Université Paris 13, Institut Galilée
Département de Mathématiques
Licence 2ème année Informatique
2013-2014

Cours de Mathématiques pour l'Informatique
Des nombres aux structures
Sylviane R. Schwer

Leçon du mardi 14 janvier 2014
Rappels concernant l'ensemble des nombres naturels

Qu'est ce qu'un nombre ? Mathématiquement, un nombre est un élément d'un ensemble structuré de nombres. Fondés sur des propriétés algébriques, il y a l'ensemble des nombres naturels, l'ensemble des nombres entiers relatifs, l'ensemble des nombres rationnels, l'ensemble des nombres réels, l'ensemble des nombres complexes, ...

Un ensemble de nombres est donc un exemple particulier de *structure algébrique*, c'est-à-dire une famille d'objets qui peuvent d'une part se combiner à l'aide de certains opérateurs pour donner un objet de même nature – ces opérateurs sont alors dits *lois* ou *opérations internes*, comme l'addition – et d'autre part se combiner avec des objets d'une autre structure pour donner des objets de cette autre structure – ces opórateurs sont alors dits *lois* ou *opérations externes*, comme la multiplication avec des réels dans les espaces vectoriels ou les ensembles de fonctions.

L'étude de ce cours porte sur l'ensemble de base des nombres, l'ensemble des entiers naturels, sur lequel se fondent les constructions de tous les autres ensembles de nombres.

Nous notons :
$\mathbb{N}$ l'ensemble des nombres naturels positifs ou nuls 0, 1, 2, 3 ...
$\mathbb{N}_*$ l'ensemble des nombres naturels strictement positifs ou nuls 1, 2, 3 ...

Nous rappelons d'abord les propriétés indispensables à connaître sur les opérations arithmétiques élémentaires : addition, multiplications, puis puis nous intéresserons à la relation d'ordre naturel – l'ordre lié à la numération – de $\mathbb{N}$. Nous terminerons par les opórateurs $\sum$ et $\prod$, appliqués aux suites ou fonctions entières à valeurs entières.

1 Propriétés élémentaires des opérations *addition* et *multiplication* dans $\mathbb{N}$

L'addition de deux nombres entiers naturels a pour résultat un nombre entier naturel appelé *somme*. La multiplication de deux nombres entiers naturels a pour résultat un nombre entier naturel appelé *produit*. Nous sacrifierons à l'usage de confondre l'opération à son résultat. Ces deux opérations sont des opérations internes de $\mathbb{N}$ définie par les égalités :

somme (+) : $n + 0 = n$ et $n + (m + 1) = (n + m) + 1$.

Si $a + b = c$, alors c est la somme de a et de b, résultat de l'addition de a et de b.

On peut dire que b est la différence entre a et c et a est la différence entre b et c.

produit ($\times$) : $n \times 0 = 0$ et $n \times (m + 1) = n \times m + n$.

Si $a \times b = c$, alors c est le produit de a et de b, résultat de la multiplication de a et de b.

On dit que c est un *multiple* de a. Il est aussi multiple de b. Réciproquement, on dit que a et b sont des *diviseurs* de c.

1.1 propriétés communes

Nous énonçons ces propriétés sans les prouver, ce qui se fait aisément par récurrence. Notons $\perp$ l'une ou l'autre des deux opérations $+$ ou $\times$.

commutativité : $\forall a, b \in \mathbb{N}, a \perp b = b \perp a$

Cette propriété permet de ne regarder le comportement des opérations que d'un seul côté. C'est pourquoi il est judicieux de commencer par la vérifier.

associativité : $\forall a, b, c \in \mathbb{N}, a \perp (b \perp c) = (a \perp b) \perp c$

1.2 éléments particuliers

élément neutre [1] $\varepsilon_\perp \in \mathbb{N}, \forall a \in \mathbb{N}, a \perp \varepsilon_\perp = \varepsilon_\perp \perp a = a$

- 0 est l'élément neutre de l'addition dans $\mathbb{N}$: $\forall a \in \mathbb{N}, 0 + a = a + 0 = a$
- 1 est l'élément neutre de la multiplication dans $\mathbb{N}$: $\forall a \in \mathbb{N}, 1 \times a = a \times 1 = a$

Un ensemble muni d'une opération associative et qui possède un élément neutre est appelé *monoïde*. Si l'opération est commutative, on dit que le monoïde est commutatif.

