a \subset n \overset{\text{lemme}}{\iff} a \subsetneq s(n)\,.$$

Corollaire

$$a \in b' \Longleftrightarrow a \subset b \Longleftrightarrow a' \subset b'$$

DEM 1 $\quad a \in b' \Longleftrightarrow a \subsetneq b' \Longleftrightarrow a \subset b$

DEM 2 $\quad a' \subset b' \Longleftrightarrow a \cup \{a\} \subset b' \Longleftrightarrow \begin{cases} a \subset b' \\ a \in b' \end{cases} \Longleftrightarrow \begin{cases} a \subset b' \\ a \subset b \end{cases} \Longleftrightarrow a \subset b$

3.3 Tout entier est l'ensemble de ses prédécesseur

comment coder des itérés finis ?

SOit n.

On veut le segment $\{0, 1, 2, ..., n-1, n\}$. Les "..." indiquent *exactement* une stabilité par s et s^{-1}. Montrons donc

$$\exists S \subset \mathbf{N}, \begin{cases} 0 \in S \qquad n \in S \qquad n' \notin S \\ \forall a \neq n, \ a \in S \Longleftrightarrow a' \in S \end{cases}$$

Vérifions que $S := n'$ marche.

Clair que $n \in n'$ et $n' \notin n'$.

$\emptyset \subset S$ et n' n'est pas vide, donc $\emptyset \subsetneq n'$, ie $0 \in S$.

Soit $a \neq n$. On a les eq $a \in S \Longleftrightarrow a \in n' \Longleftrightarrow a' \subset n' \Longleftrightarrow \begin{cases} a' \subset n' \\ a' \neq n' \end{cases} \Longleftrightarrow a' \subsetneq n' \Longleftrightarrow a' \in n'$.

3.4 0 n'est jamais sucesseur :

$$0 = s(a) \implies \emptyset = a \cup \{a\} \implies a \in \emptyset, \textit{ absurde.}$$

3.5 Soutraction

Pour $x \neq 0$, on pose $x - 1 := \cup x$. On vérifie que

$$\begin{aligned} \forall x &\in \mathbf{N},\ (x+1) - 1 = x, \\ \forall x &\in \mathbf{N}^*,\ (x-1) + 1 = x. \end{aligned}$$

Montrons par récurrence sur n que $\cup s(n) = n$. Pour $n = 0$, on a

$$\cup s(0) = \cup(\emptyset \cup \{\emptyset\}) = \cup(\{\emptyset\}) = \emptyset = 0.$$

Ensuite, supposant $\cup s(n) = n$, on a

$$\begin{aligned} \cup s(s(n)) &= \cup(s(n) \cup \{s(n)\}) = (\cup s(n)) \cup (\cup \{s(n)\}) = n \cup s(n) = n \cup n \cup \{n\} = n \cup \{n\} \\ &= s(n),\ \textit{CQFD.} \end{aligned}$$

On en déduit la seconde égalité : pour x non nul, x est un successeur $s(n)$, d'où

$$(x-1) + 1 = ((n+1) - 1) + 1 = n + 1 = x.$$

3.6 L'ordre

$\subset$ satisfait ces axiomes, donc coïncide avec $\leq$. D'après un résultat préliminaire, l'ordre strict $<$ associé est $\in$. C'est le début de la théorie des ordinaux.

Application rigolote de fondation : Montrons que tout partie non vide de $\mathbf{N}$ admet un min.
Soit A une telle partie (définissable au premier ordre). Intuitivement, il s'agit de prendre le plus petit entier de A, donc celui qui est le moins sophistiqué niveau construction. L'axiome de fondation (appliqué à $A \neq \emptyset$) nous donne un tel $a_0 \in A$ vérifiant plus précisément $A \cap a_0 = \emptyset$. Montrons que $a_0 = \min A$. Soit par l'absurde un élément $a \in A$ tel que $a < a_0$, *i. e.* $a \in a_0$, ce qui impose $a \in A \cap a_0$, *absurde.*

