

L'ARITHMÉTIQUE TOPOSIENNE DES MOTS NATURELS

PAR
GILBERT LABELLE

0. Introduction. Cette note a pour but d'expliciter une structure mathématique spéciale: $\tilde{\mathbb{Z}}$. Cette structure sera aux fonctions finies (i.e. fonctions d'un ensemble fini dans un autre) ce que l'anneau \mathbb{Z} des entiers est aux ensembles finis. Nous ne nous servons des résultats de la théorie des catégories et des topos que comme outils de base pour les constructions considérées. Le lecteur ne doit donc pas s'attendre à des résultats catégoriques fondamentaux mais bien à un nouvel anneau pouvant servir en théorie des nombres, en combinatoire et peut-être même en physique.

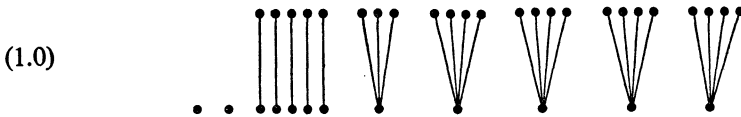
Si on désigne par E la catégorie des ensembles finis et par 2 la catégorie $0 \rightarrow 1$, on peut considérer la catégorie *dénombrable*

$$(0.0) \quad N = \text{Squel}(E^2)$$

où $\text{Squel}(C)$ désigne la catégorie des classes d'isomorphie de la catégorie C avec morphismes déduits évidents.

La catégorie E^2 étant un topos [1], on peut alors définir sur $|N|$ une multiplication, une addition, une exponentiation et un ordre de façon évidente pour finalement obtenir un demi-anneau $\tilde{\mathbb{N}} = (|N|, \cdot, +, \exp)$ ordonné *avec exponentiation*.

1. Description de $\tilde{\mathbb{N}}$. Comme les objets de E^2 sont les fonctions finies on peut représenter les objets n de N par des diagrammes du type



et les caractériser par des suites finies du type

$$(1.1) \quad n = (n_0, n_1, \dots, n_k)$$

où n_v = nombre d'éléments du codomaine de la fonction considérée dont la fibre possède v éléments.

Une expression du type (1.1) sera appelée *mot naturel*. Par exemple, (1.0) prend la forme (2, 5, 0, 1, 4). Les sommes dans le topos E^2 se faisant point par point,

Received by the editors November 22, 1972.

on déduit que l'addition des mots naturels se fait composante à composante et que tout mot naturel se décompose sous la forme "moléculaire"

$$(1.2) \quad n = n_0 \delta_0 + n_1 \delta_1 + n_2 \delta_2 + \dots + n_k \delta_k$$

où δ_ν = classe d'isomorphie de la fonction finie $\nu \rightarrow 1$ qui "identifie" ν points en un seul. Des considérations spacio-temporelles permettent d'appeler δ_0 l'apparition atomique, δ_1 la persistance atomique, δ_2 la 2-identification atomique et, en général, δ_ν la ν -identification atomique. On omet le mot atomique pour les multiples des divers δ_ν .

La multiplication, pour des raisons analogues, se réduit à la table

$$(1.3) \quad \delta_\nu \delta_\mu = \delta_{\nu\mu} \quad \nu, \mu \geq 0$$

L'exponentiation n^m demande une étude plus détaillée et on peut démontrer (via les propriétés des topos) que si $f: A_0 \rightarrow A_1$ et $g: B_0 \rightarrow B_1$ sont deux objets de E^2 alors g^f (lire g puissance f) est l'objet (i.e. la fonction finie)

$$(1.4) \quad g^f: E^2(f, g) \rightarrow B_1^{A_1}$$

défini par

$$(1.5) \quad g^f(\sigma_0, \sigma_1) = \sigma_1$$

pour chaque $\sigma = (\sigma_0, \sigma_1) \in E^2(f, g)$.

Le lecteur doit ici prendre conscience que cette exponentiation est *distincte* de l'exponentiation "usuelle" donnée par $g^f(\omega) = g \circ \omega \circ f$. La loi $n^{m+p} = n^m \cdot n^p$ montre qu'il suffit de définir les divers

$$(1.6) \quad n^{\delta\mu}$$

pour exprimer, dans $\tilde{\mathbb{N}}$, l'exponentiation générale. Un regard attentif sur les fibres et sur (1.4) et (1.5) donne finalement

$$(1.7) \quad n^{\delta\mu} = \sum_{\nu \geq 0} n_\nu \delta_{\nu\mu}$$

La relation \leq se fait composante à composante et on peut étendre $\tilde{\mathbb{N}}$ à un anneau ordonné $\tilde{\mathbb{Z}}$ avec exponentiation par des exposants positifs en acceptant dans la forme moléculaire (1.2) des coefficients n_ν négatifs.

On a donc la situation

$$\begin{array}{ccc} \mathbb{Z} & \hookrightarrow & \tilde{\mathbb{Z}} \\ \uparrow & & \uparrow \\ \mathbb{N} & \hookrightarrow & \tilde{\mathbb{N}} \end{array}$$

et \mathbb{Z} est un sous-anneau (mais non un idéal) de $\tilde{\mathbb{Z}}$. On vérifie immédiatement, pour $k \in \mathbb{Z}$ et $\mu, \nu \in \mathbb{N}$ les lois d'"absorption" suivantes:

$$\delta_\mu^{\delta\nu} = \delta_\mu^\nu, \quad k^{\delta\nu} = k \quad \text{et} \quad \delta_\mu^\nu = \delta_\mu.$$

2. Propriétés de $\tilde{\mathbb{Z}}$. Cette section contient, la plupart du temps sans démonstration, divers résultats sur $\tilde{\mathbb{Z}}$.