$\mathbb{N}$ est un monoïde commutatif additif et multiplicatif.

élément absorbant [2] $\gamma_\perp \in \mathbb{N}, \forall a \in \mathbb{N}, a \perp \gamma_\perp = \gamma_\perp \perp a = \gamma_\perp$.

- l'addition n'a pas d'élément absorbant.
- 0 est élément absorbant de la multiplication : $\forall a \in \mathbb{N}, 0 \times a = a \times 0 = 0$.

[1] On démontrera dans la seconde partie du cours que s'il existe un élément neutre, celui-ci est unique.

[2] On démontrera dans la seconde partie du cours que s'il existe un élément absorbant, celui-ci est unique.

1.3 propriétés propres aux éléments de la structure

paire d'éléments symétriques. $a, b \in \mathbb{N}$ sont symétriques relativement à l'opération $\perp$ s'ils satisfont[3] $a \perp b = b \perp a = \varepsilon_\perp$.

$(e_\perp, \varepsilon_\perp)$ est une paire d'éléments symétriques.

- Pour l'addition, a et b sont dits *opposés*. La seule paire d'éléments symétriques de $\mathbb{N}$ pour l'addition est $(0, 0)$.
- Pour la multiplication, a et b sont dits inverses. La seule paire d'éléments symétriques de $\mathbb{N}$ pour la multiplication est $(1, 1)$.

éléments réguliers $a \in \mathbb{N}$ est régulier si l'équivalence suivante est satisfaite

$$\forall b, c \in \mathbb{N}, \quad b = c \iff a \perp b = a \perp c \iff b \perp a = c \perp a.$$

- Tout entier naturel est régulier pour l'addition.
- Tout entier naturel différent de 0, élément absorbant du produit, est régulier pour la multiplication :
  $(a \times b = a \times c) \iff (b = c \ \ ou \ \ a = 0)$
  $(b \times a = c \times a) \iff (b = c \ \ ou \ \ a = 0)$

sommes et produits dont le résultat est l'élément neutre ou l'élément absorbant :

$$a \perp b = 0 \iff a = 0 \ et \ b = 0.$$
$$a + b = 1 \iff (a = 1 \text{ et } b = 0) \text{ ou } (a = 0 \text{ et } b = 1).$$
$$a \times b = 1 \iff a = 1 \ et \ b = 1.$$

1.4 propriété relative

distributivité de la multiplication par rapport à l'addition : $\forall a, b, c \in \mathbb{N}$

$$a \times (b + c) = (a \times b) + (a \times c) \qquad (a + b) \times c = (a \times c) + (b \times c)$$

1.5 autres opérations multiplicatives dans $\mathbb{N}$

Ce sont des opérations unaires de $\mathbb{N}$, définies par récurrence.

1.5.1 puissances d'un entier naturel

$\forall a \in \mathbb{N}$, $a^0 = 1$, $a^{n+1} = a \times a^n$.

La fonction puissance n'est pas distributive par rapport à l'addition : $\forall n > 1$,

$$\exists a, b \in \mathbb{N}, \qquad (a + b)^n \neq a^n + b^n$$

La fonction puissance n'est donc pas une fonction linéraire.

On a les propriétés suivantes : $\forall p, q \in \mathbb{N}$,

$$a^{p+q} = a^p \times a^q \qquad (a^p)^q = a^{p \times q}.$$

[3] On démontrera dans la seconde partie du cours que si un élément possède un symétrique, celui-ci est unique.

1.5.2 fonction factorielle

$0! = 1$, $(n+1)! = (n+1) \times n!$.