3.7 $>$ et $+$

lemme SUPER UTILE

$$a > n \iff a \geq n + 1.$$

$$a > n \begin{array}{c} \implies a \geq n \iff n \subset a \\ \iff n \in a \iff \{n\} \subset a \end{array} \iff n \cup \{n\} \subset a \iff n + 1 \geq a.$$

4 Démo formelle de récurrence (Francinou)

soit $A \subset \mathbf{N}$, $A_n = A \cap [0, n[$. Alors

$$[\forall n \in A,\ (\forall a \in A_n,\ P(a)) \implies P(n)] \implies [\forall n \in A,\ P(n)]$$

ok si A partie minorée de Z.
Pour $A = \mathbf{N}$, la prémice est tautologique, donc on amorce.
Pour A finie, il faut faire attention aux indices de début/fin.
exemple où on resort l'argumenet de minimalité : liberté de $1, a, a^2, ...a^{p-1}$ si $a^p = 0$, des $e^{\lambda \cdot}$.

5 Divers

Eg de récurrence foireuse. Soit une boite de crayons. Montrons qu'ils ont tous la même couleur. Pour $n = 1$, rien à faire. Ensuite, les crayons $\{0, ...n-1\}$ et $\{1, ..., n\}$ ont même couleur, donc tous les crayons aussi.
CA VOUS APPRENDRA A FAIR GAFFE AUX INDICES !!!!

POur rédiger une récurrece, on peut dire :
Supposons le résultat vrai pour un n dans schblurb OU
Soit n un enteir dans schubr tel que $P(n)$.
La différence : dans le premier cas, on montre clarement une implciation, dans le second, on impose la premice (mais on n'en pas besoin pour montrer l'implication !)

quand on dit qu'on récurre sur une quantité, on pose en fait $P(n)$: pour toute chose dont la quantité associé vaut n. Par exemple, la somme de deux indices.
Exemple de récurrence emboitée ? (en algèbre linéaire...)

exemples : bernoulli (ausi démo par convexité !), IAQ, Vandermonde (deux exmple qui appellent à la récurrence -> **couplge récurrence/équivalence**), $\frac{f+f^2+f^3}{3} = \mathrm{Id}$, f strictement croissante multiplicative $2 \longmapsto 2$, tout entier ≥ 2 a un diviseur premier,
Soit x un nombre réel. On suppose que $x + \frac{1}{x}$ est un entier. Montrer que $s_n := x^n + \frac{1}{x^n}$ est entier pour tout n. (binôme en rergoupant, sinon $s_n s_1 = s_{n+1} + s_{n-1}$ avec s_0 et s_1 entiers)
Nb de régions délimitée par n droites du plan deux à deux non concouranates ? chaque nouvelle droite coupe en n point, deux points consécutifs coupant chaque région en deux (région convexe car inter de demi-plans), sans oublier les points à l'infini, d'où $n+1$ région en plus, donc résultat est $\binom{n}{2} + 1$.
descente infinie : pas de suite strictement décroissante dans $\mathbf{N}$.

6 Théorème itération / récursivit

pas besoin de AC pour ça.
intuitivement, on construit une suite petit à petit en fonction des termes précédents.

1. **(itération)** *soit $f : A \longrightarrow A$, $\alpha \in A$, alors il y a une unique suite $(a_n) \in A^{\mathbf{N}}$ tq $a_0 = \alpha$ et $a_{n+1} = f(a_n)$ pour tout $n \geq 0$*
2. **(récursivité)** *soient $f_n : A^n \longrightarrow A$ pour tout $n \geq 0$ Alors il y unique suite $(a_n) \in A^{\mathbf{N}}$ tq $a_n = f_n(a_0, a_1, ..., a_{n-1})$ pour tout $n \geq 0$ (se donner f_0, c'est se donner une appliction sur le singleton $A^{I_0} = A^{\emptyset}$, donc une valeur initiale α)*
3. **(récursivité à trous)** *soit $\{n_0 < n_1 < n_2 < \cdots\}$ une partie de $\mathbf{N}$ et $F_k : A^{\{n_0, ..., n_{k-1}\}} \longrightarrow A$ pour tout $k \geq 0$. Alors il y a une unique suite $(a_{n_k})_{k \geq 0}$ tq $\forall k \geq 0,\ a_{n_k} = F_k\left((n_i \mapsto a_{n_i})_{0 \leq i < k}\right)$.*

