Ensembles finis
Opérations algébriques
Division euclidienne
Écriture des entiers naturels

(version provisoire du 14 juin 2008)

Jean-Marie Lion
Université de Rennes 1

I. Ensembles finis

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

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

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

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

I.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.

I.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.

I.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*

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

I.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* $n \leq m$.

I.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.

I.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 $m = n$.*

I.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 $m = n$.

I.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 $\operatorname{card} E$.

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

I.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.

I.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.*

I.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 $n = m$.

I.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 $E = F$.*

I.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 $E = F$.

I.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.*

I.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.

I.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 $n + m$.*

I.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 $n + m$.

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

I.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.

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

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

I.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

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

I.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.*

I.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.

I.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 $n \times m$.*

I.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.

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

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

I.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.

I.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.

II. Opérations sur les suites à valeurs dans un ensemble muni d'une loi

On considère dans cette partie un ensemble E.

II.1. notation On note $E^{\mathbf{N}}$ l'ensemble des suites à valeurs dans E. Si $u \in E^{\mathbf{N}}$ et $n \in \mathbf{N}$ on note u_n l'image de n par la suite. C'est *le n-ème terme de la suite*.

II.2. notation Soit $n \in \mathbf{N}$. Les éléments de $E^{\mathbf{N}_n}$ sont appelés *n-uplets* d'éléments de E. Si $u \in E^{\mathbf{N}_n}$ et si $i \in \mathbf{N}_n$ on note u_i l'image $u(i)$ de i par u.

On suppose que E est muni d'une loi $\top$.

II.3. définition L'ensemble

$$\mathcal{G} = \{(u,v,w) \in (E^{\mathbf{N}})^3 : \forall n \in \mathbf{N}\ u_n \top v_n = w_n\}$$

est le graphe d'une loi définie sur $E^{\mathbf{N}}$ notée également $\top$. Si $u, v, w \in E^{\mathbf{N}}$ sont telles que $u \top v = w$ alors $u_n \top v_n = w_n$ si $n \in \mathbf{N}$.

II.4. remarque Si $u, v \in E^{\mathbf{N}}$ alors $u \top v$ est la composée (u,v) (qui est application de $\mathbf{N}$ dans E^2) suivie de $\top$.

II.5. définition L'ensemble

$$\mathcal{S} = \{(u,v) \in (E^{\mathbf{N}})^2 : \forall n \in \mathbf{N}\ v_n = u_{n+1}\}$$

est le graphe d'une application de $E^{\mathbf{N}}$ dans lui -même qui est appelée *décalage des indices* ou *translation* ou encore *shift*. Si $(u,v) \in \mathcal{S}$ et $n \in \mathbf{N}$ alors $v_n = u_{n+1}$ et on pose $v = u^{\mathcal{S}}$. Si $l \in \mathbf{N}$ on note $u^{\mathcal{S}_l}$ le l-ème terme de la suite récurrente de premier terme u associée à la translation. Si $u \in E^{\mathbf{N}}$ alors $u^{\mathcal{S}}$ est la composée $n \in \mathbf{N} \mapsto n+1$ suivie de la suite u. Si $l \in \mathbf{N}$ alors la suite $u^{\mathcal{S}_l}$ est la composée $n \in \mathbf{N} \mapsto n+l$ suivie de la suite u. On a $u^{\mathcal{S}_l}_k = u_{l+k}$ si $l, k \in \mathbf{N}$.

II.6. définition L'ensemble

$$\mathcal{P} = \{(u, v) \in (E^{\mathbf{N}})^2 : v_0 = u_0 \top u_1,\ \forall n \in \mathbf{N} \setminus \{0\}\ v_n = u_{n+1}\}$$

est le graphe d'une application θ de $E^{\mathbf{N}}$ dans lui-même. Soit $u \in E^{\mathbf{N}}$ et soit $(\theta(u)^k)_{k\in\mathbf{N}}$ la suite récurrente de premier terme u associée à θ. Si $k \in \mathbf{N}$ alors $\theta(u)^k$ est une suite d'éléments de E. On pose

$$\overset{k}{\underset{i=0}{\top}} u_i = \theta(u)_0^k.$$

II.7. proposition *Si $k \in \mathbf{N}$ et $n \in \mathbf{N} \setminus \{0\}$ alors $\theta(u)_n^k = u_{n+k}$.*

II.8. preuve Si $k \in \mathbf{N}$ on note P_k la propriété : *si $n \in \mathbf{N} \setminus \{0\}$ alors* $\theta(u)_n^k = u_{n+k}$. On va montrer que pour tout $k \in \mathbf{N}$ P_k est vraie.

On a $\theta(u)^0 = u$ donc si $n \in \mathbf{N} \setminus \{0\}$ alors $\theta(u)_n^0 = u_n = u_{n+0}$ et P_0 est vraie.

Soit $k \in \mathbf{N}$ tel que P_k soit vraie. Soit $n \in \mathbf{N} \setminus \{0\}$. On a $\theta(u)_n^k = u_{n+k}$. Puisque $\theta(u)^{k+1} = \theta(\theta(u)^k)$ on a $\theta(u)_n^{k+1} = \theta(u)_{n+1}^k = u_{(n+1)+k} = u_{n+(k+1)}$. Ainsi P_{k+1} est vraie si P_k l'est.

II.9. proposition *On a $\overset{0}{\underset{i=0}{\top}} u_i = u_0$ et si $k \in \mathbf{N}$ alors $\overset{k+1}{\underset{i=0}{\top}} u_i = (\overset{k}{\underset{i=0}{\top}} u_i) \top u_{k+1}$.*

II.10. preuve Par définition $\overset{0}{\underset{i=0}{\top}} u_i = \theta(u)_0^0$. Or $\theta(u)^0 = u$. Donc $\overset{0}{\underset{i=0}{\top}} u_i = u_0$.

Si $k \in \mathbf{N}$ alors $\overset{k}{\underset{i=0}{\top}} u_i = \theta(u)_0^k$ et

$$\begin{aligned}
\overset{k+1}{\underset{i=0}{\top}} u_i &= \theta(u)_0^{k+1} \\
&= \theta(u)_0^k \top \theta(u)_1^k \\
&= (\overset{k}{\underset{i=0}{\top}} u_i) \top u_{1+k} \\
&= (\overset{k}{\underset{i=0}{\top}} u_i) \top u_{k+1}.
\end{aligned}$$

II.11. proposition *Soit $k \in \mathbf{N}$ et $u, v \in E^{\mathbf{N}}$ tels que pour tout $i \in \mathbf{N}$ inférieur ou égal à k on a $u_i = v_i$. Alors*

$$\overset{k}{\underset{i=0}{\top}} u_i = \overset{k}{\underset{i=l}{\top}} v_i.$$

II.12. preuve On va prouver par récurrence sur $k \in \mathbf{N}$ la propriété P_k suivante : *si* $u, v \in E^{\mathbf{N}}$ *sont tels que pour tout* $i \in \mathbf{N}$ *inférieur ou égal à* k *on a* $u_i = v_i$ *alors* $\overset{k}{\underset{i=0}{\top}} u_i = \overset{k}{\underset{i=l}{\top}} v_i$.

