

# AXIOMATISATION DE L'ARITHMÉTIQUE

Paul Rozière  
Paris Diderot – Paris 7

version du 15 juin 2022– (861)

La notion d'entier naturel est très primitive en mathématiques. L'axiomatisation de l'arithmétique, peut être vue comme une « définition », sachant qu'une telle définition ne peut se faire à partir de rien. Il s'agit plutôt d'une analyse de notre intuition<sup>1</sup> à propos des entiers naturels. Nous allons préciser certaines propriétés essentielles et montrer comment elles permettraient de développer l'arithmétique. Au passage on met en évidence certaines notions, comme les définitions inductives, les bons ordres, qui sont plus générales.

Les entiers naturels peuvent se représenter comme des suites d'objets identiques, par exemple des bâtons : |, ||, |||, ... et cette représentation est très primitive.

L'opération qui permet de construire les entiers est alors l'opération « ajouter un bâton » que l'on appelle « successeur » notée  $s$  et qui est une fonction des entiers naturels dans les entiers naturels.

On a besoin également d'un objet initial qui est le « 0 » (aucun bâton). On obtient alors une représentation des entiers (analogue à celle des suites de bâtons) :  $0, s0, ss0, sss0, \dots$

On peut procéder ensuite de deux façons :

- par une définition inductive qui est une définition *explicite* de l'ensemble des entiers naturels et des opérations associées, forcément dans un contexte plus général ;
- par une axiomatisation qui se contente de donner des propriétés fondamentales que doivent vérifier les entiers naturels, et que l'on peut voir comme une définition *implicite*.

Deux mathématiciens se sont intéressés à la question à la fin du XIX<sup>e</sup> siècle. En 1888 Richard Dedekind donne une définition explicite de l'ensemble des entiers naturels, mais dans un contexte ensembliste qui n'est alors pas encore bien formalisé. En 1889 Giuseppe Peano donne indépendamment une axiomatisation de l'arithmétique, qui suppose aussi implicitement un cadre ensembliste. Les deux démarches se rejoignent rapidement.

La « construction » de la totalité des entiers naturels repose chez Dedekind sur l'existence d'un ensemble infini pour lequel il utilise un argument non mathématique qui n'est pas très convaincant. L'axiomatisation de la théorie des ensembles, dans le cadre de laquelle se réalise la construction de Dedekind, est plus tardive (Zermelo 1908). Peano n'a pas ce problème avec son approche axiomatique. Mais le principe de définition par récurrence n'est énoncé en toute généralité et démontré que chez Dedekind.

## 1 Définition inductive

On se place dans un « univers » où l'on dispose d'un objet et d'une opération unaire appelons les  $0$  et  $s$ . L'ensemble des entiers naturels est alors vu comme *le plus petit ensemble*  $\mathbb{N}$  (plus petit au sens de l'inclusion) qui contient  $0$  et tel que si  $x \in \mathbb{N}$  alors  $s(x) \in \mathbb{N}$ .

Montrons que cette définition est correcte. Quand un ensemble  $A$  vérifie que si  $x \in A$  alors  $s(x) \in A$ , on dit que  $A$  est *clos par application du successeur*. Appelons  $Cl(A)$  le fait pour  $A$  de contenir  $0$  et d'être clos par successeur :

$$Cl(A) = [0 \in A \text{ et } \forall x(x \in A \Rightarrow s(x) \in A)] .$$

On remarque que si chacun des ensembles d'une famille  $(A_i)_{i \in I}$  vérifie  $Cl(A_i)$  alors leur intersection également :

$$\text{si } \forall i \in I Cl(A_i), \text{ alors } Cl\left(\bigcap_{i \in I} A_i\right) \quad (*)$$

On peut donc définir l'ensemble des entiers comme l'intersection de tous les ensembles  $A$  qui contiennent  $0$  et qui vérifient que si  $x \in A$  alors  $s(x) \in A$  :

$$\mathbb{N} = \bigcap_{Cl(A)} A .$$

1. En 1899, David Hilbert écrivait en préface à son axiomatisation de la géométrie « L'exposition des ces axiomes et leur examen approfondi [...] revient à l'analyse logique de notre intuition de l'espace ».

Mais on ne peut pas définir l'intersection d'une famille vide d'ensemble : pour que cette définition soit correcte, il faut supposer qu'il existe au moins un tel ensemble  $A$  tel que  $CI(A)$ . On reviendra dessus dans le cours sur la théorie des ensembles, après avoir précisé l'univers et l'opération en question.

Ceci étant admis,  $\mathbb{N}$  est bien un ensemble vérifiant  $CI(A)$  d'après (\*), et c'est forcément le plus petit par définition.

C'est ce que l'on appelle une *définition inductive*.

On montre facilement que  $0, s(0), s(s(0))$  etc. sont éléments de  $\mathbb{N}$ . La définition dit qu'on ne peut les construire que de cette façon là. Une autre façon est de dire que  $\mathbb{N}$  vérifie la propriété ou principe de récurrence (dit également *principe d'induction*) qui est essentiellement une autre façon d'écrire la définition :

pour toute propriété  $P$  « bien définie », si  $P(0)$  et  $\forall x \in \mathbb{N}(P(x) \Rightarrow P(s(x)))$ , alors  $\forall x \in \mathbb{N} P(x)$ .

Il suffit en effet de prendre  $A = \{x \in \mathbb{N} / P(x)\}$ , de remarquer que par hypothèse cet ensemble a  $0$  pour élément et il est clos par successeur, c'est à dire qu'il vérifie  $CI(A)$ . Il contient donc  $\mathbb{N}$ , et la propriété  $P$  est vérifiée sur  $\mathbb{N}$ .

Cependant si on n'est pas plus précis sur ce que doivent vérifier l'opération  $s$  et la constante  $0$ , on a pu définir autre chose que l'ensemble des entiers naturels : rien n'empêche par exemple que  $s(s(0)) = 0$ , et l'ensemble obtenu ne contient que deux éléments.

En théorie des ensembles on donne une définition explicite de  $0$  et  $s$  qui empêche ce genre de choses de se produire, mais là on va se contenter de décrire ce que doivent vérifier  $0$  et  $s$  (on admet qu'il est possible de trouver de tels  $0$  et  $s$ ), et on rejoint la démarche axiomatique. Ce que l'on veut obtenir c'est que chaque élément de  $\mathbb{N}$  ne puisse être obtenu que d'une seule façon, à partir de  $0$  et en passant un certain nombre de fois au successeur. On sait aussi que la structure des entiers est *librement engendrée* par  $0$  et  $s$ , il n'existe aucune relation entre les éléments de  $\mathbb{N}$  autre que celle donnée par les constructions de la définition inductive. Ceci est assuré par ces deux axiomes identifiés par Dedekind et Peano

—  $\forall x \in \mathbb{N} s(x) \neq 0$ ;

—  $\forall x, y \in \mathbb{N} (s(x) = s(y) \Rightarrow x = y)$ ;

À partir de là on peut développer l'arithmétique, mais passons d'abord à la démarche axiomatique, qui est directement inspirée de cette construction.

## 2 Axiomatisation de l'arithmétique

### 2.1 Les axiomes de Peano

Une axiomatique peut être vue comme une définition implicite : on ne dit pas « ce qu'est » un entier, mais on donne des axiomes, qui énoncent des propriétés que les entiers doivent vérifier. Ces axiomes doivent suffire pour démontrer ce que l'on sait sur les entiers, à commencer par les choses les plus évidentes intuitivement.

