

# NOMBRES

nombres-MEEF.tex

28/09/2026

# Sommaire

|          |                                             |          |
|----------|---------------------------------------------|----------|
| <b>I</b> | <b>Entiers naturels.</b>                    | <b>4</b> |
| 1        | L'ensemble des entiers naturels. . . . .    | 5        |
| 2        | Opérations dans $\mathbb{N}$ . . . . .      | 9        |
| 3        | Ordre dans $\mathbb{N}$ . . . . .           | 13       |
| 4        | Ensembles finis, ensembles infinis. . . . . | 16       |

# Introduction.

**Partie I**

**Entiers naturels.**

Dans ce chapitre, on aborde l'ensemble des entiers naturels dont l'importance est évidemment fondamentale.

Bien sûr, cet ensemble est bien connu et l'intuition qu'on en a est largement suffisante pour travailler avec. Cependant, si l'on veut construire un édifice mathématique parfaitement cohérent, on ne peut pas se contenter de l'intuition et il faut alors poser la question de la *construction de l'ensemble des entiers naturels*. Les mathématiciens se sont posé cette question et y ont répondu en montrant qu'on pouvait construire de façon rigoureuse un ensemble dont les propriétés sont précisément celles que l'on attend de  $\mathbb{N}$  si l'on se fie à l'intuition qu'on en a.

Malheureusement, cette construction ne peut être comprise que si l'on maîtrise parfaitement la théorie des ensembles dont on a déjà dit qu'elle est d'un grand degré de difficulté. La construction de  $\mathbb{N}$  dépasse donc largement les objectifs d'un cours de base.

Pour cette raison, on va se contenter d'un objectif plus modeste mais qui suffit à mettre en évidence la démarche usuelle de la construction d'une théorie. On va montrer que l'on peut réduire toutes les propriétés de  $\mathbb{N}$  à trois d'entre-elles, dites "axiomes de Peano". Ainsi, on va admettre l'existence d'un ensemble vérifiant ces trois axiomes. (C'est la démonstration de l'existence d'un tel ensemble qui est délicate et repose sur la théorie des ensembles.) Puis, on montrera que cet ensemble, dont on a admis l'existence, a toutes les vertues que l'on attend de l'ensemble intuitivement connu de tous comme l'ensemble des entiers naturels.

## 1 L'ensemble des entiers naturels.

On commence notre étude de  $\mathbb{N}$  par sa description ensembliste.

Il faut bien prendre garde à une imprécision dans le vocabulaire utilisé dans la suite. Les assertions (A1), (A2) et (A3) du Théorème 1.1 sont souvent appelés *Axiomes de Peano*. Cette appellation a l'avantage de souligner que *toutes* les propriétés de  $\mathbb{N}$  découlent de ces trois assertions. Cependant, ces axiomes sont en fait, bel et bien, des *propriétés* qui se démontrent sur la base des résultats d'un chapitre (antérieur) dit de *Théorie des ensembles*. L'énoncé qui suit est donc, au sens plein du terme, un *théorème*. Dans la suite, l'expression *présentation axiomatique* de  $\mathbb{N}$  devra donc être comprise comme *réduction des propriétés de  $\mathbb{N}$  aux trois d'entre elles, dont toutes les autres découlent*.

**Théorème 1.1 – Axiomes de Peano** – *Il existe un ensemble, noté  $\mathbb{N}$ , un élément  $0$  de  $\mathbb{N}$  et une application*

$$\begin{aligned} s &: \mathbb{N} \longrightarrow \mathbb{N} \\ n &\mapsto s(n) \end{aligned}$$

*satisfaisant les propriétés suivantes :*

(A1)  $0 \notin s(\mathbb{N})$  ;

(A2)  $s$  est injective ;

(A3) si  $A$  est un sous-ensemble de  $\mathbb{N}$  contenant  $0$  et contenant l'image par  $s$  de chacun de ses éléments, alors  $A = \mathbb{N}$ .

Les assertions (A1), (A2) et (A3) sont appelées axiomes de Peano. L'assertion (A3) est appelé l'axiome de récurrence.

*Démonstration* : La démonstration du présent théorème relève de la *Théorie des ensembles*, qui est un chapitre fondamental et assez délicat de l'édifice mathématique. Pour cette raison, on admet, ici, ce résultat. ■

**Remarque 1.2 – Axiomes de Peano, commentaires –**

1. L'application  $s$  est appelée *application successeur* ; l'image par  $s$  d'un élément est appelé le successeur de cet élément. On note 1 le successeur de 0 :  $1 = s(0)$ . Il découle de (A1) que  $0 \neq 1$ .
2. L'axiome (A3) est appelé *axiome de récurrence*. Il a une traduction immédiate qui sera énoncée dans le Théorème ??.

Il est utile de remarquer, dès à présent, que (sous-couvert de l'axiome (A3)) l'axiome (A1) est en fait équivalent à un axiome plus restrictif. C'est l'objet de l'énoncé suivant.

**Proposition 1.3 – Axiomes de Peano, compléments** – Soit  $(\mathbb{N}, 0, s)$  un triplet comme au Théorème 1.1. Alors, on a  $s(\mathbb{N}) = \mathbb{N} \setminus \{0\}$ .

*Démonstration* : Posons  $A = s(\mathbb{N}) \cup \{0\}$ .

On a,  $0 \in A$ . De plus,  $A \subseteq \mathbb{N}$ , et donc  $s(A) \subseteq s(\mathbb{N}) \subseteq s(\mathbb{N}) \cup \{0\} = A$ . L'axiome (A3) assure donc que  $A = \mathbb{N}$ . On a montré que  $s(\mathbb{N}) \cup \{0\} = \mathbb{N}$ . Il en découle que  $s(\mathbb{N}) \supseteq \mathbb{N} \setminus \{0\}$ .

Mais, d'après (A1),  $s(\mathbb{N}) \subseteq \mathbb{N} \setminus \{0\}$ . On conclut donc que  $s(\mathbb{N}) = \mathbb{N} \setminus \{0\}$ . ■

La Proposition 1.3 a une conséquence utile, et éclairante, que l'on détaille maintenant.

**Corollaire 1.4** – Soit  $(\mathbb{N}, 0, s)$  un triplet comme au Théorème 1.1.

1. Pour tout  $n \in \mathbb{N} \setminus \{0\}$ , il existe un élément  $m \in \mathbb{N}$ , et un seul, tel que  $n = s(m)$ . On note

$$p : \mathbb{N} \setminus \{0\} \longrightarrow \mathbb{N}$$

l'application ainsi définie.

2. On a  $s \circ p = \text{id}_{\mathbb{N} \setminus \{0\}}$  et  $p \circ s = \text{id}_{\mathbb{N}}$ . En particulier, l'application  $p$  est injective.

*Démonstration* : Soit  $n \in \mathbb{N} \setminus \{0\}$ . La Proposition 1.3 assure l'existence d'un élément  $m \in \mathbb{N}$  tel que  $n = s(m)$  et l'axiome (A2) garanti qu'un tel élément est unique. Cela démontre la première assertion. En outre, et par construction de  $p$ , on a  $s \circ p = \text{id}_{\mathbb{N} \setminus \{0\}}$  et  $p \circ s = \text{id}_{\mathbb{N}}$ . Et, il découle de l'égalité  $s \circ p = \text{id}_{\mathbb{N} \setminus \{0\}}$  que  $p$  est injective. La seconde assertion est démontrée. ■

Enfin, le troisième axiome de Peano a une variante très utile lorsque l'on souhaite travailler dans  $\mathbb{N} \setminus \{0\}$ . On l'énonce dès maintenant.

**Lemme 1.5** – Soit  $A$  un sous-ensemble de  $\mathbb{N} \setminus \{0\}$ . Si  $1 \in A$  et  $s(A) \subseteq A$ , alors  $A = \mathbb{N} \setminus \{0\}$ .

*Démonstration* : Soit  $B = A \cup \{0\}$ . On a que  $0 \in B$  et  $s(B) \subseteq A \subseteq B$ . Le troisième axiome de Peano assure donc que  $B = \mathbb{N}$  et, par conséquent,  $A = B \setminus \{0\} = \mathbb{N} \setminus \{0\}$ . ■

Dans toute la suite, on fixe un triplet  $(\mathbb{N}, 0, s)$  avec lequel on travaille. A ce stade, il y a un arbitraire dans ce *choix*, au sens où rien n'exclut la possibilité qu'il existe beaucoup de tels triplets, et que ceux-ci puissent être très différents. En fait, il n'en est rien, comme le souligne la Remarque 1.7. La démonstration de ce fait nécessite cependant un peu de travail préparatoire.

A ce stade de l'étude de l'ensemble des entiers naturels, nous ne disposons que des trois axiomes de Peano. Il est donc clair que toutes les propriétés de  $\mathbb{N}$  que nous serons en mesure de

démontrer seront tributaires des ces trois axiomes. Il en sera ainsi des opérations dans  $\mathbb{N}$ , addition et multiplication, de la relation d'ordre, puis, des propriétés arithmétiques.

Le Théorème 1.1 est, somme toute, très intuitif. Il s'avère que l'on peut en déduire le Théorème 1.6 ci-dessous. Cela peut paraître un peu surprenant, dans la mesure où ce dernier est moins intuitif. Il n'en reste pas moins que le Théorème 1.6 est un outil indispensable pour être en position d'utiliser efficacement les axiomes de Peano dans la construction des diverses structures essentielles dont l'ensemble des entiers naturels peut être doté.

En un sens, bien qu'étant une conséquence du Théorème 1.1, le Théorème 1.6 complète celui-ci en révélant son réel potentiel. La clé de cette observation est la suivante : Le troisième axiome de Peano suffit à *vérifier* qu'une propriété indéxée par les entiers naturels est vraie, ce qui est déjà très utile. Le Théorème 1.6, quant à lui, permet de *construire* de nouveaux objets mathématiques. Pour cette raison, il sera d'une importance cruciale dans la suite.

