Chapitre 3

CONSTRUCTION DES NOMBRES ENTIERS NATURELS

Version du 21 avril 2002

3.1 Principe de récurrence

Existence d'un ensemble infini

$$\exists x \ [\emptyset \in x \wedge \forall y \, (y \in x \Rightarrow y \cup \{y\} \in x)]$$

Si l'on convient de dire que $y \cup \{y\}$ est l' *ensemble successeur* de y , cet axiome signifie qu'il existe un ensemble ayant la propriété suivante :

$N(x)$

il contient l'ensemble vide $\emptyset$

et

le successeur de tout ensemble qui lui appartient.

C'est ce qui nous permet de dire que cet ensemble est "infini" . Une définition formelle de cette notion sera donnée plus tard (cf. définition 3.4). Cet ensemble n'est évidemment pas unique !

THEOREME *Il existe un ensemble, noté* $\mathbb{N}$ *, qui est le plus petit ayant la propriété* N *, i.e. on a* $N(\mathbb{N})$ *et si* x *est un ensemble tel que* $N(x)$ *, alors* $x \supset \mathbb{N}$ *.*

Soit u un ensemble tel que $N(u)$. Posons $A := \{x \in \mathfrak{P}(u) \mid N(x)\}$. On a $u \in A$, donc $A \neq \emptyset$ et on définit

$$\mathbb{N} := \bigcap_{x \in A} x \ .$$

On a $N(\mathbb{N})$. En effet, pour tout $x \in A$, on a $\emptyset \in x$, donc

$$\emptyset \in \bigcap_{x \in A} x = \mathbb{N} \ .$$

D'autre part, si $y \in \mathbb{N}$, quel que soit $x \in A$, on a $y \in x$, donc $y \cup \{y\} \in x$, et par suite $y \cup \{y\} \in \mathbb{N}$. Finalement soit x tel que $N(x)$. Comme ci-dessus, on montre que $N(x \cap u)$ est vraie, donc $x \cap u \in A$; on en déduit que

$$x \supset x \cap u \supset \mathbb{N} \ .$$

□

DEFINITION 1 On dit que $\mathbb{N}$ est l' *ensemble des nombres entiers naturels* . On pose

$$0 := \emptyset$$

$$1 := 0 \cup \{0\} = \{0\} = \{\emptyset\} \ ,$$

$$2 := 1 \cup \{1\} = \{0\} \cup \{1\} = \{0, 1\} = \{\emptyset, \{\emptyset\}\} \ ,$$

$$3 := 2 \cup \{2\} = \{0,1\} \cup \{2\} = \{0,1,2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \ ,$$

$$4 := 3 \cup \{3\} = \{0,1,2\} \cup \{3\} = \{0,1,2,3\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\} \ ,$$

etc...

Si $n \in \mathbb{N}$, on définit

$$n+1 := n \cup \{n\} \ .$$

Principe de récurrence *Soit $P(x)$ une propriété. On suppose que $P(0)$ est vraie et que, quel que soit n , le* pas de récurrence

$$n \in N \quad et \quad P(n) \quad entraîne \quad P(n+1)$$

soit satisfait. Alors pour tout $n \in \mathbb{N}$ la propriété $P(n)$ est vraie.

Soit $A := \{n \in \mathbb{N} \mid P(n)\}$. On a $\emptyset = 0 \in A$ et si $n \in A$, i.e. si n $\in \mathbb{N}$ et $P(n)$ est vraie, par hypothèse on en déduit $P(n+1)$, i.e. $n+1 \in A$. Ceci montre que A satisfait à la propriété de récurrence. D'après le théorème on obtient $A \supset \mathbb{N}$, mais comme par construction $A \subset \mathbb{N}$, on a finalement $A = \mathbb{N}$. Mais ceci signifie bien que $P(n)$ est vraie pour tout $n \in \mathbb{N}$. — □

DEFINITION 2 On dit que la relation $n \in \mathbb{N}$ et $P(n)$ est l' *hypothèse de récurrence* .

EXEMPLE Pour tout $n \in \mathbb{N}$, on a

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2} \ .$$

Le cas $n = 0$ est trivial. Pour démontrer la propriété de récurrence, supposons que la formule soit vraie pour n (hypothèse de récurrence) et démontrons la formule pour $n+1$:

$$\sum_{k=0}^{n+1} k = \left(\sum_{k=0}^{n} k\right) + (n+1) = \frac{n(n+1)}{2} + n + 1 = \frac{(n+1)(n+2)}{2} \ .$$

□

EXERCICE 1 Montrer par récurrence que l'on a

$$\sum_{k=0}^{n} k^3 = \frac{n^2 (n+1)^2}{4}$$

pour tout $n \in \mathbb{N}$.

EXERCICE 2 Montrer par récurrence que l'on a

$$\sum_{k=1}^{n} \frac{1}{k(k+1)} = 1 - \frac{1}{n+1}$$

pour tout $n \in \mathbb{N}$.

3.2 Propriétés élémentaires de $\mathbb{N}$

Par définition de $n+1$ on a évidemment

$$n \subset n+1 \quad \text{et} \quad n \in n+1 \ .$$

Ceci montre en particulier que $n+1 \neq \emptyset = 0$ quel que soit $n \in \mathbb{N}$.

PROPOSITION

(i) *Pour tout $n \in \mathbb{N}$ et $x \in n$, on a $x \in \mathbb{N}$ et $x \subset n$.*

(ii) *Pour tout $n \in \mathbb{N}$ et tout $x \in \mathbb{N}$ tel que $x \subset n$ et $x \neq n$, on a $x \in n$.*

(iii) *Pour tout $n \in \mathbb{N}$, on a $n \notin n$. En particulier $n \neq n+1$.*

Les démonstrations se font par récurrence.

Démonstration de (i) On considère la propriété suivante, exprimant de manière formelle ce que nous voulons démontrer :

$$P(n) : \forall x \ (x \in n \quad \Longrightarrow \quad x \in \mathbb{N} \text{ et } x \subset n) \ .$$

On a $P(0)$, car $x \in 0 = \emptyset$ est fausse, ce qui montre que

$$\forall x \ (x \in 0 \quad \Longrightarrow \quad x \in \mathbb{N} \text{ et } x \subset 0)$$

est vraie.