La propriété P_0 est vraie car si $u, v \in E^{\mathbf{N}}$ sont tels que $u_0 = v_0$ alors $\overset{0}{\underset{i=0}{\top}} u_i = u_0 = v_0 = \overset{0}{\underset{i=l}{\top}} v_i$.

Soit $k \in \mathbf{N}$ tel que P_k soit vraie. Soit $u, v \in E^{\mathbf{N}}$ sont tels que pour tout $i \in \mathbf{N}$ inférieur ou égal à $k+1$ on a $u_i = v_i$. D'après P_k on a $\overset{k}{\underset{i=0}{\top}} u_i = \overset{k}{\underset{i=l}{\top}} v_i$. Par conséquent

$$\begin{aligned} \overset{k+1}{\underset{i=0}{\top}} u_i &= (\overset{k}{\underset{i=0}{\top}} u_i) \top u_{k+1} \\ &= (\overset{k}{\underset{i=0}{\top}} v_i) \top v_{k+1} \\ &= \overset{k+1}{\underset{i=0}{\top}} v_i. \end{aligned}$$

II.13. définition Soit $k \in \mathbf{N} \setminus \{0\}$ et $u \in E^{\mathbf{N}_k}$. D'après la proposition précédente il existe $V \in E$ tel que $V = \overset{k-1}{\underset{i=0}{\top}} u_i$ quelque soit le prolongement u de v à $\mathbf{N}$. Ce nombre est noté $\overset{k-1}{\underset{i=0}{\top}} v_i$.

II.14. définition Si $l, k, h \in \mathbf{N}$ et si $u \in E^{\mathbf{N}}$ ou si $u \in E^{\mathbf{N}_h}$ avec $l+k+1 \leq h$ on pose

$$\overset{l+k}{\underset{i=l}{\top}} u_i = \theta(u^{\mathcal{S}_l})_0^k = \overset{k}{\underset{i=0}{\top}} u_{l+i}.$$

II.15. corollaire *Soit* $l, k, h \in \mathbf{N}$ *et* $u, v \in E^{\mathbf{N}}$ *ou* $u, v \in E^{\mathbf{N}_h}$ *avec* $l+k+1 \leq h$. *Si pour tout* $i \in \mathbf{N}_h$ *tel que* $l \leq i \leq l+k$ *alors*

$$\overset{l+k}{\underset{i=l}{\top}} u_i = \overset{l+k}{\underset{i=l}{\top}} v_i.$$

II.16. proposition *Supposons qu'il existe une seconde loi* $\perp$ *qui est distributive par rapport à* $\top$. *Soit* $v \in E$ *et* $u \in E^{\mathbf{N}}$. *Soit* $w \in E^{\mathbf{N}}$ *définie par* $w_i = v \perp u_i$ *si* $i \in \mathbf{N}$. *Si* $k \in \mathbf{N}$ *alors* $v \perp (\overset{k}{\underset{i=0}{\top}} u_i) = \overset{k}{\underset{i=0}{\top}} w_i$ *c'est à dire* $v \perp (\overset{k}{\underset{i=0}{\top}} u_i) = \overset{k}{\underset{i=0}{\top}} v \perp u_i$

II.17. preuve On raisonne par récurrence sur $k \in \mathbf{N}$.

Si $k=0$ on a $v \times (\overset{0}{\underset{i=0}{\top}} u_i) = v \bot u_0 = w_0 \overset{0}{\underset{i=0}{\top}} w_i$.

Soit $k \in \mathbf{N}$. On suppose que $v \bot (\overset{k}{\underset{i=0}{\top}} u_i) = \overset{k}{\underset{i=0}{\top}} w_i$. Alors

$$\begin{aligned} v \bot (\overset{k+1}{\underset{i=0}{\top}} u_i) &= v \bot ((\overset{k}{\underset{i=0}{\top}} u_i) \top u_{k+1}) \\ &= (v \bot (\overset{k}{\underset{i=0}{\top}} u_i)) \top (v \bot u_{k+1}) \\ &= (\overset{k}{\underset{i=0}{\top}} w_i) \top w_{k+1} \\ &= \overset{k+1}{\underset{i=0}{\top}} w_i. \end{aligned}$$

II.18. corollaire *Supposons qu'il existe une seconde loi $\bot$ qui est distributive par rapport à $\top$. Soit $v \in E$, $k \in \mathbf{N}$ et $u \in E^{\mathbf{N}_k}$. Soit $w \in E^{\mathbf{N}_k}$ définie par $w_i = v \bot u_i$ si $i \in \mathbf{N}_k$. Aalors $v \bot (\overset{k}{\underset{i=0}{\top}} u_i) = \overset{k}{\underset{i=0}{\top}} w_i$ c'est à dire $v \bot (\overset{k}{\underset{i=0}{\top}} u_i) = \overset{k}{\underset{i=0}{\top}} v \bot u_i$*

II.19. proposition *Si $\top$ admet un neutre e et si u est la suite constante égale à e alors pour tout $k \in \mathbf{N}$ on a $\overset{k}{\underset{i=0}{\top}} u_i = e$.*

II.20. preuve On raisonne par récurrence. Si $k=0$ alors on a $u_0 = e$ et $\overset{0}{\underset{i=0}{\top}} u_i = u_0 = e$. Soit $k \in \mathbf{N}$ tel que $\overset{k}{\underset{i=0}{\top}} u_i = e$. Puisque $u_{k+1} = e$ on a $\overset{k+1}{\underset{i=0}{\top}} u_i = (\overset{k}{\underset{i=0}{\top}} u_i) \top u_{k+1} = e \top e = e$.

II.21. proposition *Si $\top$ est associative alors pour $u \in E^{\mathbf{N}}$ $l, k \in \mathbf{N}$ on a*

$$\overset{l+k+1}{\underset{i=0}{\top}} u_i = (\overset{l}{\underset{i=0}{\top}} u_i) \top (\overset{l+k+1}{\underset{i=l+1}{\top}} u_i).$$

II.22. preuve On va prouver par récurrence sur $k \in \mathbf{N}$ la propriété P_k suivante : *pour $u \in E^{\mathbf{N}}$ $l \in \mathbf{N}$ on a*

$$\overset{l+k+1}{\underset{i=0}{\top}} u_i = (\overset{l}{\underset{i=0}{\top}} u_i) \top (\overset{l+k+1}{\underset{i=l+1}{\top}} u_i).$$

La propriété P_0 est vraie car $\overset{l+1}{\underset{i=l+1}{\top}} u_i = \overset{0}{\underset{i=0}{\top}} u_{l+1+i} = u_{l+1}$.

Soit $k \in \mathbf{N}$ tel que P_k soit vraie. Si $u \in E^{\mathbf{N}}$ on a

$$\begin{aligned}
(\overset{l}{\underset{i=0}{\top}} u_i)\top(\overset{l+k+2}{\underset{i=l+1}{\top}} u_i) &= (\overset{l}{\underset{i=0}{\top}} u_i)\top((\overset{l+k+1}{\underset{i=l+1}{\top}} u_i)\top u_{l+k+2}) \\
&= ((\overset{l}{\underset{i=0}{\top}} u_i)\top(\overset{l+k+1}{\underset{i=l+1}{\top}} u_i))\top u_{l+k+2} \quad \text{associativité de } \top \\
&= (\overset{l+k+1}{\underset{i=0}{\top}} u_i)\top u_{l+k+2} \quad \text{hypothèse } P_k \\
&= \overset{l+k+2}{\underset{i=0}{\top}} u_i
\end{aligned}$$

et donc P_{k+1} est vraie si P_k l'est.