### **Théorème 1.6 – Dedekind**

*Soient  $X$  un ensemble,  $a$  un élément de  $X$  et  $f : X \longrightarrow X$  une application de  $X$  vers  $X$ . Il existe une unique application  $u : \mathbb{N} \longrightarrow X$  de  $\mathbb{N}$  vers  $X$  satisfaisant les propriétés suivantes :*

1.  $u(0) = a$  ;
2. pour tout  $n \in \mathbb{N}$ ,  $u(s(n)) = f(u(n))$ .

*Démonstration :* On commence par montrer l'existence de  $u$ .

Par définition, il s'agit donc de construire un graphe  $G$  de  $\mathbb{N} \times X$ , dont  $u : \mathbb{N} \longrightarrow X$  sera l'application associée, c'est-à-dire que  $u = (\mathbb{N}, X, G)$ , et tel que  $u$  satisfasse les conditions 1 et 2 de l'énoncé. Ainsi,  $G$  devra vérifier que  $(0, a) \in G$  (cf. condition 1 de l'énoncé) et que, pour tous  $(n, x) \in \mathbb{N} \times X$ , si  $(n, x) \in G$ , alors  $(s(n), f(x)) \in G$  (cf. condition 2 de l'énoncé).

Ces considérations conduisent à s'intéresser aux sous-ensembles  $S$  de  $\mathbb{N} \times X$  vérifiant la propriété suivante :

$$(0, a) \in S \quad \text{et} \quad \forall (n, x) \in \mathbb{N} \times X, (n, x) \in S \implies (s(n), f(x)) \in S. \quad (1)$$

Bien-sûr, un sous-ensemble de  $\mathbb{N} \times X$  vérifiant (1) n'est pas nécessairement un graphe. Par exemple,  $\mathbb{N} \times X$  lui-même vérifie (1) et n'est pas un graphe (sauf si  $X$  est un singleton).

On note  $G$  le sous-ensemble de  $\mathbb{N} \times X$  défini comme intersection de tous les sous-ensembles de  $\mathbb{N} \times X$  vérifiant la propriété (1). Pour commencer, on observe facilement que  $G$  lui-même vérifie la propriété (1). En outre, et par définition,  $G$  est inclus dans tout sous-ensemble vérifiant la propriété (1) (en particulier,  $G$  ne contient strictement aucun sous-ensemble de  $\mathbb{N} \times X$  satisfaisant (1)). En somme, l'ensemble de tous les sous-ensemble de  $\mathbb{N} \times X$  vérifiant la propriété (1) admet  $G$  comme plus petit élément et  $\mathbb{N} \times X$  comme plus grand élément. Ce fait est crucial car il assure que  $G$  est un graphe.

Montrons donc que  $G$  est un graphe dans  $\mathbb{N} \times X$ . Pour cela, on considère l'ensemble

$$A = \{n \in \mathbb{N} ; \exists ! x \in X \mid (n, x) \in G\}.$$

Par définition, montrer que  $G$  est un graphe revient à montrer que  $A = \mathbb{N}$ . C'est ce que l'on fait maintenant, à l'aide du Théorème 1.1.

Montrons que  $0 \in A$ . Comme  $G$  vérifie (1),  $(0, a) \in G$ . Supposons, en outre, qu'il existe  $b \in X$ , avec  $b \neq a$ , tel que  $(0, b) \in G$ . Il est alors facile de voir, en utilisant l'axiome (A1), que  $G \setminus \{(0, b)\}$  vérifie (1) et, bien-sûr, est strictement contenu dans  $G$ . Ceci est une contradiction. Ainsi,  $0 \in A$ .

Soit à présent  $n \in \mathbb{N}$ . Supposons que  $n \in A$ . Par hypothèse, il existe un unique  $x \in X$  tel que  $(n, x) \in G$ . Comme  $G$  vérifie (1),  $(s(n), f(x)) \in G$ . Supposons maintenant qu'il existe  $y \in X$ ,  $y \neq f(x)$ , tel que  $(s(n), y) \in G$ .

Nous allons montrer que, sous couvert de l'existence d'un tel  $y$ ,  $G \setminus \{(s(n), y)\}$  vérifie (1).

Premièrement, comme  $G$  vérifie (1), il contient  $(0, a)$  et, d'après l'axiome (A1),  $0 \neq s(n)$  et donc  $(0, a) \neq (s(n), y)$ . Par suite,  $(0, a) \in G \setminus \{(s(n), y)\}$ .

Deuxièmement, considérons  $(m, z) \in G \setminus \{(s(n), y)\}$  et montrons que  $(s(m), f(z)) \in G \setminus \{(s(n), y)\}$ . Comme  $(m, z) \in G$ ,  $(s(m), f(z)) \in G$ . Il suffit donc de montrer que  $(s(m), f(z)) \neq (s(n), y)$ . Si l'on avait  $(s(m), f(z)) = (s(n), y)$ , il s'ensuivrait  $f(z) = y \neq f(x)$  et  $s(m) = s(n)$  et donc  $m = n$  d'après l'axiome (A2). Mais, comme  $(m, z) \in G$ , on aurait  $(n, z) \in G$  et,  $n \in A$  imposerait  $z = x$ , et donc  $f(z) = f(x)$ , contredisant ce qui précède. On conclut donc que  $(s(m), f(z)) \neq (s(n), y)$  et donc que  $(s(m), f(z)) \in G \setminus \{(s(n), y)\}$ . Ce qui établit que  $G \setminus \{(s(n), y)\}$  vérifie (1). Or ceci est absurde par minimalité de  $G$ , comme on l'a vu ci-dessus.

Ainsi, l'hypothèse de l'existence d'un tel  $y$  conduit à une contradiction et, donc, est fausse. On a donc prouvé que l'unique  $y \in X$  tel que  $(s(n), y) \in G$  est  $f(x)$ . Autrement dit,  $s(n) \in A$ .

Il reste à appliquer le Théorème 1.1 pour conclure que  $A = \mathbb{N}$ . Comme indiqué ci-dessus, cela démontre que  $G$  est un graphe de  $\mathbb{N} \times X$ . Posant alors  $u = (\mathbb{N}, X, G)$ , on a bien  $u : \mathbb{N} \rightarrow X$  telle que  $u(0) = a$  et, pour tout  $n \in \mathbb{N}$ ,  $u(s(n)) = f(u(n))$ .

Il reste à montrer l'unicité de  $u$ . Pour cela, supposons qu'il existe une application  $v : \mathbb{N} \rightarrow X$  telle que  $v(0) = a$  et, pour tout  $n \in \mathbb{N}$ ,  $v(s(n)) = f(v(n))$ . Il est facile de montrer, à l'aide d'une récurrence, que pour tout  $n \in \mathbb{N}$ ,  $u(n) = v(n)$ . Les détails sont laissés au lecteur. ■

Il est bien sûr légitime de se demander s'il peut exister plusieurs ensembles, très différents les uns des autres, satisfaisant les axiomes de Peano. Si tel était le cas, cela signifierait que ces trois axiomes, à eux seuls, ne suffisent pas à décrire l'ensemble des entiers naturels et, par conséquent, il faudrait ajouter d'autres axiomes pour bien distinguer l'ensemble qu'on cherche à construire.

En fait, il s'avère que ces trois axiomes suffisent bien à caractériser  $\mathbb{N}$  au sens suivant. Si l'on considère un triplet  $(E, e, \sigma)$  où  $E$  est un ensemble,  $e$  un élément de  $E$  et  $\sigma : E \rightarrow E$ , et si l'on suppose que ce triplet vérifie les axiomes de Peano (convenablement retranscrits pour ce triplet), alors il existe une application bijective  $\alpha : \mathbb{N} \rightarrow E$  telle que  $\alpha(0) = e$  et telle que  $\alpha \circ s = \sigma \circ \alpha$ . Cela signifie que  $E$  muni de son élément  $e$  et de son application  $\sigma$  se comporte exactement comme  $\mathbb{N}$  muni de son élément 0 et de son application  $s$ .

**Théorème 1.7 – Unicité de  $\mathbb{N}$**  – Soit  $(E, e, \sigma)$  où  $E$  est un ensemble,  $e$  un élément de  $E$  et  $\sigma : E \rightarrow E$ . On suppose que  $e \notin \sigma(E)$ , que  $\sigma$  est injective et que, pour tout sous-ensemble  $F$  de  $E$ , si  $e \in F$  et  $\sigma(F) \subseteq F$  alors  $F = E$ . Alors, il existe une application bijective  $\alpha : \mathbb{N} \rightarrow E$  telle que  $\alpha(0) = e$  et telle que  $\alpha \circ s = \sigma \circ \alpha$ .

*Démonstration* : Les détails de la démonstration sont laissées en exercice. On pourra suivre le chemin suivant.

En premier lieu, le théorème 1.6 permet de construire une application  $\alpha$  comme dans l'énoncé. En second lieu, on remarque que, le Théorème 1.6 ne reposant que sur les axiomes de Peano, il en existe une version pour le triplet  $(E, e, \sigma)$ . Cela permet de construire une application  $\beta : E \rightarrow E$ , analogue pour  $E$  de  $\alpha$  et réciproque de celle-ci.

## 2 Opérations dans $\mathbb{N}$ .

Dans cette section, on va montrer comment, à partir de la présentation axiomatique de  $\mathbb{N}$ , on peut reconstruire les opérations élémentaires dont on peut munir cet ensemble : l'addition et la multiplication.

On commence par définir l'addition de deux éléments de  $\mathbb{N}$ . Fixons un élément  $p$  de  $\mathbb{N}$ . On va définir l'opération "ajouter  $p$ " à un élément quelconque de  $\mathbb{N}$ .

Pour cela, l'outil essentiel sera le Théorème de Dedekind.

**Lemme 2.1 – L'opération ajouter  $p$**  – Soit  $p$  dans  $\mathbb{N}$ . Il existe une unique application

$$\sigma_p : \mathbb{N} \longrightarrow \mathbb{N}$$

telle que  $\sigma_p(0) = p$  et  $\sigma_p \circ s = s \circ \sigma_p$ .

