Définition itérative des entiers
(*feat* théorème 126 de Dedekind)

Marc SAGE

2015

Table des matières

Cet exposé propose un certain regard sur le texte *Qu'est-ce sont et à quoi servent les nombres ?* écrit en 1888 par Richard Dedekind. Nous travaillerons sur la traduction par Hourya Sinaceur extraite de [Dede2008] à laquelle réfèrent toutes les paginations de cet annexe.

Notre propos est simple : mettre en exergue l'approche *itérative* de fondement de l'arithmétique en opérant une sorte de *reverse mathematics* depuis le théorème 126 (existence et unicité d'une suite définie "par récurrence") vers l'axiome de l'infini de Zermelo (qui remplace le "théorème" 66 de Dedekind) :

> *notre action itérative* (au sens où un départ et une fonction itérable engendrent une suite)
> *est* ***exclusivement*** *fondée* (en un certain sens catégoriel)
> *sur les nombres* (au sens de l'axiomatique de Peano).

Nous espérons ainis convaincvre que l'*itération* est au fondement de l'arithmétique peanienne et, partant, que les nombres ne sont au fond qu'une forme discrète de la potentialité par laquelle nous *agissons* dans notre vie.

1 Introduction

Motivation.

Rappelons que l'opération ***successeur*** s agit sur un ensemble en lui rajoutant un certain élément (lui-même), *i. e.* agit comme $a \mapsto a \cup \{a\}$.

Dans l'approche ensembliste moderne, l'axiome de l'infini (il existe un ensemble contenant $\emptyset$ et stable par s) permet de disposer d'un infini *actuel* réalisant la potentialité d'un infini *potentiel* (celle de pouvoir toujours itérer), d'où l'on obtient un ensemble[1] $\mathbf{N}$ qui satisfait les axiomes de Peano avec unicité à unique isomorphisme[2] près : cet axiome permet donc d'avoir un modèle de l'arithmétique (de Peano) et ce de façon catégorique. Chemin faisant de cet infini actuel vers une structure arithmétique, il a fallu construire les opérations de l'arithmétique, ce qui se fait usuellement de manière *itérative* : l'addition se définissant par itération du successeur (à penser comme l'incrémentation $n \mapsto n+1$) et la multiplication par itération de l'addition. Pour légitimer ces constructions par itération, il suffit de pouvoir itérer n'importe quelle fonction stabilisant un ensemble donné depuis n'importe quel élément de cet ensemble. Cette possibilité est réalisée grâce à l'ensemble $\mathbf{N}$ et prend la forme du théorème (ensembliste)

$$\forall A,\ \left\{\begin{array}{c}\forall f \in A^A \\ \forall @ \in A\end{array}\right.,\ \exists! a \in A^{\mathbf{N}},\ \left\{\begin{array}{l} a_0 = @ \\ \forall n \in \mathbf{N},\ a_{n+1} = f\left(a_n\right)\end{array}\right. \quad \text{où l'on a abrégé } n+1 := s\left(n\right),$$

lequel n'est qu'une traduction moderne du théorème 126 de Dedekind.

Ce dernier nous semble par conséquent coder toute l'essence de l'arithmétique (ordinale), à travers la possibilité d'*itérer indéfiniment*, autrement dit *via* le fait que $\mathbf{N}$ soit au sens de cette possibilité un *infini itératif*. Nous nous proposons de partir de ce théorème, de regarder ce qu'il requiert pour faire sens, et d'en déduire une forme d'axiome de l'infini codant les axiomes de Peano.

En un mot : *un infini potentiel au sens* itératif *du théorème 126 de* Dedekind *doit être un infini actuel au sens* peanien *de l'axiome de l'infini.*

Fondement de notre action : objet initial.

