

# LOGIQUE ET THÉORIE DES ENSEMBLES.

Paul Rozière  
Paris 7 – M63010

28 novembre 2011

On écrit parfois  $A, B \Rightarrow C$  pour  $(A \text{ et } B) \Rightarrow C$ .  
Le signe «  $\equiv_d$  » signifie « équivaut par définition à ».

## 1 Axiomatisation de l'arithmétique

La notion d'entier naturel semble tout à fait primitive en mathématiques. On peut construire les entiers relatifs, les rationnels et finalement les réels à partir des entiers naturels et de la notion d'ensemble.

Dans un premier temps on va donner une axiomatisation des entiers naturels. On verra ensuite comment, en théorie des ensembles, on peut donner une construction des entiers, qui vérifie ces axiomes.

La notion d'entier naturel repose sur deux intuitions. La première est déjà très liée à la notion d'ensemble (fini). Deux ensembles ont même nombre d'éléments s'ils sont en bijection, c'est-à-dire qu'on peut les faire correspondre un à un. Ainsi on peut savoir, en observant une table dressée, qu'il y a autant de couteaux que de fourchettes sans avoir eu besoin de les compter. En ce sens un entier caractérise donc une classe d'ensembles finis tous en bijection. C'est le nombre entier comme *cardinal*. Nous y reviendrons dans le cadre de la théorie des ensembles.

La deuxième intuition repose sur celle de successeur : ajouter un. Les entiers sont obtenus à partir de zéro en passant au successeur. C'est plutôt le nombre entier comme *ordinal* (premier, second, troisième, etc.). C'est sur cette notion que se fonde l'axiomatisation des entiers.

### 1.1 Les axiomes de Peano

Une axiomatique est une sorte de définition implicite : les entiers sont définis par leurs propriétés.

On suppose que l'ensemble  $\mathbb{N}$  des entiers contient une constante, 0, et qu'il est 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 du successeur**  $\forall x, y \in \mathbb{N} \ (s(x) = s(y) \Rightarrow x = y)$  ;

**Récurrence** Pour toute propriété  $P$  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 que l'on construit les entiers en ajoutant 1 au précédent entier obtenu, ce en partant de 0. Les deux premiers axiomes expriment que l'on ne peut boucler ou revenir en arrière par cette opération, c'est-à-dire que la structure des entiers est *librement engendrée* par 0 et  $s$  : il n'y a pas d'autres relations entre les entiers que celles induites par la construction.

La propriété de récurrence exprime que l'on ne peut pas obtenir les entiers autrement. En effet soit  $A$  un ensemble qui contient 0, et tel que que si  $n \in A$ , alors  $s(n) \in A$ . On démontre par récurrence que la propriété  $\forall n \in \mathbb{N} n \in A$  : l'ensemble  $A$  contient  $\mathbb{N}$ .

Cependant la propriété de récurrence n'est pas un axiome aussi clair qu'il y paraît : que signifie « pour toute propriété » ? Pour la justifier on a parlé d'ensemble, et en fait on considère que cette axiomatisation suppose connue cette notion. C'est le cas le plus souvent pour les théories axiomatiques étudiées en mathématique : la notion d'ensemble et ses propriétés sont supposées connues.

On pourra donc préciser ce que l'on entend par propriété quand on abordera la théorie des ensembles proprement dite. Pour le moment on considère qu'il s'agit des propriétés que l'on définit en mathématiques. Dans ce cadre, on montre alors que l'axiome de récurrence équivaut à l'axiome suivant :

**Récurrence** Pour tout ensemble d'entiers  $I$  :

$$[0 \in I \text{ et } \forall y \in \mathbb{N} (y \in I \Rightarrow s(y) \in I)] \Rightarrow \mathbb{N} = I \text{ .}$$

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

Mais on peut donner des axiomatisations plus ou moins puissantes de l'arithmétique, suivant les propriétés que l'on autorise pour la récurrence. Par exemple on appelle « arithmétique de Peano » la théorie axiomatique, dite du premier ordre, 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, et que l'on axiomatisera au chapitre suivant.