*Démonstration* : C'est immédiat en appliquant le Théorème 1.6 avec  $X = \mathbb{N}$ ,  $f = s$  et  $a = p$ . ■

**Remarque 2.2** – On commence par souligner quelques points importants.

1. Soit  $p \in \mathbb{N}$ . Le Théorème 1.6 permet de montrer l'existence de l'application  $\sigma_p$  ci-dessus. Mais, il permet aussi de la caractériser. En effet, il affirme qu'il existe une *unique* application  $u : \mathbb{N} \longrightarrow \mathbb{N}$  telle que  $u(0) = p$  et  $u \circ s = s \circ u$ . Autrement dit, il existe une application de  $\mathbb{N}$  dans  $\mathbb{N}$ , et une seule, qui commute avec  $s$  et envoie 0 sur  $p$ , et c'est  $\sigma_p$ .
2. Ce qui précède assure en particulier que  $\sigma_0 = \text{id}_{\mathbb{N}}$  et  $\sigma_1 = s$ .

Pour préparer l'étude de l'opération d'addition, que l'on définira par la suite, commençons par un lemme très utile.

**Lemme 2.3** –

1. Pour tout  $p \in \mathbb{N}$ ,  $\sigma_{s(p)} = s \circ \sigma_p$ .
2. Pour tous  $p, n \in \mathbb{N}$ ,  $\sigma_n \circ \sigma_p = \sigma_p \circ \sigma_n$ .

*Démonstration* : 1. Soit  $p \in \mathbb{N}$ . Alors,  $s \circ \sigma_p(0) = s(p)$ . De plus,  $s \circ (s \circ \sigma_p) = s \circ (\sigma_p \circ s) = (s \circ \sigma_p) \circ s$ . Il reste à appliquer la Remarque 2.2 pour conclure que  $s \circ \sigma_p = \sigma_{s(p)}$ .

2. Fixons  $p \in \mathbb{N}$ . On considère le sous-ensemble suivant de  $\mathbb{N}$  (attaché à  $p$ ) :

$$A = \{n \in \mathbb{N} \mid \sigma_p \circ \sigma_n = \sigma_n \circ \sigma_p\}.$$

Comme  $\sigma_0 = \text{id}_{\mathbb{N}}$ , on a  $0 \in A$ . Soit à présent  $n \in \mathbb{N}$ . Supposons que  $n \in A$ , c'est-à-dire que  $\sigma_p \circ \sigma_n = \sigma_n \circ \sigma_p$ . Alors, d'après le premier point du lemme, on a :

$$\sigma_p \circ \sigma_{s(n)} = \sigma_p \circ (s \circ \sigma_n) = (\sigma_p \circ s) \circ \sigma_n = (s \circ \sigma_p) \circ \sigma_n = s \circ (\sigma_p \circ \sigma_n) = s \circ (\sigma_n \circ \sigma_p) = \sigma_{s(n)} \circ \sigma_p.$$

Ainsi,  $s(n) \in A$ . D'après l'axiome de récurrence, on a donc montré le point 2. ■

**Notation 2.4 – Notation (binaire) additive**

Pour deux éléments  $p$  et  $n$  de  $\mathbb{N}$ , on pose :  $n + p = \sigma_p(n)$ .

**Proposition 2.5 – Addition dans  $\mathbb{N}$  – L'application**

$$\begin{aligned} + & : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \\ (n, p) & \mapsto n + p \end{aligned}$$

vérifie les propriétés suivantes :

1. pour tout  $p \in \mathbb{N}$ ,  $0 + p = p$  ( $0$  est neutre pour  $+$ ) ;
2. pour tous  $n, p \in \mathbb{N}$ ,  $n + p = p + n$  (commutativité de  $+$ ) ;
3. pour tous  $n, p, q \in \mathbb{N}$ ,  $(n + p) + q = n + (p + q)$  (associativité de  $+$ ).

*Démonstration* : 1. Cela fait partie de la définition de  $\sigma_p$ .

2. Soient  $n, p \in \mathbb{N}$ . On a, compte tenu du second point du lemme 2.3 :

$$n + p = \sigma_p(n) = \sigma_p \circ \sigma_n(0) = \sigma_n \circ \sigma_p(0) = \sigma_n(p) = p + n.$$

3. Soient  $n, p, q \in \mathbb{N}$ . Par définition de  $\sigma_p$ ,  $\sigma_q$  et  $\sigma_n$ , on a,  $(n + p) + q = \sigma_q(n + p) = \sigma_q \circ \sigma_p(n) = \sigma_q \circ \sigma_p \circ \sigma_n(0)$ . De même, et en utilisant le second point de la présente proposition, on a,  $n + (p + q) = (p + q) + n = \sigma_n \circ \sigma_q \circ \sigma_p(0)$ . La seconde assertion du Lemme 2.3 donne donc que  $(n + p) + q = n + (p + q)$ .

Ceci achève la démonstration. ■

**Remarque 2.6** – On note que l'identité  $\sigma_1 = s$  de la Remarque 2.2 se récrit : pour tout  $n \in \mathbb{N}$ ,  $s(n) = n + 1$ .

L'addition dans  $\mathbb{N}$  satisfait les propriétés remarquables et très utiles suivantes.

**Proposition 2.7 – Injectivité des applications  $\sigma_n$  ; simplifiabilité de l'addition –**

1. Pour tout  $n$  dans  $\mathbb{N}$ ,  $\sigma_n$  est injective.
2. Pour tous  $n, p, q \in \mathbb{N}$ , si  $n + p = n + q$ , alors  $p = q$ .
3. Pour tout  $n \in \mathbb{N}$ ,  $s(n) \neq n$ .

*Démonstration* : On laisse les détails (faciles) au lecteur.

1. Cela se déduit, via le Lemme 2.3, des deuxième et troisième axiomes de Peano.
2. C'est une conséquence immédiate du Point 1 et de la commutativité de l'addition.
3. Soit  $n \in \mathbb{N}$  tel que  $s(n) = n$ . Alors  $n + 1 = n$  (cf. Proposition 2.2) et donc  $1 = 0$ , d'après ce qui précède. C'est une contradiction (cf. Remarque 1.2). ■

**Proposition 2.8 – Images des applications  $\sigma_n$  –**

1. Pour tout  $n$  dans  $\mathbb{N} \setminus \{0\}$ ,  $0 \notin \sigma_n(\mathbb{N})$ .
2. Pour tous  $p, q \in \mathbb{N}$ , si  $p + q = 0$ , alors  $p = q = 0$ .

*Démonstration* : On laisse les détails (faciles) au lecteur.

1. Soit  $n$  dans  $\mathbb{N} \setminus \{0\}$ . La Proposition 1.3 assure qu'il existe  $m \in \mathbb{N}$  tel que  $n = s(m)$ . Avec le Lemme 2.3, on a alors  $\sigma_n = s \circ \sigma_m$ . Il reste à utiliser le premier axiome de Peano.
2. C'est une conséquence du Point 1. ■

Dans le langage systématique de la théorie des ensembles, un magma est un couple  $(E, *)$ , où  $E$  est un ensemble et  $*$  une application  $*$  :  $E \times E \longrightarrow E$ . S'il existe un élément  $e$  de  $E$  neutre pour  $*$ , on dit que  $(E, *)$  est un magma unifère, si  $*$  est associative, on dit que  $(E, *)$  est un magma associatif, si  $*$  est commutative, on dit que  $(E, *)$  est un magma commutatif. Enfin, si

pour tous  $a, b, c$  dans  $E$ ,  $a * b = a * c$  (resp.  $b * a = c * a$ ), on dit que  $(E, *)$  est simplifiable à gauche (resp. à droite) ; on dit en outre que  $(E, *)$  est simplifiable s'il est simplifiable à gauche et à droite. De plus, et par définition, un *monoïde* est un magma, unifié, associatif.

On a donc montré, ci-dessous, le résultat suivant.

**Corollaire 2.9** – *Le couple  $(\mathbb{N}, +)$  est un monoïde, commutatif, simplifiable.*

*Démonstration* : C'est le contenu des Propositions 2.5 et 2.7. ■

On passe maintenant à la multiplication de deux éléments de  $\mathbb{N}$ . Fixons un élément  $n$  de  $\mathbb{N}$ . On va définir l'opération "multiplier par  $n$ " un élément quelconque de  $\mathbb{N}$ .

Pour cela, on utilise non seulement le Théorème de Dedekind (comme pour l'addition), mais aussi l'addition elle-même.

**Lemme 2.10** – *L'opération **multiplier par  $n$**  – Soit  $n$  dans  $\mathbb{N}$ . Il existe une unique application*

$$\mu_n : \mathbb{N} \longrightarrow \mathbb{N}$$

*telle que  $\mu_n(0) = 0$  et  $\mu_n \circ s = \sigma_n \circ \mu_n$ .*

*Démonstration* : C'est immédiat en appliquant le Théorème 1.6 avec  $X = \mathbb{N}$ ,  $f = \sigma_n$  et  $a = 0$ . ■

**Remarque 2.11** – En raisonnant comme à la Remarque 2.2, on obtient facilement que  $\mu_0$  est l'application identiquement nulle de  $\mathbb{N}$  et  $\mu_1 = \text{id}_{\mathbb{N}}$ .

**Remarque 2.12** – Soit  $n \in \mathbb{N}$ . La présente observation, conséquence immédiate de la Définition de  $\mu_n$  (cf. Lemme 2.10) justifie, à posteriori, cette définition. Elle sera aussi utile dans la démonstration du Lemme 2.13.

1. Pour tout  $p \in \mathbb{N}$ ,  $\mu_n(p + 1) = \mu_n(p) + n$ .
2. En particulier,  $\mu_n(1) = n$ .

Le procédé de démonstration des propriétés de la multiplication de deux entiers (qui reste encore à définir) est un peu plus subtil que celui des propriétés de l'addition. Nous allons par exemple démontrer que la multiplication est commutative et associative. Mais nous allons aussi devoir nous préoccuper du comportement relatif de l'addition et de la multiplication et démontrer que la multiplication est distributive sur l'addition.

Un point à ce sujet peut surprendre. En effet, il s'avère que le chemin le plus simple consiste à démontrer d'abord la distributivité, puis d'en déduire les autres propriétés.

Concernant la distributivité de la multiplication sur l'addition, il faut bien prendre garde que celle-ci contient *deux* relations à démontrer, à savoir, la distributivité à gauche et la distributivité à droite. Bien-sûr, l'une n'implique pas l'autre puisque nous n'avons pas encore démontré la commutativité de la multiplication.