DEM 1 : *Soit* $f : A \longrightarrow A$ *une application et* $a_0 \in A$. *Montrer qu'il existe une unique suite* $(a_n)_{n\geq 0}$ *vérifiant la condition initiale* $a(0) = a_0$ *ainsi que la relation de récurrence* $a_{n+1} = f(a_n)$.

Suivons humblement l'énoncé et considérons l'ensemble des $n \in \mathbf{N}$ pour lesquels il y a une suite $(a_i)_{0\leq i\leq n}$ telle que $a_i = f(a_{i-1})$ pour tout $0 < i \leq n$. Si cet ensemble ne vaut pas tout $\mathbf{N}$, son complémentaire contient un minimum n_0, mais alors en posant $a_{n_0+1} := f(a_{n_0})$ on obtient une suite définie sur $[0, n_0 + 1]$, contredisant la définition de n_0. On dispose donc pour tout $n \in \mathbf{N}$ d'une suite $(a_i^n)_{0\leq i\leq n}$: il est vital d'observer qu'une telle suite est unique (si $(b_i)_{i\leq n}$ en est une autre, en considérant par l'absurde un plus petit entier $i \leq n$ tel que $b_i \neq a_i$, on obtient immédiatement une contradication en écrivant $b_i = f(b_{i-1}) = f(a_{i-1}) = a_i$), ce qui permet de poser $a_i := a_i^n$ pour n'importe quel $n \geq i$. Alors la suite $(a_i)_{i\geq 0}$ convient et est unique (on a montré que ses restrictions à tout $[0, n]$ le sont).

DEM 2.

POsons $A' = \coprod_{n\geq 0} A^n$, $a := f_0()$, et f l'union disjointe des

$$\left\{ \begin{array}{ccc} A^n & \longrightarrow & A^{n+1} \\ (a_0, ..., a_{n-1}) & \longmapsto & (f_0(), f_1(a_0), f_2(a_0, a_1), ..., f_n(a_0, ..., a_{n-1})) \end{array} \right. .$$

D'après 1, il y a une unique suite $(a_n') \in A'^{\mathbf{N}}$ telle que $a_0' = a$ et $a_{n+1}' = f(a_n)$. Notons a_n la dernière coordonnée de a_n' Alors

$a_1' = f(a_0') = f(a) = (a, f_1(a)) = (a, a_1)$

$a_2' = f(a_1') = f(a, a_1) = (a, f_1(a), f_2(a, a_1)) = (a, a_1, a_2)$.

On lit par réc $a_n = f_n(a_0, a_1, ..., a_{n-1})$

DEM 3 (c'est 2 avec un trou)

Pour $n_{k-1} < n \leq n_k$ (on pose $n_{-1} = -1$), on définit $f_n(a_0, ..., a_n) := F_k\left(a_{n_0}, a_{n_1}, ..., a_{n_{k-1}}\right)$. Alors le point 2 nous donne une unique suite $(a_n) \in A^N$ telle que $a_n = f_n(a_0, ..., a_{n-1})$. En particulier, $a_{n_k} = f_{n_k}(\overrightarrow{a}) = F_k\left(a_{n_0}, ..., a_{n_{k-1}}\right)$, CQFD.

appliciion : pour $\overrightarrow{a} \in A^{\mathbf{N}}$, on pose $\prod_{i=1}^n a_i$. Si $a_i = i$, on note $n!$. Si a_i tous égaux, on itérère a^n, aussi noté na, $f^{\circ n}$ ou $f^{(n)}$.