II.23. corollaire *Si $\top$ est associative alors pour tout $k, l \in \mathbf{N}$ et pour tout $v \in E^{\mathbf{N}_{l+k+2}}$ on a*

$$\overset{l+k+1}{\underset{i=0}{\top}} v_i = (\overset{l}{\underset{i=0}{\top}} v_i)\top(\overset{l+k+1}{\underset{i=l+1}{\top}} v_i).$$

II.24. proposition *On suppose $\top$ associative et commutative. Soit $u = (u_i)_{i\in\mathbf{N}}, v = (v_i)_{i\in\mathbf{N}} \in E^{\mathbf{N}}$, $w = u\top v = (w_i)_{i\in\mathbf{N}}$ et $k \in \mathbf{N}$. Alors on a*

$$\overset{k}{\underset{i=0}{\top}} w_i = (\overset{k}{\underset{i=0}{\top}} u_i)\top(\overset{k}{\underset{i=0}{\top}} v_i).$$

II.25. preuve On va prouver par récurrence sur $k \in \mathbf{N}$ la propriété P_k suivante : *si $u = (u_i)_{i\in\mathbf{N}}, v = (v_i)_{i\in\mathbf{N}} \in E^{\mathbf{N}}$, $w = u\top v = (w_i)_{i\in\mathbf{N}}$ alors*

$$\overset{k}{\underset{i=0}{\top}} w_i = (\overset{k}{\underset{i=0}{\top}} u_i)\top(\overset{k}{\underset{i=0}{\top}} v_i).$$

La propriété P_0 est vraie car $\overset{0}{\underset{i=0}{\top}} w_i = w_0 = u_0\top v_0 = (\overset{0}{\underset{i=0}{\top}} u_i)\top(\overset{0}{\underset{i=0}{\top}} v_i)$.

Soit $k \in \mathbf{N}$ tel que P_k soit vraie. Soit $u = (u_i)_{i\in\mathbf{N}}, v = (v_i)_{i\in\mathbf{N}} \in E^{\mathbf{N}}$, $w = u\top v = (w_i)_{i\in\mathbf{N}}$. On a

$$
\begin{aligned}
\overset{k+1}{\underset{i=0}{\top}} w_i &= (\overset{k}{\underset{i=0}{\top}} w_i)\top w_{k+1} \\
&= (\overset{k}{\underset{i=0}{\top}} w_i)\top(u_{k+1}\top v_{k+1}) \\
&= ((\overset{k}{\underset{i=0}{\top}} u_i)\top(\overset{k}{\underset{i=0}{\top}} v_i))\top(v_{k+1}\top u_{k+1}) \quad P_k \text{ et commutativité} \\
&= (((\overset{k}{\underset{i=0}{\top}} u_i)\top(\overset{k}{\underset{i=0}{\top}} v_i))\top v_{k+1})\top u_{k+1} \quad \text{associativité} \\
&= ((\overset{k}{\underset{i=0}{\top}} u_i)\top((\overset{k}{\underset{i=0}{\top}} v_i)\top v_{k+1}))\top u_{k+1} \quad \text{associativité} \\
&= ((\overset{k}{\underset{i=0}{\top}} u_i)\top(\overset{k+1}{\underset{i=0}{\top}} v_i))\top u_{k+1} \\
&= (\overset{k}{\underset{i=0}{\top}} u_i)\top((\overset{k+1}{\underset{i=0}{\top}} v_i)\top u_{k+1}) \quad \text{associativité} \\
&= (\overset{k}{\underset{i=0}{\top}} u_i)\top(u_{k+1}\top(\overset{k+1}{\underset{i=0}{\top}} v_i)) \quad \text{commutativité} \\
&= ((\overset{k}{\underset{i=0}{\top}} u_i)\top u_{k+1})\top(\overset{k+1}{\underset{i=0}{\top}} v_i) \quad \text{associativité} \\
&= (\overset{k+1}{\underset{i=0}{\top}} u_i)\top(\overset{k+1}{\underset{i=0}{\top}} v_i)
\end{aligned}
$$

et donc P_{k+1} est vraie si P_k l'est.

II.26. corollaire *On suppose* $\top$ *associative et commutative. Soit* $k \in \mathbf{N}$, $u = (u_i)_{i\in\mathbf{N}_k}, v = (v_i)_{i\in\mathbf{N}_k} \in E^{\mathbf{N}_k}$, $w = u + v = (w_i)_{i\in\mathbf{N}_k}$. *Alors on a*

$$\overset{k-1}{\underset{i=0}{\top}} w_i = (\overset{k-1}{\underset{i=0}{\top}} u_i)\top(\overset{k-1}{\underset{i=0}{\top}} v_i).$$

II.27. proposition *On suppose que* $\top$ *est associative et commutative. Soit* $k \in \mathbf{N} \setminus \{0,1,2\}$ *et* $l \in \mathbf{N}_k$ *différents de* $k-1$. *Si* $u \in E^{\mathbf{N}_k}$ *alors*

$$\overset{k-1}{\underset{i=0}{\top}} (u \circ \sigma_{l,l+1}^{\mathbf{N}_k})_i = \overset{k-1}{\underset{i=0}{\top}} u_i.$$

II.28. preuve Soit $i \in \mathbf{N}_k$. On a $(u \circ \sigma_{l,l+1}^{\mathbf{N}_k})_l = u_{l+1}$, $(u \circ \sigma_{l,l+1}^{\mathbf{N}_k})_{l+1} = u_l$ et $(u \circ \sigma_{l,l+1}^{\mathbf{N}_k})_i = u_i$ si $i \neq l, l+1$.

Par conséquent si $l = 0$

$$\begin{aligned}
\overset{k-1}{\underset{i=0}{\top}}(u \circ \sigma_{0,1}^{\mathbf{N}_k})_i &= ((u \circ \sigma_{0,1}^{\mathbf{N}_k})_0 \top (u \circ \sigma_{0,1}^{\mathbf{N}_k})_1) \top (\overset{k-1}{\underset{i=2}{\top}}(u \circ \sigma_{0,1}^{\mathbf{N}_k})_i) \quad \text{associativité} \\
&= (u_1 \top u_0) \top (\overset{k-1}{\underset{i=2}{\top}} u_i) \\
&= (u_0 \top u_1) \top (\overset{k-1}{\underset{i=2}{\top}} u_i) \quad \text{commutativité} \\
&= \overset{k-1}{\underset{i=0}{\top}} u_i \quad \text{associativité,}
\end{aligned}$$