**Lemme 2.13** – **Distributivité à gauche** – *Soit  $n \in \mathbb{N}$ .*

*Pour tous  $p, q \in \mathbb{N}$ , on a  $\mu_n(p + q) = \mu_n(p) + \mu_n(q)$ .*

*Démonstration* : Soit  $p \in \mathbb{N}$ . On considère  $A = \{q \in \mathbb{N}, | \mu_n(p+q) = \mu_n(p) + \mu_n(q)\} \subseteq \mathbb{N}$ .

Par définition de  $\mu_n$ , il est immédiat que  $0 \in A$ . Soit à présent  $q \in A$ . Alors,  $\mu_n(p+(q+1)) = \mu_n((p+q)+1) = \mu_n(p+q) + n = (\mu_n(p) + \mu_n(q)) + n = \mu_n(p) + (\mu_n(q) + n) = \mu_n(p) + (\mu_n(q+1))$ . En effet, les première et quatrième égalités sont dues à l'associativité de l'addition, la deuxième et la cinquième à la Remarque 2.12 et la troisième à ce que  $q \in A$ . Donc,  $q+1 \in A$ .

Le troisième axiome de Peano assure donc que  $A = \mathbb{N}$ , ce qui achève la démonstration. ■

**Lemme 2.14 – Distributivité à droite** – Soient  $p, q \in \mathbb{N}$ .

Pour tout  $n \in \mathbb{N}$ , on a  $\mu_{p+q}(n) = \mu_p(n) + \mu_q(n)$ .

*Démonstration* : On fixe  $p, q \in \mathbb{N}$ . On considère  $A = \{n \in \mathbb{N}, | \mu_{p+q}(n) = \mu_p(n) + \mu_q(n)\} \subseteq \mathbb{N}$ .

Par définition de  $\mu_{p+q}$ ,  $\mu_p$  et  $\mu_q$ , il est immédiat que  $0 \in A$ . Soit à présent  $n \in A$ . On a  $\mu_{p+q}(n+1) = \mu_{p+q}(n) + (p+q) = (\mu_p(n) + \mu_q(n)) + (p+q) = (\mu_p(n) + p) + (\mu_q(n) + q) = \mu_p(n+1) + \mu_q(n+1)$ . En effet, la Remarque 2.12 assure la première et la quatrième égalité, le fait que  $n \in A$  garantit la deuxième et l'associativité et la commutativité de l'addition assurent la troisième. Donc,  $n+1 \in A$ .

Le troisième axiome de Peano assure donc que  $A = \mathbb{N}$ , ce qui achève la démonstration. ■

**Notation 2.15 – Notation (binaire) multiplicative**

Pour deux éléments  $n$  et  $p$  de  $\mathbb{N}$ , on pose :  $n \times p = \mu_n(p)$ .

**Proposition 2.16 – Multiplication dans  $\mathbb{N}$  – L'application**

$$\begin{aligned} \times & : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \\ (n, p) & \longmapsto n \times p \end{aligned}$$

vérifie les propriétés suivantes :

1. pour tout  $p \in \mathbb{N}$ ,  $0 \times p = 0 = p \times 0$  (0 est absorbant pour  $\times$ ) ;
2. pour tout  $p \in \mathbb{N}$ ,  $1 \times p = p = p \times 1$  (1 est neutre pour  $\times$ ) ;
3. pour tous  $n, p \in \mathbb{N}$ ,  $n \times p = p \times n$  (commutativité de  $\times$ ) ;
4. pour tous  $n, p, q \in \mathbb{N}$ ,  $(n \times p) \times q = n \times (p \times q)$  (associativité de  $\times$ ) ;
5. pour tous  $n, p, q \in \mathbb{N}$ ,  $n \times (p+q) = n \times p + n \times q$  et  $(p+q) \times n = p \times n + q \times n$  (distributivité de  $\times$  sur  $+$ ).

*Démonstration* : La première égalité de l'assertion 1 a été vue à la Remarque 2.11, la seconde tient à la définition de  $\mu_p$ .

La première égalité de l'assertion 2 a aussi été vue à la Remarque 2.11. Pour la seconde, il suffit d'appliquer à 0 l'identité  $\mu_p \circ s = \sigma_p \circ \mu_p$ , qui vaut par définition de  $\mu_p$ .

On démontre à présent l'assertion 3. Soit  $n \in \mathbb{N}$ . On pose  $A = \{p \in \mathbb{N} | n \times p = p \times n\}$ . Par définition de  $\mu_n$ , et puisque  $\mu_0$  est l'application identiquement nulle,  $0 \in A$ . Soit maintenant  $p \in A$ . On a  $n \times (p+1) = n \times p + n \times 1 = n \times p + n = p \times n + n = p \times n + 1 \times n = (p+1) \times n$ . En effet, le Lemme 2.13 donne la première égalité, le Lemme 2.14 donne la cinquième, le Point 2 ci-dessus donne la deuxième et la quatrième et la troisième tient à ce que  $p \in A$ . Ainsi, on a  $p+1 \in A$ . Avec l'axiome (A3), on a donc que  $A = \mathbb{N}$ . Le Point 3 est démontré.

Le Point 4 peut être démontré par récurrence sur  $n$  (à  $p$  et  $q$  fixés) en raisonnant comme pour le Point 3. Les détails sont laissés au lecteur.

Le Point 5 n'est qu'une reformulation des Lemmes 2.13 et 2.14. ■

**Proposition 2.17 – Intégrité de  $\mathbb{N}$**  – Soient  $p, q \in \mathbb{N}$ .

1. Si  $p \times q = 0$  et  $p \neq 0$ , alors  $q = 0$ .
2. Si  $p \times q = 0$ , alors  $p = 0$  ou  $q = 0$ .

*Démonstration* : 1. D'après la Proposition 1.3, il existe  $p' \in \mathbb{N}$  tel que  $p = s(p') = p' + 1$ . On a donc, par distributivité de la multiplication,  $0 = p \times q = (p' + 1) \times q = p' \times q + q$ . Il reste à appliquer la Proposition 2.8 pour conclure que  $q = 0$ .

2. Compte tenu de la commutativité de la multiplication, la seconde assertion se déduit de la première. ■

**Proposition 2.18 – Injectivité des applications  $\mu_n$  ; simplifiabilité de la multiplication**

1. Pour tout  $n$  dans  $\mathbb{N} \setminus \{0\}$  et tous  $p, q \in \mathbb{N}$ , si  $n \times p = n \times q$ , alors  $p = q$ .
2. Pour tout  $n$  dans  $\mathbb{N} \setminus \{0\}$ ,  $\mu_n$  est injective.

*Démonstration* : Il est clair que la seconde assertion est une réécriture de la première. Il reste donc à démontrer la première.

On fixe  $n \in \mathbb{N} \setminus \{0\}$  et on pose  $A = \{p \in \mathbb{N} \mid (\forall q \in \mathbb{N}, n \times p = n \times q \implies p = q)\}$ . La Proposition 2.17 assure que  $0 \in \mathbb{N}$ . Soit à présent  $p \in A$ . On suppose que, pour tout  $q$  dans  $\mathbb{N}$ ,  $n \times (p + 1) = n \times q$ . Comme  $n \neq 0$  et  $p + 1 \neq 0$  (cf. axiome (A1)), la Proposition 2.17 assure que  $n \times q \neq 0$  et donc, en particulier, que  $q \neq 0$ . La Proposition 1.3 assure donc qu'il existe  $q' \in \mathbb{N}$  tel que  $q = q' + 1$ . Mais alors,  $n \times (p + 1) = n \times (q' + 1)$ . Compte tenu de la distributivité de la multiplication et l'injectivité de  $\sigma_n$ , il s'ensuit que  $np = nq'$  et donc, puisque  $p \in A$ , que  $p = q'$ . Ce qui démontre que  $p + 1 = q$ . On a ainsi démontré que  $p + 1 \in A$ . Il reste à appliquer l'axiome (A3) pour en déduire que  $A = \mathbb{N}$ .

On a donc montré que, pour tout  $n \in \mathbb{N} \setminus \{0\}$ ,  $\{p \in \mathbb{N} \mid (\forall q \in \mathbb{N}, n \times p = n \times q \implies p = q)\} = \mathbb{N}$ , ce qui n'est qu'une formulation alternative de l'assertion 1 de l'énoncé. ■

### 3 Ordre dans $\mathbb{N}$ .

En prenant appui sur l'addition, on peut définir dans  $\mathbb{N}$  une relation d'ordre naturelle. Comme on s'y attend intuitivement, cette relation d'ordre entretiendra un lien particulièrement étroit avec l'application successeur.

**Définition 3.1** – Soient  $m, n \in \mathbb{N}$ .

1. On dira que  $m$  est inférieur ou égal à  $n$ , ou que  $n$  est supérieur ou égal à  $m$ , ce que l'on notera  $m \leq n$  ou  $n \geq m$ , si il existe  $p \in \mathbb{N}$  tel que  $n = m + p$ .
2. On dira que  $m$  est (strictement) inférieur à  $n$ , ou que  $n$  est (strictement) supérieur à  $m$ , ce que l'on notera  $m < n$  ou  $n > m$ , si  $m \leq n$  et  $m \neq n$ .
3. Au Point 1 ci-dessus on attache la relation binaire, notée  $\leq$ , définie comme le sous-ensemble

$$\{(m, n) \mid m \leq n\} \subseteq \mathbb{N} \times \mathbb{N}.$$

**Remarque 3.2** – Il découlent immédiatement de la définition que, pour tout  $n \in \mathbb{N}$ ,  $0 \leq n < s(n)$  (cf.  $0 \neq 1$  et la simplifiabilité de  $+$ ).

Le lemme suivant sera très utile.