On suppose donc donné un l'ensemble  $\mathbb{N}$  des entiers naturels, avec un élément distingué, une constante,  $0$ , et muni d'une fonction de  $\mathbb{N}$  dans  $\mathbb{N}$ , la fonction *successeur* notée  $s$ . Les *axiomes de Peano* pour les entiers sont les trois axiomes suivants :

**successeur non nul**  $\forall x \in \mathbb{N} s(x) \neq 0$ ;

**injectivité de la fonction successeur**  $\forall x, y \in \mathbb{N} (s(x) = s(y) \Rightarrow x = y)$ ;

**récurrence** Pour toute propriété  $P$  « bien définie » sur les entiers :

$$\left[ P[0] \text{ et } \forall y \in \mathbb{N} (P[y] \Rightarrow P[s(y)]) \right] \Rightarrow \forall x \in \mathbb{N} P[x].$$

L'idée est finalement la même que dans la définition précédente, c'est-à-dire que la propriété de récurrence exprime que l'on ne peut pas obtenir un entier autrement qu'en partant de  $0$  et en passant au successeur. Il est d'ailleurs possible de donner l'axiome de récurrence sous la forme ensembliste suivante.

**récurrence** Pour tout ensemble  $A \subseteq \mathbb{N}$  :

$$\left[ 0 \in A \text{ et } \forall y \in \mathbb{N} (y \in A \Rightarrow s(y) \in A) \right] \Rightarrow \mathbb{N} \subseteq A.$$

C'est le cas particulier de la récurrence pour la propriété  $x \in A$ , et la récurrence pour une propriété quelconque se déduit de celle-ci en définissant  $A$  comme l'ensemble des entiers vérifiant la propriété  $P$ , soit  $A = \{x \in \mathbb{N} / P[x]\}$ .

Une conséquence immédiate de la récurrence est le raisonnement par cas, suivant qu'un entier est nul ou un successeur.

**Lemme 2.1 (raisonnement par cas)** *Tout entier est soit 0, soit un successeur :*

$$\forall x \in \mathbb{N} (x = 0 \vee \exists y \in \mathbb{N} x = s(y)) .$$

**Démonstration.** Par récurrence : la propriété  $x = 0 \vee \exists y \in \mathbb{N} x = s(y)$  est vérifiée en 0. Elle est également vérifiée pour  $s(z)$  (c'est une démonstration par récurrence très particulière, puisque l'hypothèse de récurrence n'est pas utilisée!). ■

On appelle *prédécesseur* d'un entier naturel  $x$ , un entier naturel  $y$  dont le successeur est  $x$  ( $s(y) = x$ ). Par injectivité du successeur, si un entier possède un prédécesseur celui-ci est unique. Le lemme énonce que tout entier non nul a un prédécesseur.

Avant de continuer le développement, remarquons, que comme c'est le cas le plus souvent en mathématiques, un certain nombre de choses sont supposées connues, les propriétés de l'égalité par exemple (que Peano ajoutait à ses axiomes), mais aussi la notion d'ensemble.

L'axiome de récurrence n'est d'ailleurs pas un axiome aussi clair qu'il y paraît : que signifie « pour toute propriété »? Il faudrait préciser le langage utilisé, dans lequel s'expriment ces propriétés, pour le moment on considère qu'il s'agit des propriétés que l'on définit en mathématiques.

Mais si l'on précise le langage on aura des axiomatisations plus ou moins puissantes de l'arithmétique, suivant les propriétés que l'on autorise pour la récurrence. Par exemple l'arithmétique du premier ordre est une théorie axiomatique où la récurrence ne porte que sur des propriétés que l'on exprime avec, en plus de 0 et  $s$ , l'addition, la multiplication, les connecteurs et les quantificateurs usuels *sur les entiers*. On ne peut pas parler d'ensemble (et donc la seconde forme de la récurrence n'existe pas), si ce n'est au travers des propriétés sur les entiers définies dans le langage auquel on s'est restreint. On peut ainsi développer l'arithmétique « élémentaire », mais pas l'analyse. Une telle restriction a un intérêt en logique, mais on ne l'envisage pas pour le moment. La théorie que l'on développe est en fait relative à une notion intuitive d'ensemble.

**Exercice 1** Montrer que les trois axiomes de Peano sont indépendants : pour cela il faut construire pour chacun des axiomes un *contre-modèle*, c'est-à-dire un ensemble  $\mathcal{N}$  contenant un élément distingué, appelé 0, et sur lequel on définit une fonction  $s : \mathcal{N} \rightarrow \mathcal{N}$ , de façon que pour  $(\mathcal{N}, 0, s)$ , l'axiome dont on veut montrer qu'il est indépendant n'est pas vérifié, mais les deux autres le sont.

## 2.2 Définition par récurrence

On s'autorise à introduire un nouveau nom pour un entier ou une fonction quand on a une preuve d'existence et d'unicité. Par exemple on pose  $1 = s(0)$  car il existe un seul entier  $n$  tel que  $n = s(0)$ , ( $s$  est une fonction). De la même façon on pourrait définir (c'est juste à titre d'exemple), une fonction  $+_2 : \mathbb{N} \rightarrow \mathbb{N}$ , vérifiant  $+_2(x) = s(s(x))$ . Ces définitions sont de simples abréviations et la preuve d'existence et d'unicité est évidente.

Mais on a besoin de définitions sur les entiers plus complexes, et très utiles, les *définitions par récurrence*. On peut *définir par récurrence* une suite, par exemple d'entiers, de réels, d'ensembles etc. Ce ne sont pas de simples abréviations : la définition par récurrence d'une fonction utilise cette fonction elle-même.

Vous utilisez pourtant des définitions de suite par récurrence depuis les classes de lycée, parce que notre intuition des entiers naturels donne aussi l'intuition que ces définitions sont correctes. Dans un cadre axiomatique, il est nécessaire de le démontrer, ne serait-ce que pour montrer que nous avons bien introduit « suffisamment » d'axiomes. Dans le cas présent, la démonstration éclaire aussi les outils ensemblistes utiles (qui sont implicites dans l'axiomatisation).

**Théorème 2.2 (Définition par récurrence, Dedekind 1888)** *Soit  $E$  un ensemble non vide,  $a \in E$ , une fonction  $h : E \rightarrow E$ , alors il existe une unique fonction  $f : \mathbb{N} \rightarrow E$  vérifiant :*

$$f(0) = a ; \quad f(s(x)) = h(f(x)) .$$

Une fonction de domaine les entiers est ce que l'on appelle habituellement une suite, pour laquelle on utilise la notation indicielle pour l'argument (en notant  $n+1 = s(n)$ ,  $u_0 = a$ ,  $u_{n+1} = h(u_n)$ ), la suite est notée  $(u_n)_{n \in \mathbb{N}}$ , en abrégé  $(u_n)$ .

**Démonstration.** L'unicité se démontre très facilement par récurrence. Soit  $g$  une fonction vérifiant les mêmes équations que  $f$ . On a donc  $f(0) = g(0)$ , et, si pour un entier  $x$ ,  $f(x) = g(x)$ , alors  $f(s(x)) = h(f(x)) = h(g(x)) = g(s(x))$ .