si $l = k - 2$

$$\begin{aligned}
\overset{k-1}{\underset{i=0}{\top}}(u \circ \sigma_{0,1}^{\mathbf{N}_k})_i &= (\overset{k-3}{\underset{i=0}{\top}}(u \circ \sigma_{0,1}^{\mathbf{N}_k})_i) \top ((u \circ \sigma_{0,1}^{\mathbf{N}_k})_{k-2} \top (u \circ \sigma_{0,1}^{\mathbf{N}_k})_{k-1}) \quad \text{associativité} \\
&= (\overset{k-3}{\underset{i=0}{\top}} u_i) \top (u_{k-1} \top u_{k-2}) \\
&= (\overset{k-3}{\underset{i=0}{\top}} u_i) \top (u_{k-2} \top u_{k-1}) \quad \text{commutativité} \\
&= \overset{k-1}{\underset{i=0}{\top}} u_i \quad \text{associativité}
\end{aligned}$$

et si $l \neq 0, k-1$

$$\begin{aligned}
\overset{k-1}{\underset{i=0}{\top}}(u \circ \sigma_{0,1}^{\mathbf{N}_k})_i &= ((\overset{l-1}{\underset{i=0}{\top}}(u \circ \sigma_{0,1}^{\mathbf{N}_k})_i) \top ((u \circ \sigma_{0,1}^{\mathbf{N}_k})_l \top (u \circ \sigma_{0,1}^{\mathbf{N}_k})_{l+1})) \top (\overset{k-1}{\underset{i=l+1}{\top}}(u \circ \sigma_{0,1}^{\mathbf{N}_k})_i) \\
&\qquad\qquad \text{associativité} \\
&= ((\overset{l-1}{\underset{i=0}{\top}} u_i) \top (u_{l+1} \top u_l)) \top (\overset{k-1}{\underset{i=l+1}{\top}} u_i) \\
&= ((\overset{l-1}{\underset{i=0}{\top}} u_i) \top (u_l \top u_{l+1})) \top (\overset{k-1}{\underset{i=l+1}{\top}} u_i) \quad \text{commutativité} \\
&= \overset{k-1}{\underset{i=0}{\top}} u_i \quad \text{associativité.}
\end{aligned}$$

II.29. notation Si X est un ensemble, $u \in E^X$ et $x \in X$ on note u_x l'image de x par u.

II.30. proposition *On suppose que $\top$ est associative et commutative. Soit $k \in \mathbf{N} \setminus \{0\}$ et X un ensemble fini de cardinal k. Si $u \in E^X$ alors il existe $U \in E$ tel que $U = \overset{k-1}{\underset{i=0}{\top}}(u \circ b)_i$ quelque soit la bijection $b : \mathbf{N}_k \to X$.*

II.31. preuve On va prouver par récurrence sur $k \in \mathbf{N} \setminus \{0\}$ la propriété P_k suivante : *si X est un ensemble fini de cardinal k et si $u \in E^X$ alors il existe $U \in E$ tel que si $b : \mathbf{N}_k \to X$ une bijection alors $U = \overset{k}{\underset{i=0}{\top}}(u \circ b)_i$*

La propriété P_1 est vraie car si X est un singleton $\{x\}$ et si $b : \mathbf{N}_1 \to x$ alors $\overset{0}{\underset{i=0}{\top}}(u \circ b)_i = (u \circ b)_0 = u_x$.

La propriété P_2 est vraie car si X est une paire $\{x, y\}$ et si $b : \mathbf{N}_2 \to \{x, y\}$ alors soit $b(0) = x$, $b(1) = y$ et $\overset{1}{\underset{i=0}{\top}}(u \circ b)_i = u_0 \top u_1$ soit $b(0) = y$, $b(1) = x$ et $\overset{1}{\underset{i=0}{\top}}(u \circ b)_i = u_1 \top u_0$ qui est aussi égal à $u_0 \top u_1$ car $\top$ est commutative.

Soit $k \in \mathbf{N} \setminus \{1, 2\}$ tel que P_k soit vraie. Soit X un ensemble fini de cardinal $k + 1$ et $u \in E^X$. Soit $b : \mathbf{N}_{k+1} \to X$ une bijection.

Pour montrer P_{k+1} il suffit de montrer par récurrence sur $\delta \in \mathbf{N}$ la propriété $Q_{k\delta}$ suivante : $k < \delta$ *ou pour toute bijection* $c : \mathbf{N}_{k+1} \to X$ *telle que* $b_k = c_{k-\delta}$ *on a*

$$\overset{k}{\underset{i=0}{\top}}(u \circ b)_i = \overset{k}{\underset{i=0}{\top}}(u \circ c)_i.$$

Soit une bijection $c : \mathbf{N}_{k+1} \to X$ telle que $b_k = c_k$. Alors $b(\mathbf{N}_k)$ et $c(\mathbf{N}_k)$ sont tous les deux égaux à un sous-ensemble X' de cardinal k de X. On note b' et c' les corestrictions à X' des restrictions à $\mathbf{N}_k$ de b et c. Ce sont des bijections et par hypothèse de récurrence on a

$$\overset{k-1}{\underset{i=0}{\top}}(u \circ b')_i = \overset{k-1}{\underset{i=0}{\top}}(u \circ c')_i.$$

Par conséquent

$$\begin{aligned}
\overset{k}{\underset{i=0}{\top}}(u \circ b_i) &= (\overset{k-1}{\underset{i=0}{\top}}(u \circ b)_i) \top (u \circ b)_k \\
&= (\overset{k-1}{\underset{i=0}{\top}}(u \circ b')_i) \top (u \circ c)_k \\
&= (\overset{k-1}{\underset{i=0}{\top}}(u \circ c')_i) \top (u \circ c)_k \\
&= \overset{k}{\underset{i=0}{\top}}(u \circ c)_i.
\end{aligned}$$

Ceci prouve Q_{k0}.

Soit $\delta \in \mathbf{N}$ tel que $Q_{k\delta}$ est vraie. Si $k \leq \delta$ alors $Q_{k\delta+1}$ est vraie car alors $k < \delta + 1$. On suppose que $\delta < k$. Soit une bijection $c : \mathbf{N}_{k+1} \to X$ telle que $b_k = c_l$ avec $l = k - \delta - 1$. On pose $c_l = x$, $c_{l+1} = y$ et $d = \sigma^X_{xy} \circ c$. On a $b_k = d_{l+1} = d_{k-\delta}$. D'après $Q_{k\delta}$ on a

$$\overset{k}{\underset{i=0}{\top}}(u \circ b_i) = \overset{k}{\underset{i=0}{\top}}(u \circ d_i).$$

Soit $\sigma = c^{-1} \circ d$. Par construction on a $c \circ \sigma = d$ et $\sigma = \sigma_{ll+1}^{\mathbf{N}_{k+1}}$. Par conséquent

$$\begin{aligned}
\overset{k}{\underset{i=0}{\top}}(u \circ c)_i &= \overset{k}{\underset{i=0}{\top}}((u \circ c) \circ \sigma)_i \quad \text{proposition précédente} \\
&= \overset{k}{\underset{i=0}{\top}}(u \circ (c \circ \sigma))_i \quad \text{associativité de } \circ \\
&= \overset{k}{\underset{i=0}{\top}}(u \circ d)_i \\
&= \overset{k}{\underset{i=0}{\top}}(u \circ b)_i \quad \text{d'après } Q_{k\delta}
\end{aligned}$$

ainsi $Q_{k\delta+1}$ est vraie si $Q_{k\delta}$ l'est.