**Lemme 3.3** – Soient  $m, n \in \mathbb{N}$ . Si  $m < n$ , alors  $m + 1 \leq n$ .

*Démonstration* : Par définition de  $<$ , il existe  $p \in \mathbb{N}$  tel que  $n = m + p$  et  $m \neq n$ . En particulier,  $p \neq 0$  et il existe donc  $q \in \mathbb{N}$  tel que  $p = q + 1$ . Par suite,  $n = m + (q + 1) = (m + 1) + q$ , et donc  $n \geq m + 1$ . ■

**Proposition 3.4** – La relation binaire  $\leq$  de la Définition 3.1 est une relation d'ordre. Autrement dit :

1. pour tout  $n \in \mathbb{N}$ ,  $n \leq n$  (réflexivité) ;
2. pour tous  $m, n \in \mathbb{N}$ , si  $(m \leq n \text{ et } n \leq m)$ , alors  $m = n$  (antisymétrie) ;
3. pour tous  $m, n, p \in \mathbb{N}$ , si  $(m \leq n \text{ et } n \leq p)$ , alors  $m \leq p$  (transitivité).

*Démonstration* : Exercice. ■

Deux éléments  $m, n$  de  $\mathbb{N}$  sont dits *comparables* si  $m \leq n$  ou  $n \leq m$ . La proposition suivante montre que deux éléments de  $\mathbb{N}$  sont toujours comparables.

**Proposition 3.5** – La relation d'ordre  $\leq$  est totale. C'est-à-dire que, pour tous  $m, n \in \mathbb{N}$ ,  $m \leq n$  ou  $n \leq m$ .

*Démonstration* : On note  $A$  l'ensemble des éléments de  $\mathbb{N}$  qui sont comparables avec tout élément de  $\mathbb{N}$ . Le premier point de la Remarque 3.2 assure que  $0 \in A$ . Soit maintenant  $n \in A$ . On veut montrer que  $s(n) \in A$ .

Il s'agit donc de montrer que, pour tout  $m \in \mathbb{N}$ ,  $m$  et  $s(n)$  sont comparables..

*1er cas* :  $m \leq n$ . Alors,  $m \leq n < n + 1 = s(n)$ . (Cf. Remarque 3.2.)

*2ème cas* :  $m \geq n$ . Il existe  $p \in \mathbb{N}$  tel que  $m = n + p$ .

*1er sous-cas* :  $p = 0$ . On a  $m = n$ , c'est un cas déjà traité.

*2ème sous-cas* :  $p \neq 0$ . La Proposition 1.3 assure qu'il existe  $q \in \mathbb{N}$  tel que  $p = s(q) = q + 1$ . On a donc  $m = n + (q + 1) = (n + 1) + q$ , ce qui assure que  $m \geq s(n)$ .

On conclut que  $s(n) \in A$ . Il reste à utiliser l'axiome (A3) pour conclure que  $A = \mathbb{N}$ , ce qui termine la démonstration. ■

A ce stade, nous disposons dans  $\mathbb{N}$  de deux opérations, l'addition et la multiplication, et d'une relation d'ordre. La question de la compatibilité entre cette dernière et les opérations se pose donc. C'est cette question que nous abordons maintenant.

**Proposition 3.6** – Soient  $p, q, n$  trois éléments de  $\mathbb{N}$ . On a les résultats suivants :

1.  $p \leq q \iff p + n \leq q + n$ ;
2. si  $n \neq 0$ ,  $p \leq q \iff p \times n \leq q \times n$ .

*Démonstration* : 1. Le sens direct est presque immédiat, les détails sont laissés au lecteur.

Supposons maintenant que  $p + n \leq q + n$ . On procède par l'absurde. Supposons que  $p \not\leq q$ . Alors, d'après la Proposition 3.5, on doit avoir  $p \geq q$ . Il s'ensuit, avec le sens direct, que  $p + n \geq q + n$ . Et, par anti-symétrie de la relation  $\leq$ , on aboutit à  $p + n = q + n$ , puis à  $p = q$  (cf. Proposition 2.7) et donc à  $p \leq q$ . Ceci contredit  $p \not\leq q$ .

2. Le sens direct est une conséquence facile de la distributivité, les détails sont laissés au lecteur. (On observe d'ailleurs que la restriction à  $n \neq 0$  est ici inutile, mais le cas  $n = 0$  est sans intérêt.) Pour la réciproque, on peut procéder comme dans le cas de l'addition (mais cette fois, la restriction à  $n \neq 0$  est indispensable). Les détails sont laissés au lecteur. ■

**Corollaire 3.7** – Les applications  $s$  et  $p$  sont strictement croissantes.

*Démonstration* : La croissance de  $s$  est contenue dans la première assertion de la Proposition 3.6 ; sa croissance stricte s'en déduit par injectivité. La croissance stricte de  $p$  se déduit de la croissance de  $s$  et de l'identité  $s \circ p = \text{id}_{\mathbb{N} \setminus \{0\}}$  (cf. Corollaire 1.4). ■

**Corollaire 3.8** – Pour tout  $n \in \mathbb{N} \setminus \{0\}$ ,  $p(n) < n$ .

*Démonstration* : Soit  $n \in \mathbb{N} \setminus \{0\}$ . Si l'on suppose que  $p(n) \geq n$ , il découle du Corollaire 3.7 que  $s \circ p(n) \geq s(n)$  et donc que  $n \geq s(n)$  d'après le Corollaire 1.4. Mais, ceci contredit la Remarque 3.2. Donc  $p(n) < n$ . ■

On rappelle les définitions suivantes, qui proviennent de la théorie des ensembles.

Soit  $E$  un sous-ensemble de  $\mathbb{N}$ . Un élément  $a$  de  $\mathbb{N}$  est un *minorant* de  $E$  s'il est inférieur ou égal à tout élément de  $E$ . Un élément  $a$  de  $\mathbb{N}$  est un *plus petit élément* de  $E$  si  $a$  est dans  $E$  et est un minorant de  $E$ . Un élément  $a$  de  $\mathbb{N}$  est un *majorant* de  $E$  si il est supérieur ou égal à tout élément de  $E$ . Un élément  $a$  de  $\mathbb{N}$  est un *plus grand élément* de  $E$  si  $a$  est dans  $E$  et est un majorant de  $E$ . L'ensemble des minorants de  $E$  sera noté  $\text{Min}(E)$  ; l'ensemble des majorants de  $E$  sera noté  $\text{Maj}(E)$ . Un élément de  $\mathbb{N}$  est donc un plus petit élément (resp. plus grand élément) de  $E$  si, et seulement si, il est dans  $E \cap \text{Min}(E)$  (resp. dans  $E \cap \text{Maj}(E)$ ).

**Exercice 3.9** –

1. Toute partie de  $E$  admet au plus un plus petit (resp. plus grand) élément.
2. L'ensemble  $\mathbb{N}$  admet un plus petit élément mais n'admet pas de plus grand élément.

La Proposition 3.10 règle le problème de l'existence d'un plus petit ou plus grand élément d'un ensemble non vide. (Il est clair, par définition, que  $\emptyset$  n'admet ni l'un, ni l'autre.)

**Proposition 3.10** – Soit  $E$  un sous-ensemble non-vide de  $\mathbb{N}$ . Alors :

1.  $E$  admet un plus petit élément ;
2.  $E$  admet un plus grand élément si, et seulement si, il est majoré.

*Démonstration* : Soit  $E$  un sous-ensemble non-vide de  $\mathbb{N}$ .

1. On raisonne par l'absurde. Supposons donc que  $E$  n'a pas de plus petit élément, autrement dit que  $E \cap \text{Min}(E) = \emptyset$ .

Il est clair que  $0 \in \text{Min}(E)$ . Soit  $m \in \text{Min}(E)$ . Soit  $n \in E$ . On a  $m \leq n$ . Donc, il existe  $p \in \mathbb{N}$  tel que  $n = m + p$ . En outre, on doit avoir  $p \neq 0$ , sans quoi on aurait  $m = n \in E \cap \text{Min}(E) = \emptyset$ . Mais alors, il existe  $q \in \mathbb{N}$  tel que  $p = q + 1$ . Ce dont on déduit que  $n = (m + 1) + q$ , de sorte que  $m + 1 \leq n$ . Et, comme ceci vaut pour tout  $n \in E$ , on obtient que  $m + 1 \in \text{Min}(E)$ . L'axiome (A3) s'applique donc à  $\text{Min}(E)$  et démontre que  $\text{Min}(E) = \mathbb{N}$ . On aboutit à une contradiction avec  $E \cap \text{Min}(E) = \emptyset$ .

2. Evidemment, si  $E$  admet un plus grand élément, il est majoré. Démontrons la réciproque.

On suppose donc que  $E$  admet un majorant. En d'autres termes,  $\text{Maj}(E)$  est non-vide et on peut donc lui appliquer la première assertion : soit  $m$  un plus petit élément de  $\text{Maj}(E)$ . On va démontrer que  $m$  est un plus grand élément de  $E$ . Par définition,  $m$  est un majorant de  $E$  et il suffit donc de démontrer que  $m \in E$ . Supposons, au contraire, que  $m \notin E$ . On observe, pour commencer, que cela exclu que  $m = 0$  (sans quoi on aurait  $E = \emptyset$ ). Il existe donc  $r \in \mathbb{N}$  tel que  $m = r + 1$ . Soit  $p \in E$ . Par définition de  $m$ ,  $p \leq m$  et, par hypothèse,  $p \neq m$ . C'est-à-dire que  $p < m$ . Par le Lemme 3.3, on a donc  $p + 1 \leq m = r + 1$ . Il existe donc  $q \in \mathbb{N}$  tel que  $r + 1 = (p + 1) + q$  et donc tel que  $r = p + q$ , ce qui entraîne que  $p \leq r$ . On a donc démontré que  $r$  est un majorant de  $E$ . Or,  $m = r + 1$  et donc  $r < m$ . Ceci contredit le fait que  $m$  est un plus petit élément de  $\text{Maj}(E)$ . Ceci termine la démonstration. ■

On rappelle le point suivant de théorie des ensembles : si  $E$  est un ensemble, on note  $\mathfrak{P}(E)$  l'ensemble de tous les sous-ensembles de  $E$ .

De la Proposition 3.10 et de l'Exercice 3.9 découle la définition suivante.

**Définition 3.11** – On note  $\underline{\min} : \mathfrak{P}(\mathbb{N}) \setminus \{\emptyset\} \longrightarrow \mathbb{N}$  l'application qui à tout sous-ensemble non vide  $A$  de  $\mathbb{N}$  associe son plus petit élément.