Admettons maintenant que $n \in \mathbb{N}$ et $P(n)$ soit vraie (hypothèse de récurrence) et montrons que $P(n+1)$ est vraie. On a évidemment $n+1 \in \mathbb{N}$. Si maintenant

$$x \in n+1 = n \cup \{n\} \ ,$$

alors $x \in n$ ou $x = n$. Dans le premier cas, l'hypothèse de récurrence montre que $x \in \mathbb{N}$ et que $x \subset n \subset n+1$. Dans le second, on a $x = n \in \mathbb{N}$ et $x = n \subset n+1$. Dans les deux cas nous avons prouver $P(n+1)$.

Démonstration de (ii) On considère la propriété suivante :

$$P(n) : \forall x \ (x \in \mathbb{N} \ , x \subset n \text{ et } x \neq n \Rightarrow x \in n) \ .$$

On a $P(0)$, car $x \subset 0 = \emptyset$ et $x \neq 0 = \emptyset$ est fausse. Si maintenant $x \in \mathbb{N}$ et $P(n)$ est vraie, considérons $x \in \mathbb{N}$ tel que $x \subset n+1$ et $x \neq n+1$. Remarquons que $n \notin x$; en effet si $n \in x$, par (i) on obtient $n \subset x$, donc

$$n+1 = n \cup \{n\} \subset x \cup \{n\} \subset x \subset n+1 \ ,$$

ce qui contredit $n \neq n+1$. De $x \subset n+1 = n \cup \{n\}$ et $n \notin x$ on déduit alors que $x \subset n$.

Si $x = n$, on a évidemment $x \in n+1$. Si $x \neq n$, alors l'hypothèse de récurrence montre que $x \in n \subset n+1$.

Démonstration de (iii) On considère la propriété suivante :

$$P(n) : n \notin n \ .$$

On a $P(0)$, puisque $0 = \emptyset \notin \emptyset = 0$. Supposons maintenant que $n \in \mathbb{N}$ et $n \notin n$ et montrons que $n+1 \notin n+1$. Dans le cas contraire on aurait $n+1 \in n \cup \{n\}$, donc

$$n+1 \in n \text{ ou } n \cup \{n\} = n \ .$$

Dans le premier cas, (i) montre que $n \cup \{n\} \subset n$, donc en particulier que $n \in n$. Dans le second cas on a aussi $n \in n$, ce qui est absurde. ——————————— □

3.3 Relations d'ordre

Si $R(x,y)$ est une relation et X un ensemble, on dit que

$$R_X := \{(x,y) \in X \times X \mid R(x,y)\}$$

est le *graphe* de cette relation dans X . On a $(x,y) \in X \times X$ et $R(x,y)$ si, et seulement si, $(x,y) \in R_X$.

Réciproquement, si R est une partie de $X \times X$ alors

$$(x,y) \in R$$

est une relation, dont le graphe dans X est R . On dit que c'est une *relation sur* X ; on écrit souvent $x\ R\ y$.

DEFINITION 1 On dit que R est une *relation d'ordre* sur X si, pour tout $x,y,z \in X$, on a

(a) *Transitivité* $\quad x\ R\ y$ et $y\ R\ z \implies x\ R\ z$.

(b) *Antisymétrie* $\quad x\ R\ y$ et $y\ R\ x \implies x = y$.

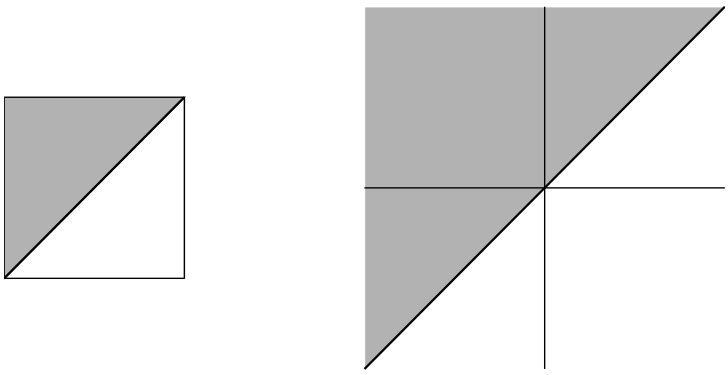
(c) *Réflexivité* $\quad x\ R\ x$.

Une relation d'ordre est souvent notée $\leqslant$ et si $x \leqslant y$, on dit que x est *plus petit* que y . On écrit aussi $y \geqslant x$ et on dit que y est *plus grand* que x . On définit $x < y$ par $x \leqslant y$ et $x \neq y$, et on dit que x est *strictement plus petit* que y . On écrit aussi $y > x$ et on dit que y est *strictement plus grand* que x .

Une relation d'ordre sur X est dite *totale* si, pour tout $x,y \in X$, on a

$$x \leqslant y \quad \text{ou} \quad y \leqslant x\ .$$

EXEMPLE 1 Les relations d'ordre $\leqslant$ sur $[0,1]$ et $\mathbb{R}$ sont totales et données par les graphes



EXEMPLE 2 Si X est un ensemble, alors la relation d'inclusion $\subset$ est une relation d'ordre sur $\mathfrak{P}(X)$. Son graphe est

$$\{(A,B) \in \mathfrak{P}(X) \times \mathfrak{P}(X) \mid A \subset B\} \ .$$

Cette relation d'ordre n'est pas totale, si X possède au moins deux éléments.

DEFINITION 2 Pour tout $n, m \in \mathbb{N}$, on écrit $n \leqslant m$ à la place de $n \subset m$.

THEOREME *La relation $\leqslant$ sur $\mathbb{N}$ est une relation d'ordre totale et, pour tout $n \in \mathbb{N}$, on a*

$$n = \{m \in \mathbb{N} \mid m < n\} \ .$$

Nous démontrons la première partie par récurrence en considérant la propriété suivante :

$$P(n) : \forall m \in \mathbb{N} \ (n \subset m \text{ ou } m \subset n) \ .$$

On a $P(0)$, puisque $0 = \emptyset \subset m$. Si maintenant $n \in \mathbb{N}$ et $P(n)$ est vraie, on a

$$(n \subset m \text{ et } n \neq m) \text{ ou } m \subset n \ .$$

Dans le premier cas, la proposition 3.2.(ii) montre que $n \in m$, donc

$$n+1 = n \cup \{n\} \subset m \cup \{n\} \subset m \ .$$

Dans le second cas, on a $m \subset n \subset n+1$, ce qu'il fallait démontrer.

Quant à la seconde partie, tout d'abord si $m \in n$, alors $m \subset n$ par la proposition 3.2.i, donc $m \leqslant n$. Mais comme $n \notin n$ par la proposition 3.2.iii, on a $m \neq n$, donc $m < n$. Réciproquement si $m < n$, alors $m \subset n$ et $m \neq n$, donc $m \in n$ par la proposition 3.2.ii. □

REMARQUE 1 Pour tout $m \in \mathbb{N}$ tel que $m < n$, on a $m+1 \leqslant n$.