II.32. définition On suppose $\top$ est associative et commutative. Soit X un ensemble fini de cardinal $k \in \mathbf{N} \setminus \{0\}$. D'après ce qui précède, si $u \in E^X$ alors il existe $U \in E$ tel que $U = \overset{k-1}{\underset{i=0}{\top}}(u \circ b)_i$ quelque soit la bijection $b : \mathbf{N}_k \to X$. Ce nombre est noté $\underset{x \in X}{\top} u_x$.

II.33. proposition *On suppose $\top$ associative et commutative. Soit $f : X \to Y$ une bijection entre deux ensembles finis. Si $v \in E^Y$ alors $u = v \circ f \in E^Y$ vérifie $\underset{y \in Y}{\top} v_y = \underset{x \in X}{\top} u_x$.*

II.34. preuve Soit k le cardinal et de X et $b : \mathbf{N}_k \to X$ une bijection. Alors f
$circb : \mathbf{N}_k =\!\!\to Y$ est une bijection et

$$\underset{y \in Y}{\top} v_y = \overset{k-1}{\underset{i=0}{\top}}(v \circ (f \circ b))_i = \overset{k-1}{\underset{i=0}{\top}}((v \circ f) \circ b)_i = \underset{x \in X}{\top} u_x.$$

II.35. proposition *On suppose $\top$ associative et commutative et qu'il existe une seconde loi $\perp$ qui est distributive par rapport à $\top$. Soit X un ensemble fini, $v \in E$ et $u \in E^X$. Soit $w \in E^X$ définie par $w_x = v \perp u_x$ si $x \in X$. Alors $v \perp (\underset{x \in X}{\top} u_x) = \underset{x \in X}{\top} w_x$ c'est à dire $v \perp (\underset{ix \in X}{\top} u_x) = \underset{x \in x}{\top} v \perp u_x$.*

II.36. preuve Soit k le cardinal et de X et $b : \mathbf{N}_k \to X$ une bijection. Alors

$$\begin{aligned}
v \perp (\underset{x \in X}{\top} u_x) &= v \perp (\overset{k-1}{\underset{i=0}{\top}}(u \circ b)_i) \\
&= \overset{k-1}{\underset{i=0}{\top}}(w \circ b)_i) \\
&= \underset{x \in X}{\top} w_x.
\end{aligned}$$

II.37. définition On suppose que $\top$ est associative et commutative. Soit X un ensemble fini non vide et $X' \subset X$ non vide. Si $u \in E^X$ on pose $\underset{x\in X'}{\top} u_x = \underset{x\in X'}{\top} u'_x$ où u' désigne la restriction de u à X'.

II.38. définition On suppose que $\top$ est associative et commutative et qu'elle possède un neutre e. Si X est un ensemble fini et $u \in E^X$ on pose $\underset{x\in\emptyset}{\top} u_x = e$.

II.39. proposition *On suppose que $\top$ est associative et commutative et possède un neutre e. Soit X un ensemble fini et $u \in E^X$ l'application constante égale à e. Alors $\underset{x\in X}{\top} u_x = e$.*

II.40. preuve Si $X = \emptyset$ alors par définition $\underset{x\in X}{\top} u_x = e$. Sinon soit $k \in \mathbf{N}\backslash\{0\}$ le cardinal de X et $b : \mathbf{N}_k \to X$ une bijection alors $u \circ b \in E^{\mathbf{N}_k}$ est l'application constante égale à e. Donc

$$\underset{x\in X}{\top} u_x = \overset{k-1}{\underset{i=0}{\top}} (u \circ b)_i = e.$$

II.41. définition Une *partition* d'un ensemble X est une famille $(X_y)_{y\in Y}$ de sous-ensembles non vides de X indexées par un ensemble non vide Y telle que

$$X = \bigcup_{y\in\mathcal{Y}} X_y$$

et telle que pour tout $(y, y') \in \mathcal{Y}^2$, $X_y \cap X'_y = \emptyset$ dès que $y \neq y'$.

II.42. proposition *On suppose que $\top$ est associative et commutative. Soit X et Y deux ensembles finis, $(X_y)_{y\in Y}$ une partition de X et $u \in E^X$. Soit $v \in E^Y$ l'application définie par $v_y = \underset{x\in X_y}{\top} u_x$ si $y \in Y$. Alors*

$$\underset{x\in X}{\top} u_x = \underset{y\in Y}{\top} v_y$$

c'est à dire

$$\underset{x\in X}{\top} u_x = \underset{y\in Y}{\top} (\underset{x\in X_y}{\top} u_x).$$

II.43. preuve On va prouver par récurrence que si $k \in \mathbf{N} \setminus \{0\}$ la propriété P_K suivante est vraie : *Soit X et Y deux ensembles finis, $(X_y)_{y\in Y}$ une partition de X et $u \in E^X$. On suppose que Y est de cardinal au plus k. Soit $v \in E^Y$ l'application définie par $v_y = \underset{x\in X_y}{\top} u_x$ si $y \in Y$. Alors $\underset{x\in X}{\top} u_x = \underset{y\in Y}{\top} v_y$.*

La propriété P_1 est vraie : si le cardinal de Y est 1 alors Y est un singleton $\{y\}$, $X_y = X$ et $\underset{y\in Y}{\top} v_y = v_y = \underset{x\in X_y}{\top} u_x = \underset{x\in X}{\top} u_x$.

Soit $k \in \mathbf{N}\setminus\{0\}$ telle que P_k est vraie. Soit X et Y deux ensembles finis, $(X_y)_{y\in Y}$ une partition de X et $u \in E^X$. On suppose que Y est de cardinal $k+1$. Soit $\beta : \mathbf{N}_{k+1} \to Y$ une bijection. On pose $z = \beta(k)$, $Y' = Y\setminus\{z\}$ et $X' = X \setminus X_z$. L'ensemble Y' est de cardinal k et la famille $(X_y)_{y\in Y'}$ est une partition de X'.

On a $v_z = (v\circ\beta)_k$

$$\underset{y\in Y'}{\top} v_y = \overset{k-1}{\underset{j=0}{\top}} (v\circ\beta)_j$$

et

$$\begin{aligned}\underset{y\in Y}{\top} v_y &= \overset{k}{\underset{j=0}{\top}} (v\circ\beta)_j \\ &= (\overset{k-1}{\underset{j=0}{\top}} (v\circ\beta)_j)\top(v\circ\beta)_k \\ &= (\underset{y\in Y'}{\top} v_y)\top v_z.\end{aligned}$$