Le théorème 126 peut se formuler aisément dans un cadre catégoriel. Il s'énonce en effet (de manière très compactée) sous la forme d'un diagramme sagittal :

$$\begin{array}{ccccc} o & \xrightarrow{\subset} & N & \xrightarrow{\sigma} & N \\ \downarrow & & \downarrow & \exists! a & \downarrow \\ \forall @ & \xrightarrow{\subset} & A & \xrightarrow{\forall f} & A \end{array}.$$

Prenons pour objets les triplets (a, f, A) tels que A contienne a et soit stable par f. Un morphisme entre deux tels triplets (a, f, A) et (b, g, B) sera défini par une application $\varphi : A \longrightarrow B$ faisant commuter le diagramme

$$\begin{array}{ccccc} a & \xrightarrow{\subset} & A & \xrightarrow{f} & A \\ \downarrow & & \downarrow \varphi & & \varphi \downarrow \\ b & \xrightarrow{\subset} & B & \xrightarrow{g} & B \end{array}.$$

Alors le théorème 126 nous dit qu'un triplet (o, σ, N) tel que $\left\{\begin{array}{c} o \text{ appartient à } N \\ N \text{ est stable par } \sigma \end{array}\right.$ et $\left\{\begin{array}{c} \sigma \text{ est injective} \\ \sigma \text{ n'atteint pas } o \end{array}\right.$ est un objet *initial* de cette catégorie[3]. *Les nombres forment donc cet objet initial* et c'est en ce sens que nous disons que le théorème 126 les caractérise comme le fondement de notre action.

Axiomes de l'infini.

Pourquoi, dans l'axiome de l'infini, prend-on comme objet à éviter le vide et pour fonctionnelle injective le successeur ?

Fixons plus généralement un objet o (généralisant le vide) et une fonctionnelle σ partout définie (généralisant le successeur). On abrégera par commodité $a' := \sigma\left(a\right)$ pour tout objet a.

[1] défini comme l'intersection de tous les ensembles contenant $\emptyset$ et stables par s

[2] un morphisme d'un (N, s) vers un (N', s') est une application $f : N \longrightarrow N'$ faisant commuter le carré évident (*i. e.* telle que $f \circ s = s' \circ f$)

[3] En corollaire tombe son unicité à (unique) isomorphisme près.

Introduisons quelques notations pour faciliter notre discours :

$$\underset{o}{\overset{\sigma}{\text{Chaine}}}\, I \quad \text{abrège} \quad \begin{cases} \forall i \in i,\ i' \in I \\ o \in I \end{cases} \quad (\textit{i. e.} : I \text{ est une } \sigma\text{-chaîne contenant } o)\,;$$

$$\underset{o}{\overset{\sigma}{\text{Infini}}} \quad \text{abrège} \quad \exists I,\ \underset{o}{\overset{\sigma}{\text{Chaine}}}\, I \quad (\textit{i. e.} : \text{il y a une } \sigma\text{-chaîne contenant } o)\,;$$

Nous conviendrons d'appeler $\underset{o}{\overset{\sigma}{\text{Infini}}}$ l'***axiome de l'infini*** de ***départ*** o et de ***pas*** σ. Ainsi l'axiome de l'infini de Dedekind-Peano s'écrit-il $\underset{\emptyset}{\overset{s}{\text{Infini}}}$ et est-il un axiome de l'infini au sens précédent.

Notre propos, rappelons-le, est de mettre en relief l'aspect *itératif*[4] du fondement de l'arithmétique. Dans cette perspective, les axiomes de l'infini sus-définis sont *typiquement itératifs* : ils affirment l'existence d'ensembles dans lesquels on peut itérer une certaine fonctionnelle sur un certain objet. De ce point de vue, l'axiome usuel vaut autant que les autres[5], sous de bonnes conditions à déterminer sur σ. Annonçons tout de suite la couleur : on peut montrer[6] que

en restreignant aux pas σ injectifs évitant leur départ o,
tous les énoncés $\underset{o}{\overset{\sigma}{\text{Infini}}}$ *sont équivalents.*

Motivons les deux conditions ci-dessus. Si un ensemble $\{o, o', o'', o''', ...\}$ postulé par $\underset{o}{\overset{\sigma}{\text{Infini}}}$ est par malheur fini, la σ-orbite[7] de o devra "boucler" ; le premier itéré sur lequel elle revient est alors ou bien o (cas d'une orbite en forme de "0") ou bien un itéré plus loin (cas d'une orbite en forme de "∂"). Le premier cas peut être évité en empêchant σ d'atteindre o, le second en imposant son injectivité. L'absence de "boucle", de "torsion", nous incite à appeler

$$\textbf{\textit{platitude}} \quad \text{l'énoncé } \underset{o}{\overset{\sigma}{\text{Plat}}} \text{ abrégeant } \begin{cases} \sigma \text{ est injective} \\ \sigma \text{ n'atteint pas } o \end{cases}.$$