On a $m \subset n$ et $m \neq n$, donc $m \in n$ par la proposition 3.2.ii et par suite

$$m+1 = m \cup \{m\} \subset n \cup \{m\} \subset n \ .$$

□

REMARQUE 2 On peut interpréter tout $n \in \mathbb{N}$ tel que $n \neq 0$ comme étant l'ensemble intuitif $\{0, 1, \ldots, n-1\}$. Mais cela n'est pas nécessaire comme le montre la Mathématique non-standard, qui fait la distinctinction entre l' *infini potentiel* , i.e la construction successive des ensemble $0 = \emptyset$, $1 = \{0\}$, $2 = \{0,1\}$, $3 = \{0,1,2\}$, etc. . . , et l' *infini actuel* représenté par $\mathbb{N}$. Cela revient à admettre l'existence d'entiers naturels $n \in \mathbb{N}$, dits non-standard ou illimités, qui ne peuvent être écrits explicitement sur du papier, i.e. dans le système formel.

3.4 Ensembles finis et infinis

THEOREME *Soit $n \in \mathbb{N}$. Si une application $f : n \longrightarrow n$ est injective, alors f est surjective.*

Si $n = 0$ alors, pour toute application $f : \emptyset \longrightarrow \emptyset$, on a $\mathrm{Gr}\, f = \emptyset$, puisque

$$\mathrm{Gr}\, f \subset \emptyset \times \emptyset = \emptyset \ .$$

Elle est surjective, car pour tout y , $y \in \emptyset$ est fausse, donc entraîne l'existence d'un $x \in \emptyset$ tel que $f(x) = y$.

Supposons que l'assertion soit vraie pour $n \in \mathbb{N}$ et soit $f : n+1 \longrightarrow n+1$ une application injective. Rappelons que $n+1 = \{x \in \mathbb{N} \mid x \leqslant n\}$ et que n est à la fois une partie $\{x \in \mathbb{N} \mid x < n\}$ et un élément de $n+1$.

Si l'image par f de la partie $n \subset n+1$ est contenue dans n , on peut considérer l'application

$$g : n \longrightarrow n : x \longmapsto f(x) \ .$$

Elle est évidemment injective, puisque f est injective, donc surjective par l'hypothèse de récurrence. Ceci montre que l'image par f de la partie n est n . L'injectivité de f montre alors que l'image par f de l'élément n est n et par suite que f est surjective.

Considérons maintenant l'autre cas, i.e. il existe $m < n$ tel que $f(m) = n$. Par l'injectivité de f on a $f(n) < n$. Considérons alors l'application

$$\tilde{f} : n+1 \longrightarrow n+1 : x \longmapsto \begin{cases} f(n) & x = m \\ f(x) \quad \text{si} & x \neq m, n \\ n & x = n \end{cases} \ .$$

Elle est injective, puisqu'on a seulement permuté les images de m et n . Comme $\tilde{f}(n) = n$, on a donc $\tilde{f}(x) \neq n$ pour tout $x < n$. Nous sommes donc ramené au cas précédent, qui montre que $\tilde{f}$ est surjective. On en déduit immédiatement que f est surjective. ———————— □

COROLLAIRE

(i) Soient $n, m \in \mathbb{N}$. S'il existe une bijection de n sur m , alors $n = m$.

(ii) Soit A un ensemble. S'il existe $n, m \in \mathbb{N}$ et des bijections

$$f : n \longrightarrow A \quad \text{et} \quad g : m \longrightarrow A \ ,$$

alors $n = m$.

Démonstration de (i) D'après le théorème 3.3 nous pouvons supposer, au besoin en échangeant n et m , que $m \subset n$. Soit alors $f : n \longrightarrow m$ une bijection et considérons l'application injective

$$g : m \longrightarrow n : x \longmapsto x \ .$$

Par la proposition 2.7.i, l'application $g \circ f : n \longrightarrow n$ est injective, donc surjective par le théorème. On en déduit par la proposition 2.7.ii que g est surjective, donc que

$$m = g(m) = n \ .$$

Démonstration de (ii) En effet, on a le diagramme

$$\begin{array}{ccc} & \overset{-1}{g} & \\ A & \longrightarrow & m \\ f \uparrow & \nearrow & \\ & & \overset{-1}{g} \circ f \\ n & & \end{array}$$

et $\overset{-1}{g} \circ f : n \longrightarrow m$ est une bijection par la proposition 2.7.i. ——————————— □

Ceci nous permet de poser la

DEFINITION Un ensemble A est dit *fini* s'il existe $n \in \mathbb{N}$ et une bijection de n sur A . On dit que n est le *nombre d'éléments* de A ou sa *cardinalité* , noté $\#(A)$.

Si $n \longrightarrow A : k \longmapsto a_k$ est une bijection, on dit que $(a_k)_{k=0,\ldots,n-1}$ est une *énumération (finie)* de A .

Un ensemble qui n'est pas fini est dit *infini* . On dit que A est *dénombrable* si A est fini ou s'il existe une bijection de $\mathbb{N}$ sur A . Si cette bijection est notée

$$\mathbb{N} \longrightarrow A : k \longmapsto a_k \ ,$$

on dit que $(a_k)_{k\in\mathbb{N}}$ est une *énumération (infinie dénombrable)* de A .

REMARQUE Si A est un ensemble à n éléments et s'il existe une bijection de A sur un ensemble B , alors B a n éléments.

EXERCICE 1 Soient $m, n \in \mathbb{N}$ et X_m, X_n des ensembles à m respectivement n éléments. Trouver des conditions nécessaires et suffisantes sur m, n pour qu'il existe une application

$$f : X_m \longrightarrow X_n$$

telle que

(a) f soit injective.
(b) f soit surjective.
(c) f soit bijective.

EXERCICE 2 Existe-t-il une application bijective $f : \mathbb{N} \longrightarrow \mathbb{Z}$?

3.5 Généralisation du principe de récurrence

Récurrence à partir de m *Soient* $P(x)$ *une propriété et* $m \in \mathbb{N}$ *. Si* $P(m)$ *est vraie et si, quel que soit* n *, on a*

$$n \in \mathbb{N}\ ,\ n \geqslant m \text{ et } P(n) \quad \textit{entraîne} \quad P(n+1)\ ,$$

alors la propriété $P(n)$ *est vraie pour tout* $n \in \mathbb{N}$ *tel que* $n \geqslant m$ *.*

Il suffit d'appliquer le principe de récurrence 3.1 à la propriété

$$R(x) : x \in \mathbb{N} \quad \text{et} \quad x \geqslant m \quad \text{entraîne} \quad P(x)\ .$$

On a $R(0)$. En effet si $m = 0$, on a bien $P(0)$, tandis que si $m \neq 0$, alors $0 \geqslant m$ est fausse.