Or d'après P_k on a

$$\underset{y\in Y'}{\top} v_y = \underset{x\in X'}{\top} u_x.$$

Ainsi

$$\underset{y\in Y}{\top} v_y = (\underset{x\in X'}{\top} u_x)\top v_z$$

On désigne par n le cardidal de X, par n' et par m celui de Y_z. On a $n = n' + m$. Le cardinal de $\mathbf{N}_{n'}$ est n' et celui de $\mathbf{N}_n \setminus \mathbf{N}_{n'}$ est m. Il existe donc des bijections $b' : \mathbf{N}_{n'} \to X'$ et $c : \mathbf{N}_n \setminus \mathbf{N}_{n'} \to X_z$. Alors l'application $b : \mathbf{N}_n \to X$ définie par $b(i) = b'(i)$ si $i \in \mathbf{N}_n$ et $b(i) = c(i)$ si $i \in \mathbf{N}_n \setminus \mathbf{N}_{n'}$ est une bijection telle que $b(\mathbf{N}_{n'}) = X'$ et $b(\mathbf{N}_n \setminus \mathbf{N}_{n'}) = X_z$. On a donc

$$\underset{x\in X}{\top} u_x = \overset{n-1}{\underset{i=0}{\top}} (u\circ b)_i$$

$$\underset{x\in X'}{\top} u_x = \overset{n'-1}{\underset{i=0}{\top}} (u\circ b)_i$$

$$v_z = \overset{n-1}{\underset{i=n'}{\top}} (u\circ b)_i$$

et donc

$$\underset{x\in X}{\top} u_x = (\underset{x\in X'}{\top} u_x)\top v_z = \underset{y\in Y}{\top} v_y.$$

Ceci prouve que P_{k+1} est vraie si P_k l'est.

II.44. corollaire *On suppose que $\top$ est associative et commutative et possède un neutre e. Soit X un ensemble fini et $u \in E^X$. On pose $X' = \{x \in X : u(x) \neq e\}$. Alors* $\underset{x\in X}{\top} u_x = \underset{x\in X'}{\top} u_x$.

II.45. preuve Si $X = \emptyset$ alors $X' = \emptyset$ et $\underset{x\in X}{\top} u_x = \underset{x\in\emptyset}{\top} u_x = e = \underset{x\in X'}{\top} u_x$. On suppose que X est non vide. Soit $Z = X \setminus X' = \{x \in X : u(x) = e\}$. On a $\underset{x\in Z}{\top} u_x = 0$ et $\underset{x\in X}{\top} u_x = (\underset{x\in X'}{\top} u_x)\top(\underset{x\in Z}{\top} u_x) = \underset{x\in X'}{\top} u_x$.

II.46. proposition *On suppose que $\top$ est associative et commutative et possède un neutre e. Soit $(X_y)_{y\in Y}$ une famille finie d'ensembles finis deux à deux disjoints. Soit $X = \bigcup_{y\in Y} X_y$ et $u \in E^X$. Soit $v \in E^Y$ l'application définie par $v_y = \underset{x\in X_y}{\top} u_x$ si $y \in Y$. Alors*

$$\underset{x\in X}{\top} u_x = \underset{y\in Y}{\top} v_y$$

c'est à dire

$$\underset{x\in X}{\top} u_x = \underset{y\in Y}{\top}(\underset{x\in X_y}{\top} u_x).$$

II.47. preuve Si $Y = \emptyset$ alors $X = Y = \emptyset$, le graphe de u est l'ensemble vide ainsi que celui de v. On a donc $\underset{x\in X}{\top} u_x = \underset{x\in\emptyset}{\top} u_x = e = \underset{y\in Y}{\top} v_y = \underset{y\in Y}{\top} v_y$.

Si $X = \emptyset$ alors $\underset{x\in X}{\top} u_x = \underset{x\in\emptyset}{\top} u_x = e$ et pour tout $y \in Y$ $v_y = e$ donc $\underset{y\in Y}{\top} v_y = e$.

On suppose X et Y non vides. On pose $Y' = \{y \in Y : X_y \neq \emptyset\}$ et $Z = \{y \in Y : X_y = \emptyset\}$. On a $Y' \cup Z = Y$ et $Y' \cap Z = \emptyset$. Ainsi

$$\underset{y\in Y}{\top} v_y = (\underset{y\in Y'}{\top} v_y) + (\underset{y\in Z}{\top} v_y).$$

Or, si $y \in Z$ alors $v_y = \underset{x\in\emptyset}{\top} u_x = e$ donc $\underset{y\in Z}{\top} v_y = e$ et

$$\underset{y\in Y}{\top} v_y = (\underset{y\in Y'}{\top} v_y) + e = \underset{y\in Y'}{\top} v_y.$$

La famille $(X_y)_{y\in Y'}$ est une partition de X qui est non vide. Donc

$$\underset{x\in X}{\top} u_x = \underset{y\in Y'}{\top} v_y = \underset{y\in Y}{\top} v_y.$$

II.48. notation Si $\top = +$ alors $\overset{k}{\underset{i=0}{+}} u_i$ est noté $\sum_{i=0}^{k} u_i$ et si $\top = \times$ alors $\overset{k}{\underset{i=0}{\times}} u_i$ est noté $\prod_{i=0}^{k} u_i$.

II.49. remarque Parfois on pose

$$\sum_{i=0}^{k} u_i = u_0 + ... + u_k$$

et

$$\prod_{i=0}^{k} u_i = u_0 \times ... \times u_k.$$

Si de plus tous les u_i sont égaux à un a et si $k \geq 1$ alors on pose

$$\sum_{i=1}^{k} u_i = ka \text{ et } \prod_{i=1}^{k} u_i = a^k.$$

On a

$$(l+k)a = la + ka \text{ et } a^{l+k} = a^l \times a^k \text{ avec } k, l \geq 1.$$

Si $+$ admet un neutre noté 0 la formule $(l+k)a = la + ka$ garde un sens avec $k, l \in \mathbf{N}$ en posant $0a = 0$.

Si $\times$ admet un neutre noté 1 la formule $a^{l+k} = a^l \times a^k$ garde un sens avec $k, l \in \mathbf{N}$ en posant $a^1 = 1$.

II.50. remarque Si les lois $+$ et $\times$ admettent des neutres alors les suites $(ka)_{k\in\mathbf{N}}$ et $(a^k)_{k\in\mathbf{N}}$ sont les suites récurrentes de premier terme 0 et 1 associées aux application $x \mapsto x + a$ et $x \mapsto ax$.

II.51. proposition *Soit X un ensemble fini et $u \in \mathbf{N}^X$ une application de X dans $\mathbf{N}$. S'il existe $x_0 \in X$ tel que $u_{x_0} \neq 0$. alors $0 < \sum_{x\in X} u_x$.*

II.52. preuve On écrit $\sum_{x\in X} u_x = u_{x_0} + \sum_{x\in X\setminus\{x_0\}} u_x$. Puisque $u_{x_0} \neq 0$ on en déduit que $0 \leq \sum_{x\in X\setminus\{x_0\}} u_x < u_{x_0} + \sum_{x\in X\setminus\{x_0\}} u_x = \sum_{x\in X} u_x$.

II.53. proposition *Soit $(X_y)_{y\in Y}$ une famille finie d'ensembles finis. Alors $X = \bigcup_{y\in Y} X_y$ est fini et $\operatorname{card} X \leq \sum_{y\in Y} \operatorname{card} X_y$. L'égalité n'a lieu que si les $X_y, y \in Y$ forment une partition.*

II.54. preuve On raisonne par récurrence sur le cardinal de Y. Si le cardinal de Y est 0 alors $X = Y = \emptyset$. Si le cardinal de Y est 1 alors Y est un singleton $\{y\}$ et $X = X_y$ est fini et $\operatorname{card} X = \operatorname{card} X_y$.

