Les entiers naturels

(version provisoire du 14 juin 2008)

Jean-Marie Lion
Université de Rennes 1

On donne une présentation un peu théorique des entiers naturels. En particulier, on part d'axiomes définissant $\mathbf{N}$, on construit des opérations $+$ et $\times$. Les preuves proposées sont excessivement détaillées.

I. Les entiers naturels

Dans cette partie on introduit un nouvel axiome qui affirme l'existence des entiers naturels. Dans la dernière partie du texte on montrera que cet axiome est une conséquence des axiomes de la théorie des ensembles.

I.1. axiome Il existe un ensemble bien ordonné noté $(\mathbf{N}, \leq)$, qui ne possède pas de majorant mais qui est tel que chacun de ses sous-ensembles non vides, s'il est majoré, admet un plus grand élément. Les éléments de $\mathbf{N}$ s'appellent les *entiers naturels.*

I.2. premières propriétés

Soit $n, m \in \mathbf{N}$. On dit que n est *inférieur ou égal* à m et que m est *supérieur ou égal* à n si $n \leq m$. Si de plus $n \neq m$ on dit que n est *strictement inférieur* à m et que m est *strictement supérieur* à n et on note $n < m$. On a toujours l'alternative suivante $n \leq m$ ou $m < n$.

On note 0 et on appelle *zéro* le plus petit élément de $\mathbf{N}$. Tout entier naturel différent de zéro est dit *non nul.* Puisque $\mathbf{N}$ n'est pas majoré il n'est pas réduit au singleton $\{0\}$ et $\mathbf{N} \setminus \{0\}$ possède un plus petit élément noté 1 et appelé *un.*

Soit $n \in \mathbf{N}$ un entier naturel. Puisque $\mathbf{N}$ n'est pas majoré le sous-ensemble $\{m \in \mathbf{N} : n < m\}$ admet un plus petit élément qu'on note $n + 1$ et qui est appelé *successeur* de n. On a $n < n+1$. Le successur de 1 est noté 2 et appelé *deux.*

Soit $n \in \mathbf{N} \setminus \{0\}$ un entier naturel non nul. Puisque $0 \leq n$ et $0 \neq n$ le sous-ensemble $\{m \in \mathbf{N} : \ m < n\}$ est non vide et majoré par n. Il admet donc un plus grand élément. Soit n' ce plus grand élément. On a $n' < n$. Montrons que $n' + 1 = n$. Si $n' + 1 < n$ alors $n' + 1 \in \{m \in \mathbf{N} : \ m < n\}$ et donc $n'+1 \leq n'$. Ce n'est pas possible donc $n \leq n'+1$. Puisque $n'+1$ est le plus petit élément de $\{m \in \mathbf{N} : n' < m\}$, si $n < n'+1$ alors $n \leq n'$. Ce n'est pas possible donc $n'+1 \leq n$. Ainsi, puisque $n \leq n'+1$ et $n'+1 \leq n$ on a $n'+1 = n$. L'entier naturel n' également noté $n-1$ s'appelle le *prédécesseur* de n. Si $n \in \mathbf{N} \setminus \{0\}$ on a donc $(n-1)+1 = n$.

I.3. proposition *Soient $n, m \in \mathbf{N}$ tels que $n < m$. Alors $n+1 < m+1$.*

I.4. preuve Puisque $n < m$ alors $n+1 \leq m$. De plus $m < m+1$ et donc $m \leq m+1$. Par transitivité $n+1 \leq m+1$. Si $n+1 = m+1$ alors on a $m+1 \leq m$. Ceci est impossible car $m < m+1$. Ainsi $n+1 \leq m+1$ et $n+1 \neq m+1$ c'est à dire $n+1 < m+1$.

I.5. corollaire *Si $n, m \in \mathbf{N}$ tels que $n+1 = m+1$ alors $n = m$.*

I.6. corollaire *Si $n \in \mathbf{N}$ alors $(n+1)-1 = n$.*

I.7. proposition *Soient $n, m \in \mathbf{N}$ tels que $n < m$. Alors $n \leq m-1$.*

I.8. preuve En effet $m-1$ est par définition le plus grand des entiers strictement plus petits que m. Il est donc supérieur ou égal à n qui est un entier strictement plus petit que m.

I.9. proposition (principe de récurrence) *Soit E un sous-ensemble non vide de $\mathbf{N}$ tel que pour tout entier n, si $n \in E$ alors $n+1 \in E$. Alors $E = \{n \in \mathbf{N} : m \leq n\}$ où m est le plus petit élément de E. En particulier si $0 \in E$ alors $E = \mathbf{N}$.*

I.10. preuve Soit E un sous-ensemble non vide de $\mathbf{N}$ tel que pour tout entier n, si $n \in E$ alors $n+1 \in E$. Soit m le plus petit élément de E. On a $E \subset \{n \in \mathbf{N} : m \leq n\}$. Raisonnons par l'absurde et supposons que $E \neq \{n \in \mathbf{N} : m \leq n\}$. Alors le sous-ensemble $\{n \in \mathbf{N} : m \leq n\} \setminus E$ serait non vide et possèderait un plus petit élément m'. On aurait $m < m'$. Par conséquent $m \leq m'-1$ et $m'-1 \notin \{n \in \mathbf{N} : m \leq n\} \setminus E$. Ceci impliquerait que $m'-1 \in E$ et donc $m' = (m'-1)+1$ serait également dans E. C'est la contradiction recherchée.

I.11. définition Une *suite* est une famille indexée par les entiers naturels c'est à dire une application dont l'ensemble de départ est $\mathbf{N}$.

I.12. corollaire (raisonnement par récurrence) *Soit $(P_n)_{n \in \mathbf{N}}$ une suite de propriétés. On suppose que P_0 est vraie (véracité au rang 0) et que pour tout entier naturel n la propriété P_{n+1} est vraie pourvu que la propriété P_n le soit (hérédité de la propriété). Alors pour tout entier n la propriété P_n est* *vraie.*

I.13. preuve On considère l'ensemble E suivant :

$$E = \{n \in \mathbf{N} : P_n \text{ vraie}\}.$$

L'ensemble E contient 0 car P_0 est vraie. Si E contient un entier n (i.e. si P_n est vraie pour un entier donné) alors P_{n+1} est vraie d'après l'hypothèse d'hérédité et donc le successeur $n+1$ de n appartient à E. D'après la proposition précédente (principe de récurrence) $E = \mathbf{N}$.

I.14. corollaire (variante raisonnement par récurrence) *Soit $(P_n)_{n\in\mathbf{N}}$ une suite de propriétés. On suppose que P_0 est vraie (véracité au rang 0) et que pour tout entier naturel n la propriété P_{n+1} est vraie pourvu que les propriétés P_k le soient pour les $k \in \mathbf{N}$ tels $k \leq n$. Alors pour tout entier n la propriété P_n est vraie.*

I.15. preuve Si $n \in \mathbf{N}$ on note Q_n la proriété « $\forall k \in \mathbf{N}\ ((k \leq n) \Rightarrow P_k)$ » et on considère l'ensemble E suivant :

$$E = \{n \in \mathbf{N} : Q_n \text{ vraie}\}.$$

L'ensemble E contient 0 car $Q_0 = P_0$ est vraie. Si E contient un entier n (i.e. si Q_n est vraie pour un entier donné) alors P_{n+1} est vraie d'après l'hypothèse et donc Q_{n+1} qui est $Q_n \wedge P_{n+1}$ est vraie. D'après le principe de récurrence $E = \mathbf{N}$. Ainsi si $n \in \mathbf{N}$ alors Q_n est vraie et donc P_n également.

I.16. définition Soit E un ensemble, f une application de E dans lui-même et a un élément de E. On appelle *suite récurrente associée à f et de premier terme a* toute suite $(x_n)_{n\in\mathbf{N}}$ d'éléments de E telle que $x_0 = a$ et pour tout $n \in \mathbf{N}$, $x_{n+1} = f(x_n)$.

I.17. proposition (existence et unicité de suite récurrente de premier terme donné et associée à une application) *Soit E un ensemble, f une application de E dans lui-même et a un élément de E. Il existe alors une unique suite $(x_n)_{n\in\mathbf{N}}$ d'éléments de E telle que $x_0 = a$ et pour tout $n \in \mathbf{N}$, $x_{n+1} = f(x_n)$.*

I.18. preuve Pour tout $n \in \mathbf{N}$ considérons la propriété P_n suivante : *il existe une unique application x^n de $\{m \in \mathbf{N} : m \leq n\}$ dans E telle que $x^n(0) = a$ et telle que si $m \in \mathbf{N}$ et $m < n$ alors $x^n(m+1) = f(x^n(m))$.*

Montrons que pour tout $n \in \mathbf{N}$ la propriété P_n est vraie. On raisonne par récurrence.

Véracité au rang 0. La propriété P_0 est vraie : x^0 est définie de façon unique par $x^0(0) = a$.