Les équivalences ci-dessus peuvent alors s'écrire (on sous-entend une quantification universelle) :

$$\left(\underset{o}{\overset{\sigma}{\text{Plat}}} \text{ et } \underset{O}{\overset{\Sigma}{\text{Plat}}}\right) \Longrightarrow \left(\underset{o}{\overset{\sigma}{\text{Infini}}} \Longleftrightarrow \underset{O}{\overset{\Sigma}{\text{Infini}}}\right).$$

Platitude et arithmétique.

Revenant à Dedekind, il ressort que la platitude apparaît dans la définition 71 d'un système simplement infini, notion caractérisée par quatre conditions (α, β, γ et δ) dont sont issues les axiomes de Peano[8] (les conditions ci-dessus sont celles γ et δ). Afin de resserrer le lien entre arithmétique (au sens de Peano) et infini (en notre sens itératif), introduisons deux autres énoncés[9] :

$$\underset{o}{\overset{\sigma}{\text{InfiniMin}}} \quad \text{abrège} \quad \exists N,\ \begin{cases} \underset{o}{\overset{\sigma}{\text{Chaine}}}\, N \\ \forall I,\ \underset{o}{\overset{\sigma}{\text{Chaine}}}\, I \Longrightarrow N \subset I \end{cases} \quad (\textit{i. e.} : \text{il y a une plus petite } \sigma\text{-chaîne contenant } o).$$

$$\underset{o}{\overset{\sigma}{\text{Peano}}} \quad \text{abrège} \quad \underset{o}{\overset{\sigma}{\text{InfiniMin}}} \text{ et } \underset{o}{\overset{\sigma}{\text{Plat}}} \quad (\textit{i. e.} : \text{il y a une plus petite } \sigma\text{-chaîne sans boucles contenant } o).$$

On observera alors que :

[4] Selon nous, les entiers codent notre *action*. Une action *illimitée* signifie l'absence d'obstacle à l'action, *i. e.* que l'on peut toujours agir. C'est pourquoi l'on code l'*infinité* des entiers par un ensemble stable par une action (et contenant un point de départ).

[5] D'un tout autre point de vue – celui technique –, le choix du départ $\emptyset$ et de pas s facilite grandement la technique ordinale. En effet, on définit habituellement l'ordre $a \leq b$ par l'inclusion des segments initiaux associés, définition qui est une identité précisément pour le choix $(\emptyset, s)$.

[6] Voici une esquisse de preuve (les détails ne seront pas retranscrits). Soient (o, σ) et (O, Σ) deux tels couples. Notons N l'"infini minimal" associé à (o, σ). L'idée est d'adapter la démonstration du théorème 126 avec départ O et pas Σ (mais sans ensemble stable associé puisque nous en cherchons précisément l'existence !) : l'image de la "suite" obtenue – si elle faisait sens – serait un infini pour O et Σ. Or l'axiome de remplacement nous légitime précisément la considération de cette image.

[7] sa suite des itérés

[8] On lira dans la note de bas de page 178 : *De l'aveu de son auteur, l'axiomatique de Peano est inspirée de cette définition 71.*

[9] le choix de la lettre N n'est pas anodin : lorsque $\binom{\sigma}{o} = \binom{s}{\emptyset}$, on retrouve $N = \mathbf{N}$

1. le prédicat $\underset{o}{\overset{\sigma}{\text{Chaine}}}$ traduit la condition α (être une σ-chaîne) et un bout de celle β (contenir o) ;
2. la condition de minimalité dans $\underset{o}{\overset{\sigma}{\text{InfiniMin}}}$ équivaut à l'autre bout de la condition β ("hérédité" de la récurrence) ;
3. les conditions distinguant $\underset{o}{\overset{\sigma}{\text{Peano}}}$ de $\underset{o}{\overset{\sigma}{\text{InfiniMin}}}$ sont exactement celles γ et δ (platitude) ;
4. les énoncés $\underset{o}{\overset{\sigma}{\text{InfiniMin}}}$ et $\underset{o}{\overset{\sigma}{\text{Infini}}}$ sont *équivalents* (si I dénote une σ-chaîne contenant o, alors l'intersection de ces dernières incluses dans I fait sens et est un candidat pour notre N).