L'existence demande une construction ensembliste du graphe de la fonction. Une construction possible serait de procéder par approximations finies successives, puis de prendre la réunion de celles-ci en montrant qu'elles se « recollent » bien. Celle qui est proposée ci-dessous procède à l'inverse par intersection de façon analogue à la définition inductive de  $\mathbb{N}$ .

La fonction que l'on souhaite définir est de  $\mathbb{N}$  dans  $E$ . On a besoin d'abord, pour pouvoir définir une propriété de clôture, de travailler sur les relations entre éléments de  $\mathbb{N}$  et de  $E$ , soit des sous-ensembles de  $\mathbb{N} \times E$ , plutôt que des fonctions. On obtiendra le graphe de la fonction  $f$  comme un sous-ensemble de  $\mathbb{N} \times E$  particulier (dont il faudra montrer que c'est le graphe d'une fonction).

La propriété de clôture est directement inspirée de la définition de  $f$ , elle porte sur  $R \subseteq \mathbb{N} \times E$

$$Cl(R) \equiv_d (0, a) \in R \text{ et } \forall n \in \mathbb{N} \forall y \in E ((n, y) \in R \Rightarrow (s(n), h(y)) \in R)$$

(on vérifie facilement que si  $R$  est le graphe d'une fonction  $f$ , on retrouve les équations de l'énoncé pour définir  $f$ ).

L'ensemble des  $R \subseteq (\mathbb{N} \times E)$  qui vérifient  $Cl(R)$  est non vide car  $\mathbb{N} \times E$  satisfait évidemment la propriété de clôture. On peut donc poser

$$G = \bigcap_{Cl(R)} R.$$

Il s'agit de montrer que  $G$  est le graphe d'une fonction.

- On a bien  $Cl(G)$  (la propriété de clôture passe à l'intersection);
- Tout élément  $n$  de  $\mathbb{N}$  possède une image par la relation de graphe  $G$ , ceci se démontre par récurrence sur  $n$ :

$n = 0$ : comme  $G$  satisfait  $Cl(G)$ ,  $(0, a) \in G$ ;

$n \mapsto n + 1$ : Par hypothèse de récurrence  $n$  a une image  $x$  par la relation de graphe  $G$ , alors  $s(n)$  a pour image  $h(x)$  (car  $Cl(G)$ ).

- Tout élément  $n$  de  $\mathbb{N}$  possède une unique image par la relation de graphe  $G$ . Ceci se démontre par récurrence et utilise les deux autres axiomes de Peano.

$n = 0$ : Supposons que l'image de 0 n'est pas unique, c'est-à-dire qu'il existe  $b \neq a$  tel que  $(0, b) \in G$ . Montrons alors que  $G' = G \setminus \{(0, b)\}$  satisfait la propriété de clôture ce qui entraînera  $G \subseteq G'$  et donc une contradiction. En effet  $(0, a) \in G'$  car  $Cl(G)$  et  $b \neq a$ . Supposons  $(n, x) \in G$ , alors comme  $Cl(G)$ ,  $(s(n), h(x)) \in G$ , et comme  $s(n) \neq 0$  (axiome de Peano),  $(s(n), h(x)) \in G'$ .

$n \mapsto n + 1$ : Par hypothèse de récurrence  $n$  a une seule image, que l'on appelle  $x$  par la relation de graphe  $G$ . On sait que  $s(n)$  a pour image  $h(x)$ . Supposons que  $s(n)$  a pour image  $y \neq h(x)$ . On pose  $G' = G \setminus \{(s(n), y)\}$ , et on va aboutir à une contradiction en montrant que  $G'$  satisfait la propriété de clôture. En effet

—  $(0, a) \in G$ , or  $0 \neq s(n)$  (axiome de Peano) donc  $(0, a) \in G'$ ;

— soit  $(m, z) \in G'$ , alors  $(m, z) \in G$ , donc  $(s(m), h(z)) \in G$  (propriété de clôture).

Si  $m \neq n$ ,  $s(m) \neq s(n)$  (axiome de Peano, le successeur est injectif), donc  $(s(m), h(z)) \in G'$ .

Si  $m = n$ ,  $n$  a pour seule image  $x$  par  $G$  (hypothèse de récurrence) donc par  $G'$ , et on a bien  $(s(n), h(x)) \in G'$  car  $y \neq h(x)$ . ■

Le théorème de définition par récurrence est bien différent de l'axiome de récurrence. On peut d'ailleurs vérifier (exercice suivant) que, pour l'existence on a besoin d'utiliser que le successeur d'un entier est non nul, et l'injectivité du successeur, qui sont deux axiomes indépendants de l'axiome de récurrence.

**Exercice 2** Démontrez que chacun des deux axiomes, le successeur d'un entier est non nul, et l'injectivité du successeur, sont bien nécessaires pour le théorème de définition par récurrence (existence de la fonction) (*Indication : utilisez les contre-modèles de l'exercice 1*).

Le théorème précédent permet par exemple de définir par récurrence la fonction  $f : \mathbb{N} \rightarrow \mathbb{N}$ ,  $x \mapsto 2x$ :

$$f(0) = 0; \quad f(s(x)) = s \circ s(f(x)).$$

Les opérations de base de l'arithmétique comme l'addition et la multiplication peuvent se définir également par récurrence. Comme elles ont deux arguments, il faut définir par récurrence une fonction qui à un entier associe une fonction de  $\mathbb{N}$  dans  $\mathbb{N}$  pour utiliser le théorème 2.2. Plutôt que de traiter ces cas particuliers directement, on peut les obtenir comme conséquence du corollaire suivant sur les définitions par récurrence avec paramètres.

**Corollaire 2.3 (Définition par récurrence avec paramètres)** Soit  $A$  un ensemble,  $E$  un ensemble non vide, deux fonctions  $g : A \rightarrow E$ , et  $h : (E \times A) \rightarrow E$ , alors il existe une unique fonction  $f : (\mathbb{N} \times A) \rightarrow E$  vérifiant :

$$f(0, y) = g(y) ; \quad f(s(x), y) = h(f(x, y), y)$$

On peut avoir plusieurs paramètres en prenant pour  $A$  un produit cartésien. Le cas où  $A$  est réduit à un élément équivaut à l'absence de paramètres, et ce corollaire est donc aussi une généralisation du théorème 2.2.

**Démonstration.** On note  $E^A$  l'ensemble des fonctions de  $A$  dans  $E$ . L'idée est de définir par récurrence la fonction  $\tilde{f} : \mathbb{N} \rightarrow E^A$  qui à un entier  $x$  associe la fonction  $f_x : y \mapsto f(x, y)$ .

**Unicité :** soient  $f : (\mathbb{N} \times A) \rightarrow E$  vérifiant  $f(0, y) = g(y) = f'(0, y)$ ,  $f(s(x), y) = h(f(x, y), y)$ . Soit  $\tilde{f} : \mathbb{N} \rightarrow E^A$ ,  $x \mapsto f_x$  avec  $f_x : A \rightarrow E$ ,  $y \mapsto f(x, y)$ . Si on pose  $\tilde{h} : E^A \rightarrow E^A$ ,  $\tilde{h}(\zeta) : y \mapsto h(\zeta(y), y)$ , la fonction  $\tilde{f}$  vérifie :

$$\tilde{f}(0) = g ; \quad \tilde{f}(s(x)) = \tilde{h}(\tilde{f}(x))$$

et c'est l'unique fonction vérifiant ces deux équations d'après le théorème 2.2. Si une autre fonction  $f' : (\mathbb{N} \times A) \rightarrow E$  vérifiait les mêmes équations que  $f$ , on associerait de la même façon  $\tilde{f}' : \mathbb{N} \rightarrow E^A$  vérifiant les mêmes équations que  $\tilde{f}$ , d'où  $\tilde{f}' = \tilde{f}$ , d'où  $f' = f$ .