Hérédité de la propriété. Soit n un entier naturel. Supposons que P_n soit vraie. On considère l'application $\overline{x}^n$ de $\{m \in \mathbf{N} : m \leq n+1\}$ dans E définie par $\overline{x}^n(m) = x^n(m)$ si $m \leq n$ et $\overline{x}^n(n+1) = f(\overline{x}^n(n))$. Par construction de $\overline{x}^n$ à partir de x^n et de f, l'application $\overline{x}^n$ vérifie les propriétés suivantes : $\overline{x}^n(0) = a$ et pour tout $m \in \mathbf{N}$ tel que $m < n+1$ on a $\overline{x}^n(m+1) = f(\overline{x}^n(m))$. Considérons une seconde application $\tilde{x}^n$ de $\{m \in \mathbf{N} : m \leq n+1\}$ dans E qui vérifie ces propriétés : $\tilde{x}^n(0) = a$ et pour tout $m \in \mathbf{N}$ tel que $m < n+1$ on a $\tilde{x}^n(m+1) = f(\tilde{x}^n(m))$. Par conséquent, d'après P_n supposée vraie les restrictions de $\overline{x}^n$ et de $\tilde{x}^n$ à $\{m \in \mathbf{N} : m \leq n\}$ sont égales. Il vient alors que $\tilde{x}^n(n) = \overline{x}^n(n)$ et donc

$$\tilde{x}^n(n+1) = f(\tilde{x}^n(n)) = f(\overline{x}^n(n)) = \overline{x}^n(n+1).$$

Ainsi les applications $\tilde{x}^n$ et $\overline{x}^n$ sont égales : on pose donc $x^{n+1} = \tilde{x}^n = \overline{x}^n$. Ceci prouve P_{n+1}.

Remarquons que la démonstration précédente implique que si $n \in \mathbf{N}$ alors $x^{n+1}(n+1) = f(x^n(n))$.

Soit $(x_n)_{n\in\mathbf{N}}$ la suite définie par $x_n = x^n(n)$ si $n \in \mathbf{N}$. On a $x_0 = x^0(0) = a$ et si $n \in \mathbf{N}$ alors

$$x_{n+1} = x^{n+1}(n+1) = f(x^n(n)) = f(x_n).$$

Considérons maintenant une seconde suite $(x'_n)_{n\in\mathbf{N}}$ qui vérifie $x'_0 = a$ et pour tout $n \in \mathbf{N}$, $x'_{n+1} = f(x'_n)$. Soit $n \in \mathbf{N}$. D'après la propriété P_n on a $x'_n = x^n(n) = x_n$. Ainsi les suites $(x_n)_{n\in\mathbf{N}}$ et $(x'_n)_{n\in\mathbf{N}}$ sont égales. Ceci achève la preuve de la proposition.

I.19. notation Si $n \in \mathbf{N}$ on pose $\mathbf{N}_n = \{k \in \mathbf{N} : k < n\}$. Soit E un ensemble. Si $n \in \mathbf{N}$ et si $x \in E^{\mathbf{N}}$ ou $x \in E^{\mathbf{N}_m}$ avec $m \in \mathbf{N}$ $n < m$ alors $(x_i)_{i\leq n}$ et $(x_0, ..., x_n)$ désignent la restriction de x à $\mathbf{N}_{n+1}$.

I.20. proposition *Soit E un ensemble, $(f_n)_{n\in\mathbf{N}}$ une famille d'applications telle que si $n \in \mathbf{N}$ le domaine de f_n est $E^{n+1} \times \mathbf{N}^{n+1}$ et l'ensemble d'arrivée E. Si $a \in E$ il existe une unique suite $(u_n)_{n\in\mathbf{N}}$ d'éléments de E telle que $u_0 = a$ et pour tout $n \in \mathbf{N}$, $u_{n+1} = f_n((u_0, ..., u_n), (0, ..., n))$.*

I.21. preuve On considèdre $\theta = (\alpha, \beta, \gamma) \in (E^{\mathbf{N}} \times \mathbf{N}^{\mathbf{N}} \times \mathbf{N})^{(E^{\mathbf{N}} \times \mathbf{N}^{\mathbf{N}} \times \mathbf{N})}$ telle que si $v = (x, y, n) \in E^{\mathbf{N}} \times \mathbf{N}^{\mathbf{N}} \times \mathbf{N}$ alors
- $\alpha(x, y, n)_k = x_k$ si $k \in \mathbf{N}$ est tel que $k \neq n+1$

- $\alpha(x, y, n+1) = f_n((x_i)_{i\leq n}, (y_i)_{i\leq n})$
- $\alpha(x, y, n) = y$
- $\gamma(x, y, n) = n + 1$.

On pose $\mathcal{A} = (A, N, 0)$ où A est la suite constante égale à a et N est l'identité de $\mathbf{N}$: si $n \in \mathbf{N}$ alors $A_n = a$ et $N_n = n$. Soit $v = (x, y, z)$ la suite récurrente de premier terme $\mathcal{A}$ associée à θ : si $n \in \mathbf{N}$ on a $v_n = (x_n, y_n, z_n)$ avec $x_n \in E^{\mathbf{N}}$, $y_n \in \mathbf{N}^{\mathbf{N}}$ et $z_n \in \mathbf{N}$. Si $k \in \mathbf{N}$ et $n \in \mathbf{N}$ $x_n(k)$ désigne le k-ème terme de la suite x_n.

Puisque $z_0 = 0$ et que $z_{n+1} = z_n + 1$ si $n \in \mathbf{N}$, on en déduit que pour tout $n \in \mathbf{N}$ $z_n = n$.

Puisque y_0 est l'identité de $\mathbf{N}$ et que $y_{n+1} = y_n$ si $n \in \mathbf{N}$, on en déduit que pour tout $n \in \mathbf{N}$ y_n est l'identité de $\mathbf{N}$.

Soit $k \in \mathbf{N}$. Puisque pour tout $n \in \mathbf{N}$ tel que $k \leq n$ on a $x_n(k) = x_{n+1}(k)$ on en déduit que pour tout $n \in \mathbf{N}$ tel que $k \leq n$ on a $x_n(k) = x_k(k)$.

Puisque que $x_0(0) = a$ et que pour tout $n \in \mathbf{N}$ on a

$$x_{n+1}(n+1) = f_n((x_n(i))_{i\leq n}, (y_n(i))_{i\leq n})$$

c'est à dire

$$x_{n+1}(n+1) = f_n((x_i(i))_{i\leq n}, (i)_{i\leq n})$$

ou encore

$$x_{n+1}(n+1) = f_n((x_0(0), ..., x_n(n)), (0, ..., n)).$$

Par conséquent la suite $u = (u_n)_{n\in\mathbf{N}}$ définie par $u_n = x_n(n)$ si $n \in \mathbf{N}$ vérifie $u_0 = a$ et si $n \in \mathbf{N}$ $u_{n+1} = f_n((u_0, ..., u_n), (0, ..., n))$.

Montrons maintenant l'unicité d'une telle suite u. Soit $v \in E^{\mathbf{N}}$ tel que $v_0 = a$ et si $n \in \mathbf{N}$ $v_{n+1} = f_n((v_0, ..., v_n), (0, ..., n))$. L'ensemble $E = \{n \in \mathbf{N} : \forall k \in \mathbf{N}\ ((k \leq n) \Rightarrow (u_k = v_k))\}$ contient 0 car $u_0 = a = v_0$. Si $n \in \mathbf{N}$ appartient à E alors pour tout $k \in \mathbf{N}$ tel que $k \leq n$ on a $u_k = v_k$ et donc

$$u_{n+1} = f_n((u_0, ..., u_n), (0, ..., n)) = f_n((v_0, ..., v_n), (0, ..., n)) = v_{n+1}$$

et donc pour tout $k \in \mathbf{N}$ tel que $k \leq n+1$ $u_k = v_k$. Ainsi si $n \in \mathbf{N}$ appartient à E c'est encore le cas de $n+1$. Puisque $0 \in E$ on a donc $E = \mathbf{N}$: pour tout $n \in \mathbf{N}$ $u_n = v_n$. Les suites u et v sont égales.

I.22. proposition *Soit* $(E, \mathcal{R})$ *un ensemble ordonné et* $f : \mathbf{N} \to E$ *telle que si* $n \in \mathbf{N}$ *alors* $f(n) \neq f(n+1)$ *et* $f(n)\mathcal{R}f(n+1)$. *Alors* f *est strictement croissante.*

I.23. preuve Si $n \in \mathbf{N}$ on note P_n la propriété suivante : *la restriction f_n de f à $\{m \in \mathbf{N} : m \leq n\}$ est strictement croissante.*

Montrons que pour tout $n \in \mathbf{N}$ la propriété P_n est vraie. On raisonne par récurrence.

Véracité au rang 0. La propriété P_0 est trivialement vrai.

Hérédité de la propriété. Soit n un entier naturel. Supposons que P_n soit vraie. Soient $k, l \in \{m \in \mathbf{N} : m \leq n+1\}$ tels que $k < l$. Si $l \leq n$ alors $k \leq n$ et $f_{n+1}(k) = f_n(k) \neq f_n(l) = f_{n+1}(l)$ et $f_{n+1}(k) = f_n(k)\mathcal{R}f_n(l) = f_{n+1}(l)$. Supposons maintenant que $l = n+1$. Alors $k \leq n < n+1 = l$ et donc d'une part

$$f_{n+1}(k) = f_n(k)\mathcal{R}f_n(n) = f(n)$$

d'après P_n et d'autre part

$$f(n)\mathcal{R}f(n+1) = f_{n+1}(n+1) = f_{n+1}(l)$$

et

$$f(n) \neq f(n+1) = f_{n+1}(n+1) = f_{n+1}(l)$$

d'après l'hypothèse sur f. Par transitivité de $\mathcal{R}$ il vient

$$f_{n+1}(k)\mathcal{R}f_{n+1}(l) \text{ et } f_{n+1}(k) \neq f_{n+1}(l).$$

Ainsi P_{n+1} est vraie.

La fonction f est strictement croissante car si $m < n$ alors d'après P_n $f(m) = f_n(m)\mathcal{R}f_n(n) = f(n)$ et $f(m) = f_n(m) \neq f_n(n) = f(n)$.