Supposons maintenant que $R(n)$ soit vraie et montrons que $R(n+1)$ l'est aussi. Soit donc $n+1 \geqslant m$ et il nous suffit de prouver $P(n+1)$. Si $n+1 = m$, c'est bien le cas puisque $P(m)$ est vraie. Si $n+1 > m$, on a $n \geqslant m$ et en appliquant $R(n)$ on obtient $P(n)$. Mais par la propriété de récurrence on en déduit $P(n+1)$. ——— □

PROPOSITION *L'application* $x \longmapsto x+1 : \mathbb{N} \longrightarrow \{n \in \mathbb{N} \mid n \neq 0\}$ *est bijective. En particulier, pour tout* $n \in \mathbb{N}$ *tel que* $n \neq 0$ *, il existe un unique* $x \in \mathbb{N}$ *tel que* $n = x+1$ *.*

Démontrons la surjectivité de $f : x \longmapsto x+1$ sur $\{n \in \mathbb{N} \mid n \neq 0\}$ par récurrence sur n à partir de 1 . On a évidemment $1 = 0+1 = f(0)$ et le pas de récurrence est trivialement vérifié puisque

$$n+1 = f(n)\ !$$

Pour l'injectivité, étant donné $u, v \in \mathbb{N}$ tels que $u \neq v$, nous pouvons par le théorème 3.3 supposer que $u < v$. Grâce à la remarque 3.3.1 on a alors

$$f(u) = u+1 \leqslant v < v+1 = f(v)\ ,$$

donc $f(u) \neq f(v)$. ——— □

DEFINITION On pose $\mathbb{N}^* := \{n \in \mathbb{N} \mid n \neq 0\}$ et pour tout $n \in \mathbb{N}^*$, l'unique nombre naturel x tel que $n = x+1$ est désigné par $n-1$.

Plus généralement on a la

Récurrence générale à partir de m *Soient* $P(x)$ *une propriété et* $m \in \mathbb{N}$ *. Si pour tout* $n \in \mathbb{N}$ tel que $n \geqslant m$ *, le* pas de récurrence

$$\forall l\,[m \leqslant l < n \Rightarrow P(l)] \quad \Longrightarrow \quad P(n)$$

est satisfait, alors la propriété $P(n)$ *est vraie pour tout* $n \in \mathbb{N}$ *tel que* $n \geqslant m$ *.*

Remarquons que le pas de récurrence, pour $n = m$, est un théorème si, et seulement si, $P(m)$ est vraie, puisque le membre de gauche de l'implication est trivialement satisfait !

EXERCICE L'ensemble $A := \{n \in \mathbb{N} \mid 2^n < n!\}$ est infini.

3.6 Addition dans $\mathbb{N}$

DEFINITION 1 Soit X un ensemble. Pour $n \in \mathbb{N}$, on dit qu'une famille

$$(x_j)_{j\in n} = (x_j)_{j=0,\dots,n-1}$$

d'éléments de X , i.e. une application de $n = \{j \in \mathbb{N} \mid j < n\}$ dans X , est une *suite (finie) à n éléments)* dans X .

On dit qu'une famille $(x_k)_{k\in\mathbb{N}}$ d'éléments de X , i.e. une application de $\mathbb{N}$ dans X , est une *suite (infinie)* dans X .

L'ensemble des suites finies à n éléments est évidemment désigné par X^n , celui des suites infinies par $X^{\mathbb{N}}$.

EXERCICE 1 Montrer que, pour tout ensemble X , on a $X^0 = X^{\emptyset} = \{\emptyset\}$ et que X^n peut être défini par récurrence en posant

$$X^{n+1} := X^n \times X \ .$$

Comment faut-il préciser cette assertion ?

Il faut en particulier identifier $\{0\} \times X$ avec X !

Suites récurrentes *Si $\Phi : X \longrightarrow X$ est une application et $x_0 \in X$, alors il existe une unique suite $(x_k)_{k\in\mathbb{N}}$ dans X telle que*

$$x_{k+1} = \Phi(x_k) \quad \textit{pour tout } k \in \mathbb{N} \ .$$

On dit que $(x_k)_{k\in\mathbb{N}}$ a été définie par récurrence en partant de x_0 .

La démonstration n'est pas immédiate et nous l'omettrons.

DEFINITION 2 Pour tout $a \in \mathbb{N}$, on définit par récurrence

$$a + 0 := a \quad \text{et} \quad a + (k+1) := (a+k) + 1 \ ,$$

en utilisant l'application $\Phi : \mathbb{N} \longrightarrow \mathbb{N} : x \longmapsto x + 1$.

EXEMPLE On a

$$2 + 2 = 2 + (1 + 1) = (2 + 1) + 1 = 3 + 1 = 4 \ .$$

THEOREME *L'addition dans* $\mathbb{N}$

$$\mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} : (a, b) \longmapsto a + b$$

est associative, commutative, 0 *est son élément neutre et tout élément est simplifiable, i.e. pour tout $a, b, c \in \mathbb{N}$, on a*

(i) associativité

$$(a + b) + c = a + (b + c)$$

(ii) commutativité
$$a + b = b + a$$

(iii) neutralité
$$a + 0 = 0 + a = a$$

(iv) simplification
$$a + c = b + c \quad \Longrightarrow \quad a = b \ .$$

Les démonstrations se font par récurrence. On prouve d'abord la neutralité de 0 . Traitons le cas de l'associativité en raisonnant par récurrence sur c . Si $c = 0$, on a

$$(a + b) + 0 = a + b = a + (b + 0) \ .$$

Si la formule est vraie pour c , alors

$$(a + b) + (c + 1) = [(a + b) + c] + 1 = [a + (b + c)] + 1 =$$

$$= a + [(b + c) + 1] = a + [b + (c + 1)] \ .$$

La commutativité s'obtient de manière analogue. Quant à la simplification, il suffit d'utiliser le fait que $\Phi : x \longmapsto x + 1$ est injective par la proposition 3.5. ——— □

PROPOSITION *L'addition dans* $\mathbb{N}$ *est compatible avec l'ordre, i.e. pour tout* $a, b, c \in \mathbb{N}$ *, on a*

compatibilité
$$a \leqslant b \quad \Longrightarrow \quad a + c \leqslant b + c \ .$$

C'est immédiat par récurrence sur c . ——— □

REMARQUE La définition d'une suite récurrente peut se généraliser de la manière suivante :

Soient, pour tout $n \in \mathbb{N}$, une application $\Phi_n : X^n \longrightarrow X$. Alors il existe une unique suite $(x_k)_{k\in\mathbb{N}}$ dans X telle que

$$x_n = \Phi_n (x_0, \ldots, x_{n-1}) \quad \text{pour tout } n \in \mathbb{N} \ .$$

On remarquera que $X^0 = \{0\}$ (exemple 2.6.6) ; il est donc raisonnable de poser $(x_0, \ldots, x_{-1}) = 0$. L'application $\Phi_0 : X^0 \longrightarrow X$ est donc univoquement déterminée par $x_0 := \Phi_0 (0)$.