En conséquence, un couple $\binom{\sigma}{o}$ vérifiera les axiomes de PEANO ssi il vérifie l'axiome $\underset{o}{\overset{\sigma}{\text{Infini}}}$ couplé aux deux restrictions donnant l'équivalence des axiomes de l'infini. En d'autres termes,

la platitude (qui suffit à l'équivalence des axiomes de l'infini) est
ce qu'il faut et suffit de rajouter à l'infini (au sens itératif)
pour obtenir l'arithmétique (au sens peanien).

Cette description devrait complètement démystifier ces conditions suffisantes. Peut-on alors poser la question de leur *nécessité* ?

Nécessité de la platitude ?

Revenons à l'équivalence conséquence de la platitude :

$$\left(\underset{o}{\overset{\sigma}{\text{Plat}}} \text{ et } \underset{O}{\overset{\Sigma}{\text{Plat}}}\right) \Longrightarrow \left(\underset{o}{\overset{\sigma}{\text{Infini}}} \Longleftrightarrow \underset{O}{\overset{\Sigma}{\text{Infini}}}\right).$$

Bien que cette équivalence redonne un sens itératif à l'axiome de l'infini et s'inscrive dans la perspective structuraliste qui traverse les remarques 130 et 131 de DEDEKIND, elle *n'est pas* notre cible. *Ses hypothèses*, en revanche, – la platitude – le sont, dans une démarche de *reverse mathematics*.

Dans cette perspective, quel théorème souhaitons-nous voir équivalent à la platitude ? Nous l'avons annoncé : c'est le théorème 126, lequel permet d'itérer une fonction *dans un ensemble déjà donné*[10] sur un objet de cet ensemble, et que nous avons signalé comme décrivant (en un sens catégoriel) le fondement de notre action.

2 *Reverse mathematics* : du théorème 126 de Dedekind aux axiomes de Peano

Le cadre formel est le langage ensembliste, écrit au premier ordre, muni des axiomes : *extension*, *parties*, *remplacement* – mais pas *infini* ! Rappelons que *remplacement* donne *séparation*, ce qui avec *parties* permet de construire tous les ensembles fonctionnels $B^A = \text{Fonc}(A, B)$.

On se donne :

1. un objet o ;
2. une fonctionnelle σ définie partout (dont les images $\sigma(x) =: x'$ seront notées avec des primes) ;
3. un ensemble N pour lequel le théorème 126 *fait sens* et est vérifié. Rappelons cet énoncé :

$$\#126 : \qquad \forall A,\ \begin{cases} \forall f \in A^A \\ \forall @ \in A \end{cases},\ \exists! a \in A^{\mathbf{N}},\ \begin{cases} \forall n \in N,\ a_{n'} = f(a_n) \\ a_0 = @ \end{cases}.$$

Objectif : montrer $\underset{o}{\overset{\sigma}{\text{Peano}}}$!

Nous allons démontrer (dans l'ordre) chaque point annoncé en police grasse droite :

***N* est une chaîne**

[10] si l'esprit itératif est le même, la différence technique est de taille car met en jeu les axiomes de remplacement

σ ne fixe personne
o n'est pas atteint
N est la plus petite chaîne
N vérifie le théorème de récurrence
Tout élément autre que o est atteint

[pause pour donner la direction]

N possède une suite de segments initiaux
N vérifie le théorème de récurrence forte
Un lemme de comparaison
σ est injective

Trois points sur quatre.

Convenons d'appeler ***chaîne*** tout ensemble satisfaisant $\underset{o}{\overset{\sigma}{\text{Chaîne}}}$, *i. e.* contenant o et stable par σ.