I.24. proposition (l'application successeur est strictement croissante) *L'application f de $\mathbf{N}$ dans $\mathbf{N}$ définie par $f(n) = n+1$ si $n \in \mathbf{N}$ est strictement croissante.*

I.25. preuve En effet si $n \in \mathbf{N}$ on a $n < n+1 < (n+1)+1$ et donc $f(n) < f(n+1)$. La proposition précédente permet de conclure

I.26. proposition (unicité des entiers naturels) *Soit un ensemble bien ordonné noté $(\mathbf{N}', \leq')$, qui ne possède pas de majorant mais qui est tel que chacun de ses sous-ensembles non vides, s'il est majoré, admet un plus grand élément. Alors il existe un isomorphisme $f : (\mathbf{N}, \leq) \to (\mathbf{N}, \leq')$ d'ensembles bien ordonnés. Cet isomorphisme est unique.*

I.27. preuve On note $0'$ le plus petit élément de $\mathbf{N}'$, on note $1'$ le successseur de $0'$ dans $\mathbf{N}'$, si $n \in \mathbf{N}'$ on note $n + 1'$ son successeur dans $\mathbf{N}'$ et si $n' \neq 0$ on note $n' - 1$ son prédécesseur dans $\mathbf{N}'$.

Pour tout $n \in \mathbf{N}$ considérons la propriété P_n suivante : *il existe une unique application* f_n *de* $\{m \in \mathbf{N} : m \leq n\}$ *dans* $\mathbf{N}'$ *telle que* $f_n(0) = 0'$ *et telle que si* $m \in \mathbf{N}$ *et* $m < n$ *alors* $f_n(m+1) = f_n(m) + 1'$.

Montrons que pour tout $n \in \mathbf{N}$ la propriété P_n est vraie. On raisonne par récurrence.

Véracité au rang 0. La propriété P_0 est vraie : $f_0(0)$ est définie de façon unique par $f_0(0) = 0'$.

Hérédité de la propriété. Soit n un entier naturel. Supposons que P_n soit vraie. On considère l'application $\overline{f}_n$ de $\{m \in \mathbf{N} : m \leq n+1\}$ dans $\mathbf{N}'$ définie par $\overline{f}_n(m) = f_n(m)$ si $m \leq n$ et $\overline{f}_n(n+1) = f_n(n) + 1'$. Par construction de $\overline{f}_n$ à partir de f_n, l'application $\overline{f}_n$ vérifie les propriétés suivantes : $\overline{f}_n(0) = 0'$ et pour tout $m \in \mathbf{N}$ tel que $m < n+1$ on a $\overline{f}_n(m+1) = \overline{f}_n(m) + 1'$. Considérons une seconde application $\tilde{f}_n$ de $\{m \in \mathbf{N} : m \leq n+1\}$ dans $\mathbf{N}$ qui vérifie ces propriétés : $\tilde{f}_n(0) = 0'$ et pour tout $m \in \mathbf{N}$ tel que $m < n+1$ on a $\tilde{f}_n(m+1) = \tilde{f}_n(m) + 1'$. Par conséquent, d'après P_n supposée vraie les restrictions de $\overline{f}_n$ et de $\tilde{f}_n$ à $\{m \in \mathbf{N} : m \leq n\}$ sont égales. Il vient alors que $\tilde{f}_n(n) = \overline{f}_n(n)$ et donc

$$\tilde{f}_n(n+1) = \tilde{f}_n(n) + 1' = \overline{f}_n(n) + 1' = \overline{f}_n(n+1).$$

Ainsi les applications $\tilde{f}_n$ et $\overline{f}_n$ sont égales. Ceci prouve P_{n+1}.

Remarquons que la démonstration précédente implique que si $n \in \mathbf{N}$ alors $f_{n+1}(n+1) = f_n(n) + 1'$.

Soit f l'application de $\mathbf{N}$ dans $\mathbf{N}'$ définie par $f(n) = f_n(n)$ si $n \in \mathbf{N}$. Alors l'application f vérifie les propriétés suivantes : $f(0) = 0'$ et pour tout $n \in \mathbf{N}$

$$f(n+1) = f_{n+1}(n+1) = f_n(n) + 1' = f(n) + 1'$$

et donc $f(n) <' f(n+1)$. D'après la proposition précédente f est strictement croissante.

Il reste à montrer que f est bijective. Puisqu'elle est strictement croissante, il suffit de montrer qu'elle est surjective. Raisonnons par l'absurde en supposant que l'ensemble $\mathbf{N}' \setminus f(\mathbf{N})$ soit non vide. Soit m' son plus petit élément. Puisque $f(0) = 0'$ et que l'élément m' n'a pas d'antécédent par f, cet élement m' est différent de $0'$ et il admet un prédécesseur n' : $n' + 1' = m'$. Cet élément n' admet un antécédent $n \in \mathbf{N}$: $f(n) = n'$. Par conséquent $f(n+1) = n' + 1' = m'$. C'est la contradiction recherchée.

II. L'addition et la multiplication des entiers naturels

Dans cette partie on définit et on étudie l'addition et la multiplication qui sont deux lois de compositions internes sur $\mathbf{N}$.

II.1. définition Soit $m \in \mathbf{N}$ un entier naturel. La suite récurrente de premier terme m et associée à l'application f de $\mathbf{N}$ dans $\mathbf{N}$ définie par $f(n) = n + 1$ est notée $(m+n)_{n\in\mathbf{N}}$. L'*addition de deux entiers naturels* est l'application de $\mathbf{N} \times \mathbf{N}$ dans $\mathbf{N}$ (c'est à dire une loi de composition interne définie sur $\mathbf{N}$) qui à tout couple $(m, n) \in \mathbf{N} \times \mathbf{N}$ associe le terme $m + n$.

II.2. proposition *L'addition admet* 0 *comme neutre.*

II.3. preuve Par définition, si $n \in \mathbf{N}$ on a $n + 0 = n$. Il reste à montrer que $0 + n = n$. On le montre par récurrence sur n.

Véracité au rang 0. Par définition de l'addition $0 + 0 = 0$.

Hérédité. Soit $n \in \mathbf{N}$. Supposons que $0 + n = n$. Puisque par définition de l'addition on a $0 + (n + 1) = (0 + n) + 1$ il vient que $0 + (n + 1) = n + 1$. C'est ce qu'il fallait démontrer pour conclure.

II.4. proposition *L'addition est associative.*

II.5. preuve Il suffit de montrer par récurrence sur $n \in \mathbf{N}$ que si $k, l, n \in \mathbf{N}$ on a $(k + l) + n = k + (l + n)$.

Véracité au rang 0. Puisque 0 est le neutre pour l'addition on a $(k+l)+0 = k + l = k + (l + 0)$ pour $k, l \in \mathbf{N}$ quelconques.

Hérédité. Soit $n \in \mathbf{N}$. Supposons que $(k+l)+n = k+(l+n)$ si $k, l \in \mathbf{N}$ quelconque. Alors on a

$$\begin{array}{rcll} (k + l) + (n + 1) & = & ((k + l) + n) + 1 & \text{par définition de } + \\ & = & (k + (l + n)) + 1 & \text{par hypothèse de récurrence} \\ & = & k + ((l + n) + 1) & \text{par définition de } + \\ & = & k + (l + (n + 1)) & \text{par définition de } + . \end{array}$$

L'hérédité est prouvée ainsi que la proposition.

II.6. proposition *L'addition est commutative.*

II.7. preuve Il suffit de montrer par récurrence sur $n \in \mathbf{N}$ que si $k, l \in \mathbf{N}$ avec $k, l \leq n$ on a $k + l = l + k$.

Véracité au rang 0. Nécessairement $k = l = 0$ et $k + l = l + k$.

Véracité au rang 1. Puisque 0 est le neutre on a $0+0 = 0$, $0+1 = 1+0 = 0 + 1 = 1$ et évidemment $1 + 1 = 1 + 1$.

Hérédité. Soit $n \in \mathbf{N}$ et $1 \leq n$. Supposons que $k + l = l + k$ si $k, l \in \mathbf{N}$ avec $k, l \leq n$. Soient $k, l \in \mathbf{N}$ avec $k, l \leq n + 1$. Si $k, l \leq n$, l'hypothèse de récurrence implique que $k + l = l + k$. Si $k = l = n + 1$ on a évidemment $k + l = l + k$. Il reste donc à considérer le cas où $l = n + 1$ et $k \leq n$ et le cas $l \leq n$ et $k = n + 1$ qui sont en fait les mêmes cas. On suppose donc $k \leq n$ et $l = n + 1$. On a

$$\begin{aligned}
k + (n + 1) &= (k + n) + 1 \text{ par associativité de } + \\
&= (n + k) + 1 \text{ par hypothèse de récurrence} \\
&= n + (k + 1) \text{ par associativité de } + \\
&= n + (1 + k) \text{ par hypothèse de récurrence} \\
&= (n + 1) + k \text{ par associativité de } + .
\end{aligned}$$

L'hérédité est prouvée ainsi que la proposition.

II.8. proposition *L'addition respecte strictement l'ordre. Si $k, l, n \in \mathbf{N}$ et $k < l$ alors $k + n < l + n$.*

II.9. preuve Puisque l'addition est commutative il suffit de montrer par récurrence sur $n \in \mathbf{N}$ que si $k, l \in \mathbf{N}$ et $k < l$ alors $k + n < l + n$ et $n + k < n + l$.

La propriété est vraie pour $n = 0$ car 0 est le neutre de l'addition.

