Arithmétique de Nim

Pierre Karpman

5 juillet 2008

Table des matières

Remerciements

Merci à Pierre Hyvernat pour avoir bien voulu m'encadrer pour ce stage et à toute l'équipe de logique du LAMA pour les discussions intéressantes et amusantes.

Introduction

Le but de cet exposé est de présenter deux opérations sur les entiers plutôt inhabituelles. Ensemble, elles permettent entre autres d'obtenir une « famille » de corps, avec beaucoup de propriétés intéressantes. La plus grosse partie de ce travail a pour base le chapitre 6 de [1]. La grande majorité (mais pas tous) les résultats dont j'ai fait la démonstration se retrouvent dans cet ouvrage, de même que ceux dont j'ai admis la démonstration. L'article [2] m'a aussi été utile pour certains points, notamment pour explorer les liens entre l'arithmétique de Nim et la théorie de jeux, bien que je n'en parle pas ici. Je termine cette introduction en précisant dès maintenant qu'on pourra trouver en annexe des exemples de calculs ainsi que les tables des opérations pour le corps à 16 éléments.

0 Conventions et notations

Voici les conventions et notations qui seront utilisées tout au cours de cet exposé.

0.1 Opérations

On notera $+_{\mathrm{N}}$ et $\times_{\mathrm{N}}$ les symboles d'addition et de multiplication de Nim respectivement. Les symboles utilisés pour l'addition et la multiplication habituelle sur les entiers seront ceux généralement utilisés, c'est à dire $+$ ou $\times$. Les relations d'inégalité seront toujours utilisées suivant leur sens usuel (c'est à dire que l'ordre qu'elles définissent est l'ordre usuel des entiers).

0.2 Ordinaux

Étant donné que les opérations de Nim peuvent s'étendre aux ordinaux transfinis, on considèrera dès le début que les nombres manipulés sont des ordinaux au sens de J. von Neumann. En particulier un nombre n est considéré comme l'ensemble des nombres plus petit que lui, et que 0 est l'ensemble vide noté $\emptyset$. On aura aussi par exemple $\mathbb{N} \cong \omega$, avec ω étant le plus petit ordinal infini.

0.3 Mex

Dans tout ce qui suit, soit X un ensemble d'ordinaux, $\operatorname{mex} X$ est le plus petit ordinal qui n'est pas dans X.

0.4 Union de deux ensembles

Soient X et Y deux ensembles et x' et y' n'importe quel élément de X et Y respectivement, on utilisera la notation $\{x', y'\}$ pour désigner $X \cup Y$.

0.5 Ensemble des éléments plus petits qu'un nombre

On notera généralement a' n'importe quel nombre positif strictement plus petit que a. L'ensemble des nombres plus petit que a sera donc noté $\{a'\}$ à la place de $\{a'|a' < a\}$ (la convention sur les ordinaux nous permet normalement de noter cet ensemble a, mais cette notation étant parfois ambigüe, il est parfois préférable d'adopter la notation alternative ci-dessus).

0.6 Commutativité, etc.

Il est possible que de temps à autre on suppose implicitement que l'addition et la multiplication de Nim vérifient toutes les bonnes propriétés des opérations d'un corps commutatif avant que cela soit démontré, afin d'éviter de surcharger les énoncés et démonstrations de certaines propriétés non symétriques en considérant les multiples cas possibles.

1 L'addition de Nim

1.1 Une première définition

Notre but avoué est d'obtenir une structure de groupe sur ω pour notre addition $+_{\mathrm{N}}$. Les symétriques pour la loi de composition d'un groupe étant uniques, on peut en déduire que $+_{\mathrm{N}}$ doit vérifier les propriétés suivantes :

$$\forall a' \neq a, \forall b' \neq b \quad a +_{\mathrm{N}} b' \neq a +_{\mathrm{N}} b \text{ et } a' +_{\mathrm{N}} b \neq a +_{\mathrm{N}} b \tag{1}$$

L'idée est donc de prendre pour $a +_{\mathrm{N}} b$ le plus petit nombre « possible » c'est à dire le plus petit nombre qui vérifie les deux équations ci-dessus pour les nombres plus petits que les deux nombres à additionner. On décide donc que notre addition sera la suivante :