La fonction factorielle n'est pas distributive par rapport à l'addition :

$$\exists p, q \in \mathbb{N}, \qquad (p+q)! \neq p! + q!$$

La fonction factorielle n'est donc pas une fonction linéraire.

2 Ordre naturel sur $\mathbb{N}$

L'ordre naturel correspond à l'ordre d'énumération des nombres cardinaux appris dès la petite enfance : un, deux, trois, quatre, ... 0 est ajouté en tête de la séquence.

Mathématiquement, la relation inférieure ou égale, notée $\leq$, est définie dans $\mathbb{N}$ par

$$m \leq n \quad \Longleftrightarrow \quad \exists p \in \mathbb{N}, \quad n = m + p.$$

On dit que m est <u>un</u> prédécesseur de n ou que n est <u>un</u> successeur de m.

Si $p = 1$, on dit que m est <u>le</u> prédécesseur de n ou que n est <u>le</u> successeur de m.

Si $p \neq 0$, alors l'inégalité est stricte et l'on note $m < n$.

2.1 Propriétés de la relation d'ordre naturel

C'est une relation d'ordre c'est-à-dire

- réflexive : $\forall n \in \mathbb{N}, \qquad n \leq n$
- antisymétrique : $\forall n, m \in \mathbb{N}, \quad m \leq n \quad \text{et} \quad n \leq m \quad \Rightarrow \quad n = m$
- transitive : $\forall n, m, p \in \mathbb{N}, \quad m \leq n \quad \text{et} \quad n \leq p \quad \Rightarrow \quad m \leq p$

  De plus,
  $m < n \quad \text{et} \quad n \leq p \quad \Rightarrow \quad m < p,$
  $m \leq n \quad \text{et} \quad n < p \quad \Rightarrow \quad m < p.$

linéaire ou totale : $\forall n, m \in \mathbb{N}$, soit $n = m$ soit $n < m$ soit $m < n$.

avec 0 comme plus petit élément : $\forall n \in \mathbb{N}$, $0 \leq n$.

Cette propriété est essentielle car elle permet d'affirmer que tout entier n n'a qu'un nombre fini d'entiers naturels plus petits que lui. C'est la base des démonstrations par récurrence. En particulier, les preuves élémentaires de terminaison des algorithmes.

Toute partie de $\mathbb{N}$ possède un plus petit élément

sans plus grand élément : $\forall n \in \mathbb{N}, \exists p \in \mathbb{N}, n < p$.

discrète : tout entier naturel n non nul possède

- un plus proche voisin qui lui est inférieur – $n - 1$ – c'est le plus grand de ses prédécesseurs.

- un plus proche voisin qui lui est supérieur – $n+1$ – c'est le plus petit de ses successeurs.

0 n'a pas de prédécesseur, son successeur est 1.

Toute partie bornée de $\mathbb{N}$ est finie.

Toute partie finie de $\mathbb{N}$ possède un plus grand élément.

compatible avec la somme et le produit[4] **:** $\forall m, n, p \in \mathbb{N}$,

- $m \leq n \iff m + p \leq n + p$
- $m < n \iff m + p < n + p$
- $m \leq n$ et $p \neq 0 \iff m \times p \leq n \times p$
- $m < n$ et $p \neq 0 \iff m \times p < n \times p$.

2.1.1 soustraction dans $\mathbb{N}$

Si $a + b = c$ alors $a \leq c$ et $b \leq c$. Nous avons dit que a était la différence entre b et c et b la différence entre a et c. La différence est une relation symétrique[5]. L'opération arithmétique *soustraction* qui permet le calcul d'une différence entre deux nombres quelconques a et b impose que son premier argument soit plus grand ou égal à son second argument. Ce n'est donc pas une opération définie sur tout $\mathbb{N}$.

Soit $a, c \in \mathbb{N}$, $a \leq c$, $c - a$ est défini par $b \in \mathbb{N}$ tel que $c = a + b$.