En fait on utilise souvent le résultat suivant formulé de manière plus intuitive. Considérons, pour tout $n \in \mathbb{N}$, une propriété P_n qui dépend de $n + 1$ variables et un ensemble x_0 tel que $P_0 (x_0)$. Il existe alors une suite $(x_k)_{k\in\mathbb{N}}$ d'ensembles telle que $P_n (x_0, .., x_n)$ soit vraie pour tout $n \in \mathbb{N}$ si, pour tout $n \in \mathbb{N}^*$, en admettant que

$$P_k (x_0, \ldots, x_k) \text{ soit vraie pour tout } k \in \mathbb{N}^* \text{ tel que } k < n \ ,$$

on peut construire explicitement un ensemble x_n tel que

$$P_n (x_0, \ldots, x_n) \text{ soit vraie.}$$

EXERCICE 2 Démontrer la commutativité de l'addition des nombres naturels. Pour cela démontrer tout d'abord par récurrence que, pour tout $a \in \mathbb{N}$, on a

$$a + 0 = 0 + a \quad \text{et} \quad a + 1 = 1 + a \ .$$

EXERCICE 3 Si M est une partie de $\mathbb{N}$ satisfaisant à la propriété suivante

$$3 \in M \quad \text{et} \quad m \in M \Longrightarrow 2m \pm 1 \in M \ ,$$

alors M est l'ensemble des nombres entiers naturels impairs $\geqslant 3$.

EXERCICE 4 Les *nombres de Fibonacci* sont définis récursivement par

$$a_0 := 1 \quad , \quad a_1 := 1 \quad \text{et} \quad a_{n+1} := a_n + a_{n-1} \text{ pour tout } n \geqslant 1 \ .$$

Déterminer l'ensemble des $n \in \mathbb{N}$ tels que

$$a_n \leqslant \left(\frac{3}{2}\right)^n \ .$$

Pour la définition des puissances et le calcul dans $\mathbb{Q}$ voir 3.12 et 4.6.

3.7 Le comptage

La proposition 3.5 peut être généralisée.

LEMME *Pour tout $a \in \mathbb{N}$, l'application*

$$x \longmapsto x + a : \mathbb{N} \longrightarrow \{y \in \mathbb{N} \mid y \geqslant a\}$$

est bijective.

Pour tout $x \in \mathbb{N}$, la proposition 3.6 montre que $x + a \geqslant a$, et cette application est injective par la règle de simplification (théorème 3.6). La surjectivité se démontre par récurrence sur y à partir de a . Le cas $y = a$ est trivial, et si y est de la forme $x + a$, alors

$$y + 1 = (x + a) + 1 = x + (a + 1) = x + (1 + a) = (x + 1) + a \ .$$

□

COROLLAIRE *Pour tout $a, b \in \mathbb{N}$, l'équation*

$$x + a = b$$

possède au moins une solution $x \in \mathbb{N}$ si, et seulement si, $a \leqslant b$. Dans ce cas cette solution est unique.

DEFINITION Cette unique solution est notée $b - a$.

THEOREME *Si A et B sont des ensembles finis disjoints, alors*

$$\#(A \cup B) = \#(A) + \#(B) \ .$$

Soient $n = \#(A)$, $m = \#(B)$ et $f : n \longrightarrow A$, $g : m \longrightarrow B$ des bijections. Par le lemme et la proposition 3.6, l'application

$$h : m \longrightarrow \{x \in \mathbb{N} \mid n \leqslant x < n + m\} : x \longmapsto x + n$$

est bijective et on a

$$n + m = \{x \in \mathbb{N} \mid 0 \leqslant x < n\} \cup \{x \in \mathbb{N} \mid n \leqslant x < n + m\} \ .$$

Il est alors clair que l'application

$$n + m \longrightarrow A \cup B : x \longmapsto \begin{cases} f(x) & 0 \leqslant x < m \\ & \text{si} \\ g(h^{-1}(x)) & m \leqslant x < n + m \end{cases}$$

est bijective, ce qui finit de prouver le théorème. □

EXERCICE Soient A, B et C des ensembles. Montrer

(a)
$$\#(A \cup B) + \#(A \cap B) = \#(A) + \#(B) \ .$$

(b)
$$\#(A \cup B \cup C) =$$

$$= \#(A) + \#(B) + \#(C) - \#(A \cap B) - \#(A \cap C) - \#(B \cap C) + \#(A \cap B \cap C) \ .$$

Utiliser l'exercice 2.5.

3.8 Multiplication dans $\mathbb{N}$

DEFINITION Pour tout $a \in \mathbb{N}$, on définit par récurrence

$$a \cdot 0 := 0 \quad \text{et} \quad a \cdot (k+1) := a \cdot k + a \ .$$

THEOREME *La multiplication dans* $\mathbb{N}$

$$\mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} : (a,b) \longmapsto a \cdot b$$

est associative, commutative, 1 *est son élément neutre et tout élément de* $\mathbb{N} \setminus \{0\}$ *est simplifiable, i.e. pour tout* $a, b, c \in \mathbb{N}$ *, on a*

(i) associativité $\quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$

(ii) commutativité $\quad a \cdot b = b \cdot a$

(iii) neutralité $\quad a \cdot 1 = 1 \cdot a = a$

(iv) simplification $\quad c \neq 0$ *et* $a \cdot c = b \cdot c \quad \Longrightarrow \quad a = b \ .$

PROPOSITION *La multiplication dans* $\mathbb{N}$ *est distributive par rapport à l'addition et compatible avec l'ordre, i.e. pour tout* $a, b, c \in \mathbb{N}$ *, on a*