**Existence :** Soit  $\tilde{h} : E^A \rightarrow E^A$ ,  $\tilde{h}(\zeta) : y \mapsto h(\zeta(y), y)$ . Soit  $\tilde{f} : \mathbb{N} \rightarrow E^A$  la fonction définie par récurrence :

$$\tilde{f}(0) = g ; \quad \tilde{f}(s(x)) = \tilde{h}(\tilde{f}(x))$$

On pose maintenant  $f(x, y) = (\tilde{f}(x))(y)$ . La fonction  $f : (\mathbb{N} \times A) \rightarrow E$  vérifie bien les deux équations souhaitées. ■

L'addition, la multiplication, l'exponentielle se définissent toutes trois par récurrence avec un paramètre :

$$\begin{aligned} x + 0 &= x ; & x + s(y) &= s(x + y) \\ x \cdot 0 &= 0 ; & x \cdot s(y) &= x \cdot y + x \\ x^0 &= 1 ; & x^{s(y)} &= x^y \cdot x . \end{aligned}$$

On pose  $1 = s(0)$ , et on a immédiatement par les deux équations qui définissent l'addition que  $x + 1 = s(x)$ . On peut donc écrire  $x + 1$  pour  $s(x)$ . On a également que  $x \cdot 1 = x$  par les deux équations qui définissent la multiplication.

On a parfois besoin de définitions par récurrence où l'argument de la fonction que l'on définit apparaît également comme « paramètre », comme our cette définition de la fonction factorielle :

$$0! = 1 ; \quad (n + 1)! = n! \cdot (n + 1) .$$

Ce n'est pas une définition par récurrence avec paramètre du type des précédentes, car le « paramètre »  $n + 1$  dépend de  $n$ .

On déduit à nouveau du principe de définition par récurrence que celle-ci est correcte. On énonce le résultat avec paramètres, même s'il n'y en a pas pour la fonction factorielle.

**Corollaire 2.4 (Définition par récurrence, paramètres dépendant de l'argument)**

Soit  $A$  un ensemble,  $E$  un ensemble non vide, deux fonctions  $g : A \rightarrow E$ , et  $h : (E \times \mathbb{N} \times A) \rightarrow E$ , alors il existe une unique fonction  $f : (\mathbb{N} \times A) \rightarrow E$  vérifiant

$$f(0, y) = g(y) ; \quad f(s(x), y) = h(f(x, y), x, y) .$$

**Démonstration.** On définit par récurrence avec paramètre la fonction  $\tilde{f} : (\mathbb{N} \times A) \rightarrow (\mathbb{N} \times E)$ ,  $(n, y) \mapsto (n, f(n, y))$ , puis la fonction  $f$  en prenant la seconde projection. On note  $p_1 : (\mathbb{N} \times E) \rightarrow \mathbb{N}$  et  $p_2 : (\mathbb{N} \times E) \rightarrow E$  la première et la seconde projection, on définit  $\tilde{f}$  par :

$$\tilde{f}(0, y) = (0, (g(y)) ; \quad \tilde{f}(s(x), y) = \left( p_1(\tilde{f}(x, y)), h(p_2(\tilde{f}(x, y)), p_1(\tilde{f}(x, y)), y) \right) .$$

L'unicité se déduit de même (ou se démontre directement par récurrence). ■

On a vu comme application la définition de la factorielle. La récurrence avec paramètre dépendant de l'argument permet également de définir l'ensemble des entiers de 0 à  $x$ , notons le  $I_x$  :

$$I_0 = \{0\} ; I_{s(x)} = I_x \cup \{s(x)\} . \tag{1}$$

**Exercice 3 (définition par récurrence avec substitution de paramètre)** Soit  $A$  un ensemble,  $E$  un ensemble non vide, trois fonctions  $g : A \rightarrow E$ ,  $h : (E \times A) \rightarrow E$ , et  $\sigma : A \rightarrow A$ . Montrer qu'alors il existe une unique fonction  $f : (\mathbb{N} \times A) \rightarrow E$  vérifiant :

$$f(0, y) = g(y) ; \quad f(s(x), y) = h(f(x, \sigma(y)), y)$$

(Indication : reprendre la démonstration de la récurrence avec paramètre)

Les définitions par récurrence avec substitution de paramètre sont utiles par exemple quand on définit une fonction par récurrence sur la longueur d'une suite finie, ou la hauteur d'un arbre fini : la suite ou l'arbre est alors le paramètre.

## 2.3 Quelques propriétés de l'addition, de la multiplication et de l'exponentielle

On retrouve les propriétés usuelles de ces opérations. On montre en particulier que l'addition et la multiplication sont toutes deux associatives et commutatives, et que la multiplication est distributive sur l'addition, à savoir pour tous entiers  $x$ ,  $y$  et  $z$  :

- $x + (y + z) = (x + y) + z$ ;
- $0 + x = x$ ;
- $s(x) + y = s(x + y)$ ;
- $x + y = y + x$ ;
- $x \cdot (y + z) = x \cdot y + x \cdot z$ ;
- $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ ;
- $0 \cdot x = 0$ ;
- $s(x) \cdot y = x \cdot y + y$ ;
- $x \cdot y = y \cdot x$ ;
- $1 \cdot x = x \cdot 1 = x$ .

**Exercice 4** Démontrer ces propriétés par récurrence (dans l'ordre indiqué).

On a également les propriétés usuelles de la fonction puissance, pour tous entiers naturels  $x$ ,  $y$  et  $z$  :

- $0^{x+1} = 0$ ;
- $1^x = 1$ ;
- $x^1 = x$ ;
- $(x \cdot y)^z = x^z \cdot y^z$ ;
- $x^{y+z} = x^y \cdot x^z$ ;
- $(x^y)^z = x^{y \cdot z}$ .