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

**Lemme 1.1 (raisonnement par cas)** *Tout entier est soit 0, soit un successeur :*

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

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

**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.

## 1.2 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 (on ne le fait pas, 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. D'un point de vue axiomatique, il est nécessaire de démontrer que ces définitions sont correctes.

**Théorème 1.2 (Définition par récurrence)** *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 une suite, pour laquelle on utilise très souvent 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  $(u_n)$ .

L'existence sera démontrée plus tard, dans le chapitre sur la théorie des ensembles. On peut déjà remarquer qu'il faudra nécessairement utiliser que le successeur d'un entier est non nul, et l'injectivité du successeur, qui sont deux axiomes indépendants de celui de démonstration par récurrence. Il s'agit donc bien d'un théorème tout à fait différent de l'axiome de récurrence.

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  $f(s(x)) = h(f(x)) = h(g(x)) = g(s(x))$ .

**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 montrer l'existence de la fonction définie par récurrence (*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 une fonction de  $\mathbb{N}$  dans  $\mathbb{N}$  par récurrence, ce qui se fait directement par le théorème 1.2. 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 1.3 (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 1.2.

**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 1.2. 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 pour 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 1.4 (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  $I_x$  :

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

**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.

### 1.3 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  $z$  :

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

**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.

## 1.4 Ordre

### 1.4.1 Les axiomes d'ordre

On dit que la relation  $\leq$  sur un ensemble  $E$  non vide est une *relation d'ordre* 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 :

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

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 :

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

et on montre que pour un ordre strict ces trois cas sont exclusifs.

L'*ordre large associé*  $\leq$  à un ordre strict  $<$  est défini par  $x \leq y \equiv_d x < y \text{ ou } x = y$ .

### Proposition 1.5 (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 6** 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 :

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

### 1.4.2 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 1.6 (définition de l'ordre sur les entiers)** Il existe une unique relation sur  $\mathbb{N}$ , notée  $\leq$  vérifiant :

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

**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 1.7** 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 :

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

**Démonstration.** On montre successivement :

- (1)  $x \leq x$ , immédiat par cas (lemme 1.1).
- (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 1.6). 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 1.1), 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)  $x \leq y$  ou  $y \leq x$ , 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). ■

### 1.4.3 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 1.8** *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 1.6 (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 1.1  $z = 0$ , donc  $x + 0 = x = 0$ .

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

- $(\exists z \in \mathbb{N} x + z = s(y)) \Leftrightarrow (\exists z \in \mathbb{N} x + z = y \text{ ou } x = s(y))$ .  
On suppose que  $x + z = s(y)$ . On raisonne par cas (lemme 1.1) 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  $x + s(z) = s(x + z) = s(y)$ . ■

## 1.5 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.

### 1.5.1 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 1.9** *Soit  $k$  un entier naturel. Pour toute propriété  $P$  sur les entiers :*

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

$y \geq k, P[y] \Rightarrow P[s(y)]$  est une abréviation pour  $(y \geq k \text{ et } P[y]) \Rightarrow P[s(y)]$

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

- En 0 la propriété est soit  $P[k]$ , si  $k = 0$ , soit évidente car  $k$  est un successeur et  $0 \geq k$  est faux.
- 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  $s(y) \geq k$ . 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  $\forall x \in \mathbb{N} (x \leq k \Rightarrow P[x])$ . ■

### 1.5.2 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 1.10** *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  $x \leq s(z) \equiv x \leq z$  ou  $x = s(z)$ , 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 1.11 (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 (il est indispensable, pour obtenir cette propriété pour les entiers, de se servir du lemme 1.1, que l'on a obtenu par récurrence).

Si  $x = 0$ , comme  $\forall z < 0 P[0] \Rightarrow P[0]$ , 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 n'est pas 0, ni même 2, si on faisait une récurrence « forte » à partir du rang 2, mais n'importe quel nombre premier.