Soit $k \in \mathbf{N}$. On suppose que pour toute famille $(X_y)_{y\in Y}$ d'ensembles finis telle que $\operatorname{card} Y = k$ la réunion $X = \bigcup_{y\in\ Y} X_y$ est finie et $\operatorname{card} X \leq \sum_{y\in Y} \operatorname{card} X_y$, l'égalité n'ayant lieu que si les $X_y, y \in Y$ forment une partition.

Soit Y un ensemble de cardinal $k+1$ et $(X_y)_{y\in Y}$ une famille d'ensembles finis.

Supposons que les $X_y, y \in Y$ forment une partition. Soit $z \in Y$. On pose $Y' = Y \setminus \{z\}$ et $X' = \bigcup_{y\in\ Y'} X_y$. Alors les $X_y, y \in Y'$ forment une partition de X' et puisque le cardinal de Y' est k on a $\operatorname{card} X' = \sum_{y\in Y'} \operatorname{card} X_y$. De plus X' et X_z forment une partition de X. On a donc

$$\operatorname{card} X = \operatorname{card} X' + \operatorname{card} X_z = \left(\sum_{y\in Y'} \operatorname{card} X_y\right) + \operatorname{card} X_z = \sum_{y\in Y} \operatorname{card} X_y.$$

Supposons que les $X_y, y \in Y$ ne forment pas une partition. Il existe donc $z, z' \in Y$ distincts tels que $X_{z'} \cap X_z \neq \emptyset$. On pose $Y' = Y \setminus \{z\}$ et $X' = \bigcup_{y\in\ Y'} X_y$. On a $X' \cap X_z \neq \emptyset$ car $X_{z'} \cap X_z \subset X' \cap X_z$ mais $X = X' \cup X_z$. Par conséquent $\operatorname{card} X < \operatorname{card} X' + \operatorname{card} X_z$. Puisque le cardinal de Y' est k on a $\operatorname{card} X' \leq \sum_{y\in Y'} \operatorname{card} X_y$. Ainsi

$$\operatorname{card} X < \left(\sum_{y\in Y'} \operatorname{card} X_y\right) + \operatorname{card} X_z = \sum_{y\in Y} \operatorname{card} X_y.$$

II.55. proposition *Soit $(X_y)_{y\in Y}$ une famille finie d'ensembles finis. Alors*

$$\operatorname{card}\left(\bigcup_{y\in\ Y} X_y\right) = \sum_{U\subset Y, U\neq\emptyset} (-1)^{\operatorname{card} U} \operatorname{card}\left(\bigcap_{u\in U} X_u\right).$$

II.56. preuve On va montrer par récurrence sur $k \in \mathbf{N}$ la propriété P_k suivante : *si $(X_y)_{y\in Y}$ une famille finie d'ensembles finis avec* $\operatorname{card} Y = k$ *alors*

$$\operatorname{card}\left(\bigcup_{y\in\ Y} X_y\right) = \sum_{U\subset Y, U\neq\emptyset} (-1)^{\operatorname{card} U} \operatorname{card}\left(\bigcap_{u\in U} X_u\right).$$

Aux rangs $k = 0, 1$ ou 2 le résultat est trivial ou déjà prouvé précédemment.

Soit $k \in \mathbf{N}$. Supposons $k \geq 2$ et que P_k est vraie. Prouvons P_{k+1}.

Soit Y un ensemble de cardinal $k+1$ et $(X_y)_{y \in Y}$ une famille d'ensembles finis. On pose $X = \bigcup_{y \in Y} X_y$. Soit $z \in Y$. On pose $Y' = Y \setminus \{z\}$ et $X' = \bigcup_{y \in Y'} X_y$. On a

$$\operatorname{card} X = \operatorname{card} X' + \operatorname{card} X_z - \operatorname{card} (X' \cap X_z) \quad \text{(I)}.$$

D'après P_k on a

$$\operatorname{card} X' = \sum_{U \subset Y', U \neq \emptyset} (-1)^{\operatorname{card} U} \operatorname{card} \left(\bigcap_{u \in U} X_u \right) \quad \text{(II)}.$$

On a

$$\operatorname{card} X_z = \sum_{U = \{z\}} (-1)^{\operatorname{card} U} \operatorname{card} \left(\bigcap_{u \in U} X_u \right) \quad \text{(III)}.$$

On a

$$X' \cap X_z = \left(\bigcap_{y \in Y'} X_y \right) \cap X_z = \bigcap_{y \in Y'} (X_y \cap X_z).$$

D'après P_k on a donc

$$\begin{aligned}
\operatorname{card} (X' \cap X_z) &= \sum_{U' \subset Y', U' \neq \emptyset} (-1)^{\operatorname{card} U'} \operatorname{card} \left(\bigcap_{u \in U'} (X_u \cap X_z) \right) \\
&= \sum_{U' \subset Y', U' \neq \emptyset} (-1)^{\operatorname{card} U'} \operatorname{card} \left(\left(\bigcap_{u \in U'} X_u \right) \cap X_z \right) \\
&= \sum_{U' \subset Y', U' \neq \emptyset} (-1)^{\operatorname{card} U'} \operatorname{card} \left(\bigcap_{u \in U' \cup \{z\}} X_u \right) \\
&= - \sum_{U' \subset Y', U' \neq \emptyset} (-1)^{\operatorname{card} U' \cup \{z\}} \operatorname{card} \left(\bigcap_{u \in U' \cup \{z\}} X_u \right) \\
&= \sum_{U \subset Y, z \in U, U \setminus \{z\} \neq \emptyset} (-1)^{\operatorname{card} U} \operatorname{card} \left(\bigcap_{u \in U} X_u \right)
\end{aligned}$$

et donc

$$-\operatorname{card} (X' \cap X_z) = \sum_{U \subset Y, z \in U, U \setminus \{z\} \neq \emptyset} (-1)^{\operatorname{card} U} \operatorname{card} \left(\bigcap_{u \in U} X_u \right) \quad \text{(IIII)}.$$

Or si U est un sous-ensemble non vide de Y alors il vérifie une et une seule des conditions suivantes :
- $U \subset Y'$,
- $U = \{z\}$,
- $U = U' \cup \{z\}$, avec $U' \subset Y'$ non vide.