• $c - a - b = c - (a + b) = c - (b + a) = c - b - a$, mais la soustraction n'est ni commutative ni associative.

• $a - b = b - a \iff a = b$. Si $a \neq b$, seul $a - b$ ou $b - a$ est défini.

• $[(a - b) - c = a - (b - c) \iff c = 0$.

• 0 est élément neutre à droite : $a - 0 = a$.

• Le produit est distributif pour la soustraction : $a \times (b - c) = a \times b - a \times c$.

• La relation d'ordre naturel est compatible avec la soustraction : $\forall a, b, c \in \mathbb{N}$,
$(a \leq b \iff a - c \leq b - c)$ et $(a < b \iff a - c < b - c)$.

2.1.2 approximation dans $\mathbb{N}$

Tout entier non nul m peut servir de mesure, c'est-à-dire que l'on peut encadrer tout nombre entier naturel entre deux multiples successifs de p. On dit que $\mathbb{N}$ est un ensemble *archimédien*.

$$\forall p \in \mathbb{N}_*, \forall n \in \mathbb{N}, \exists a \in \mathbb{N}, \qquad a \times p \leq n < (a+1) \times p$$

2.2 Intervalles de $\mathbb{N}$ muni de son ordre naturel

La notion d'intervalle est commune à tous les ensembles munis d'une relation d'ordre. Elle généralise la notion géométrique de segment, qui permet de définir la notion de convexité.

[5] Une relation *Rel* dans un ensemble E est symétrique si $\forall a, b \in E, a \ Rel \ b \iff b \ Rel \ a$.

Définition 2.2.1 (intervalles bornés) *Soit E un ensemble muni d'une relation d'ordre $\leq$. Soient deux éléments a et b de E tels que $a \leq b$. On définit*

l'intervalle fermé $[a, b] = \{n \in E, a \leq n \leq b\}$

l'intervalle semi-ouvert à droite $[a, b[= \{n \in E, a \leq n < b\}$

l'intervalle semi-ouvert à gauche $]a, b] = \{n \in E, a < n \leq b\}$

l'intervalle ouvert $]a, b[= \{n \in E, a < n < b\}$

$\mathbb{N}$ étant un ensemble sans plus grand élément pour l'ordre naturel, on définit des

Définition 2.2.2 (intervalles non bornés de $\mathbb{N}$) *Soir $a \in \mathbb{N}$.*

l'intervalle fermé infini $[a, \infty[= \{n \in \mathbb{N}, a \leq n\}$

l'intervalle ouvert infini $]a, \infty[= \{n \in \mathbb{N}, a < n\}$

En revanche, les ensembles $\{n \in N, n \leq a\}$ et $\{n \in N, n < a\}$ définissent des intervalles bornés de $\mathbb{N}$ puisque cet ensemble possède un plus petit élément. Ces intervalles sont appelées sections commençantes.

On notera $[[a]]$ l'ensemble $\{n \in N, n \leq a\}$ qui s'écrit aussi $[0, a]$.

$< \mathbb{N}, \leq >$ étant un ordre discret, toute partie propre de $\mathbb{N}$ ne contenant pas 0 qui peut s'exprimer sous une forme intervallaire bornée [resp. non bornée], peut s'écrire sous la forme intervallaire bornée [resp. non bornée] de n'importe quel type. Par exemple,

$$]a, b[= [a + 1, b[=]a, b + 1] = [a + 1, b + 1] \qquad]a, \infty[= [a + 1, \infty[$$

Les singletons $\{a\}$ sont des intervalles. Si $a \neq 0$ alors $\{a\} = [a] =]a-1, a] = [a, a+1[=]a - 1, a + 1[$ mais $\{0\}$ ne possède que deux écritures intervalaires $[0, 0]$ et $[0, 1[$.

L'ordre naturel de $\mathbb{N}$ étant total, $\mathbb{N}$ est lui-même un intervalle non borné, il ne possède qu'une seule écriture intervallaire $N = [0, \infty[$.