**Exercice 5** Démontrer ces propriétés par récurrence.

**Exercice 6** Montrer, à partir des axiomes de Peano ou des propriétés déjà démontrées, la régularité de l'addition, à savoir que pour tous entiers naturels  $x$ ,  $z$  et  $z'$  :

$$z + x = z' + x \Rightarrow z = z' ; \quad x + z = x + z' \Rightarrow z = z' .$$

**Exercice 7** Montrer, à partir des axiomes de Peano et des propriétés déjà démontrées, que pour tous entiers naturels  $x$  et  $y$  :

$$x + y = 0 \Rightarrow (x = 0 \text{ et } y = 0) ; \quad x \cdot y = 0 \Rightarrow (x = 0 \text{ ou } y = 0) .$$

## 2.4 Ordre

### 2.4.1 Les axiomes d'ordre

On dit que la relation  $\leq$  sur un ensemble  $E$  non vide est une *relation d'ordre*, ou relation d'*ordre large*, sur cet ensemble quand elle est réflexive, transitive et antisymétrique :

$$\begin{aligned} \forall x \in E \quad x \leq x & \quad \text{(réflexivité)} \\ \forall x, y, z \in E \quad [(x \leq y \text{ et } y \leq z) \Rightarrow x \leq z] & \quad \text{(transitivité)} \\ \forall x, y \in E \quad [(x \leq y \text{ et } y \leq x) \Rightarrow x = y] & \quad \text{(antisymétrie)} \end{aligned}$$

Un *ensemble ordonné*, ou un ordre en abrégé, est un ensemble non vide muni d'une relation d'ordre. C'est un *ordre total* quand de plus deux éléments sont toujours comparables :

$$\forall x, y \in E \quad (x \leq y \vee y \leq x) \quad \text{(totalité)}$$

La relation d'*ordre strict associé* à la relation d'ordre large  $\leq$  est la relation  $<$ , définie par

$$x < y \equiv_d x \leq y \text{ et } x \neq y .$$

On peut axiomatiser directement les ordres stricts : la relation  $<$  sur  $E$  est une *relation d'ordre strict* quand

$$\begin{aligned} \forall x \in E \neg x < x & \quad (\text{irréflexivité}) \\ \forall x, y, z \in E [(x < y \text{ et } y < z) \Rightarrow x < z] & \quad (\text{transitivité}) \end{aligned}$$

Une relation d'ordre strict total vérifie de plus la propriété de trichotomie :

$$\forall x, y \in E (x < y \vee x = y \vee y < x) \quad (\text{trichotomie})$$

Pour un ordre strict ces trois cas sont exclusifs (par irréflexivité et transitivité).

L'ordre large associé  $\leq$  à un ordre strict  $<$  est défini par  $x \leq y \equiv_d x < y \vee x = y$ .

### Proposition 2.5 (ordre large et ordre strict)

- i. Si  $(E, \leq)$  est un ordre (large), et  $<$  est la relation d'ordre strict associée,  $(E, <)$  est un ordre strict, et que si de plus  $(E, \leq)$  est un ordre total,  $(E, <)$  est un ordre strict total.
- ii. si  $(E, <)$  est un ordre strict, et  $\leq$  l'ordre large associé, alors  $(E, \leq)$  est un ordre large, et que si de plus  $(E, <)$  est un ordre strict total,  $(E, \leq)$  est un ordre total.

**Exercice 8** Démontrer la proposition précédente. Pour la deuxième partie on peut d'abord démontrer que si  $(E, <)$  est un ordre strict, alors la propriété d'antisymétrie pour les ordres stricts est vérifiée :

$$\forall x, y \in E (x < y \Rightarrow \neg y < x) \quad (\text{antisymétrie stricte})$$

### 2.4.2 L'ordre sur les entiers

On a défini par récurrence l'ensemble  $I_x$  des entiers inférieurs ou égaux à  $x$  (voir page 5). On peut donc définir la relation d'ordre sur  $\mathbb{N}$  par  $x \in I_y$ .

**Proposition 2.6 (définition de l'ordre sur les entiers)** Il existe une unique relation sur  $\mathbb{N}$ , notée  $\leq$  vérifiant :

- $\forall x \in \mathbb{N} (x \leq 0 \Leftrightarrow x = 0)$  ;
- $\forall x, y \in \mathbb{N} [x \leq s(y) \Leftrightarrow (x \leq y \vee x = s(y))]$ .

**Démonstration.** La relation  $x \leq y \equiv_d x \in I_y$  vérifie bien ces équivalences. D'autre part, si  $\leq$  est une relation vérifiant ces équivalences, la suite  $(J_x)$  définie par  $J_x = \{z \in \mathbb{N} / z \leq x\}$  vérifie les équations définissant la suite  $(I_x)$ , donc  $J_x = I_x$ , donc  $x \leq y$  si et seulement si  $x \in I_y$ . ■

**Proposition 2.7** La relation  $\leq$  définie sur  $\mathbb{N}$  est bien une relation d'ordre total sur  $\mathbb{N}$ . La relation d'ordre strict associée  $<$  vérifie

$$x < y \Leftrightarrow s(x) \leq y ; \quad x < s(y) \Leftrightarrow x \leq y .$$

On a de plus

$$x \leq y \Leftrightarrow s(x) \leq s(y) ; \quad x < y \Leftrightarrow s(x) < s(y) .$$

**Démonstration.** On montre successivement

- (1)  $x \leq x$ , immédiat par cas (lemme 2.1).
- (2)  $x \leq s(x)$ , conséquence du précédent.
- (3)  $x \leq y, y \leq z \Rightarrow x \leq z$ , par récurrence sur  $z$ .  
 $z = 0$  : si  $y \leq 0$ , par définition  $y = 0$  donc  $x = 0$ .  
 De  $z$  à  $s(z)$  : on a  $x \leq y$  et  $y \leq s(z)$ . On utilise la définition (proposition 2.6). Soit  $y \leq z$ , donc par hypothèse de récurrence,  $x \leq z$ , donc  $x \leq s(z)$ . Soit  $y = s(z)$  donc  $x \leq s(z)$ .
- (4)  $s(x) \leq s(y) \Rightarrow x \leq y$ , par la définition, injectivité du successeur, (2) et transitivité (3).  
 Par définition  $s(x) \leq s(y)$  signifie  $s(x) \leq y$  ou  $s(x) = s(y)$ . Dans le second cas  $x = y$ . Sinon, comme d'après (2)  $x \leq s(x)$ , par transitivité  $x \leq y$ .
- (5)  $\neg s(x) \leq x$ , par récurrence sur  $x$  d'après (4).  
 $x = 0$  : définition et axiome de Peano  
 De  $x$  à  $s(x)$  : par hypothèse de récurrence, d'après (4).
- (6)  $x \leq y, y \leq x \Rightarrow x = y$ , par cas sur  $x$  (lemme 2.1), transitivité (3) et (5).
- (7)  $x \leq y \Rightarrow s(x) \leq s(y)$ , par récurrence sur  $y$ .

Si  $y = 0$ , De  $x \leq 0$  on déduit  $x = 0$  par définition et  $s(x) = s(0)$ .

De  $y$  à  $s(y)$  : supposons  $x \leq s(y)$ . Soit  $x \leq y$ , et par hypothèse de récurrence  $s(x) \leq s(y)$  donc par définition  $s(x) \leq s(s(y))$ , soit  $x = s(y)$  et alors  $s(x) = s(s(y))$ .

(8)  $0 \leq x$ , par récurrence sur  $x$  (immédiate en utilisant la définition).

(9)  $x \leq y \vee y \leq x$ , par récurrence sur  $x$ , en utilisant (8), puis (7) et (2).

De  $x$  à  $s(x)$  : par hypothèse de récurrence  $y \leq x$  ou  $x \leq y$ . Dans le premier cas  $y \leq s(x)$  par définition. Si  $x \leq y$ , alors  $s(x) \leq s(y)$  par (7). Soit  $s(x) \leq y$  et c'est fini, soit  $s(x) = s(y)$  donc  $y = x$ , donc  $y \leq s(x)$  par (2).

Ordre strict :

(10)  $x < s(y) \Rightarrow x \leq y$ , par définition de l'ordre et de l'ordre strict associé.

(11)  $x \leq y \Rightarrow x < s(y)$ , par définition de l'ordre, de l'ordre strict associé et (5).