Définition 1. $a +_{\mathrm{N}} b = \mathrm{mex}\{a' +_{\mathrm{N}} b\,,\, a +_{\mathrm{N}} b'\}$

Ceci donne une définition récursive de $+_{\mathrm{N}}$. Il est alors remarquable que celle-ci permet à notre addition de vérifier (1). Il est intéressant de préciser que les ensembles $\{a' +_{\mathrm{N}} b\}$ et $\{a +_{\mathrm{N}} b'\}$ peuvent être vus comme des « suites » indexées par les $\{0 \dots a-1\}$ et les $\{0 \dots b-1\}$, et dans le cas particulier où a ou b est 0, la suite $\{a'\}$ ou $\{b'\}$ à considérer est vide.

1.2 Une définition alternative

De manière surprenante, la définition donnée ci-dessus se trouve être équivalente à celle ci :

Définition 2. *Soient $a, b \in \omega$, soient a_2, b_2 leurs représentations en base 2, on assimile a_2 et b_2 à des vecteurs de $\mathbb{F}_2^n$ où $\mathbb{F}_2$ est le corps fini à deux éléments, avec n le nombre de chiffres nécessaires pour écrire le plus grand des nombres a_2 et b_2. On définit alors $+_{\mathrm{N}}$ comme l'addition composante par composante des vecteurs a_2 et b_2.*

De manière équivalente, cela se formule en disant que $+_{\mathrm{N}}$ est l'addition sans retenue (ou encore le « ou exclusif » xor) sur les chaînes de n bits représentant a et b.

On a alors les propriétés immédiates suivantes :

$$\forall a \in \omega \quad a +_{\mathrm{N}} 0 = a \tag{2}$$

$$\forall a \in \omega \quad a +_{\mathrm{N}} a = 0 \tag{3}$$

$$\forall a, b \in \omega \quad a +_{\mathrm{N}} b = 0 \Leftrightarrow a = b \tag{4}$$

$$\forall a < b = 2^n, n \in \omega \quad a +_{\mathrm{N}} b = a + b \tag{5}$$

un cas particulier utile de ces équations étant :

$$\forall m, n \in \omega \quad (2^m +_{\mathrm{N}} 2^n = 2^m + 2^n) \Leftrightarrow (m \neq n) \text{ et } (2^m +_{\mathrm{N}} 2^n = 0) \Leftrightarrow (m = n) \tag{6}$$

Et on a aussi :

Propriété 1. $+_{\mathrm{N}}$ *est commutative*

Propriété 2. $+_{\mathrm{N}}$ *est associative*

L'équivalence entre les deux définitions peut alors se prouver en montrant que toutes ces propriétés sont vérifiées par les deux définitions. On remarquera au passage que l'équation (2) et les propriétés 1 et 2 sont des propriétés générales que doit vérifier la loi de composition d'un groupe, tandis que (3), (4), (5), (6) sont déjà spécifiques à $+_{\mathrm{N}}$.

Pour finir on donne le théorème suivant qui sera prouvé un peu plus tard :

Théorème 1. $\forall n \in \omega \quad (2^n, +_{\mathrm{N}})$ *est un groupe abélien, et* $(\omega, +_{\mathrm{N}})$ *est un groupe abélien.*

1.3 Démonstrations des premières propriétés de $+_{\mathrm{N}}$

On va montrer que la définition 1 vérifie aussi les équations et propriétés vérifiées par la définition 2, ce qui est intéressant pour montrer comment travailler avec une telle définition.

Démonstration. (2). On raisonne par récurrence sur a.

On a $0 +_{\mathrm{N}} 0 = 0$. En effet, $\{a' +_{\mathrm{N}} 0\,,\, 0 +_{\mathrm{N}} b' | a' < 0, b' < 0\} = \emptyset$, et $\operatorname{mex} \emptyset = 0$.

Si on suppose que $a' +_{\mathrm{N}} 0 = a'$, on a alors $a +_{\mathrm{N}} b, b = 0 = \operatorname{mex}\{\underbrace{a +_{\mathrm{N}} b'}_{\emptyset}, \underbrace{0 +_{\mathrm{N}} a'}_{a'}\} = a$.