(i) distributivité $\quad a \cdot (b+c) = a \cdot b + a \cdot c$

(ii) compatibilité $\quad a \leqslant b \quad \Longrightarrow \quad a \cdot c \leqslant b \cdot c \ .$

En outre, étant donné $n \in \mathbb{N}$ *, on a la*

(iii) division avec reste : pour tout $x \in \mathbb{N}$ *, il existe* $q, r \in \mathbb{N}$ *uniques tels que*

$$x = q \cdot n + r \quad et \quad r < n \ .$$

Les démonstrations sont laissées au lecteur. ——————————— □

COROLLAIRE *Si* A *et* B *sont des ensembles finis, alors*

$$\#(A \times B) = \#(A) \cdot \#(B) \ .$$

On le démontre par récurrence sur le nombre d'éléments n de A . Si $n = 0$, on a $A = \emptyset$, donc $A \times B = \emptyset$ et par suite $\#(A \times B) = 0$. Supposons donc que la formule soit vraie pour n et soit A un ensemble à $n+1$ éléments. En choisissant $a \in A$, on a

$$A \times B = [(A \setminus \{a\}) \times B] \cup \{a\} \times B \ .$$

Comme les deux ensembles de cette réunion sont disjoints on obtient

$$\#(A \times B) = \#((A \setminus \{a\}) \times B) + \#(\{a\} \times B) = n \cdot \#(B) + \#(B) =$$

$$= (n+1) \cdot \#(B) = \#(A) \cdot \#(B) \ .$$

□

EXERCICE Montrer que tout nombre naturel $n \in \mathbb{N}$ est ou bien pair, i.e. il existe $k \in \mathbb{N}$ tel que $n = 2k$, ou bien impair, i.e. il existe $k \in \mathbb{N}$ tel que $n = 2k - 1$.

3.9 Somme et produit d'une suite

Soit X un ensemble muni de deux opérations, appelées addition et multiplication et notées $+$ respectivement $\cdot$, i.e. on se donne

$$+ : X \times X \longrightarrow X : (x, y) \longmapsto x + y \quad \text{et} \quad \cdot : X \times X \longrightarrow X : (x, y) \longmapsto x \cdot y \ .$$

DEFINITION Soient $m, n \in \mathbb{N}$ tels que $m \leqslant n$ et $(x_k)_{k=m,\ldots,n}$ une suite finie de X . On définit par récurrence la *somme* et le *produit de* $(x_k)_{k=m,\ldots,n}$ par :

$$\sum_{k=m}^{m} x_k := x_m \quad \text{et} \quad \sum_{k=m}^{l+1} x_k := \left(\sum_{k=m}^{l} x_k \right) + x_{l+1} \text{ si } m \leqslant l < n \ ,$$

ainsi que

$$\prod_{k=m}^{m} x_k := x_m \quad \text{et} \quad \prod_{k=m}^{l+1} x_k := \left(\prod_{k=m}^{l} x_k \right) \cdot x_{l+1} \text{ si } m \leqslant l < n \ .$$

On vérifie facilement les formules suivantes obtenues en changeant l'indice de sommation :

$$l = k - m + p \quad \text{ou} \quad k = l - p + m$$

$$\sum_{k=m}^{n} x_k = \sum_{l=p}^{p+n-m} x_{l-p+m} \ .$$

De même

$$\prod_{k=m}^{n} x_k = \prod_{l=p}^{p+n-m} x_{l-p+m} \ .$$

Si les opérations sont associatives, pour tout $p \in \mathbb{N}$ tel que $m < p \leqslant n$, on a

$$\sum_{k=m}^{n} x_k = \left(\sum_{k=m}^{p-1} x_k \right) + \left(\sum_{k=p}^{n} x_k \right)$$

et

$$\prod_{k=m}^{n} x_k = \left(\prod_{k=m}^{p-1} x_k \right) \cdot \left(\prod_{k=p}^{n} x_k \right) \ .$$

Si les opérations sont associatives et commutatives, pour toutes suites finies $(x_k)_{k=m,\ldots,n}$ et $(y_k)_{k=m,\ldots,n}$ de X , on a

$$\sum_{k=m}^{n} (x_k + y_k) = \left(\sum_{k=m}^{n} x_k \right) + \left(\sum_{k=m}^{n} y_k \right)$$

et

$$\prod_{k=m}^{n} (x_k \cdot y_k) = \left(\prod_{k=m}^{n} x_k \right) \cdot \left(\prod_{k=m}^{n} y_k \right)$$

Si en plus la multiplication est distributive par rapport à l'addition, alors

$$\left(\sum_{k=m}^{n} x_k\right) \cdot \left(\sum_{l=p}^{q} y_l\right) = \sum_{k=m}^{n} \left(\sum_{l=p}^{q} x_k \cdot y_l\right) = \sum_{l=p}^{q} \left(\sum_{k=m}^{n} x_k \cdot y_l\right) \ .$$

EXEMPLE Calculons

$$\sum_{k=0}^{n} (2k+1) = \sum_{k=0}^{n} 2k + \sum_{k=0}^{n} 1 = 2 \cdot \sum_{k=0}^{n} k + (n+1) =$$

$$= 2 \cdot \frac{n\,(n+1)}{2} + n + 1 = (n+1)^2 \ .$$

REMARQUE Si l'addition, respectivement la multiplication, possède un élément neutre noté 0 , respectivement 1 , il est souvent commode de définir la somme, respectivement le produit, sur une famille d'indices vide par 0 , respectivement 1 .

Par exemple

$$\sum_{k=m}^{m-1} x_k = 0 \quad \text{et} \quad \prod_{k=n+1}^{n} x_k = 1 \ .$$

EXERCICE 1 Montrer par récurrence que, pour tout $k \in \mathbb{N}^*$, on a

$$\sum_{l=1}^{2k} (-1)^{l+1} \cdot \frac{1}{l} = \sum_{l=1}^{k} \frac{1}{k+l} \ .$$

EXERCICE 2 Soit $a \in \mathbb{N}$ tel que $a \geqslant 2$. Montrer que, pour tout $n \in \mathbb{N}$, il existe un $c_n \in \mathbb{N}$ tel que

$$a^n - 1 = c_n \cdot (a-1) \ ,$$

et que ces c_n satisfont à la relation de récurrence

$$c_0 := 0 \quad \text{et} \quad c_{n+1} := a \cdot c_n + 1 \text{ pour tout } n \in \mathbb{N} \ .$$

EXERCICE 3 Déterminer l'ensemble des $n \in \mathbb{N}$ tels que

$$n^2 < 2^n \ .$$

Pour la définition des puissances entières voir 3.12.