(12)  $s(x) \leq y \Rightarrow x < y$ , car de  $s(x) \leq y$ , on déduit  $x \neq y$  par (5), et  $x \leq y$  par (2) et (3).

(13)  $x < y \Rightarrow s(x) \leq y$ , d'après (7) et l'injectivité du successeur.

(14)  $x < y \Leftrightarrow s(x) < s(y)$ , d'après (4) et (7) (même propriété pour l'ordre large), et avec (12) et (13). ■

### 2.4.3 Addition et ordre

On aurait pu également définir la relation d'ordre sur les entiers à partir de l'addition, comme le montre la proposition suivante.

**Proposition 2.8** Pour deux entiers naturels  $x$  et  $y$  :

$$x \leq y \equiv \exists z \in \mathbb{N} \ x + z = y .$$

**Démonstration.** Il suffit de montrer les deux propriétés qui définissent l'ordre pour la relation  $\exists z \in \mathbb{N} \ x + z = y$  (en utilisant les deux propriétés définissant l'addition), et d'appliquer la proposition 2.6 (unicité).

—  $(\exists z \in \mathbb{N} \ x + z = 0) \Leftrightarrow x = 0$ .

Supposons  $x + z = 0$ . Comme  $x + s(z') = s(x + z') \neq 0$  (axiome),  $z$  n'est pas un successeur, donc d'après le lemme 2.1  $z = 0$ , donc  $x + 0 = x = 0$ .

Pour la réciproque on a bien  $0 + 0 = 0$ .

—  $(\exists z \in \mathbb{N} \ x + z = s(y)) \Leftrightarrow (\exists z \in \mathbb{N} \ x + z = y \vee x = s(y))$ .

On suppose que  $x + z = s(y)$ . On raisonne par cas (lemme 2.1) sur  $z$ . Si  $z = 0$ ,  $x = s(y)$ . Si  $z = s(z')$ ,  $s(x + z') = x + s(z') = s(y)$  et par injectivité du successeur,  $x + z' = y$ .

Pour la réciproque on distingue deux cas. Soit  $x = s(y)$ , on a  $s(y) = s(y) + 0$  donc  $s(y) \leq s(y)$ . Soit on a  $z$  tel que  $x + z = y$ . Alors  $x + s(z) = s(x + z) = s(y)$ . ■

Du résultat de l'exercice 6, on déduit l'unicité du  $z$  tel que  $x + z = y$ , quand  $x \leq y$ , ce qui permet d'introduire la soustraction comme opération partielle :  $y - x$  est défini seulement quand  $x \leq y$ , et vérifie  $x + (y - x) = y$ .

## 2.5 Propriétés de récurrence et de bon ordre

On déduit de l'axiome de récurrence des propriétés de récurrence plus générales (en apparence) et souvent utilisées.

### 2.5.1 Récurrence à partir d'un certain rang

Il est courant d'avoir besoin de la récurrence seulement à partir d'un certain rang, qui est un entier quelconque, un cas particulier étant la récurrence à partir de 0, déjà énoncée.

**Proposition 2.9** Soit  $k$  un entier naturel. Pour toute propriété  $P$  sur les entiers

$$\left[ P[k] \text{ et } \forall y \in \mathbb{N} \left( (y \geq k \text{ et } P[y]) \Rightarrow P[s(y)] \right) \right] \Rightarrow \forall x \in \mathbb{N} \ (x \geq k \Rightarrow P[x]) .$$

**Démonstration.** On suppose  $P[k]$  (1) et  $\forall y \in \mathbb{N} \left( (y \geq k \text{ et } P[y]) \Rightarrow P[s(y)] \right)$  (2). Il suffit de démontrer  $x \geq k \Rightarrow P[x]$  par récurrence simple (à partir de 0).

— En 0 la propriété est évidente si  $k$  est un successeur, car alors  $0 \leq k$  est faux, et quand  $k = 0$ , c'est  $P[k]$ ;

— Pour l'étape de récurrence on suppose  $y \geq k \Rightarrow P[y]$ , et  $s(y) \geq k$ , c'est-à-dire (propriété de l'ordre)  $s(y) = k$  ou  $y \geq k$ . Si  $s(y) = k$ , on a bien  $P[k]$  par hypothèse (1). Si  $y \geq k$ , on a par hypothèse de récurrence  $P[y]$ , donc  $P[s(y)]$  par hypothèse (2). On a donc bien  $\forall x \in \mathbb{N} \ (x \geq k \Rightarrow P[x])$ . ■



### 2.5.2 Récurrence « forte »

On peut également avoir besoin de l'hypothèse de récurrence pour des entiers plus petits que le prédécesseur immédiat. C'est la propriété de récurrence appelée parfois « forte ». Si  $y$  est un entier, on utilise l'abréviation

$$\forall z \leq y P[z] \equiv_d \forall z \in \mathbb{N} (z \leq y \Rightarrow P[z]) .$$

On pourra utiliser aussi l'abréviation  $\exists z \leq y P[z] \equiv_d \exists z \in \mathbb{N} (z \leq y \text{ et } P[z])$ .

**Proposition 2.10** *Pour toute propriété  $P$  sur les entiers*

$$\left[ P[0] \text{ et } \forall y \in \mathbb{N} (\forall z \leq y P[z] \Rightarrow P[s(y)]) \right] \Rightarrow \forall x \in \mathbb{N} P[x] .$$

Il est bien sûr possible d'en énoncer une variante à partir d'un certain rang, comme au paragraphe précédent.

**Démonstration.** On suppose  $P[0]$  et  $\forall y \in \mathbb{N} (\forall z \leq y P[z] \Rightarrow P[s(y)])$ , et on montre la propriété  $\forall z \leq x P[z]$  pour tout entier naturel  $x$  par récurrence sur  $x$ . On en déduit alors  $\forall x \in \mathbb{N} P[x]$ .

La propriété a été supposée en 0. Pour l'étape de récurrence, comme par définition  $x \leq s(z) \equiv x \leq z \vee x = s(z)$ , on a bien, vu l'hypothèse,  $\forall z \leq y P[z] \Rightarrow \forall z \leq s(y) P[z]$ . ■

Une autre version de la récurrence forte, uniquement en terme d'ordre (strict), ne fait plus référence au successeur. En effet les deux hypothèses se regroupent en une seule.

**Proposition 2.11 (récurrence bien fondée)** *Pour toute propriété  $P$  sur les entiers*

$$\forall y \in \mathbb{N} (\forall z < y P[z] \Rightarrow P[y]) \Rightarrow \forall x \in \mathbb{N} P[x] .$$

**Démonstration.** On suppose  $\forall y \in \mathbb{N} (\forall z < y P[z] \Rightarrow P[y])$  et on montre  $\forall x \in \mathbb{N} P[x]$  par cas, en utilisant la récurrence forte.

- Si  $x = 0$ , comme  $\forall z < y P[0] \Rightarrow P[0]$ , et que l'hypothèse est vide, on a  $P[0]$ .
- Si  $x = s(x')$ , comme  $x < s(x') \equiv x \leq x'$ , on a l'hypothèse de récurrence forte. ■

Comme exemple d'application montrons que tout nombre strictement supérieur à 1 possède un diviseur premier (résultat que l'on trouve dans les éléments d'Euclide).