□

Démonstration. (3). On raisonne par récurrence sur a.

Si $a = 0$ le résultat est vérifié.

Soit $a \neq 0$, alors $a +_{\mathrm{N}} a' \neq 0\ \forall a'$ puisque $a' +_{\mathrm{N}} a' = 0\ \forall a'$, donc $b +_{\mathrm{N}} a' = \operatorname{mex}\{b +_{\mathrm{N}} a''\,,\, b' +_{\mathrm{N}} a'\}$ avec $b = a$ et on a un b' tel que $b' +_{\mathrm{N}} a' = 0$ pour tout a'.

Donc $0 \notin \{a +_{\mathrm{N}} a'\,,\, a' +_{\mathrm{N}} a\}$ donc $a +_{\mathrm{N}} a = 0$. □

Démonstration. (4). $a +_{\mathrm{N}} b = 0 \Leftrightarrow 0 \notin \{a +_{\mathrm{N}} b'\,,\, a' +_{\mathrm{N}} b\}$

Comme $\forall a \in \omega \quad a +_{\mathrm{N}} a = 0$, on a donc $a \neq b'$ et $b \neq a'$. Ce qui implique $b \leq a$ et $a \leq b$ et donc $a = b$.

□

Démonstration. Propriété 1.

On raisonne par récurrence double sur a et b.

On a $0 +_{\mathrm{N}} 1 = 1 +_{\mathrm{N}} 0$.

Supposons que $\forall a' < a\ \forall a'' \leq a \quad a'' +_{\mathrm{N}} a' = a' +_{\mathrm{N}} a''$

Supposons que $\forall b' < b\ \forall b'' \leq b \quad b'' +_{\mathrm{N}} b' = b' +_{\mathrm{N}} b''$.

Supposons que $a > b$.

On a alors :

$$a +_{\mathrm{N}} b = \mathrm{mex}\{\underbrace{a +_{\mathrm{N}} b'}_{b' +_{\mathrm{N}} a}, \underbrace{a' +_{\mathrm{N}} b}_{b +_{\mathrm{N}} a'}\} = \mathrm{mex}\{a +_{\mathrm{N}} b' \,,\, a' +_{\mathrm{N}} b\} = b +_{\mathrm{N}} a$$

□

1.4 Démonstrations d'autres propriétés de $+_{\mathrm{N}}$; équivalence des définitions 1 et 2

On démontre tout d'abord le lemme suivant :

Lemme 1. *Si a est pair, alors $a +_{\mathrm{N}} 1 = a + 1$ et si a est impair alors $a +_{\mathrm{N}} 1 = a - 1$.*

Démonstration. : On raisonne par récurrence sur a.

On a $0 +_{\mathrm{N}} 1 = 1$ et $1 +_{\mathrm{N}} 1 = 0$. On peut aussi facilement vérifier que $2 +_{\mathrm{N}} 1 = 3$ et $3 +_{\mathrm{N}} 1 = 2$.

Supposons que le lemme est vérifié pour les a'.

Si a est pair, alors $a +_{\mathrm{N}} 1 = \mathrm{mex}\{a +_{\mathrm{N}} 0 \,,\, a' +_{\mathrm{N}} 1\}$ avec $\{a' +_{\mathrm{N}} 1\} = \{1, 0, 3, 2, \ldots, a-3, a-1, a-2\} = \{0, 1, \ldots, a-1\}$ puisque $a - 1$ est impair, et donc $a +_{\mathrm{N}} 1 = a + 1$.

Si a est impair, alors $a +_{\mathrm{N}} 1 = \mathrm{mex}\{a +_{\mathrm{N}} 0 \,,\, a' +_{\mathrm{N}} 1\}$ avec $\{a' +_{\mathrm{N}} 1\} = \{1, 0, 3, 2, \ldots, a-2, a-3, a\} = \{0, 1, \ldots, a-2, a\}$ puisque $a - 1$ est pair, et donc $a +_{\mathrm{N}} 1 = a - 1$.