## 4 Ensembles finis, ensembles infinis.

On rappelle que deux ensembles sont dits *équipotents* s'il existe une bijection de l'un vers l'autre.

La relation d'ordre sur  $\mathbb{N}$  permet d'introduire la notion d'*intervalle* de  $\mathbb{N}$  qui, elle-même, mène à celle d'*ensemble fini*, puis de *cardinal d'un ensemble fini*.

**Définition 4.1 – Intervalle de  $\mathbb{N}$**  – Soient  $m, n \in \mathbb{N}$  tels que  $m \leq n$ . On appelle intervalle associé à  $(m, n)$  le sous-ensemble de  $\mathbb{N}$  défini par

$$[m, n] = \{a \in \mathbb{N} \mid m \leq a \leq n\}.$$

**Définition 4.2 – Ensemble fini, ensemble infini** – Soit  $E$  un ensemble.

1. On dit que  $E$  est fini s'il est vide ou s'il existe  $n \in \mathbb{N} \setminus \{0\}$  tel que  $[1, n]$  et  $E$  soient équipotents.
2. On dit que  $E$  est infini si  $E$  n'est pas fini.

Ainsi, les ensembles finis de référence sont  $\emptyset$  et les  $[1, n]$  où  $n$  est un élément non nul de  $\mathbb{N}$ .

On va maintenant préciser le lien entre un ensemble fini et un tel ensemble de référence pour pouvoir définir la notion de *cardinal* d'un ensemble. La clé pour cela est le Théorème 4.5.

Dans la plupart des résultats de cette section, la notion de *transposition* et celle de *section d'une surjection* joueront un rôle important. On en précise donc dès maintenant les définitions et les résultats utiles attachés.

**Remarque 4.3 – Transpositions** – Soit  $E$  un ensemble non vide, soient  $a, b \in E$ . Il est clair qu'il existe une application (et une seule) telle que

$$\begin{array}{ccc} E & \longrightarrow & E \\ x & \mapsto & x \quad \text{si } x \neq a \text{ et } x \neq b \\ a & \mapsto & b \\ b & \mapsto & a \end{array}.$$

(On observe que le cas  $a = b$  n'est pas exclu et que, dans ce cas, l'application ci-dessus est  $\text{id}_E$ .) Comme la composée de cette application avec elle-même est  $\text{id}_E$ , elle est inversible et est sa propre application réciproque.

Dans la suite, l'application ci-dessus sera appelée la transposition de  $a$  et  $b$  dans  $E$ .

On rappelle que, si  $E$  et  $F$  sont des ensembles et  $f : E \longrightarrow F$  une application, on appelle section de  $f$  toute application  $g : F \longrightarrow E$  telle que  $f \circ g = \text{id}_F$ . Il résulte de la définition que, si  $f$  admet une section, alors  $f$  est surjective et que toute section de  $f$  est injective.

Etant donnés  $m, n \in \mathbb{N} \setminus \{0\}$ , on associe maintenant une section explicite à toute surjection de  $[1, m]$  dans  $[1, n]$ .

**Lemme 4.4** – Soient  $m, n \in \mathbb{N} \setminus \{0\}$  et  $\pi : \llbracket 1, m \rrbracket \longrightarrow \llbracket 1, n \rrbracket$  une application surjective. Il existe une application comme suit :

$$\begin{array}{ccc} \iota & : & \llbracket 1, n \rrbracket \longleftarrow \llbracket 1, m \rrbracket \\ & i & \mapsto \min(\pi^{-1}(\{i\})) \end{array} .$$

De plus,  $\iota$  est une section de  $\pi$  et est (donc) injective.

*Démonstration* : Comme  $\pi$  est surjective, pour tout  $1 \leq i \leq n$ , on peut appliquer le premier point de la Proposition 3.10 à  $\pi^{-1}(\{i\})$ . Ceci assure l'existence de l'application  $\iota$ . Le fait que  $\pi \circ \iota = \text{id}_{\text{dcg}1, n}$  est immédiat (et entraîne l'injectivité de  $\iota$ ). ■

On peut maintenant passer à l'étude des applications entre intervalles  $\llbracket 1, n \rrbracket$ ,  $n \in \mathbb{N} \setminus \{0\}$ .

**Théorème 4.5** – Soient  $m, n \in \mathbb{N} \setminus \{0\}$ .

1. Il existe une application injective de  $\llbracket 1, m \rrbracket$  vers  $\llbracket 1, n \rrbracket$  si et seulement si  $m \leq n$ .
2. Il existe une application surjective de  $\llbracket 1, m \rrbracket$  vers  $\llbracket 1, n \rrbracket$  si et seulement si  $m \geq n$ .
3. Il existe une application bijective de  $\llbracket 1, m \rrbracket$  vers  $\llbracket 1, n \rrbracket$  si et seulement si  $m = n$ .

*Démonstration* : 1. Pour commencer, on observe que si  $m = 1$ , pour tout entier  $n \in \mathbb{N} \setminus \{0\}$ , l'équivalence est immédiate. (Dans le corps de la démonstration à suivre, cela permettra de considérer  $p(m)$  (cf. Corollaire 1.4), sans crainte qu'il soit nul.)

On considère le sous-ensemble  $A$  de  $\mathbb{N} \setminus \{0\}$  des entiers naturels  $n$  non nuls tels que, pour tout entier  $m \in \mathbb{N} \setminus \{0, 1\}$ , l'existence d'une application injective de  $\llbracket 1, m \rrbracket$  vers  $\llbracket 1, n \rrbracket$  entraîne que  $m \leq n$  :

$$A = \{n \in \mathbb{N} \setminus \{0\} \mid \forall m \in \mathbb{N} \setminus \{0, 1\}, (\text{il existe une injection } \llbracket 1, m \rrbracket \longrightarrow \llbracket 1, n \rrbracket \implies m \leq n)\} .$$

Nous allons montrer que  $A = \mathbb{N} \setminus \{0\}$ .

Pour commencer, supposons qu'il existe une injection  $\iota : \llbracket 1, m \rrbracket \longrightarrow \llbracket 1, 1 \rrbracket$ . Comme  $\llbracket 1, 1 \rrbracket = \{1\}$  et comme  $\iota$  est injective, on doit avoir  $m = 1 = n$ . Ainsi, on a  $1 \in A$ .

Soit à présent  $n \in A$ . Considérons  $m \in \mathbb{N} \setminus \{0, 1\}$  et une injection  $\iota : \llbracket 1, m \rrbracket \longrightarrow \llbracket 1, n+1 \rrbracket$ . Considérons l'application de transposition de  $\iota(m)$  et  $n+1$  dans  $\llbracket 1, n+1 \rrbracket$  :

$$\begin{array}{ccc} \kappa & : & \llbracket 1, n+1 \rrbracket \longrightarrow \llbracket 1, n+1 \rrbracket \\ & r & \mapsto r \quad \text{si } r \neq \iota(m) \text{ et } r \neq n+1 \\ & \iota(m) & \mapsto n+1 \\ & n+1 & \mapsto \iota(m) \end{array} ,$$

(cf Remarque 4.3). L'application  $\kappa \circ \iota : \llbracket 1, m \rrbracket \longrightarrow \llbracket 1, n+1 \rrbracket$  est injective et envoie  $m$  sur  $n+1$ . De plus, comme  $m \neq 1$ , on a  $p(m) \neq 0$  et, d'après le Corollaire 3.8,  $p(m) \neq m$  et  $\llbracket 1, p(m) \rrbracket \subseteq \llbracket 1, m \rrbracket$ . Ainsi, par une restriction adéquate des ensembles de départ et d'arrivée,  $\kappa \circ \iota$  induit une injection  $\llbracket 1, p(m) \rrbracket \longrightarrow \llbracket 1, n \rrbracket$ .

Mais, d'une part, si  $p(m) = 1$ , on a  $p(m) \leq n$  et il est clair que  $p(m) \leq n$ . D'autre part, si  $p(m) \neq 1$ , et comme  $p(m) \neq 0$ , puisque  $m \neq 1$  et  $n \in A$ , on a  $p(m) \leq n$ . Dans tous les cas,  $p(m) \leq n$ , et en appliquant  $s$  il vient (cf. Corollaire 1.4) que  $m \leq n+1$ .

Ce qui précède démontre que  $n+1 \in A$ . Il reste à appliquer le Lemme 1.5 pour conclure que  $A = \mathbb{N} \setminus \{0\}$ . On a donc démontré que, s'il existe une application injective de  $\llbracket 1, m \rrbracket$  vers  $\llbracket 1, n \rrbracket$ , alors  $m \leq n$ . Réciproquement, si  $m \leq n$ , il est clair que l'application  $\llbracket 1, m \rrbracket \longrightarrow \llbracket 1, n \rrbracket$ ,  $a \mapsto a$ , est injective. La première assertion est donc établie.

2. Supposons qu'il existe une application surjective  $\pi : \llbracket 1, m \rrbracket \longrightarrow \llbracket 1, n \rrbracket$ . D'après le Lemma 4.4, on dispose d'une application injective

$$\begin{array}{ccc} \iota : \llbracket 1, n \rrbracket & \longleftrightarrow & \llbracket 1, m \rrbracket \\ i & \mapsto & \min(\pi^{-1}(\{i\})) \end{array} .$$

La première assertion du présent théorème assure donc que  $n \leq m$ . Réciproquement, si l'on suppose  $n \leq m$ , on a  $\llbracket 1, n \rrbracket \subseteq \llbracket 1, m \rrbracket$ , d'où l'existence d'une application

$$\begin{array}{ccc} \llbracket 1, m \rrbracket & \longrightarrow & \llbracket 1, n \rrbracket \\ r & \mapsto & r \quad \text{si } 1 \leq r \leq n, \\ r & \mapsto & 1 \quad \text{sinon} \end{array}$$

qui est clairement surjective. La deuxième assertion est donc établie.

3. La troisième assertion découle immédiatement des deux précédentes. ■

**Corollaire 4.6** – Soit  $E$  un ensemble fini et non vide. Il existe un élément  $n \in \mathbb{N} \setminus \{0\}$ , et un seul, tel que  $E$  et  $\llbracket 1, n \rrbracket$  soient équipotents.