Soit  $z$  un entier naturels strictement supérieur à 1. Si  $z$  est premier il se divise bien lui-même. Supposons donc que  $z$  n'est pas premier, c'est-à-dire que, comme  $z > 1$ ,  $z$  a un diviseur  $y$ ,  $y > 1$   $y < z$ . Par hypothèse de récurrence  $y$  a un diviseur premier, qui est donc également un diviseur de  $z$ .

Dans cette démonstration, on voit bien que, naturellement, le cas de base (celui pour laquelle la démonstration ne fait pas appel à un entier strictement plus petit) n'est pas 0, ni même 2, en faisant une récurrence « forte » à partir du rang 2, mais n'importe quel nombre premier. La récurrence bien fondée, ou les propriétés de même nature comme la propriété de bon ordre ou le principe de descente infinie que l'on va voir à la section suivante, est particulièrement utile quand il n'y a pas un seul cas de base, ou pas de cas de base bien déterminé a priori.

**Exercice 9 (définition par récurrence sur la suite des valeurs)** Le but de cet exercice est de généraliser le théorème de définition par récurrence 2.2 d'une façon similaire à celle utilisée pour généraliser le théorème de récurrence ci-dessus. On va montrer que l'on peut généraliser les définitions par récurrence à un appel récursif sur un entier strictement plus petit (et non nécessairement le précédent) : soit  $A$  et  $E$  deux ensembles non vides, trois fonctions  $g : A \rightarrow E$ , et  $h : (E \times A) \rightarrow E$  et  $\gamma : \mathbb{N} \rightarrow \mathbb{N}$  telle que  $\gamma(0) = 0$  et  $\forall x \in \mathbb{N}^* \gamma(x) < x$ , on veut montrer qu'il existe une unique fonction  $f : (\mathbb{N} \times A) \rightarrow E$  vérifiant

$$f(0, a) = g(a) \quad \text{et si } x > 0, \quad f(x, a) = h(f(\gamma(x), a), a)$$

1. Montrer l'unicité.
2. Montrer l'existence en définissant directement, par récurrence avec paramètre dépendant de l'argument (corollaire 2.4), une fonction  $F : (\mathbb{N} \times A) \rightarrow E^{\mathbb{N}}$  qui vérifiera  $F(x, a)(p) = f(p, a)$  si  $p \leq x$ , et  $F(x, a)(p) = 0$  sinon (la fonction  $F(x, a)$  représentera la suite finie des valeurs de  $f(p, a)$  pour  $p \leq x$ ).

On pourrait généraliser à plusieurs appels récursifs, à un appel récursif sur la suite de tous les précédents...

### 2.5.3 Bon ordre

La relation  $\leq$  définit un *bon ordre* sur l'ensemble  $E$  quand

- la relation  $\leq$  est un ordre total sur  $E$ ;
- tout sous-ensemble de  $E$  *non vide* a un *plus petit élément*, c'est-à-dire que pour tout sous-ensemble  $I$  de  $E$  non vide, il existe un élément  $a$  de  $E$  tel que :

$$a \in I \text{ et } \forall x \in I \ a \leq x .$$

On dit aussi que  $(E, \leq)$  est bien ordonné.

Dans la définition de bon ordre, on peut se passer de l'hypothèse de totalité. En effet soient  $x$  et  $y$  deux éléments de  $E$  ordonné par  $\leq$ . Si tout ensemble non vide a un plus petit élément, alors en particulier  $\{x, y\}$ , ce qui signifie que ceux-ci sont comparables.

Les ensembles  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$  ne sont pas bien ordonnés par l'ordre usuel.

**Proposition 2.12** *L'ensemble  $(\mathbb{N}, \leq)$  est bien ordonné.*

En fait la propriété de bon ordre est équivalente à la récurrence bien fondée pour les ordres totaux, comme le montre la proposition suivante (la récurrence bien fondée est reformulée en termes ensemblistes). On déduira donc de celle-ci et de la proposition 2.11 que  $(\mathbb{N}, \leq)$  est bien ordonné.

**Proposition 2.13** *Un ensemble (non vide) totalement ordonné  $(E, \leq)$  est bien ordonné si et seulement s'il vérifie la propriété de récurrence bien fondée, c'est-à-dire que pour tout sous-ensemble  $J$  de  $E$  :*

$$\forall y (\forall z < y \ z \in J \Rightarrow y \in J) \Rightarrow J = E .$$

On écrit  $\forall z < y \ P[z]$  ( $P$  ne dépend pas de  $y$ ) pour  $\forall z \in E \ (z < y \Rightarrow P[z])$ .

**Démonstration.** Comme  $J$  est un sous-ensemble de  $E$ ,  $J = E$  équivaut à  $\forall x \in J \ x \in E$ . On reformule par contraposée la propriété de récurrence bien fondée :

$$\exists x \in E \ x \notin J \Rightarrow \exists y \in E \ (\forall z < y \ z \in J \text{ et } y \notin J)$$

La récurrence bien fondée équivaut donc à cette propriété pour tout sous-ensemble  $J$  de  $E$ . Comme tout sous-ensemble  $J$  de  $E$  est le complémentaire d'un sous-ensemble  $I$  de  $E$  et réciproquement, la récurrence bien fondée équivaut à ce que pour tout sous-ensemble  $I$  de  $E$  :

$$\exists x \in E \ x \in I \Rightarrow \exists y \in E \ (\forall z < y \ z \notin I \text{ et } y \in I) .$$

Cette dernière propriété exprime que tout sous-ensemble non vide  $I$  de  $E$  a un élément minimal  $y$ . Comme  $(E, \leq)$  est totalement ordonné, cet élément minimal est le plus petit élément de  $I$  (si  $z \in I$ ,  $z < y$  n'est pas possible car  $y$  est minimal, donc  $z \geq y$  par totalité). La récurrence bien fondée équivaut donc à la propriété de bon ordre. ■

La propriété de bon ordre, comme la seconde forme de la récurrence, fait référence à la notion d'ensemble, mais on aurait pu aussi bien en donner une version en terme de « propriété ».

On réécrit la démonstration du résultat d'Euclide (tout nombre a un diviseur premier), en utilisant directement la propriété de bon ordre. Soit  $z$  un entier naturels strictement supérieur à 1. Soit  $I$  l'ensemble des diviseurs strictement supérieurs à 1 de  $z$ . Cet ensemble  $I$  est non vide car  $z > 1$  et  $z \mid z$ , et possède donc un plus petit élément, soit  $p$ . Si  $p$  a un autre diviseur que 1 et lui même, ce diviseur est aussi un diviseur de  $z$ , et ceci contredirait que  $p$  est le plus petit élément de  $I$ , donc  $p$  est premier.

On voit bien que cette démonstration est très proche de celle par récurrence ci-dessus, les arguments sont identiques.

Une façon un peu différente d'exprimer la propriété de bon ordre est le principe de descente infinie de Fermat<sup>2</sup>.

**Corollaire 2.14** *Il n'existe pas de suite infinie décroissante d'entiers naturels.*

**Démonstration.** En effet si  $(u_n)$  est une telle suite,  $\{u_n \mid n \in \mathbb{N}\}$  serait un ensemble non vide qui n'aurait pas de plus petit élément, ce qui contredit que  $\mathbb{N}$  est bien ordonné. ■

Euclide utilise la descente infinie pour démontrer que tout nombre entier strictement supérieur à 1 possède un diviseur premier : on raisonne par l'absurde, en supposant le contraire on fabrique une suite décroissante infinie d'entiers.