Soit $n \in \mathbf{N}$. Supposons que si $k, l \in \mathbf{N}$ et $k < l$ alors $k + n < l + n$. Considérons de tels k et l. On a $k+1 < l+1$ puisque l'application successeur est strictement croissante. Par conséquent, en utilisant l'associativité et la commutativité de l'addition on obtient $k+(n+1) = (k+1)+n$ et $l+(n+1) = (l + 1) + n$. Or, par hypothèse de récurrence on a $(k + 1) + n < (l + 1) + n$. Finalement ceci donne l'inégalité recherchée $k + (n + 1) < l + (n + 1)$.

II.10. corollaire *Tout élément de $\mathbf{N}$ est régulier pour l'addition. En particulier, si $n, k, l \in \mathbf{N}$ sont tels que $n + k = n + l$ alors $k = l$.*

II.11. preuve Si $k \neq l$, on peut toujours supposer, quitte à les permuter, que $k < l$. La proposition précédente permet de conclure car l'addition est commutative.

II.12. proposition *Soit $m, n \in \mathbf{N}$. Si $m \leq n$ il existe un unique $k \in \mathbf{N}$ tel que $m + k = n$.*

II.13. preuve L'unicité résulte du respect strict de l'ordre par l'addition. On raisonne par récurrence sur $n \in \mathbf{N}$. Si $n = 0$ c'est immédiat. Soit $n \in \mathbf{N}$. On suppose que si $m \in \mathbf{N}$ vérifie $m \leq n$ alors il existe $k \in \mathbf{N}$ tel que $m + k = n$. Soit $m \in \mathbf{N}$ tel que $m \leq n + 1$. Si $m = n + 1$ on prend $k = 0$. Sinon $m \leq n$ et il existe par hypothèse de récurrence $h \in \mathbf{N}$ tel que $m + h = n$. Alors $k = h + 1$ vérifie $m + k = n + 1$.

II.14. notation Si $m, n, k \in \mathbf{N}$ vérifient $m + k = n$ on pose $k = n - m$.

II.15. remarque Puisque l'addition respecte strictement l'ordre, d'après la proposition précédente $n - m$ existe et est unique si et seulement si $m \leq n$.

II.16. proposition *L'ordre* $\leq$ *est l'unique ordre sur* $\mathbf{N}$ *compatible avec l'addition et tel que* $0 \leq 1$.

II.17. preuve Expliquons l'unicité. Soit $\leq'$ un ordre sur $\mathbf{N}$ qui est compatible avec l'adddition et tel que $0 \leq' 1$. On note M l'ensemble

$$M = \{n \in \mathbf{N} : 0 \leq' n\}.$$

On va montrer par récurrence que $M = \mathbf{N}$. L'ensemble M est non vide car il contient 0 et 1. Soit $n \in M$. Puisque l'ordre $\leq'$ est compatible avec l'addition et que $0 \leq' 1$ il vient $n \leq' n + 1$. Puisque $n \in M$ on a aussi $0 \leq' n$. Par transitivité de $\leq'$ il vient $0 \leq' n + 1$ et donc $(n + 1) \in M$. Ceci prouve que $M = \mathbf{N}$. Il reste à montrer que si $n, m \in \mathbf{N}$ sont tels que $m \leq n$ alors $m \leq' n$. Soit donc $n, m \in \mathbf{N}$ tels que $m \leq n$. Il existe donc $k \in \mathbf{N}$ tel $n = m + k$. On a donc $0 \leq' k$. Puisque $\leq'$ est compatible avec l'addition ceci implique que $m \leq' n$.

II.18. définition Soit $m \in \mathbf{N}$ un entier naturel. La suite récurrente de premier terme 0 et associée à l'application f de $\mathbf{N}$ dans $\mathbf{N}$ définie par $f(n) = n + m$ est notée $(n \times m)_{n \in \mathbf{N}}$. La *multiplication de deux entiers naturels* est l'application de $\mathbf{N} \times \mathbf{N}$ dans $\mathbf{N}$ (c'est à dire une loi de composition interne définie sur $\mathbf{N}$) qui à tout couple $(n, m) \in \mathbf{N} \times \mathbf{N}$ associe le terme $n \times m$.

II.19. proposition *L'entier naturel* 0 *est absorbant pour la multiplication.*

II.20. preuve Par définition $0 \times m = 0$ si $m \in \mathbf{N}$. Il reste à montrer que $n \times 0 = 0$ si $n \in \mathbf{N}$. On le montre par récurrence sur n.

On va utiliser le fait que l'entier naturel $n \times 0$ est un terme de la suite récurrente de premier terme 0 associée à l'application f de $\mathbf{N}$ dans $\mathbf{N}$ définie par $f(n) = n + 0$.

Véracité au rang 0. On vient de voir que $0 \times 0 = 0$.

Hérédité. Soit $n \in \mathbf{N}$. Supposons que $n \times 0 = 0$. Par définition de la multiplication on a $(n+1) \times 0 = f(n \times 0)$. Il vient donc $(n+1) \times 0 = f(0) = 0 + 0 = 0$.

II.21. proposition *La multiplication admet* 1 *comme neutre.*

II.22. preuve Par définition, si $m \in \mathbf{N}$ on a $1 \times m = 0 + m = m$. Il reste à montrer que $n \times 1 = n$. On le montre par récurrence sur n.

Véracité au rang 0. Puisque 0 est absorbant $0 \times 1 = 0$.

Hérédité. Soit $n \in \mathbf{N}$. Supposons que $n \times 1 = n$. Par définition de la multiplication on a $(n+1) \times 1 = f(n \times 1)$ où f est l'application de $\mathbf{N}$ dans $\mathbf{N}$ définie par $f(n) = n+1$. Par conséquent on a

$$\begin{array}{rcl} (n+1) \times 1 & = & f(n \times 1) \\ & = & f(n) \\ & = & n+1. \end{array}$$

II.23. proposition *La multiplication est distributive par rapport à l'addition.*

II.24. preuve On montre par récurrence sur $n \in \mathbf{N}$ que si $k, l \in \mathbf{N}$ alors

$$n \times (k+l) = (n \times k) + (n \times l).$$

La propriété est vraie aux rangs 0 et 1 car 0 est neutre pour + et absorbant pour $\times$ pendant que 1 est neutre pour $\times$. Soit $n \in \mathbf{N}$. On suppose que si $k, l \in \mathbf{N}$ alors $n \times (k+l) = (n \times k) + (n \times l)$. Alors

$$\begin{array}{rcl} (n+1) \times (k+l) & = & (n \times (k+l)) + (k+l) \text{ par définition de } \times \\ & = & ((n \times k) + (n \times l)) + (k+l) \text{ par hypothèse de récurrence} \\ & = & ((n \times k) + k) + ((n \times l) + l) \text{ par associativité et par} \\ & & \qquad\qquad\qquad\qquad\qquad\quad \text{commutativité de } + \\ & = & ((n+1) \times k) + ((n+1) \times l) \text{ par définition de } \times. \end{array}$$

On montre maintenant par récurrence sur $l \in \mathbf{N}$ que si $k, n \in \mathbf{N}$ alors

$$(k+l) \times n = (k \times n) + (l \times n).$$

La propriété est vraie aux rangs 0 et 1 car 0 est neutre pour + et absorbant pour $\times$, 1 est neutre pour $\times$ et par définition de $\times$. Soit $l \in \mathbf{N}$. On suppose que si $k, n \in \mathbf{N}$ alors $(k+l) \times n = (k \times n) + (l \times n)$. Alors

$$\begin{array}{rcl} (k+(l+1)) \times n & = & ((k+l)+1)) \times n \text{ par associativité de } + \\ & = & ((k+l) \times n) + n \text{ par définition de } \times \\ & = & ((k \times n) + (l \times n)) + n \text{ par hypothèse de récurrence} \\ & = & (k \times n) + ((l \times n) + n) \text{ par associativité de } + \\ & = & (k \times n) + ((l+1) \times n)) \text{ par définition de } \times. \end{array}$$

II.25. proposition *La multiplication est associative.*

II.26. preuve On montre par récurrence sur $k \in \mathbf{N}$ que si $l, n \in \mathbf{N}$ alors

$$k \times (l \times n) = (k \times l) \times n.$$

La propriété est vraie aux rangs 0 et 1 car 0 est absorbant et 1 est neutre pour $\times$. Soit $k \in \mathbf{N}$. On suppose que si $l, n \in \mathbf{N}$ alors $k \times (l \times n) = (k \times l) \times n$. Alors

$$\begin{array}{rcl} ((k+1) \times l) \times n & = & ((k \times l) + l) \times n \text{ par définition de } \times \\ & = & ((k \times l) \times n) + (l \times n) \text{ par distributivité de } \times \\ & = & (k \times (l \times n)) + (l \times n) \text{ par hypothèse de récurrence} \\ & = & (k+1) \times (l \times n) \text{ par définition de } \times . \end{array}$$

II.27. proposition *La multiplication est commutative.*

II.28. preuve On montre par récurrence sur $n \in \mathbf{N}$ que si $n, m \in \mathbf{N}$ alors $n \times m = m \times n$.

C'est vrai pour $n = 0$ car 0 est absorbant pour la multiplication. Soit $n \in \mathbf{N}$. On suppose que pour tout $m \in \mathbf{N}$ on a $n \times m = m \times n$. Alors

$$\begin{array}{rcl} (n+1) \times m & = & (n \times m) + m \text{ par définition de } \times \\ & = & (m \times n) + m \text{ par hypothèse de récurrence} \\ & = & (m \times n) + (m \times 1) \text{ car 1 est le neutre de } \times \\ & = & m \times (n+1) \text{ par distributivité de } \times . \end{array}$$

II.29. convention On utilise les propriétés d'associativité et de commutativité de $+$ et $\times$ et on donne la priorité de $\times$ sur $+$ pour simplifier le parenthésage. Le symbole $\times$ et parfois omis. Ainsi le produit $a \times b$ peut être noté ab.