Par analogie avec la géométrie, on dira qu'une partie de $\mathbb{N}$ est convexe si quelque soit deux de ses éléments, elle contient tout l'intervalle entre eux. Les seules parties convexes de $\mathbb{N}$ pour l'ordre naturel sont les intervalles de $\mathbb{N}$.

2.2.1 Parties s-héréditaires de $\mathbb{N}$ pour son ordre naturel.

Une relation d'ordre total discrète définit une fonction succession, qui à chaque élément lui associe, s'il existe, son successeur.

Soit la fonction $s : \left| \begin{array}{ccc} \mathbb{N} & \longrightarrow & \mathbb{N}_* \\ x & \longmapsto & x + 1 \end{array} \right.$.

Une partie A de $\mathbb{N}_*$ est dite *s-héréditaire* si elle est stable par s, c'est-à-dire si $s(A) \subset A$.

$s(\{3, 5, 8\}) = \{4, 6, 9\}$; $s([a, b[) = [a + 1, b + 1[$; $s([a, \infty[= [a + 1, \infty[$

Les seules parties héréditaires non vides de $\mathbb{N}$ sont les intervalles infinis. En fait l'une des caractéristiques de $\mathbb{N}$ est

Proposition 2.1 (principe de récurrence) *Si une partie de $\mathbb{N}$ contient 0 et est s-héréditaire alors c'est $\mathbb{N}$ lui-même.*

3 Opérateurs $\sum$ et $\prod$

Soient $(u_k)_{k\in\mathbb{N}}$ une suite définie sur $\mathbb{N}$, $a, b \in \mathbb{N}$. On définit $\sum_{k=a}^{b} u_k$ et $\prod_a^b$ par :

$$\text{si a=b} \qquad \sum_{k=a}^{b} u_k = u_b \qquad \text{et} \qquad \prod_{k=a}^{b} u_k = u_b$$

$$\text{si a<b} \qquad \sum_{k=a}^{b} u_k = \sum_{k=a}^{b-1} u_k + u_b \qquad \text{et} \qquad \prod_{k=a}^{b} u_k = \prod_{k=a}^{b-1} u_k \times u_b$$

L'indice k, appelé indice muet, peut être remplacé par n'importe quelle autre lettre différente des paramêtres a et b. C'est une sorte de calcul intégral sur des intervalles bornés de $\mathbb{N}$ muni de son ordre naturel[6].

$$\sum_{k=a}^{b} u_k = \sum_{i=a}^{b} u_i \qquad \text{et} \qquad \prod_{k=a}^{b} u_k = \prod_{i=a}^{b} u_i$$

3.1 Opération sur les indices

3.1.1 translation

Il s'agit de faire des translations d'intervalles. Si l'on déplace les bornes de l'intervalle $[a, b]$ à gauche dans $\sum$ ou $\prod$, il faut compenser en déplaçant l'intervalle à droite dans l'expression des u_n. Par exemple,

$$\sum_{k=a}^{b} u_k = \sum_{k=0}^{b-a} u_{a+k} \qquad \text{et} \qquad \prod_{k=a}^{b} u_k = \prod_{k=0}^{b-a} u_{a+k}.$$

On peut donc ne considérer que des intervalles de la forme $[0, n]$.

3.1.2 inversion du sens de lecture

$$\sum_{k=0}^{n} u_k = \sum_{k=0}^{n} u_{n-k} \qquad \text{et} \qquad \prod_{k=0}^{n} u_k = \prod_{k=0}^{n} u_{n-k}$$

3.1.3 relation de Chasles

Soit $c \in \mathbb{N}$, $a < c < b$[7]

$$\sum_{k=a}^{b} u_k = \sum_{k=a}^{c} u_k + \sum_{k=c+1}^{b} u_k = \sum_{k=a}^{c-1} u_k + \sum_{k=c}^{b} u_k \qquad \text{et} \qquad \prod_{k=a}^{b} u_k = \prod_{k=a}^{c} u_k \times \prod_{k=c+1}^{b} u_k = \prod_{k=a}^{c-1} u_k \times \prod_{k=c}^{b} u_k$$

[6] L'ordre naturel de $\mathbb{N}$ étant discret, on fera attention au fait qu'un nombre réel correspond à un point de la droite géométrique, alors qu'un nombre entier naturel correspond à un segment de longueur un. Ainsi, dans $\mathbb{R}$, $\int_a^a f(t)dt = 0$, mais dans $\mathbb{N}$, $\sum_a^a f(t)dt = f(a)$.