*Démonstration* : L'existence d'un tel élément  $n$  est assurée par la définition d'ensemble fini. Supposons maintenant que  $m, n$  soient des éléments de  $\mathbb{N} \setminus \{0\}$  tels que, d'une part,  $E$  et  $\llbracket 1, m \rrbracket$  et d'autre part  $E$  et  $\llbracket 1, n \rrbracket$  soient équipotents. Alors,  $\llbracket 1, m \rrbracket$  et  $\llbracket 1, n \rrbracket$  sont équipotents. Le Théorème 4.5 assure alors que  $m = n$ . ■

**Définition 4.7** – Soit  $E$  un ensemble fini et non vide. L'unique élément  $n \in \mathbb{N} \setminus \{0\}$  tel que  $E$  et  $\llbracket 1, n \rrbracket$  soient équipotents (cf. Corollaire 4.6) est appelé le cardinal de  $E$  et est noté  $\text{card}(E)$ . En outre, on pose  $\text{card}(\emptyset) = 0$ .

La définition du *cardinal d'un ensemble fini* telle qu'adoptée ci-dessus peut paraître un peu éloignée de l'intuition qu'on en a. Intuition suivant laquelle la détermination du cardinal d'un ensemble passe par l'énumération de ses éléments, qui à son tour permet de les compter. En fait, il n'en est rien et c'est ce que clarifie la remarque suivante.

**Remarque 4.8 – Énumération et dénombrement** – Soit  $E$  un ensemble fini et non vide et soit  $n \in \mathbb{N} \setminus \{0\}$  son cardinal.

1. Par définition,  $\llbracket 1, n \rrbracket$  et  $E$  sont équipotents. Soit  $e : \llbracket 1, n \rrbracket \longrightarrow E$  une bijection. On a

$$E = \{e(i), 1 \leq i \leq n\} = \{e(1), \dots, e(n)\}.$$

Ainsi, l'application  $e$  détermine-t-elle une *énumération* des éléments de  $E$ , si l'on convient que l'élément  $e(i)$  de  $E$  est affecté (par  $e$ ) du numéro  $i$ ,  $1 \leq i \leq n$ .

2. Bien sûr, chaque bijection de  $\llbracket 1, n \rrbracket$  vers  $E$  détermine une telle énumération. Dans la suite, une telle application sera parfois appelée une *énumération de  $E$* .

3. Dans cette présentation formelle, le *nombre d'éléments de  $E$*  se retrouve dans le cardinal de  $E$  et précède toute énumération de  $E$ .

**Remarque 4.9** – Les résultats suivants sont immédiats.

1. Pour tout  $n \in \mathbb{N} \setminus \{0\}$ ,  $\text{card}(\llbracket 1, n \rrbracket) = n$ .
2. Tout entier naturel est le cardinal d'un ensemble fini.

On poursuit l'étude précédente des intervalles de  $\mathbb{N}$  de la forme  $\llbracket 1, n \rrbracket$ ,  $n \in \mathbb{N} \setminus \{0\}$ , par une série de résultats très utiles.

**Théorème 4.10** – Soit  $n \in \mathbb{N} \setminus \{0\}$ .

1. Pour tout sous-ensemble  $F$  de  $\llbracket 1, n \rrbracket$ ,  $F$  est fini et  $\text{card}(F) \leq n$ .
2. Pour tout sous-ensemble  $F$  de  $\llbracket 1, n \rrbracket$ ,  $\text{card}(F) = n$  si, et seulement si,  $F = \llbracket 1, n \rrbracket$ .

*Démonstration* : 1. On note  $A$  l'ensemble des entiers naturels non nuls tels que, pour tout sous-ensemble  $F$  de  $\llbracket 1, n \rrbracket$ ,  $F$  est fini et  $\text{card}(F) \leq n$ . Il est clair que  $1 \in A$ . Soit  $n \in A$ .

Considérons  $F \subseteq \llbracket 1, n+1 \rrbracket$ . Si  $F = \llbracket 1, n+1 \rrbracket$ ,  $F$  est fini, de cardinal  $n+1$  (et donc majoré par  $n+1$ ). Sinon, on a  $F \subset \llbracket 1, n+1 \rrbracket$  (inclusion stricte). Dans ce cas, il existe  $1 \leq a \leq n+1$  tel que  $a \notin F$ . Soit alors  $t$  la transposition de  $a$  et  $n+1$  dans  $\llbracket 1, n+1 \rrbracket$ . Comme  $t$  est une bijection, il est clair que  $n+1 = t(a) \notin t(F)$ . Par suite,  $t(F) \subseteq \llbracket 1, n \rrbracket$ . Mais, puisque  $n \in A$ , cela impose que  $t(F)$  est fini et de cardinal majoré par  $n$ . Comme  $F$  et  $t(F)$  sont équipotents,  $F$  est aussi fini et de cardinal majoré par  $n$  et donc par  $n+1$ . On a ainsi que  $n+1 \in A$ .

Il reste à utiliser le Lemme 1.5 pour conclure.

2. Il est clair que le résultat est vrai lorsque  $n = 1$ . On suppose donc maintenant que  $n \neq 1$ , ce qui assure que  $p(n) \neq 0$ .

Soit  $n \in \mathbb{N} \setminus \{0, 1\}$ . Soit  $F$  un sous-ensemble de  $\llbracket 1, n \rrbracket$ . Si  $F \subset \llbracket 1, n \rrbracket$  (inclusion stricte), en utilisant une transposition adéquate, (cf. démonstration du point 1) on démontre que  $F$  est équipotent à un sous-ensemble de  $\llbracket 1, p(n) \rrbracket$ , et donc, d'après le point 1,  $\text{card}(F) \leq p(n) < n$ . Par contrapposition, on vient de démontrer que, si  $\text{card}(F) \leq p(n) < n$ , alors  $F = \llbracket 1, n \rrbracket$ . Comme l'assertion réciproque est évidente, le Point 2 est établi. ■

**Théorème 4.11** – Soit  $n \in \mathbb{N} \setminus \{0\}$  et  $f : \llbracket 1, n \rrbracket \longrightarrow \llbracket 1, n \rrbracket$  une application. Les assertions suivantes sont équivalentes :

- (i)  $f$  est bijective ;
- (ii)  $f$  est injective ;
- (iii)  $f$  est surjective.

*Démonstration* : Il suffit de démontrer que (ii)  $\Leftrightarrow$  (iii).

1. On commence par démontrer que (ii)  $\Rightarrow$  (iii).

On considère l'ensemble  $A$  des éléments de  $\mathbb{N} \setminus \{0\}$  vérifiant la propriété suivante : toute application injective de  $\llbracket 1, n \rrbracket$  dans  $\llbracket 1, n \rrbracket$  est surjective.

Comme l'unique application de  $\llbracket 1, 1 \rrbracket$  dans  $\llbracket 1, 1 \rrbracket$  est  $\text{id}_{\llbracket 1, 1 \rrbracket}$ ,  $1 \in A$ . Considérons  $n \in A$ . Soit  $f : \llbracket 1, n+1 \rrbracket \longrightarrow \llbracket 1, n+1 \rrbracket$  une application injective. On note  $t : \llbracket 1, n+1 \rrbracket \longrightarrow \llbracket 1, n+1 \rrbracket$  la transposition de  $f(n+1)$  et  $n+1$  dans  $\llbracket 1, n+1 \rrbracket$  (cf. 4.3). Alors,  $t \circ f : \llbracket 1, n+1 \rrbracket \longrightarrow \llbracket 1, n+1 \rrbracket$  est une injection qui envoie  $n+1$  sur  $n+1$ . Elle induit donc une application injective

$$\begin{aligned} g & : \llbracket 1, n \rrbracket \longrightarrow \llbracket 1, n \rrbracket \\ r & \mapsto t \circ f(r) \end{aligned}$$

Comme  $n \in A$ , il s'ensuit que  $g$  est surjective. Cela entraîne que  $t \circ f$  est surjective, et donc que  $f$  l'est. On a donc démontré que  $n+1 \in A$ . Le Lemme 1.5 démontre donc que  $A = \mathbb{N} \setminus \{0\}$ .

Ce qui précède démontre que (ii)  $\Rightarrow$  (iii).

2. On démontre maintenant que (iii)  $\Rightarrow$  (ii).

Soit  $n \in \mathbb{N} \setminus \{0\}$  et  $\pi : \llbracket 1, n \rrbracket \longrightarrow \llbracket 1, n \rrbracket$  une surjection. D'après le Lemme 4.4, on dispose d'une injection  $\iota : \llbracket 1, n \rrbracket \longrightarrow \llbracket 1, n \rrbracket$ ,  $i \mapsto \underline{\min}(\pi^{-1}(\{i\}))$ . Et, comme on a montré que (ii)  $\Rightarrow$  (iii), on sait que  $\iota$  est surjective. Par conséquent,

$$\forall 1 \leq j \leq n, \exists 1 \leq i \leq n \mid j = \underline{\min}(\pi^{-1}(\{i\})).$$

Considérons  $1 \leq i \leq n$ . Posons  $a = \underline{\min}(\pi^{-1}(\{i\}))$  et soit  $b \in \underline{\min}(\pi^{-1}(\{i\}))$ . Alors,  $a \leq b$ . Mais, d'après ce qui précède, il existe  $1 \leq j \leq n$  tel que  $b = \underline{\min}(\pi^{-1}(\{j\}))$ . Ainsi,  $b \in \pi^{-1}(\{i\}) \cap \pi^{-1}(\{j\})$

et, par suite,  $i = \pi(b) = j$  et finalement  $a = b$ . On vient de démontrer que  $\pi^{-1}(\{i\})$  est un singleton. Comme ceci vaut pour tout  $1 \leq i \leq n$ ,  $\pi$  est injective. On a démontré que (iii)  $\Rightarrow$  (ii).

La démonstration est complète. ■

Les résultats précédents s'attachent à décliner les propriétés majeures des ensembles  $\llbracket 1, n \rrbracket$ , pour  $n \in \mathbb{N} \setminus \{0\}$ . Par la définition même d'ensemble fini, il va donc de soi que les résultats en question s'étendent à tous les ensembles finis. C'est cette extension que l'on décrit maintenant. On obtient ainsi des résultats analogues au Lemme 4.4 et aux Théorèmes 4.5, 4.10, 4.4, 4.5 et 4.11. Ils s'énoncent comme suit.