3.10 Permutations

Soit A un ensemble fini à n éléments, par exemple un ensemble de n livres, et $(a_k)_{k=0,\dots,n-1}$, $(b_k)_{k=0,\dots,n-1}$ deux énumérations de A , i.e. deux bibliothèques différentes faites avec ces livres. Désignons par $f, g : n \longrightarrow A$ les deux applications bijectives correspondantes, i.e. telles que pour tout $k = 0, \dots, n-1$, on ait

$$a_k = f(k) \quad \text{et} \quad b_k = g(k) \ .$$

Considérons le diagramme

$$\begin{array}{ccccc} & & \sigma & & \\ n & & \longrightarrow & & n \\ & \searrow & & \nearrow & \\ f & & & & \overset{-1}{g} \\ & & A & & \end{array}$$

i.e. $\sigma := \overset{-1}{g} \circ f$. On a

$$a_k = f(k) = g \circ \overset{-1}{g} \circ f(k) = g(\sigma(k)) = b_{\sigma(k)}$$

et σ est une bijection de n sur n , permettant de retrouver le k-ième livre de la première bibliothèque dans la seconde.

DEFINITION 1 Une bijection de n sur n s'appelle une *permutation* de n . On pose

$$n! := \prod_{k \in n} (k+1) \ .$$

On dit *factorielle* n (ou n factorielle).

On a

$$0! = 1 \quad \text{et} \quad (n+1)! = (n+1) \cdot n! \ .$$

DEFINITION 2 Si A, B sont des ensembles, on désigne par $Bij(A, B)$ l'ensemble des bijections de A sur B .

LEMME *Soient A, B des ensembles à n éléments et $f : n \longrightarrow A$, $g : n \longrightarrow B$ des bijections. Alors toute injection $\sigma : A \longrightarrow B$ est surjective et l'application*

$$\Phi : Bij(A, B) \longrightarrow Bij(n, n) : \sigma \longmapsto \overset{-1}{g} \circ \sigma \circ f$$

est bijective.

En effet on a le diagramme

$$\begin{array}{ccc} & \overset{\sigma}{\longrightarrow} & \\ A & & B \\ f \uparrow & & \uparrow g \\ n & \longrightarrow & n \\ & \overset{-1}{g} \circ \sigma \circ f & \end{array}$$

La proposition 2.7.i montre alors que $\overset{-1}{g} \circ \sigma \circ f$ est injective, donc bijective par le théorème 3.4. La seconde partie est immédiate puisque, pour tout $\tau \in Bij(n,n)$, on a

$$\overset{-1}{\Phi}(\tau) = g \circ \tau \circ \overset{-1}{f} .$$

□

THEOREME *Pour tout ensembles A, B à n éléments, il y a $n!$ applications bijectives de A sur B , i.e.*

$$\#(Bij(A,B)) = n! .$$

D'après le lemme, on peut supposer que $A = B = n$. Le résultat est clair pour $n = 0$ car la seule application de $\emptyset$ dans $\emptyset$ est celle dont le graphe est $\emptyset$ et elle est évidemment bijective. Il l'est aussi pour $n = 1$; la seule application de 1 dans 1 est $0 \longmapsto 0$. Supposons donc que le résultat soit vrai pour n et soit $\sigma : n+1 \longrightarrow n+1$ une bijection. Considérons l'application

$$\tau_\sigma : n \longrightarrow n : x \longmapsto \begin{cases} \sigma(x) & \sigma(x) < \sigma(n) \\ & \text{si} \\ \sigma(x) - 1 & \sigma(x) > \sigma(n) \end{cases} .$$

On montre immédiatement que l'application

$$Bij(n+1, n+1) \longrightarrow n+1 \times Bij(n,n) : \sigma \longmapsto (\sigma(n), \tau_\sigma)$$

est bijective, donc

$$\#(Bij(n+1, n+1)) = (n+1) \cdot \#(Bij(n,n)) = (n+1) \cdot n! = (n+1)!$$

par le corollaire 3.8. □

EXERCICE Déterminer l'ensemble des $n \in \mathbb{N}$ tels que

(a)
$$n! \leqslant 2^n .$$

(b)
$$n! \leqslant \left(\frac{n}{2}\right)^n .$$

3.11 Coefficients binomiaux

DEFINITION Pour tout $n, k \in \mathbb{N}$, on définit par récurrence sur n le *coefficient binomial* $\binom{n}{k}$ en posant

$$\binom{0}{0} := 1 \quad \text{et} \quad \binom{0}{k} := 0 \text{ pour tout } k \geqslant 1 \ ,$$

et

$$\binom{n+1}{0} := 1 \quad \text{et} \quad \binom{n+1}{k} := \binom{n}{k-1} + \binom{n}{k} \text{ pour tout } k \geqslant 1 \ .$$

Cette définition peut être visualisée à l'aide du *triangle de Pascal* :

$n \diagdown k$	0	1	2	3	4	5	6
0	1	0	0	0	0	0	0
1	1	1	0	0	0	0	0
2	1	2	1	0	0	0	0
3	1	3	3	1	0	0	0
4	1	4	6	4	1	0	0
5	1	5	10	10	5	1	0
6	1	6	15	20	15	6	1

LEMME *Pour tout $n \in \mathbb{N}$, on a*

$$\binom{n}{0} = \binom{n}{n} = 1 \quad \textit{et} \quad \binom{n}{k} = 0 \quad \textit{pour tout } k \in \mathbb{N} \textit{ tel que } k > n \ .$$

Le cas $n = 0$ est clair. Si l'assertion est vraie pour n , alors

$$\binom{n+1}{0} = 1$$

et

$$\binom{n+1}{n+1} = \binom{n}{n+1} + \binom{n}{n} = 0 + 1 = 1$$

et, pour tout $k > n+1$, il vient

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1} = 0 \ ,$$

puisque $k - 1 > n$. □

PROPOSITION *Pour tout $n, k \in \mathbb{N}$, le nombre de parties à k éléments d'un ensemble à n éléments est $\binom{n}{k}$.*

Le cas $n = 0$ est clair, puisque la seule partie de $\emptyset$ est $\emptyset$. Supposons alors que la proposition soit vraie pour n et soit A un ensemble à $n+1$ éléments. La seule partie à 0 éléments étant $\emptyset$, nous pouvons admettre que $k \geqslant 1$. Choisissons $a \in A$. Si X est une partie de A à k éléments, on a

$$X \subset A \setminus \{a\}$$

ou bien

$$X = Y \cup \{a\} \ , \quad \text{où } Y \text{ est une partie de } A \setminus \{a\} \text{ à } k-1 \text{éléments.}$$