**Exercice 7 (définition par récurrence sur la suite des valeurs)** Le but de cet exercice est de généraliser le théorème de définition par récurrence 1.2 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 une fonction  $F : (\mathbb{N} \times A \times \mathbb{N}) \rightarrow E$  telle que  $F(x, a, p) = f(p, a)$  si  $p \leq x$ ,  $F(x, a, p) = 0$  sinon.

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

### 1.5.3 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 :

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

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. C'est une propriété particulière à  $\mathbb{N}$  parmi les ensembles de nombres usuels (et pour l'ordre usuel!).

**Proposition 1.12** *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 1.11 que  $(\mathbb{N}, \leq)$  est bien ordonné.

**Proposition 1.13** *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.

**Corollaire 1.14** *Il n'existe pas de suite infinie décroissante d'entiers naturels.*

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

On pourrait bien sûr utiliser la descente infinie pour une variante de la démonstration de la propriété que tout nombre entier strictement supérieur à 1 possède un diviseur premier (on raisonne par l'absurde, en supposant le contraire pour fabriquer une suite décroissante infinie).

## 1.6 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 de  $E$ , le plus petit élément de l'ensemble des majorants stricts de  $E$ . Un élément de  $E$  n'a pas forcément de successeur, mais si celui-ci existe, il est unique (un ensemble ordonné a au plus un plus petit élément).

**Lemme 1.15** *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  $x = y$ . ■

**Proposition 1.16** *Soit  $(\mathbf{N}, \leq)$  un ensemble ordonné, tel que :*

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

$$\forall x \in \mathbf{N} (x = 0 \text{ ou } \exists y \in \mathbf{N} x = s(y)) .$$

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

**Démonstration.**

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

## 1.7 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).

Cependant, dans tout ce chapitre, on a utilisé les notions intuitives d'ensemble d'entiers et de propriété sur les entiers, sans les avoir définies précisément. On n'a donc pas complètement axiomatisé l'arithmétique. De plus la construction des réels utilise de façon nécessaire la notion d'ensemble (une suite de rationnels peut être définie par son graphe qui est un ensemble). Ce chapitre peut se réinterpréter et se compléter dans le cadre de l'axiomatisation de la théorie des ensembles, qui est l'objet du chapitre suivant.

# Index

antisymétrie, 5	ordre strict, 6
antisymétrie stricte, 6	ordre total, 5
Axiomes de Peano, 1	
	plus petit élément, 9
bien ordonné, 9	
bon ordre, 9	
définition par récurrence, 3	récurrence, 1
définition par récurrence avec paramètres, 3	récurrence « forte », 8
définition par récurrence avec substitution de paramètre, 5	récurrence à partir d'un certain rang, 8
définition par récurrence dépendant de l'argument, 4	récurrence bien fondée, 8
définition par récurrence sur la suite des valeurs, 9	réflexivité, 5
descente infinie, 10	raisonnement par cas sur les entiers, 2
	relation d'ordre, 5
ensemble ordonné, 5	
irréflexivité, 6	successeur (entiers), 1
	successeur (ordre), 11
	transitivité, 5, 6
	trichotomie, 6

## Table des matières

<b>1</b>	<b>Axiomatisation de l'arithmétique</b>	<b>1</b>
1.1	Les axiomes de Peano . . . . .	1
1.2	Définition par récurrence . . . . .	3
1.3	Quelques propriétés de l'addition, de la multiplication et de l'exponentielle . . .	5
1.4	Ordre . . . . .	5
1.4.1	Les axiomes d'ordre . . . . .	5
1.4.2	L'ordre sur les entiers . . . . .	6
1.4.3	Addition et ordre . . . . .	7
1.5	Propriétés de récurrence et de bon ordre . . . . .	8
1.5.1	Récurrence à partir d'un certain rang . . . . .	8
1.5.2	Récurrence « forte » . . . . .	8
1.5.3	Bon ordre . . . . .	9
1.6	Une axiomatisation des entiers par l'ordre . . . . .	11
1.7	Conclusion . . . . .	11