**Corollaire 4.12** – *Soient  $E$  et  $F$  des ensembles finis et non-vides. Toute application surjective de  $E$  dans  $F$  admet une section.*

*Démonstration* : Cela se déduit du Lemme 4.4. Les détails sont laissés en exercice. ■

**Corollaire 4.13** – *Soient  $E$  et  $F$  des ensembles finis et non-vides.*

1. *Il existe une application injective de  $E$  vers  $F$  si et seulement si  $\text{card}(E) \leq \text{card}(F)$ .*
2. *Il existe une application surjective de  $E$  vers  $F$  si et seulement si  $\text{card}(E) \geq \text{card}(F)$ .*
3. *Il existe une application bijective de  $E$  vers  $F$  si et seulement si  $\text{card}(E) = \text{card}(F)$ .*

*Démonstration* : Cela se déduit du Théorème 4.5. Les détails sont laissés en exercice. ■

**Corollaire 4.14** – *Soient  $E$  un ensemble fini.*

1. *Tout sous-ensemble de  $E$  est fini de cardinal au plus égal à celui de  $E$ .*
2. *Pour tout sous-ensemble  $F$  de  $E$ ,  $\text{card}(F) = \text{card}(E)$  si, et seulement si,  $F = E$ .*

*Démonstration* : Cela se déduit du Théorème 4.10. Les détails sont laissés en exercice. ■

**Corollaire 4.15** – *Soient  $E$  un ensemble fini et  $f : E \longrightarrow E$  une application. Les assertions suivantes sont équivalentes :*

- (i)  *$f$  est bijective ;*
- (ii)  *$f$  est injective ;*
- (iii)  *$f$  est surjective.*

*Démonstration* : Cela se déduit du Théorème 4.11. Les détails sont laissés en exercice. ■

**Remarque 4.16** – Le corollaire 4.15 est faux pour les ensembles infinis. Il permet d'ailleurs de démontrer qu'un ensemble est infini. Par exemple, l'application  $s : \mathbb{N} \longrightarrow \mathbb{N}$ ,  $n \mapsto n + 1$  est injective (axiome (A2)), mais pas surjective (axiome (A1)). On en déduit que  $\mathbb{N}$  est infini.

On poursuit cette section par les résultats décrivant le comportement du cardinal des ensembles finis au regard des opérations ensemblistes (union, intersection, produit cartésien).

Pour cela, le lemme suivant sera utile.

**Lemme 4.17** – *Soit  $k \in \mathbb{N} \setminus \{0\}$ . Alors, pour tout  $n \in \mathbb{N} \setminus \{0\}$   $\sigma_k(\llbracket 1, n \rrbracket) = \llbracket 1 + k, n + k \rrbracket$ .*

*Démonstration* : On pose  $A = \{n \in \mathbb{N} \setminus \{0\} \mid \sigma_k(\llbracket 1, n \rrbracket) = \llbracket 1 + k, n + k \rrbracket\}$ .

Il est immédiat que  $1 \in A$ . Soit  $n \in A$ . On a  $\llbracket 1, n + 1 \rrbracket = \llbracket 1, n \rrbracket \sqcup \{n + 1\}$  (union disjointe) et donc,

$$\sigma_k(\llbracket 1, n + 1 \rrbracket) = \sigma_k(\llbracket 1, n \rrbracket) \sqcup \sigma_k(\{n + 1\}) = \llbracket 1 + k, n + k \rrbracket \sqcup \{n + 1 + k\} = \llbracket 1 + k, n + 1 + k \rrbracket.$$

En effet, la première égalité se déduit de l'injectivité de  $\sigma_k$ , la seconde de ce que  $n \in A$  et la troisième est claire. On a démontré que  $n + 1 \in A$ .

Il reste à appliquer le Lemme 1.5 pour conclure. ■

**Proposition 4.18** – Soit  $G$  un ensemble et  $E$  et  $F$  deux sous-ensembles finis de  $G$ .

1. Si  $E \cap F = \emptyset$ , alors  $E \cup F$  est fini et  $\text{card}(E \cup F) = \text{card}(E) + \text{card}(F)$ .
2. Si  $E \subseteq F$ , alors  $F \setminus E$  est fini, et  $\text{card}(F) = \text{card}(E) + \text{card}(F \setminus E)$ .
3. On a  $\text{card}(E \cup F) + \text{card}(E \cap F) = \text{card}(E) + \text{card}(F)$ .

*Démonstration* : Si  $E$  ou  $F$  est vide, le résultat est trivial. On suppose donc, dans ce qui suit, que ni  $E$  ni  $F$  n'est vide, et on note  $m$  et  $n$  leurs cardinaux respectifs,  $m, n \in \mathbb{N} \setminus \{0\}$ .

1. Soient  $e : \llbracket 1, m \rrbracket \longrightarrow E$  et  $f : \llbracket 1, n \rrbracket \longrightarrow F$  des énumérations de  $E$  et  $F$ , respectivement. D'après la Proposition 2.7 et le Lemme 4.17, on a une bijection  $t : \llbracket 1, n \rrbracket \longrightarrow \llbracket m+1, m+n \rrbracket$ ,  $i \mapsto m+i$  et donc d'une bijection  $f \circ t^{-1} : \llbracket m+1, m+n \rrbracket \longrightarrow F$ . Il s'ensuit que l'application

$$\begin{array}{lll} \llbracket 1, m+n \rrbracket & \longrightarrow & E \sqcup F \\ i & \mapsto & e(i) \quad \text{si } i \in \llbracket 1, m \rrbracket \\ i & \mapsto & f \circ t^{-1}(i) \quad \text{si } i \in \llbracket m+1, m+n \rrbracket \end{array}$$

est une bijection. On en déduit que  $E \cup F$  est fini, de cardinal  $m+n$ .

2. Puisque  $F$  est fini et  $F \setminus E \subseteq F$ ,  $F \setminus E$  est fini, d'après le Corollaire 4.14. Et, comme  $F = E \sqcup (F \setminus E)$ , le deuxième point résulte du premier.

3. On a  $E \cup F = (E \setminus (E \cap F)) \sqcup F$ . Donc, d'après les deux premiers points,  $E \cup F$  est fini, et  $\text{card}(E \cup F) = \text{card}((E \setminus (E \cap F)) \sqcup F) = \text{card}(E \setminus (E \cap F)) + \text{card}(F)$  et, par conséquent,  $\text{card}(E \cup F) + \text{card}(E \cap F) = \text{card}((E \setminus (E \cap F)) \sqcup F) + \text{card}(E \cap F) = \text{card}(E \setminus (E \cap F)) + \text{card}(E \cap F) + \text{card}(F)$ . Il s'ensuit, d'après le deuxième point que  $\text{card}(E \cup F) + \text{card}(E \cap F) = \text{card}(E) + \text{card}(F)$ . ■

**Proposition 4.19** – Soient  $E$  et  $F$  deux ensembles finis. Alors,  $E \times F$  est un ensemble fini, de cardinal  $\text{card}(E)\text{card}(F)$ .

*Démonstration* : Pour commencer, et pour tout  $e \in E$ , on fait les observations suivantes :

- (i)  $E \times F = \{(e, y), y \in F\} \sqcup \{(x, y), x \in E, y \in F, x \neq e\}$  ;
- (ii)  $\{e\} \times F$  et  $F$  sont équipotents.

Sur la base de ces observations, une récurrence sur le cardinal de  $E$  permet de démontrer le résultat. Les détails sont laissés en exercice. ■

La relation d'ordre de  $\mathbb{N}$  est l'ingrédient de départ pour définir les ensembles finis (via les intervalles). Au delà de ce fait, les résultats précédemment établis mènent au résultat suivant, qui caractérise les sous-ensembles finis de  $\mathbb{N}$ .

**Proposition 4.20 – Finitude et majoration** – Soit  $E$  un sous-ensemble non-vide de  $\mathbb{N}$ . Les assertions suivantes sont équivalentes :

- (i)  $E$  est fini ;
- (ii)  $E$  est majoré ;
- (iii)  $E$  a un plus grand élément.

*Démonstration* : On commence par montrer que (i) entraîne (ii).

On procède par récurrence sur le cardinal de  $E$ . On note  $A$  le sous-ensemble des éléments  $n$  de  $\mathbb{N}$  tels que tout sous-ensemble fini et non-vide de  $\mathbb{N}$  de cardinal  $n$  soit majoré. Il est clair que  $1 \in A$ . Soit  $n \in A$ . Considérons un sous-ensemble non-vide, fini et de cardinal  $n+1$  de  $\mathbb{N}$ . On note qu'alors  $n+1 \geq 2$ . Soit  $e \in E$ . On a que  $E = (E \setminus \{e\}) \sqcup \{e\}$ . D'après la Proposition 4.18,  $E \setminus \{e\}$  est de cardinal  $n$  et, par hypothèse de récurrence, il est donc majoré. Soit  $m \in \mathbb{N}$  un majorant de  $E \setminus \{e\}$ . Il est immédiat que le plus grand élément entre  $m$  et  $e$  est alors un majorant de  $E$ . Ainsi, on a démontré que  $n+1 \in A$ . Le Lemme 1.5 permet de conclure que  $A = \mathbb{N} \setminus \{0\}$ .

Ceci démontre le résultat souhaité.

Montrons maintenant que  $(ii)$  entraîne  $(i)$ . Soit  $E$  un sous-ensemble non-vide et majoré de  $\mathbb{N}$  et soit  $m$  un majorant de  $E$ . On a bien sûr  $E \subseteq \{0\} \sqcup \llbracket 1, m \rrbracket$ . D'après la Proposition 4.18  $\{0\} \sqcup \llbracket 1, m \rrbracket$  est fini et donc, d'après le Corollaire 4.14,  $E$  est fini.

A ce stade, on a démontré l'équivalence des deux premières assertions. L'équivalence de celles-ci avec la troisième a déjà été établie : c'est le contenu de la Proposition 3.10. ■