N est une chaîne. Soient $A, f, @$ et a comme dans #126.

L'égalité $a_0 = @$ faisant sens, son membre de gauche a_0 fait sens, *i. e.* la fonction a est définie en o, donc ce dernier appartient au domaine N de a.

Soit $n \in N$. L'égalité $a_{n'} = f(a_n)$ faisant sens, son membre de gauche $a_{n'}$ fait sens, *i. e.* la fonction a est définie en n', donc ce dernier appartient au domaine N de a. Finalement, N est stable par σ.

σ ne fixe personne. Soit $n \in N$ tel que $n' = n$. Soit A un ensemble à deux éléments, par exemple[11] $\{\emptyset, \mathfrak{P}(\emptyset)\}$. Notons f la transposition des éléments de A : observer que f n'a aucun point fixe. Prenons n'importe quel départ $@ \in A$. Soit a la suite donnée par #126. On a alors les égalités $a_n = a_{n'} = f(a_n)$, ce qui montre que f fixe a_n, d'où la contradiction.

o n'est pas successeur. Soit $m \in N$ tel que $m' = o$. Soit A un ensemble à deux éléments. Soit f constante sur A. Posons $@$ l'élément de A non atteint par f. Soit a la suite donnée par #126. On a alors les égalités $@ = a_o = a_{m'} = f(a_m)$, ce qui est absurde.

N est la plus petite chaîne. Précisons que c'est ici *et seulement ici* que nous utiliserons l'*unicité* de la suite a dans #126, ce qui permet de cerner la force de cette partie du #126.

Suivant Dedekind (théorème 79), définissons A par l'intersection de toutes les chaînes : cela fait sens puisque N en est une. Il nous suffit de montrer que A, qui est incluse dans la chaîne N, *contient* en fait ce dernier.

Définissons à présent une suite $u : N \longrightarrow N$ qui vaut l'identité sur A et qui coïncide ailleurs[12] avec σ. Montrons que cette suite u et la suite identité (que nous noterons v) vérifient toutes deux les conditions de #126 avec départ o et pas σ : par l'unicité, elle devront coïncider, en particulier en dehors de A, d'où $\sigma = \mathrm{Id}$ sur $N \setminus A$, ce qui s'écrit $\forall n \in N \setminus A\ ,\ n' = n$, ce qui montrera que σ (qui ne fixe personne) fixe en fait tous les $n \in N \setminus A$, d'où la vacuité de ce dernier – et la conclusion recherchée $N \subset A$.

Par définition, la suite u coïncide avec v sur A ; puisque $o \in A$, elles ont même départ $u_o = o = v_o$. Soit maintenant $n \in N$. Il est immédiat que $v_{n'} = n' = \sigma(n)$. Par ailleurs, si $n \in A$, alors $n' \in A$ (car A est une chaîne), d'où les égalités $u_{n'} = \mathrm{Id}(n') = n' = \sigma(n)$; si cette fois $n \notin A$, alors $n' \notin A$ (sinon la partie $A \amalg \{n\}$ serait une chaîne strictement plus grande), d'où les égalités $u_{n'} = \sigma(n') = \sigma(u_n)$, ce qui conclut.

N vérifie le théorème de récurrence. Rappelons ce schéma de théorèmes : *pour tout prédicat P singulaire, on a l'implication*

$$(P_o \wedge [\forall n \in N,\ P_n \implies P_{n'}]) \implies (\forall n \in N,\ P_n)\,.$$

Considérons un prédicat P vérifiant la conjonction ci-dessus. Suivons Dedekind (théorème 80). La partie $\{n \in N\ ;\ P_n\}$ est par hypothèse une chaîne, donc contient la chaîne minimale N, ce qui conclut.