II.30. proposition *La multiplication par un entier non nul respecte strictement l'ordre. En particulier, si $k, l, n \in \mathbf{N}$, $k < l$ et $n \neq 0$ alors $k \times n < l \times n$.*

II.31. preuve Puisque la multiplication est commutative il suffit de montrer par récurrence sur $n \in \mathbf{N}$ que si $k, l \in \mathbf{N}$ et $k < l$ alors $k \times n < l \times n$ ou $n = 0$.

La propriété est vraie pour $n = 0$ et $n = 1$ car 0 est absorbant et 1 est le neutre pour la multiplication.

Soit $n \in \mathbf{N}$ non nul. Supposons que si $k, l \in \mathbf{N}$ et $k < l$ alors $k \times n < l \times n$. Considérons $k, l \in \mathbf{N}$ tels que $k < l$. On a $k < l$ et donc $k \times n < l \times n$. Cette seconde inégalité implique $(k \times n) + k < (l \times n) + k$ et l'inégalité $k < l$ implique

$(l\times n)+k < (l\times n)+l$. Par transitivité de l'ordre on a $(k\times n)+k < (l\times n)+l$. Puisque $k \times (n+1) = (k \times n) + k$ et $l \times (n+1) = l \times n + l$ il vient $k \times (n+1) < l \times (n+1)$.

II.32. corollaire *Tout élément non nul de* $\mathbf{N}$ *est régulier pour la multiplication. En particulier, si* $n, k, l \in \mathbf{N}$ *sont tels que* $n \times k = n \times l$ *alors* $n = 0$ *ou* $k = l$.

II.33. preuve Si $k \neq l$, on peut toujours supposer, quitte à les permuter, que $k < l$. La proposition précédente permet de conclure car la multiplication est commutative.

III. Ensembles finis

III.1. notation Si $n \in \mathbf{N}$ on note $\mathbf{N}_n$ l'ensemble $\{k \in \mathbf{N} : k < n\}$.

III.2. exemple $\mathbf{N}_0 = \emptyset$, $\mathbf{N}_1 = \{0\}$ et $\mathbf{N}_2 = \{0, 1\}$.

III.3. proposition *Si* $n \leq m$ *alors* $\mathbf{N}_n \subset \mathbf{N}_m$.

III.4. preuve Soit $k \in \mathbf{N}_n$. Alors $k \leq n$ et $n \leq m$. Par transitivité $k \leq m$ et donc $k \in \mathbf{N}_m$.

III.5. définition Un ensemble E est dit *fini* s'il existe $n \in \mathbf{N}$ tel que E et $\mathbf{N}_n$ soient en bijection.

III.6. remarque Soit $n \in \mathbf{N}$, $b : \mathbf{N}_n \to E$ une bijection et $f : E \to F$ une surjection. La composée $f \circ b$ est une surjection. Par conséquent si $y \in F$ l'ensemble $(b \circ f)^{-1}(\{y\})$ est un sous-ensemble non vide de $\mathbf{N}$. Il admet donc un plus petit élément : $\min(b \circ f)^{-1}(\{y\})$ existe et il vérifie

$$f(b(\min(b \circ f)^{-1}(\{y\}))) = y.$$

De plus si $y, y' \in F$ sont différents les ensembles $(b\circ f)^{-1}(\{y\})$ et $(b\circ f)^{-1}(\{y'\})$ sont disjoints et donc $\min(b \circ f)^{-1}(\{y\})$ et $\min(b \circ f)^{-1}(\{y'\})$ sont différents et, puisque b est injective

$$b(\min(b \circ f)^{-1}(\{y\})) \neq b(\min(b \circ f)^{-1}(\{y'\})).$$

Ceci démontre sans recours à l'axiome du choix la proposition suivante.

III.7. proposition *Soit* $n \in \mathbf{N}$, $b : \mathbf{N}_n \to E$ *une bijection et* $f : E \to F$ *une surjection. Alors on définit une injection* $g : F \to E$ *qui vérifie* $f(g(y)) = y$ *si* $y \in F$ *en posant*

$$g(y) = b(\min(b \circ f)^{-1}(\{y\})).$$

III.8. proposition *Soit* $n, m \in \mathbf{N}$. *S'il existe une injection* $\mathbf{i}$ *de* $\mathbf{N}_n$ *dans* $\mathbf{N}_m$ *ou une surjection* $\mathbf{s}$ *de* $\mathbf{N}_m$ *dans* $\mathbf{N}_n$ *alors* $n \leq m$.

III.9. preuve Si $n \in \mathbf{N}$ on considère la propriété P_n suivante : *Pour tout* $m \in \mathbf{N}$ *s'il existe une injection* $\mathbf{i}$ *de* $\mathbf{N}_n$ *dans* $\mathbf{N}_m$ *ou une surjection* $\mathbf{s}$ *de* $\mathbf{N}_m$ *dans* $\mathbf{N}_n$ *implique* $n \leq m$.

Montrons par récurrence sur $n \in \mathbf{N}$ que pour tout $n \in \mathbf{N}$ la propriété P_n est vraie.

Le cas $n = 0$. On a $\mathbf{N}_0 = \emptyset$. Si $m \in \mathbf{N}$ alors $\emptyset_m^{\mathbf{N}} = \{(\emptyset, \mathbf{N}_m, \emptyset)\}$ et $(\emptyset, \mathbf{N}_m, \emptyset)$ est injective. Si de plus $0 < m$ alors $\mathbf{N}_m^{\emptyset} = \emptyset$. Par conséquent P_0 est vraie.

Soit $n \in \mathbf{N}$ tel que P_n soit vraie. Soit $m \in \mathbf{N}$. On suppose qu'il existe une injection $\mathbf{i}$ de $\mathbf{N}_{n+1}$ dans $\mathbf{N}_m$. Puisque $0 < n+1$, l'ensemble $\mathbf{N}_{n+1}$ est non vide et donc $\mathbf{N}_{n+1}^{\mathbf{N}_0} = \mathbf{N}_{n+1}^{\emptyset} = \emptyset$. Puisque $\mathbf{i} \in \mathbf{N}_{n+1}^{\mathbf{N}_m}$ on a $0 < m$. On pose $\mathbf{i}' = \sigma_{m-1\mathbf{i}(n)}^{\mathbf{N}_m} \circ \mathbf{i}$. L'application $\mathbf{i}'$ qui est la composée de deux injections est une injection. De plus $\mathbf{i}'(n) = m-1$. Puisque $\mathbf{i}'$ est injective, ceci implique que si $k \in \mathbf{N}_{n+1} \setminus \{n\}$ (c'est à dire si $k \in \mathbf{N}_n$) alors $\mathbf{i}'(k) \in \mathbf{N}_m \setminus \{m-1\} = \mathbf{N}_{m-1}$. Par conséquent $\mathbf{i}'(\mathbf{N}_n) \subset \mathbf{N}_{m-1}$. On peut donc considérer la corestriction $\mathbf{i}''$ à $\mathbf{N}_{m-1}$ de la restriction de $\mathbf{i}'$ à $\mathbf{N}_{n-1}$. C'est une injection car $\mathbf{i}'$ en est une. D'après P_n ceci implique que $n-1 \leq m-1$ et donc que $n \leq m$. On suppose maintenant qu'il existe une surjection $\mathbf{j}$ de $\mathbf{N}_m$ dans $\mathbf{N}_{n+1}$. Ceci implique qu'il existe une injection $\mathbf{i}$ de $\mathbf{N}_{n+1}$ dans $\mathbf{N}_m$. D'après ce qui précède ceci implique encore que $n \leq m$. Ainsi P_{n+1} est vérifiée dès que P_{n+1} l'est.

Ceci démontre par récurrence la proposition.

III.10. proposition *Soit* E *un ensemble fini et* $m, n \in \mathbf{N}$. *S'il existe des bijections* $f : E \to \mathbf{N}_n$ *et* $g : E \to \mathbf{N}_m$ *alors* $m = n$.

III.11. preuve S'il existe des bijections $f : E \to \mathbf{N}_n$ et $g : E \to \mathbf{N}_m$ alors les composées $g \circ f^{-1} : \mathbf{N}_n \to \mathbf{N}_m$ et $f \circ g^{-1} : \mathbf{N}_m \to \mathbf{N}_n$ sont des bijections. D'après la proposition ceci implique que $n \leq m$ et que $m \leq n$ et donc que $m = n$.

III.12. définition Si E est un ensemble fini l'unique entier n tel qu'il existe une bijection $b : \mathbf{N}_n \to E$ s'appelle *cardinal* de E et il est noté $\operatorname{card} E$.

III.13. proposition *Soit* $f : E \to F$ *une bijection. L'ensemble* E *est fini si et seulement si l'ensemble* F *est fini.*

III.14. preuve Si E est fini il existe $n \in \mathbf{N}$ et $b : E \to \mathbf{N}_n$ une bijection. Alors $b \circ f^{-1} : F \to \mathbf{N}_n$ est une bijection et F est fini. Si F est fini il existe

$n \in \mathbf{N}$ et $b : F \to \mathbf{N}_n$ une bijection. Alors $b \circ f : E \to \mathbf{N}_n$ est une bijection et E est fini.

III.15. proposition *Soit E et F deux ensembles finis. Il existe une bijection de E dans F si et seulement si ils ont même cardinal.*

III.16. preuve Supposons que E et F ont le même cardinal n. Il existe donc des bijections $f : E \to \mathbf{N}_n$ et $g : F \to \mathbf{N}_n$. Alors $g^{-1} \circ f : E \to F$ est une bijection.