[7] Ici aussi, l'ordre discret intervient, l'identité n'est pas la même que celle correspondant aux intégrales des fonctions rélles.

3.1.4 linéarité de $\sum$ et non linéarité de $\prod$

Soit $\lambda \in \mathbb{N}$,

$$\sum_{k=a}^{b} \lambda u_k = \lambda \sum_{k=a}^{b} u_k \qquad \text{mais attention} \qquad \prod_{k=a}^{b} \lambda u_k = \lambda^{b-a+1} \sum_{k=a}^{b} u_k$$

Soit $(v_k)_{k\in\mathbb{N}}$ une seconde suite définie sur $\mathbb{N}$,

$$\sum_{k=a}^{b} u_k + \sum_{k=a}^{b} v_k = \sum_{k=a}^{b} (u_k + v_k) \qquad \text{et} \qquad \prod_{k=a}^{b} u_k \times \prod_{k=a}^{b} v_k = \prod_{k=a}^{b} (u_k \times v_k)$$

3.2 fonctions entières à plusieurs variables entières

Les suites entièrres sont des fonctions entières à une variable. Les sommes et produits des valeurs des fonctions à 2 variables se font sur des domaines de dimension 2[8]. Les deux variables correspondent à deux indices qui peuvent être ind´épendants ou d´épendants. Dans le premier cas, les valeurs des indices d´écrivent un rectangle, les opórateurs peuvent être permuter (sans toucher aux arguments) :

$$(*) \sum_{k=0}^{n} \sum_{i=0}^{m} f(k,i) = \sum_{i=0}^{m} \sum_{k=0}^{n} f(k,i) \qquad \text{et} \qquad \prod_{k=0}^{n} \prod_{i=0}^{m} f(k,i) = \prod_{i=0}^{m} \prod_{k=0}^{n} f(k,i)$$

Dans le second cas, les indices sont liés, la permutation des sommations ou produits est plus compliquée. Par exemple, ils peuvent d´écrire un triangle comme dans

$$(**) \sum_{k=0}^{n} \sum_{i=0}^{k} f(k,i) = \sum_{i=0}^{n} \sum_{k=i}^{n} f(k,i) \qquad \text{et} \qquad \prod_{k=0}^{n} \prod_{i=0}^{k} f(k,i) = \prod_{i=0}^{n} \prod_{k=i}^{n} f(k,i)$$

Représenter sous forme d'un tableau $n \times m$ le domaine de sommation ou de produit permet d'opérer la permutation des sommations ou des produits sans difficulté. Pour $n = 3$ et $m = 4$, on a

Table 1: position des indices

i=4	f(4,0)	f(4,1)	f(4,2)	f(4,3)
i=3	f(3,0)	f(3,1)	f(3,2)	f(3,3)
i=2	f(2,0)	f(2,1)	f(2,2)	f(2,3)
i=1	f(1,0)	f(1,1)	f(1,2)	f(1,3)
i=0	f(0,0)	f(0,1)	f(0,2)	f(0,3)
(*)	k=0	k=1	k=2	k=3

i=3	f(3,0)	f(3,1)	f(3,2)	f(3,3)
i=2	f(2,0)	f(2,1)	f(2,2)	-
i=1	f(1,0)	f(1,1)	-	-
i=0	f(0,0)	-	-	-
(**)	k=0	k=1	k=2	k=3

[8]La généralisation à la dimension n est laissée au lecteur.