Tout élément autre que le départ est successeur. Montrons par récurrence (théorème 78)

$$\forall n \in N,\ n \neq o \implies \exists a \in N,\ n = a'.$$

[11] *remplacement* donne *paire*, les objets $\emptyset$ et $\mathsf{P}(\emptyset)$ étant distincts puisque le second n'est pas vide (il contient $\emptyset$)

[12] l'idée est de garder la même relation de récurrence, la même condition initiale mais de changer de "condition initiale" en dehors de A (*i. e.* dans la zone hors d'atteinte de la relation de récurrence) en décalant tous les éléments hors de A

L'initialisation s'écrit "$o \neq o \implies \exists ...$", ce qui est de la forme "*faux implique [whatever]*" et est donc tautologique Soit ensuite un $n \in N$. On veut montrer l'implication "$n' \neq o \implies \exists a,\ n' = a'$", qui est de la forme "*[whatever] implique vrai*" (prendre $a := n$), donc vraie.

Une pause.

Donnons une autre démonstration du fait que o n'est pas successeur, laquelle nous servira d'inspiration pour montrer l'injectivité de σ.

Soit m (comme "moins un") un antécédent de o. L'idée est de "perturber" la boucle des itérés en insérant un élément étranger entre m et o, élément qui perturberait l'itération sans pourtant être visible dans les hypothèses de #126. Le diagramme suivant pourra nous guider :

$$\begin{array}{ccccccccc} \boldsymbol{\mu} & \longrightarrow & \longrightarrow & o & \longrightarrow & o' & \longrightarrow & \cdots \\ \uparrow & f & & \uparrow & & \sigma & & \downarrow \\ & \nwarrow & \longleftarrow & m & \longleftarrow & \cdots & \longleftarrow & \cdots \end{array}$$

Soit μ un objet hors[13] de N et notons $\overline{N} := N \amalg \{\mu\}$. On définit une application f stabilisant $\overline{N}$ qui agit sur $N \setminus m$ comme σ et qui agit ailleurs comme $m \mapsto \mu \mapsto o$. Soit a la suite à valeurs dans $\overline{N}$ de départ o et de pas f donnée par #126. Montrons $\forall n \in N,\ a_n = n$ par récurrence : l'égalité $a_m = m$ nous mènera alors droit à la contradiction suivant les égalités

$$o = a_0 = a_{m'} = f(a_m) = f(m) = \mu \qquad \text{(et sachant que } N \text{ contient } o \text{ et pas } \mu).$$

L'initialisation $a_o = o$ traduit le départ choisi pour a. Soit maintenant $n \in N$ tel que $a_n = n$. Si $n = m$, on a alors $a_{n'} = a_{m'} = a_o = o = m' = n'$. Dans le cas contraire, f agit sur n comme σ, d'où $a_{n'} = f(a_n) = f(n) = \sigma(n) = n'$, ce qui conclut.

Pour montrer l'injectivité de σ, nous allons reprendre l'idée ci-dessus :

perturber l'itération suivant une boucle.

Toutefois, l'orbite que nous avions en forme de "0" (une boucle) va devenir en forme de "∂", il va pousser un "segment initial" à la boucle que nous allons perturber (dans le schéma suivant, m est un élément de la boucle qui a même image O qu'un élément μ hors de cette boucle) :

$$\begin{array}{ccccccccccccccc} o & \longrightarrow & o' & \longrightarrow & \cdots & \longrightarrow & \mu & \longrightarrow & \longrightarrow & O & \longrightarrow & \cdots & \longrightarrow & \cdots \\ & & & & & & \uparrow & f & & \uparrow & & \sigma & & \downarrow \\ & & & & & & & \nwarrow & \longleftarrow & m & \longleftarrow & \cdots & \longleftarrow & \cdots \end{array} .$$

Tout va marcher à l'identique, sauf quand il faudra préciser en quel sens μ vient *avant* m, ce qui fait l'objet du **lemme de comparaison** ci-après, que nous démontrons à l'aide d'une forme *forte* de récurrence. N'ayant cependant pas défini de relation d'ordre sur N (on pourrait suivre le § 7 de Dedekind mais ce dernier utilise naturellement l'injectivité que nous souhaitons établir), nous allons construire un analogue des segments entiers $[0, n]$ et formuler une récurrence forte à l'aide de ces derniers. La récurrence forte nous servira par ailleurs dans la preuve de l'injectivité de σ.

Reprise.