Supposons qu'il existe une bijection $b : E \to F$. Soit n le cardinal de E, m celui de F et $f : E \to \mathbf{N}_n$, $g : F \to \mathbf{N}_m$ des bijections. Alors la composée $g \circ (b \circ f^{-1}) : \mathbf{N}_n \to \mathbf{N}_m$ est une bijection donc $n = m$.

III.17. proposition *Soit $E \subset F$. Si F est fini alors E l'est également et $\operatorname{card} E \leq \operatorname{card} F$. S'il y a égalité des cardinaux alors $E = F$.*

III.18. preuve Soit $n = \operatorname{card} E$ et $m = \operatorname{card} F$. Soit $f : E \to \mathbf{N}_n$ et $g : F \to \mathbf{N}_m$ des bijections et soit $i : E \to F$. L'inclusion de E dans F. Alors l'application $h = g \circ (i \circ f^{-1}) : \mathbf{N}_n \to \mathbf{N}_m$ est une injection et donc $n \leq m$.

On suppose que $E \neq F$. Il existe $x \in F \setminus E$. On considère l'application $k = \sigma^{\mathbf{N}_m}_{g(x)m-1} \circ h$. C'est une injection et $k(\mathbf{N}_n) \subset \mathbf{N}_m \setminus \{m-1\} = \mathbf{N}_{m-1}$. Par conséquent $n \leq m-1$ et donc $n < m$. C'est pourquoi si $n = m$ alors $E = F$.

III.19. proposition *Soit E et F deux ensembles finis de même cardinal et soit $f : E \to F$. Si f est injective ou surjective alors f est une bijection.*

III.20. preuve Supposons que f soit injective. Alors la corestriction f' de f à $f(E)$ est une bijection. Par conséquent E et $f(E)$ ont même cardinal. Puisque E à même cardinal que F ceci implique que $f(E)$ est un sous-ensemble de l'ensemble fini F et qu'ils ont même cardinal. Ainsi $f(E) = F$ et f est bijective.

Supposons que f soit surjective. Alors il existe $g : F \to E$ telle que pour tout $y \in E$ $f \circ g(y) = y$. Ainsi g est injective entre deux ensembles finis de même cardinal. D'après la première partie de la démonstration g est une bijection. Puisque g est une bijection et que pour tout $y \in E$ $f \circ g(y) = y$, la fonction f est la réciproque de g. C'est donc une bijection.

III.21. proposition *Soit $n, m \in \mathbf{N}$. Soit E et F deux ensembles finis disjoints. Si E est de cardinal n et F de cardinal m alors $E \cup F$ est fini de cardinal $n + m$.*

III.22. preuve Soit $f : E \to \mathbf{N}_n$ et $g : F \to \mathbf{N}_m$ deux bijections. On considère l'application $h : E \cup F \to \mathbf{N}$ définie de la façon suivante. Si $x \in E$ alors $h(x) = f(x)$ et si $x \in F$ alors $h(x) = n + g(x)$.

Soit $x \in E \cup F$. Si $x \in E$ alors $h(x) = f(x) \leq n - 1 \leq n + m - 1$ et si $x \in F$ alors $0 \leq g(x) \leq m - 1$ donc $n \leq h(x) = n + g(x) \leq n + m - 1$. Ainsi $h(E \cup F) \subset \mathbf{N}_{n+m}$, $h(E) \subset \mathbf{N}_n$ et $h(F) \subset \mathbf{N}_{n+m} \setminus \mathbf{N}_n$. La corestriction $j : E \cup F \to \mathbf{N}_{n+m}$ de h à $\mathbf{N}_{n+m}$ est bien définie.

Soit $k \in \mathbf{N}_{n+m}$. Si $k \in \mathbf{N}_n$ alors $x = f^{-1}(k)$ vérifie $j(x) = f(x) = k$. Si $k \in \mathbf{N}_{n+m} \setminus \mathbf{N}_n$ alors il existe $l \in \mathbf{N}$ tel que $n + l = k$. Puisque $k \leq n + m - 1$ on a $l \leq m - 1$, c'est à dire $l \in \mathbf{N}_m$. Alors $x = g^{-1}(l)$ vérifie $j(x) = g(x) = k$. L'application j est surjective.

Soit $x, x' \in E \cup F$ tels que $j(x) = j(x')$. Puisque $h(E) \subset \mathbf{N}_n$ et $h(F) \subset \mathbf{N}_{n+m} \setminus \mathbf{N}_n$ nécessairement $x, x' \in E$ ou $x, x' \in F$. Si $x, x' \in E$ alors $f(x) = j(x) = j(x') = f'(x')$ et donc $x = x'$. Si $x, x' \in F$ alors $n + f(x) = j(x) = j(x') = n + f'(x')$, d'où $f(x) = f(x')$ et donc $x = x'$. L'application j est injective.

On vient de montrer l'existence d'une bijection de $E \cup F$ dans $\mathbf{N}_{n+m}$. Par conséquent $E \cup F$ est fini de cardinal $n + m$.

III.23. corollaire *Soit E et F deux ensembles finis. Alors $E \cap F$, $E \setminus F$ et $E \cup F$ sont finis.*

III.24. preuve Puisque E est fini et que $E \cap F$ et $E \setminus F$ sont inclus dans E ils sont finis. Les ensembles $E \setminus F$ et F sont finis et leur intersection est vide. Par conséquent leur réunion qui est égale à E est finie.

III.25. corollaire *Soit E et F deux ensembles finis. Alors*

$$\operatorname{card}(E \cup F) = \operatorname{card} E + \operatorname{card} F - \operatorname{card}(E \cap F).$$

III.26. preuve Puisque E et $F \setminus E$ sont disjoints et que $E \cup F = E \cup (F \setminus E)$ on a

$$\operatorname{card}(E \cup F) = \operatorname{card} E + \operatorname{card}(F \setminus E).$$

De même, puisque $E \cap F$ et $F \setminus E$ sont disjoints et que $F = (E \cap F) \cup (F \setminus E)$ on a $\operatorname{card} F = \operatorname{card}(E \cap F) + \operatorname{card}(F \setminus F)$ c'est à dire

$$\operatorname{card}(F \setminus F) = \operatorname{card} F - \operatorname{card}(E \cap F).$$

En combinant ces égalités on obtient

$$\begin{aligned} \operatorname{card}(E \cup F) &= \operatorname{card} E + \operatorname{card}(F \setminus E) \\ &= \operatorname{card} E + \operatorname{card} F - \operatorname{card}(F \setminus E). \end{aligned}$$

III.27. corollaire *Soit E et F deux ensembles finis. Alors* $\operatorname{card}(E \cup F) \leq \operatorname{card} E + \operatorname{card} F$, *l'égalité n'ayant lieu que si E et F sont disjoints.*

III.28. preuve C'est une conséquence immédiate de l'égalité

$$\operatorname{card}(E \cup F) = \operatorname{card} E + \operatorname{card} F - \operatorname{card}(E \cap F)$$

et du fait que $0 < \operatorname{card}(E \cap F)$ sauf si E et F sont disjoints.

III.29. proposition *Soit $n, m \in \mathbf{N}$. Soit E et F deux ensembles finis. Si E est de cardinal n et F de cardinal m alors $E \times F$ est fini de cardinal $n \times m$.*

III.30. preuve On prouve par récurrence sur $m \in \mathbf{N}$ la propriété P_m suivante : *si $n \in \mathbf{N}$, si E et F sont des ensembles finis, et E est de cardinal n et F de cardinal m alors $E \times F$ est fini de cardinal $n \times m$.*

Le cas $m = 0$. Le seul ensemble de cardinal 0 est l'ensemble vide et $E \times \emptyset = \emptyset$ quelque soit l'ensemble E.

Soit $m \in \mathbf{N}$ tel que P_m est vraie. Soit $n \in \mathbf{N}$, E un ensemble fini de cardinal n et F un ensemble fini de cardinal $m + 1$. Puisque $0 < m + 1$ l'ensemble F est non vide. Soit $f \in F$. On pose $F' = F \setminus \{f\}$. Les ensembles F' et $\{f\}$ sont des sous-ensembles de l'ensemble F qui est fini. Ils sont donc eux même finis. Le cardinal du singleton $\{f\}$ est 1. Notons m' le cardinal de F'. Puisque $F' \cup \{f\} = F$ et que $F' \cap \{f\} = \emptyset$ on a $m' + 1 = m + 1$ et donc $m' = m$.

D'après P_m supposée vraie le cardinal de $E \times F'$ est $n \times m$. L'ensemble $E \times \{f\}$ est le graphe de l'application définie sur E constante égale à f. Il est en bijection avec l'ensemble fini E. Par conséquent son cardinal est celui de E c'est à dire n.

Or l'ensemble $E \times F$ est la réunion des deux ensembles finis $E \times F'$ et $E \times \{f\}$. De plus $(E \times F') \cap (E \times \{f\}) = \emptyset$. Par conséquent $E \times F$ est fini et son cardinal est la somme du cardinal de $E \times F'$ et du cardinal de $E \times \{f\}$ c'est à dire $(n \times m) + n$. Puisque $\times$ est distributive par rapport à $+$ on a $(n \times m) + n = n \times (m + 1)$. Ainsi le cardinal de $E \times F$ est $n \times (m + 1)$. Ceci prouve que si P_m est vraie alors P_{m+1} l'est aussi.