Par l'hypothèse de récurrence il y a $\binom{n}{k}$ parties possibles dans le premier cas et $\binom{n}{k-1}$ parties possibles dans le second. On a donc

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$$

parties à k éléments dans A , ce qu'il fallait démontrer. ——————————— □

EXERCICE Montrer par récurrence que, pour tout $n, m \in \mathbb{N}$ tels que $n \geqslant m$, on a

$$\sum_{l=m}^{n} \binom{l}{m} = \binom{n+1}{m+1} .$$

3.12 Formule du binôme et somme géométrique

Soit X un ensemble muni d'une addition et d'une multiplication. Nous supposerons que ces opérations sont associatives, commutatives et possèdent chacune un élément neutre, noté respectivement 0 et 1 , et que la multiplication est distributive par rapport à l'addition.

DEFINITION Pour tout $x \in X$ et $n \in \mathbb{N}$, on définit $n \cdot x$ et x^n par récurrence sur n en posant

$$0 \cdot x := 0 \quad \text{et} \quad x^0 := 1$$

ainsi que

$$(n+1) \cdot x := n \cdot x + x \quad \text{et} \quad x^{n+1} := x^n \cdot x \ .$$

Pour tout $n, m \in \mathbb{N}$ et $x, y \in X$, on vérifie facilement les formules :

$$x \cdot (n \cdot y) = n \cdot (x \cdot y) \ , \ n \cdot (x+y) = n \cdot x + n \cdot y \ , \ (n+m) \cdot x = n \cdot x + m \cdot x \ ,$$

ainsi que

$$x^n \cdot x^m = x^{n+m} \ , \ (x^n)^m = x^{n \cdot m} \text{ et } x^n \cdot y^n = (x \cdot y)^n \ .$$

Formule du binôme *Pour tout $x, y \in X$ et $n \in \mathbb{N}$, on a*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot x^k \cdot y^{n-k} \ .$$

Les cas $n = 0, 1, 2$ sont bien connus. Supposons donc la formule vraie pour n et démontrons-la pour $n+1$. On a

$$(x+y)^{n+1} = (x+y) \cdot (x+y)^n = (x+y) \cdot \sum_{k=0}^{n} \binom{n}{k} \cdot x^k \cdot y^{n-k} =$$

$$= x \cdot \sum_{k=0}^{n} \binom{n}{k} \cdot x^k \cdot y^{n-k} + y \cdot \sum_{k=0}^{n} \binom{n}{k} \cdot x^k \cdot y^{n-k} =$$

$$= \sum_{k=0}^{n} \binom{n}{k} \cdot x^{k+1} \cdot y^{n-k} + \sum_{k=0}^{n} \binom{n}{k} \cdot x^k \cdot y^{n-k+1} =$$

$$= \sum_{k=0}^{n-1} \binom{n}{k} \cdot x^{k+1} \cdot y^{n-k} + \binom{n}{n} \cdot x^{n+1} \cdot y^0 + \binom{n}{0} \cdot x^0 \cdot y^{n+1} + \sum_{k=1}^{n} \binom{n}{k} \cdot x^k \cdot y^{n-k+1} =$$

$$= \binom{n}{0} \cdot x^0 \cdot y^{n+1} + \sum_{j=1}^{n} \binom{n}{j-1} \cdot x^j \cdot y^{n-j+1} + \sum_{k=1}^{n} \binom{n}{k} \cdot x^k \cdot y^{n-k+1} + \binom{n}{n} \cdot x^{n+1} \cdot y^0 =$$

$$= \binom{n}{0} \cdot x^0 \cdot y^{n+1} + \sum_{k=1}^{n} \left[\binom{n}{k-1} + \binom{n}{k} \right] \cdot x^k \cdot y^{n-k+1} + \binom{n}{n} \cdot x^{n+1} \cdot y^0 =$$

$$= \binom{n+1}{0} \cdot x^0 \cdot y^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} \cdot x^k \cdot y^{n-k+1} + \binom{n+1}{n+1} \cdot x^{n+1} \cdot y^0 =$$

$$= \sum_{k=0}^{n+1} \binom{n+1}{k} \cdot x^k \cdot y^{n+1-k} \ ,$$

en ayant utilisé le lemme 3.11. □

COROLLAIRE *On a*

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n \quad et \quad \sum_{k=0}^{n} (-1)^k \cdot \binom{n}{k} = 0 \ .$$

En particulier l'ensemble des parties d'un ensemble à n éléments a 2^n éléments.

Il suffit de prendre $X = \mathbb{N}$ et $x = y = 1$, respectivement $x = -1$ et $y = 1$, et d'utiliser la formule du binôme. □

Somme géométrique Pour tout $x \in X$ et tout $m, n \in \mathbb{N}$, on a

$$(1-x) \cdot \sum_{k=m}^{n} x^k = x^m - x^{n+1} \ .$$

En effet, on a

$$(1-x) \cdot \sum_{k=m}^{n} x^k = \sum_{k=m}^{n} x^k - \sum_{k=m}^{n} x^{k+1} =$$

$$= x^m + \sum_{k=m+1}^{n} x^k - \sum_{k=m+1}^{n} x^k - x^{n+1} = x^m - x^{n+1} \ .$$

□

REMARQUE Si X est un corps (cf. 4.5) et $x \neq 1$, alors

$$\sum_{k=m}^{n} x^k = \frac{x^m - x^{n+1}}{1-x} \ .$$

EXERCICE 1 Soit $n \in \mathbb{N}^*$. Montrer que la cardinalité de l'ensemble des parties ayant au moins $n+1$ éléments dans un ensemble à $2n$ éléments est égale à

$$\frac{1}{2} \cdot \left(2^{2n} - \binom{2n}{n} \right) \ ,$$

en utilisant la formule du binôme

$$2^{2n} = \sum_{l=0}^{2n} \binom{2n}{l} \ .$$

EXERCICE 2 Soient $n \in \mathbb{N}^*$ et $x \in X$. Montrer que

$$\prod_{k=0}^{n-1} \left(1 + x^{2^k}\right) = \sum_{l=0}^{2^n-1} x^l \ ,$$

puis que

$$(1-x)\left[\prod_{k=0}^{n-1} \left(1 + x^{2^k}\right) - 1\right] = x\left(1 - x^{2^n-1}\right) \ .$$