N **possède une suite de segments initiaux.** Montrons l'existence d'une suite (S_n) de parties de N telle[14] que

$$S_0 = \{o\} \qquad \text{et} \qquad \forall n \in N,\ \overset{o}{\underset{n}{\in}} S_n \qquad \text{et } \forall n \in N,\ S_{n'} = S_n \cup \{n'\}.$$

Notons f l'application[15] $\begin{cases} \mathfrak{P}(N) & \longmapsto & \mathfrak{P}(N) \\ A & \mapsto & \{o\} \cup \sigma(A) \end{cases}$. Le #126 nous donne une suite (S_n) de départ $\{o\}$ et de pas f. Montrons $\forall n \in N,\ S_{n'} = S_n \cup \{n'\}$ par récurrence. L'initialisation vient des égalités

$$S_{o'} = f(S_o) = \{o\} \cup \sigma(S_0) = S_0 \cup \sigma(\{o\}) = S_0 \cup \{\sigma(o)\} = S_0 \cup \{o'\}.$$

[13] on peut s'inspirer du paradoxe de Russell pour affirmer que $\{n \in N\ ;\ n \notin n\}$ en est un

[14] La croissance d'une telle suite n'a *a priori* aucune raison d'être stricte. On comparera par ailleurs les propriété des segments S_n avec la définition des parties $Z_n := N \setminus \langle n' \rangle$ de la définition 98.

[15] pour rajouter un élément "au bout", on décale tout le monde et on rajoute le premier élément décalé à l'autre bout

On par ailleurs, étant donné un $n \in N$ tel que $S_{n'} = S_n \cup \{n'\}$, les égalités

$$\begin{aligned} S_{n''} &= f(S_{n'}) = \{o\} \cup \sigma(S_{n'}) = \{o\} \cup \sigma(S_n \cup \{n'\}) = \{o\} \cup \underline{\sigma(S_n) \cup \sigma(\{n'\})} \\ &= \underline{\{o\} \cup \sigma(S_n)} \cup \sigma(\{n'\}) = f(S_n) \cup \{\sigma(n')\} = S_{n'} \cup \{n''\}, \text{ ce qui conclut la récurrence.} \end{aligned}$$

L'appartenance $o \in S_n$ est immédiate par récurrence vu les inclusions $S_n \subset S_{n'}$. Vu par ailleurs les appartenances $n' \in S_n \cup \{n'\} \subset S_{n'}$, tout élément a qui est un successeur vérifie $a \in S_a$, appartenance qui reste valide lorsque $a = o$ vu le choix de S_o.

N vérifie le théorème de récurrence forte. Soit P un prédicat singulaire. Montrons l'implication

$$P_o \wedge [\forall n \in N,\ (\forall s \in S_n,\ P_s) \Longrightarrow P_{n'}] \Longrightarrow [\forall n \in N,\ P_n]$$

Notons $\mathfrak{P}_a$ le prédicat $\forall s \in S_a,\ P_s$ (d'argument a). Remarquer pour tout $n \in N$ l'implication $\mathfrak{P}_n \Longrightarrow P_n$ (vu que $n \in S_n$). Supposons la conjonction ci-dessus. Montrons $\forall n \in N,\ \mathfrak{P}_n$ par récurrence, d'où il viendra la conclusion $\forall n \in N,\ P_n$ attendue. L'initialisation $\mathfrak{P}_o$ s'écrit $\forall s \in S_o,\ P_s$, *i. e.* $\forall s \in \{o\},\ P_s$, ou encore P_o, ce qui est un conjoint de l'hypothèse. Soit maintenant $n \in N$ tel que $\mathfrak{P}_n$. Par l'autre conjoint, on obtient $P_{n'}$; comme le prédicat P est (d'après $\mathfrak{P}_n$) vérifié sur S_n, il l'est sur $S_n \cup \{n'\} = S_{n'}$, ce qui conclut à $\mathfrak{P}_{n'}$.

Un lemme de comparaison. Vu – chez les naturels – la visée $S_n = [0, n]$, on pourrait (mais on ne le fera pas) définir $a \leq b$ par $S_a \subset S_b$. Nous allons montrer l'analogue du caractère total de $\leq$, à savoir

$$\forall a, b \in N,\ [a \in S_b \text{ ou } b \in S_a].$$

Soit $a \in N$.