III.31. définition Un ensemble qui n'est pas fini est dit *infini.*

III.32. proposition *L'ensemble* $\mathbf{N}$ *est infini.*

III.33. preuve Supposons que $\mathbf{N}$ soit fini et soit n son cardinal. Puisque $\mathbf{N}_n \subset \mathbf{N}$ mais que $\mathbf{N}_n \neq \mathbf{N}$ le cardinal de $\mathbf{N}_n$ est strictement inférieur à celui de $\mathbf{N}$, c'est à dire $n < n$. Cette contradiction permet de conclure que $\mathbf{N}$ est infini.

III.34. remarque L'application s de $\mathbf{N}$ dans $\mathbf{N}$ qui a n associe son successeur $n+1$ est une injection mais ce n'est pas une surjection. L'application p de $\mathbf{N}$ dans $\mathbf{N}$ qui à 0 associe 0 et qui à $n \in \mathbf{N}$ différent de 0 associe $n-1$ est une surjection qui n'est pas une injection.

IV. Les entiers naturels vus par von Neuman et Peano

Dans la présentation précédente des entiers naturels le bon ordre est mis en avant avec le fait que tout sous-ensemble non vide et majoré admet un plus grand élément sans que les entiers naturels possèdent dans leur globalité un majorant. Avec ce point de vue, l'existence de successeurs et de prédécesseurs ainsi que le principe de récurrence sont des conséquences de ces axiomes. Plus précisément on a démontré que l'ensemble $\mathbf{N}$ des entiers naturels possède les propriétés suivantes.

0. Tout entier naturel n a un unique successeur noté $n+1$
   et le successeur de 0 est noté 1.
1. Deux entiers naturels ayant même successeur sont égaux.
2. Aucun entier naturel n'a lui-même ou 0 pour successeur.
3. Un sous-ensemble F de $\mathbf{N}$ contenant 0 est égal à $\mathbf{N}$
   s'il contient le successeur de chacun de ses éléments.

En revanche chez von Neuman et Peano le principe de récurrence et l'existence de successeurs font partie des axiomes mais pas l'existence d'un bon ordre tel que tout sous-ensemble non vide majoré admette un plus grans élément. Nous allons voir l'équivalence des deux points de vue.

IV.1. proposition *Soit (E, e, s) où E est un ensemble, e un élément de E et $s : E \to E$ une application vérifiant les conditions suivantes.*

1. L'application s est injective.

2. Si $x \in E$ alors $s(x) \neq x$ et $s(x) \neq e$.

3. Un sous-ensemble F de E contenant e est égal à E si $s(x) \in F$ pour tout $x \in F$.

Alors il existe un unique bon ordre sur E tel que E n'admet pas de majorant, tout sous-ensemble non vide et majoré de E admet un plus grand élément et pour tout $x \in E$ $s(x)$ est le plus petit des majorants de x et différents de x. Pour cet ordre e est le plus petit élément de E.

IV.2. preuve Si $x \in E$ on considère la propriété P_x suivante :

Il existe un sous-ensemble E_x et une famille de sous-ensembles $(E_x^y)_{y\in E_x}$ vérifiant :
1. e et x appartiennent à $E_x = E_x^x$,
2. $E_x^e = \{e\}$ et si $y \in E_x$ alors $y \in E_x^y$,
3. si $y, y' \in E_x$ et $y \neq y'$ alors $E_x^y \subset E_x^{y'} \setminus \{y'\}$ ou $E_x^{y'} \subset E_x^y \setminus \{y\}$,
4. si $y \in E_x$ et $y \neq x$ alors $s(y) \in E_x \setminus E_x^y$ et $E_x^{s(y)} = E_x^y \cup \{s(y)\}$,
5. si $y \in E_x$ et $y \neq e$ il existe $y' \in E_x^y$ tel que $s(y') = y$.

Montrons que P_x est vraie si $x \in E$. Soit P le sous-ensemble des $x \in E$ tels que P_x soit vraie. Il suffit de montrer que $P = E$. Ce sous-ensemble contient e (P_e est vraie) : on a $E_e = \{e\} = E_e^e$. Soit $x \in E$. Supposons que $x \in P$ c'est à dire que P_x soit vraie. Soit E_x et $(E_x^y)_{y\in E_x}$ donnés par P_x. Supposons que $s(x) = y \in E_x$. Puisque $E_x^x = E_x$ contient strictement $E_x^y \setminus \{y\}$ on a $E_x^y \subset E_x^x \setminus \{x\}$. Par hypothèse sur s, $s(x) \neq e$. Il existe donc $y' \in E_x^y$ tel que $s(y') = y$. Or x est l'unique antécédent par s de $s(x)$ car s est injective. Donc $y' = x$ et $y' \in E_x^y \subset E_x \setminus \{x\}$. Cette contradiction implique que $s(x) \notin E_x$. On pose $E_{s(x)} = E_x \cup \{s(x)\} = E_{s(x)}^{s(x)}$ et pour $y \in E_{s(x)} \setminus \{s(x)\}$ c'est à dire pour $y \in E_x$ on pose $E_{s(x)}^y = E_x^y$. On a bien $s(x) \notin E_x = E_{s(x)}^x$ et $E_{s(x)}^{s(x)} = E_{s(x)}^x \cup \{s(x)\}$. Puisque $E_{s(x)}^y = E_x^y$ si $y \in E_x$ il résulte de P_x

1. e et $s(x)$ appartiennent à $E_{s(x)} = E_{s(x)}^{s(x)}$,
2. $E_{s(x)}^e = \{e\}$ et si $y \in E_x$ alors $y \in E_{s(x)}^y$,
3. si $y, y' \in E_{s(x)}$ et $y \neq y'$ alors $E_{s(x)}^y \subset E_{s(x)}^{y'} \setminus \{y'\}$ ou $E_{s(x)}^{y'} \subset E_{s(x)}^y \setminus \{y\}$,
4. si $y \in E_{s(x)}$ et $y \neq s(x)$ alors $s(y) \in E_{s(x)} \setminus E_{s(x)}^y$ et $E_{s(x)}^{s(y)} = E_{s(x)}^y \cup \{s(y)\}$,
5. si $y \in E_{s(x)}$ et $y \neq e$ il existe $y' \in E_{s(x)}^y$ tel que $s(y') = y$.

Ainsi $P_{s(x)}$ est vraie dès que P_x est vraie, c'est à dire $s(x) \in P$ dès que $x \in P$. Puisqu'on a vérifié également que P_e est vraie c'est à dire que $e \in P$. Ceci implique que $P = E$ c'est à dire que pour tout x dans E la propriété P_x est vraie.

Montrons que pour chaque $x \in E$ le sous-ensemble E_x et la famille $(E_x^y)_{x\in E}$ sont uniques (propriété U_x). Il suffit de considérer le sous-ensemble U des x de E tels que le sous-ensemble E_x et la famille $(E_x^y)_{x\in E}$ sont uniques et de montrer que $U = E$. Ce sous-ensemble contient e puisque nécessairement $E_e = E_e^e = \{e\}$ (U_e est vraie). Soit $x \in E$. Supposons que $x \in U$ et considérons $E_{s(x)}$ et $(E_{s(x)}^y)_{y\in E_{s(x)}}$ qui vérifient $P_{s(x)}$. On a $E_{s(x)}^x = E_{s(x)} \setminus \{s(x)\}$. Si $y \in E_{s(x)} \setminus \{x, s(x)\}$ alors $E_{s(x)}^y \subset E_{s(x)} = E_{s(x)}^{s(x)}$ et donc d'après la condition 3.

$E^y_{s(x)} \subset E^{s(x)}_{s(x)} \setminus \{s(x)\} = E^x_{s(x)}$. Puisque $x \neq y$ il vient encore d'après la condition 3. $E^y_{s(x)} \subset E^x_{s(x)} \setminus \{x\}$. Par conséquent l'ensemble $E^x_{s(x)} = E_{s(x)} \setminus \{s(x)\}$ et la famille $(E^y_{s(x)})_{y \in E_{s(x)} \setminus \{s(x)\}}$ vérifient P_x. L'hypothèse d'unicité U_x implique que $E_{s(x)} \setminus \{s(x)\} = E_x$ et que $E^y_{s(x)} = E^y_x$ si $y \in E_{s(x)} \setminus \{s(x)\} = E_x$. On en déduit que $E^{s(x)}_{s(x)} = E_{s(x)}$ est nécessairement égal à $E_x \cup \{s(x)\}$. Ceci prouve que $U_{s(x)}$ est vraie si U_x est vraie, c'est à dire que $s(x) \in U$ dès que $x \in U$. Puisque $e \in U$ on peut donc conclure que $U = E$.

Montrons que pour chaque $x \in E$ on a $E^y_x = E_y$ si $y \in E_x$ (propriété T_x). Il suffit de considérer le sous-ensemble T des x de E tels que $E^y_x = E_y$ si $y \in E_x$ et de montrer que $T = E$. Ce sous-ensemble contient e puisque $E_e = E^e_e = \{e\}$ (T_e est vraie). Soit $x \in E$. Supposons que $x \in T$ et considérons $E_{s(x)}$ $(E^y_{s(x)})_{y \in E_{s(x)}}$ donnés par $P_{s(x)}$. On a bien $E^{s(x)}_{s(x)} = E_{s(x)}$. De plus, l'ensemble $E_{s(x)} \setminus \{s(x)\}$ et la famille $(E^y_{s(x)})_{y \in E_{s(x)} \setminus \{s(x)\}}$ vérifient P_x. L'hypothès d'unicité U_x implique que $E_{s(x)} \setminus \{s(x)\} = E_x$ et que $E^y_{s(x)} = E^y_x$ si $y \in E_{s(x)} \setminus \{s(x)\} = E_x$. Puisque T_x est supposée vraie, on en déduit que si $y \in E^{s(x)}_{s(x)} = E_{s(x)}$ est différent de $s(x)$ (i.e si $y \in E_x$) alors $E^y_{s(x)} = E^y_x = E_y$. Ainsi $T_{s(x)}$ est vraie dès que T_x est vraie, c'est à dire $s(x) \in T$ si $x \in T$. Puisque T_e est vraie ($e \in T$) ceci prouve que T_x est vraie pour tout $x \in E : T = E$.