Considérons pour chaque $n = \sum_{v \geq 0} n_v \delta_v \in \tilde{\mathbb{Z}}$, les nombres entiers

$$(2.0) \quad \langle n \rangle_k = \sum_{v \geq 0} v^k n_v \quad \text{où} \quad 0 \leq k \in \mathbb{N}.$$

On appellera $\langle n \rangle_k$ le *moment d'ordre k de n* et, en particulier, $\langle n \rangle_0$ et $\langle n \rangle_1$ la *masse* et la *pré-masse* de n respectivement.

Dans le cas où $n \in \mathbb{N}$ on a que $\langle n \rangle_0$ est la cardinalité du “codomaine” de n et $\langle n \rangle_1$ est celle du “domaine” de n .

On a l'identité remarquable suivant reliant la *masse* à l'*exponentiation*:

$$(2.1) \quad \langle n \rangle_0 = n^{\delta_0}.$$

En effet,

$$n^{\delta_0} = \left(\sum_{v \geq 0} n_v \delta_v \right)^{\delta_0} = \sum_{v \geq 0} n_v \delta_{v_0} = \sum_{v \geq 0} n_v \delta_1 = \sum_{v \geq 0} n_v = \langle n \rangle_0.$$

On vérifie que $\langle \cdot \rangle_0: \tilde{\mathbb{Z}} \rightarrow \mathbb{Z}$ est un morphisme d'anneaux à exponentiation à exposants positifs tandis que $\langle \cdot \rangle_k: \tilde{\mathbb{Z}} \rightarrow \mathbb{Z}$ n'est qu'un morphisme d'anneau si $k > 0$ incohérent avec l'exponentiation. Néanmoins,

$$(2.2) \quad \langle n^m \rangle_k = \langle n \rangle_0^{m_0} \langle n \rangle_k^{m_1} \langle n \rangle_{2k}^{m_2} \cdots \langle n \rangle_{rk}^{m_r}$$

si $n = \sum_{v \geq 0} n_v \delta_v$ et $m = \sum_{0 \leq \mu \leq r} m_\mu \delta_\mu$.

Si on définit l'ordre de n par

$$(2.3) \quad \omega(n) = \max\{v \mid n_v \neq 0\}$$

on démontre alors aisément que

$$(2.4) \quad \omega(m+n) \leq \omega(m) \vee \omega(n),$$

$$(2.5) \quad \omega(m \cdot n) = \omega(m) \cdot \omega(n),$$

$$(2.6) \quad \omega(n^p) = (\omega(n))^{\langle p \rangle_1},$$

$$(2.7) \quad \omega(n) = \lim_{\mu \rightarrow \infty} |\langle n \rangle_\mu|^{1/\mu}.$$

Pour chaque v tel que $0 \leq v \in \mathbb{N}$ on a l'identité

$$(2.8) \quad (m+n)^{\delta_v} = m^{\delta_v} + n^{\delta_v}.$$

Comme chaque δ_v est strictement positif cette identité montre que le théorème de Fermat est faux pour certains anneaux *ordonnés* avec exponentiation par des exposants positifs car un infinité $\{\delta_0, \delta_1, \delta_2, \delta_3, \dots\}$ de tels exposants sont possibles dans (2.8).

Les relations générales $(m \cdot n)^p = m^p \cdot n^p$, $m^{n+p} = m^n \cdot m^p$ et $(m^n)^p = m^{n^p}$ sont toujours satisfaites. Il n'en est pas de même pour le binôme de Newton qui explicite $(m+n)^p$.

On a toutefois d'identité "combinatoire"

$$(2.9) \quad (m+n)^p = \sum_{0 \leq a \leq p} \binom{p_0}{q_0} \binom{p_1}{q_1} \cdots \binom{p_r}{q_r} m^a n^{p-a}$$

où $0 \leq q = \sum_{v \geq 0} q_v \delta_v$, et $m, n \in \tilde{\mathbb{Z}}$. Ceci "étend" le binôme de Newton.

L'identité du multinôme possède une généralisation immédiate et permet d'expliciter n^p en fonction de n_0, n_1, \dots et de p_0, p_1, \dots .

On vérifie facilement que les *diviseurs de zéro* dans $\tilde{\mathbb{Z}}$ sont précisément les *apparitions* (i.e. nombres du type $n = n_0 \delta_0$) et les nombres de masse *nulle* (i.e. nombres n tels que $\langle n \rangle_0 = 0$).

L'anneau $\tilde{\mathbb{Z}}$, contrairement à \mathbb{Z} , n'est pas un anneau premier.

Le seul *nilpotent* de $\tilde{\mathbb{Z}}$ est 0 tandis que ses *idempotents*, au nombre de quatre, sont:

$$0, \delta_0, 1 - \delta_0, 1$$

où 1 désigne δ_1 par le plongement $\mathbb{Z} \hookrightarrow \tilde{\mathbb{Z}}$.

RÉFÉRENCE

1. J. W. Gray, *The Meeting of the Midwest Category Seminar in Zurich*. Août 1970. Springer-Verlag Lecture Notes.