On déduit donc de (I), (II), (III) et (IIII) que

$$\begin{aligned} \operatorname{card} X &= \sum_{U \subset Y', U \neq \emptyset} (-1)^{\operatorname{card} U} \operatorname{card} \left(\bigcap_{u \in U} X_u \right) \\ &\quad + \sum_{U = \{z\}} (-1)^{\operatorname{card} U} \operatorname{card} \left(\bigcap_{u \in U} X_u \right) \\ &\quad + \sum_{U \subset Y, z \in U, U \setminus \{z\} \neq \emptyset} (-1)^{\operatorname{card} U} \operatorname{card} \left(\bigcap_{u \in U} X_u \right) \end{aligned}$$

c'est à dire

$$\operatorname{card} X = \sum_{U \subset Y, U \neq \emptyset} (-1)^{\operatorname{card} U} \operatorname{card} \left(\bigcap_{u \in U} X_u \right).$$

III. La division euclidienne des entiers naturels

III.1. définition Soit $a \in \mathbf{N} \setminus \{0\}$ et $b \in \mathbf{N}$. On appelle *reste* et *quotient* de la *division euclidienne* de b par a des entiers naturels q et r tels que

$$b = qa + r \text{ et } r < a.$$

III.2. lemme (division euclidienne) *Soit $a \in \mathbf{N} \setminus \{0\}$ et $b \in \mathbf{N}$. Il existe un unique couple $(q, r) \in \mathbf{N}^2$ tel que*

$$b = qa + r \text{ et } r < a.$$

III.3. preuve Prouvons d'abord l'existence d'un couple (q, r) formé d'un quotient q et d'un reste r de la division euclidienne de b par a. Soit B l'ensemble

$$B = \{n \in \mathbf{N} : \exists k \in \mathbf{N}, n = b - ka\}.$$

L'ensemble B est non vide car $b \in B$ (prendre $k = 0$). Il possède donc un plus petit élément qu'on note r. Or si $n \in B$ et si $n \geq a$ alors l'entier naturel $n - a$ appartient à B. En effet puisque $n \in B$ il existe $k \in \mathbf{N}$ tel que $n = b - ka$.

Par conséquent l'entier naturel $n-a$ vérifie $n-a = b-(k+1)a$ et appartient bien à B. Ainsi le plus petit élément r de B vérifie $r < a$. Puisque $r \in B$ il existe $q \in \mathbf{N}$ tel que $r = b - qa$ c'est à dire $b = qa + r$. L'existence est prouvée.

Considérons un second couple $(q', r') \in \mathbf{N}^2$ tel que

$$b = q'a + r' \text{ et } r' < a.$$

Quitte à permuter les couples (q, r) et (q', r') on peut supposer que $r \geq r'$. Il vient donc

$$(q' - q)a = (r - r') \in \mathbf{N}$$

et $r - r' < a$. Or 0 est le seul entier naturel qui soit un multiple de a en étant strictement plus petit que a. Par conséquent $r - r' = 0$ et puisque $a \neq 0$ alors que $(q' - q)a = 0$ on a aussi q'=q. L'unicité est prouvée.

III.4. corollaire (la propriété d'Archimède) *Soit $a \in \mathbf{N} \setminus \{0\}$ et $b \in \mathbf{N}$. Il existe $k \in \mathbf{N}$ tel que $b < ka$.*

III.5. preuve Soit q et r les entiers naturels qui sont respectivement le quotient et le reste de la division euclidienne de b par a. On a

$$b = qa + r \text{ et } r < a.$$

Par conséquent $b < qa + a = (q + 1)a$ et $k = q + 1 \in \mathbf{N}$ est un entier naturel qui permet de conclure.

III.6. proposition *Si $a, x \in \mathbf{N} \setminus \{0\}$ et $l \in \mathbf{N}$ alors $xa^l \neq 0$.*

III.7. preuve On raisonne par récurrence sur l. On a $xa^0 = x \neq 0$. On considère $l \in \mathbf{N}$ tel que $xa^l \neq 0$. Alors on a $xa^{l+1} = (xa^l)a \neq 0$ car c'est le produit de $xa^l \neq 0$ et de $a \neq 0$.

III.8. proposition *Soit $a \in \mathbf{N} \setminus \{0, 1\}$, $n \in \mathbf{N} \setminus \{0\}$, $k \in \mathbf{N}$ et $x = (x_0, ..., x_k) \in \mathbf{N}_a^{k+1}$. Si $n = \sum_{i \in \mathbf{N}_{k+1}} x_i a^i$ alors x_0 est le reste de la division euclidienne de n par a et $\sum_{i \in \mathbf{N}_k} x_{i+1} a^i$ est le quotient.*

III.9. preuve On a

$$n = \sum_{i \in \mathbf{N}_{k+1}} x_i a^i = \left(\sum_{i \in \mathbf{N}_k} x_{i+1} a^i \right) a + a_0$$

et $a_0 < a$.

III.10. définition Soit $a \in \mathbf{N}\backslash\{0,1\}$, $n \in \mathbf{N}\backslash\{0\}$, $k \in \mathbf{N}$ et $x = (x_0, ..., x_k) \in \mathbf{N}_a^{k+1}$. Si $n = \sum_{i \in \mathbf{N}_{k+1}} x_i a^i$ et $x_k \neq 0$ alors on dit que $(x_0, ..., x_k)$ est *une écriture de n dans la base a.*

III.11. proposition *Soit $a \in \mathbf{N}\backslash\{0,1\}$. Alors tout entier non nul $n \in \mathbf{N}\backslash\{0\}$ possède une et une seule écriture dans la base a.*

III.12. preuve On va prouver par récurrence sur $n \in \mathbf{N}$ la propriété P_n suivante : $n = 0$ ou n possède une et une seule écriture dans la base a.

La propriété P_0 est vraie. Soit $n \in \mathbf{N}$ tel que $n < a$. Montrons que P_n est vraie. On a $n = n \times 1$ et donc n admet (n) comme écriture en base a. Si $(x_0, ..., x_k)$ est une écriture de n en base a alors $x_0 = n$ et $\sum_{i \in \mathbf{N}_k} x_{i+1} a^i = 0$ car la division euclidienne de n par a donne $n = 0a + n$. Par conséquent $k = 0$ ou les x_{i+1} sont tous nuls. Ceci prouve que (n) est l'unique écriture de n en base a. Ainsi P_n est vraie si $n < a$.

Soit $n \in \mathbf{N}$. On suppose que P_m est vraie pour tout $m \leq n$. Si $n < a - 1$ alors $n + 1 < a$ et P_{n+1} est vraie d'après ce qui précède. On suppose que $a - 1 \leq n$. Soit q et r le quotient et le reste de la division euclidienne de $n + 1$ par a. On a $n + 1 = qa + r$ avec $r < a$ et $1 \leq q$. Puisque $1 < a$ on a $q < qa \leq n+1$. Or $1 \leq q$. Par hypothèse de récurrence q qui est non nul admet une unique écriture $y = (y_0, ..., y_k)$ en base a. Si on pose $x = (x_0, ..., x_{k+1})$ avec $x_0 = r$ et si $1 \leq i \leq k + 1$, $x_i = y_{i-1}$ alors on a $n = \sum_{i \in \mathbf{N}_{k+2}} x_i a^i$ avec $x = (x_0, ..., x_{k+1}) \in \mathbf{N}_a^{k+2}$ et $x_{k+1} \neq 0$. C'est une écriture de n en base a. Si $z = (z_0, ..., z_l)$ en est une seconde alors d'après les propositions précédentes $z_0 = x_0$ est le reste de la division euclidienne de n par a et $(z_1, ..., z_l)$ est une écriture en base a du quotient q de la division euclidienne de n par a. D'après l'hypothèse de récurrence cette écriture $(z_1, ..., z_l)$ est nécessairement égale à l'écriture $y = (y_0, ..., y_k)$. Ainsi $z = (z_0, ..., z_l) = (x_0, ..., x_{k+1}) = x$. Ceci achève la preuve de P_{n+1}.