Montrons que tout $x \in E$ vérifie la propriété O_x suivante : si $y \in E$ est différent de x alors $E_x \neq E_y$ et $E_x \subset E_y$ ou $E_y \subset E_x$. Il suffit de considérer le sous-ensemble O des x de E tels que O_x soit vraie et de montrer que $O = E$. Ce sous-ensemble contient e. En effet $E_e = \{e\}$ et si $y \in E$ est différent de e alors e et y appartiennent à E_y donc $E_e \neq E_y$ et $E_e \subset E_y$. Supposons que $x \in O$ et considérons $y \in E$. Si $y \in E_x$ alors $E_y \subset E_x$. Puisque $E_x = E^x_{s(x)} = E_{s(x)} \setminus \{s(x)\}$ on a $E_y \subset E_{s(x)}$ et $E_y \neq E_{s(x)}$. Si $y \notin E_x$ alors $x \neq y$ et, puisque O_x est supposée vraie, $E_x \subset E_y$ et $E_x \neq E_y$. Puisque $x \neq y$, on a $s(x) \in E_y$ et $E_{s(x)} = E^{s(x)}_y \subset E_y$. De plus si $s(x) \neq y$ alors $s(s(x)) \in E^{s(s(x))}_y \setminus E^{s(x)}_y \subset E_y \setminus E^{s(x)}_y = E_y \setminus E_{s(x)}$: ainsi $E_{s(x)} \neq E_y$. Finalement on vient de prouver que si $x \in O$ alors $s(x) \in O$. Puisque $e \in O$ on en déduit que $O = E$.

Si x et y dans E on dit que $x \leq y$ si $E_x \subset E_y$, ce qui est équivalent à $x \subset y$. On vient de montrer que $\leq$ est une relation d'ordre total qui admet e comme plus petit élément de E.

Si $x \in E$ ses majorants sont les $y \in E$ tels que $E_x \subset E_y$ c'est à dire les $y \in E$ tels que $x \in E_y$ d'après T_y. De plus, d'après ce qui précède, si $E_x \subset E_y$ et $x \neq y$ alors $E_x \subset E_{s(x)} \subset E_y$ et $E_x \neq E_{s(x)}$. Par conséquent $s(x)$ est bien le plus petit des majorants de x et différents de x.

Si $x \in E$ on note B_x la propriété suivante : tout sous-ensemble de E qui contient un élément inférieur ou égal à x admet un plus petit élément et tout sous ensemble de E majoré par x admet un plus grand élément. Il suffit de considérer le sous-ensemble B des x de E tels que B_x soit vraie et de montrer que $B = E$. La propriété B_e est vraie et $e \in B$ car $E_e = \{e\}$ et e est le plus petit élément de E. Soit $x \in E$. On suppose que la propriété B_x est vraie c'est à dire que $x \in B$. On considère des sous-ensembles Y et Z de E tels que Y contienne un élément $y \leq s(x)$ et Z soit majoré par $s(x)$. On considère $Y' = Y \cup \{x\}$. Puisque B_x est vraie et que $x \in Y'$, Y' possède un plus petit élément noté y_m : on a $y_m \leq x$. Si $y_m \in Y$ alors c'est le plus petit élément de Y. Si $y_m \notin Y$ alors $y_m = x$ et alors aucun élément de E_x n'appartient à Y et $s(x)$ est le plus petit élément de Y. Si $s(x) \in Z$ alors $s(x)$ est le plus grand élément de Z. Sinon $Z \subset E_x$ et puisque B_x est supposée vraie, Z possède un plus grand élément. On vient de prouver que $B_{s(x)}$ est vraie dès que B_x est vraie. Or B_e est vraie. Par conséquent B_x est vraie pour tout $x \in E$. Ceci signifie que $\leq$ est un bon ordre sur E et que tout sous-ensemble non vide et majoré de E admet un plus grand élément.

Pour cet ordre l'ensemble E n'est pas majoré car tout $x \in E$ est tel que $x \leq s(x)$ et $x \neq s(x)$.

Il reste à montrer que $\leq$ est l'unique ordre sur E pour lequel E n'admet pas de majorant, tout sous-ensemble non vide et majoré de E admet un plus grand élément et pour tout $x \in E$ $s(x)$ est le plus petit des majorants de x et différents de x. Soit $\leq'$ un ordre sur e tel que E n'admet pas de majorant, tout sous-ensemble non vide et majoré de E admet un plus grand élément et pour tout $x \in E$ $s(x)$ est le plus petit des majorants de x et différents de x. Supposons que l'ensemble M des $(x, y) \in E \times E$ tels que $x \neq y$, $x \leq y$ et $y \leq' x$ soit non vide. Soit $(x_0, y_0) \in M$. On note $\mathcal{M}$ l'ensemble des $y \in E$ tels que $(x_0, y) \in M$. Ce sous-ensemble de E est non vide car $(x_0, y_0) \in M$. Soit y_m le plus petit élément de $\mathcal{M}$ pour (pour $\leq$). Puisque $x_0 \neq y_m$ et $x_0 \leq y_m$ nécessairement $y_m \neq e$ et il existe $y' \in E$ tel que $s(y') = y_m$. On a donc $y' \leq' s(y') = y_m$ mais aussi $y' \notin M_1$. Deux cas se présentent a priori. Le cas $x_0 = y'$ est à exclure car il impliquerait $x_0 = y' \leq' s(y') = y_m$ et $x_0 = y' \neq s(y') = y_m$. Ce qui est contraire au fait que $y_m \in \mathcal{M}$. Le second cas est celui $x_0 \neq y'$. Puisque $y_m = s(y')$ est le plus petit des majorants de y' pour $\leq$ et que $x_0 \leq y_m$ et $x_0 \neq y_m$ nécessairement $x_0 \leq y'$ et $x_0 \neq y'$. Ceci, combiné à $y' \notin \mathcal{M}$ implique $x_0 \neq y'$ et $x_0 \leq' y'$. Or $y' \leq' s(y') = y_m$. Par conséquent par transitivité de l'ordre $x_0 \leq' y_m$. Comme $x_0 \neq y_m$ et $x_0 \leq y_m$

on a donc $(x_0, y_m) \notin M$. C'est contraire à l'hypothèse de départ. Ainsi M est vide et pour tout $(x, y) \in E \times E$ on a $x \leq' y'$ dès que $x \leq y$. Les ordres $\leq$ et $\leq'$ sont donc les mêmes.

Pour conclure on fait le lien avec l'axiome 7 (l'axiome de l'infini) du chapitre de théorie des ensembles avec les entiers naturels.

IV.3. proposition *Il existe un triplet (E, e, s) où E est un ensemble, e un élément de E et $s : E \to E$ une application vérifiant les conditions suivantes.*

1. L'application s est injective.

2. Si $x \in E$ alors $s(x) \neq x$ et $s(x) \neq e$.

3. Un sous-ensemble F de E contenant e est égal à E si $s(x) \in F$ pour tout $x \in F$.

IV.4. preuve D'après l'axiome 7 il existe un ensemble $\mathbf{E}$ dont l'ensemble vide $\emptyset$ est un élément et tel que si $x \in \mathbf{E}$ alors $x \cup \{x\} \in \mathbf{E}$. On note s l'application de $\mathbf{E}$ dans $\mathbf{E}$ qui à $x \in \mathbf{E}$ associe $s(x) = x \cup \{x\}$. L'application s est clairement injective d'après l'axiome 9. On considère le sous-ensemble $\mathcal{E}$ de l'ensemble des parties de $\mathbf{E}$ formé des sous-ensembles de $\mathbf{E}$ qui vérifient comme $\mathbf{E}$ les conditions de l'axiome 7 : si $E' \in \mathcal{E}$ alors $\emptyset \in E'$ et pour tout $x \in E'$, on a $s(x) \in E'$. On note E l'intersection de tous les sous-ensembles de $\mathbf{E}$ qui sont des éléments de $\mathcal{E}$. Puisque $\emptyset$ est dans tous les ensembles qui sont des éléments de $\mathcal{E}$ il est également élément de l'intersection E de ces ensembles. Si $x \in E$ alors x et $s(x)$ appartiennent à tous les ensembles qui sont des éléments de $\mathcal{E}$: par conséquent $s(x)$ est également élément de l'intersection E de ces ensembles. Ainsi E appartient à $\mathcal{E}$ et vérifie les deux premières conditions. Un sous-ensemble F de E qui contient e et qui est tel que $s(x) \in F$ si $x \in F$ est également dans $\mathcal{E}$ et par conséquent E est inclus dans F. Cette double inclusion implique que $E = F$: l'ensemble E vérifie donc la troisième propriété.

repères bibliographiques

- Jean-Louis Krivine, Théorie des ensembles
- E. Ramis, C. Deschamps et J. Odoux, Cours de mathématiques spéciales
- Gilbert Lelièvre, Aperçu de la théorie axiomatique des ensembles, appendice à Compléments d'Analyse dans les Cahiers de Fontenay
- Wikipédia, Théorie axiomatique des ensembles - Axiomes de Peano - Construction des entiers naturels