Montrons[16] $\forall n \in N,\ S_a \subsetneq S_n \Longrightarrow S_{a'} \subset S_n$ par récurrence sur n. La prémisse de l'initialisation s'écrit $S_a \subsetneq S_o$, *i. e.* $S_a \subsetneq \{o\}$, ce qui revient à la vacuité de S_a, laquelle est absurde puisque $o \in S_a$, d'où le caractère tautologique de l'initialisation. Soit maintenant $n \in N$ tel que $S_a \subsetneq S_n \Longrightarrow S_{a'} \subset S_n$ et supposons $S_a \subsetneq S_{n'}$. Alors $a \neq n'$ (sinon le $\subsetneq$ précédent serait un $=$), *i. e.* $a \notin \{n'\}$, d'où l'appartenance $a \in S_a \setminus \{n'\} \subset S_{n'} \setminus \{n'\} \subset S_n$ et (par hypothèse de récurrence) l'inclusion $S_{a'} \subset S_n$; jointe à $S_n \subset S_{n'}$, elle conclut.

Montrons $\forall n \in N,\ [S_a \subset S_n \text{ ou } S_n \subset S_a]$ par récurrence sur n. L'inclusion (connue) $\{o\} \subset S_a$ est un disjoint de l'initialisation, validant cette dernière. Soit maintenant $n \in N$ tel que $S_a \subset S_n$ ou $S_n \subset S_a$. Dans le premier cas, on a immédiatement $S_a \subset S_{n'}$: sinon, le deuxième cas donne une inclusion *stricte* $S_n \subsetneq S_a$, d'où il vient $S_{n'} \subset S_a$ d'après le paragraphe précédent, ce qui conclut la récurrence.

Pour conclure, il suffit de coupler les appartenances $a \in S_a$ et $b \in S_b$ à l'une des inclusions $S_a \subset S_b$ ou $S_b \subset S_a$.

σ est injective. Soient par l'absurde m et μ distincts dans N ayant même successeur. Quitte à échanger les rôles, on peut supposer d'après le lemme $\mu \in S_m$ (*i. e.* que μ vient "avant" m). Définissons une application $f : N \longrightarrow N$ qui envoie m sur μ et qui agit ailleurs comme σ :

$$\begin{array}{ccccccccccccccc} o & \longrightarrow & o' & \longrightarrow & \cdots & \longrightarrow & \mu & \longrightarrow & \longrightarrow & \mu' = m' & \longrightarrow & \cdots & \longrightarrow & \cdots \\ & & & & & & \uparrow & f & & \uparrow & & \sigma & & \downarrow \\ & & & & & & & \nwarrow & \longleftarrow & m & \longleftarrow & \cdots & \longleftarrow & \cdots \end{array}.$$

Soit a la suite à valeurs dans N de départ o et de pas f donnée par #126. Montrons $\forall n \in N,\ a_n = n$ par récurrence forte : les deux égalités résultantes pour $n \in \{m, \mu\}$ nous mèneront alors, avec celle $m' = \mu'$, droit à la contradiction suivant les égalités

$$\begin{cases} a_{m'} = f(a_m) = f(m) = \mu \\ a_{\mu'} = f(a_\mu) = f(\mu) = \mu' \end{cases} \qquad (\mu \text{ ne pouvant être fixé par } \sigma).$$

L'initialisation $a_o = o$ traduit le départ choisi pour a. Soit maintenant $n \in N$ tel que $\forall s \in S_n,\ a_s = s$. Si $n = m$, puisque $\mu \in S_m$, on peut utiliser l'hypothèse de récurrence forte et affirmer[17] $a_\mu = \mu$, d'où l'on tire

$$a_{n'} = a_{m'} = a_{\mu'} = f(a_\mu) = f(\mu) = \sigma(\mu) = \mu' = m' = n'.$$

Sinon, on a directement $a_{n'} = f(a_n) = f(n) = \sigma(n) = n'$, ce qui conclut.

[16] analogue chez les naturels de l'implication $a < b \Longrightarrow a + 1 \leq b$

[17] C'est pour *cette seule égalité* qu'ont été développés les points précédents de cette section