2. Le nom est dû à Fermat, qui a mis en avant la descente infinie pour la démonstration de certaines propriétés arithmétiques, mais elle est déjà utilisée dans les Éléments d'Euclide.

## 2.6 Une axiomatisation des entiers par l'ordre

On va maintenant montrer que l'on pourrait axiomatiser  $\mathbb{N}$  à partir de la notion d'ordre. La propriété de bon ordre ne suffit pas, il existe des ensembles bien ordonnés qui ne représentent manifestement pas les entiers. Par exemple si on ajoute à  $\mathbb{N}$  un élément  $\omega$  « au bout de  $\mathbb{N}$  », c'est-à-dire que l'ordre sur  $\mathbb{N} \cup \{\omega\}$  est le prolongement de l'ordre sur  $\mathbb{N}$  qui vérifie  $\forall x \in \mathbb{N} x < \omega$ , on obtient un ensemble bien ordonné (exercice), qui ne vérifie pas l'axiome de récurrence.

Si  $(E, \leq)$  est un ensemble ordonné, on appelle *successeur* d'un élément  $x$  de  $E$ , le plus petit élément de l'ensemble des majorants stricts de  $x$ . Un élément de  $E$  n'a pas forcément de successeur, mais si celui-ci existe, il est unique, car un ensemble ordonné a au plus un plus petit élément.

**Lemme 2.15** *Si  $(E, \leq)$  est totalement ordonné, et si deux éléments  $x$  et  $y$  ont le même successeur, alors  $x = y$ .*

**Démonstration.** Comme l'ordre est total,  $x \leq y$  ou  $y \leq x$ . On suppose, quitte à intervertir  $x$  et  $y$ , que  $x \leq y$ . Soit  $s_x$  le successeur de  $x$ . Si  $x < y$ , alors  $s_x \leq y$ , or  $s_x$  est aussi le successeur de  $y$ , donc un majorant strict de  $y$ , ce n'est pas possible; donc  $x = y$ . ■

Le *prédécesseur* d'un élément  $n$  de  $E$  est un élément dont  $n$  est le successeur. D'après le lemme 2.15, dans un ensemble totalement ordonné, tout élément de  $E$  a au plus un prédécesseur (mais il peut ne pas en avoir).

**Proposition 2.16** *Soit  $(\mathbb{N}, \leq)$  un ensemble ordonné, tel que*

- $(\mathbb{N}, \leq)$  est un bon ordre, le plus petit élément de  $\mathbb{N}$  est noté  $0$ ;
- Tout élément  $x$  de  $\mathbb{N}$  a un successeur noté  $s(x)$ ;
- Tout élément de  $\mathbb{N}$  différent de  $0$  est le successeur d'un autre élément :

$$\forall x \in \mathbb{N} (x = 0 \vee \exists y \in \mathbb{N} x = s(y)).$$

Alors  $(\mathbb{N}, 0, s)$  satisfait les axiomes de Peano.

Le dernier axiome est l'énoncé du lemme 2.1, avec le successeur pris au sens des ensembles ordonnés.

**Démonstration.**

- Pour tout  $x$ ,  $s(x) \neq 0$ , car  $x < s(x)$  et  $0$  est par définition le plus petit élément de  $\mathbb{N}$ .
- L'injectivité du successeur est donnée par le lemme 2.15.
- On montre la forme ensembliste de la récurrence. Soit  $I$  un sous-ensemble de  $\mathbb{N}$  tel que  $0 \in I$  et  $\forall y \in \mathbb{N} (y \in I \Rightarrow s(y) \in I)$ . Soit  $J$  le complémentaire de  $I$  dans  $\mathbb{N}$ . Si  $J$  était non vide, il aurait un plus petit élément, soit  $x$ . Comme par hypothèse  $0 \in I$ ,  $x \neq 0$ , donc  $x = s(y)$  par le troisième axiome. On a  $y \in I$ , car  $x$  est le plus petit élément de  $J$ , mais ceci contredit l'hypothèse. Donc  $J = \emptyset$ , donc  $I = \mathbb{N}$ . ■

**Exercice 10** Montrer que l'on a une axiomatisation équivalente en remplaçant le deuxième axiome « Tout élément de  $\mathbb{N}$  a un successeur » par « Tout élément de  $\mathbb{N}$  possède un majorant strict ».

## 2.7 Conclusion

Il reste encore à faire pour développer les notions arithmétiques élémentaires, par exemple la division euclidienne, mais les trois axiomes de Peano le permettent, comme le montrent les premières propriétés développées.

Il est également possible d'en déduire une construction des entiers relatifs (comme différences de deux entiers naturels), des rationnels (comme quotients d'un relatif et d'un relatif non nul), et des réels (comme coupures sur les rationnels, ou comme suites de Cauchy de rationnels).

Pour ces constructions, particulièrement pour celles des réels, on a besoin des notions d'ensemble d'entiers et de propriété sur les entiers, notions déjà utilisées au début de ce chapitre sans les avoir axiomatisées. Ce chapitre peut se réinterpréter et se compléter dans le cadre de l'axiomatisation de la théorie des ensembles.

## Bibliographie

DEDEKIND, Richard (1888). *Was sind und was sollen die Zahlen?* Brunswick : Vieweg.

PEANO, Giuseppe (1889). *Arithmetices principia, nova methodo exposita*. Turin : Bocca.

# Index

antisymétrie, 6	ordre large, 6
antisymétrie stricte, 7	ordre strict, 7
Axiomes de Peano, 2	ordre total, 6
bien ordonné, 10	plus petit élément, 10
bon ordre, 10	prédécesseur, entiers, 3
descente infinie, 10	prédécesseur, ordre, 11
définition inductive, 2	raisonnement par cas sur les entiers, 3
définition par récurrence, 3	relation d'ordre, 6
définition par récurrence avec paramètres, 5	récurrence, 2
définition par récurrence avec substitution de paramètre, 6	récurrence « forte », 9
définition par récurrence dépendant de l'argument, 5	récurrence bien fondée, 9
définition par récurrence sur la suite des valeurs, 9	récurrence à partir d'un certain rang, 8
ensemble ordonné, 6	réflexivité, 6
induction, 2	successeur, entiers, 2
irréflexivité, 7	successeur, ordre, 11
	transitivité, 6, 7
	trichotomie, 7

## Table des matières

<b>1 Définition inductive</b>	<b>1</b>
<b>2 Axiomatisation de l'arithmétique</b>	<b>2</b>
2.1 Les axiomes de Peano	2
2.2 Définition par récurrence	3
2.3 Quelques propriétés de l'addition, de la multiplication et de l'exponentielle	6
2.4 Ordre	6
2.4.1 Les axiomes d'ordre	6
2.4.2 L'ordre sur les entiers	7
2.4.3 Addition et ordre	8
2.5 Propriétés de récurrence et de bon ordre	8
2.5.1 Récurrence à partir d'un certain rang	8
2.5.2 Récurrence « forte »	9
2.5.3 Bon ordre	10
2.6 Une axiomatisation des entiers par l'ordre	11
2.7 Conclusion	11
<b>Bibliographie</b>	<b>11</b>
<b>Index</b>	<b>12</b>