□

On veut maintenant montrer le théorème 1 dans le cas fini et l'équation (5).

Démonstration. On raisonne encore une fois par récurrence, sur les puissances de 2 cette fois.

On vérifie facilement que $(2\,,\, +_{\mathrm{N}})$ est un groupe, et que les éléments de 2 vérifient (5).

On commence par montrer que si la somme des éléments de 2^n est interne (n'oublions pas non plus que (1) est aussi toujours vérifiée) et que ses éléments vérifient (5), alors les éléments de 2^{n+1} vérifient (5).

Il suffit de montrer que pour tout $a < 2^n \quad a +_{\mathrm{N}} 2^n = a + 2^n$.

On raisonne par récurrence sur a.

On a $2^n +_{\mathrm{N}} 0 = 2^n$ et $2^n +_{\mathrm{N}} 1 = 2^n + 1$ immédiatement en utilisant (2) et le lemme 1.

Supposons que $2^n +_{\mathrm{N}} a' = 2^n + a'$. On a alors

$$2^n +_{\mathrm{N}} a = \mathrm{mex}\{\underbrace{(2^n)' +_{\mathrm{N}} a}_{\{(2^n)'\}}\,,\, \underbrace{2^n +_{\mathrm{N}} a'}_{\{2^n + a'\}}\} = 2^n + a$$

□

Il s'ensuit que si la somme des éléments de 2^n est interne, alors la somme des éléments de 2^{n+1} est interne : c'est une conséquence directe de (5) et de (6) appliquées aux éléments de 2^{n+1}.

On termine alors la démonstration du théorème 1 en donnant la :

Démonstration. Propriété 2.

Supposons que $(2^n\,,\, +_{\mathrm{N}})$ est un groupe abélien et que (5) est vérifiée pour tout a dans ω.

Tout élément de 2^{n+1} peut s'écrire comme la somme (au sens usuel) des puissances de 2 de 0 à n, qui est égale à la somme de Nim de ces mêmes puissances.

On note

$$a = \sum_{i=0}^{n} \delta_i \times 2^i \qquad b = \sum_{j=0}^{n} \epsilon_j \times 2^j \qquad c = \sum_{k=0}^{n} \zeta_k \times 2^k$$

On a donc

$$(a +_{\mathrm{N}} b) +_{\mathrm{N}} c = \sum_{i=0}^{n-1} \delta_i \times 2^i + \sum_{j=0}^{n-1} \epsilon_j \times 2^j + \sum_{k=0}^{n-1} \zeta_k \times 2^k + (\delta_n \times 2^n +_{\mathrm{N}} \epsilon_n \times 2^n) +_{\mathrm{N}} \zeta_n \times 2^n$$

Mais

$$(\delta_n \times 2^n +_{\mathrm{N}} \epsilon_n \times 2^n) +_{\mathrm{N}} \zeta_n \times 2^n = \delta_n \times 2^n +_{\mathrm{N}} (\epsilon_n \times 2^n +_{\mathrm{N}} \zeta_n \times 2^n) = \delta_n \times 2^n +_{\mathrm{N}} \epsilon_n \times 2^n +_{\mathrm{N}} \zeta_n \times 2^n$$

□

La démonstration du théorème 1 dans le cas infini (c'est à dire montrer que $(\omega\,,\, +_{\mathrm{N}})$ est un groupe abélien) est alors une conséquence directe de (2), (3) et des propriétés 1 et 2.

Avec tout ceci, il est facile de constater l'équivalence des définitions 1 et 2, puisque pour additionner deux nombres on peut les décomposer en base 2 et les additionner chiffre par chiffre selon la règle du xor, ces opérations de conversion étant maintenant légales.

1.5 Encore d'autres propriétés de $+_{\mathbf{N}}$

Il est maintenant facile de montrer que :

$$\forall m, n < 2^p \quad n +_{\mathrm{N}} (2^p +_{\mathrm{N}} m) = n +_{\mathrm{N}} (2^p + m) = (n +_{\mathrm{N}} m) + 2^p \tag{7}$$

Démonstration.

$$n +_{\mathrm{N}} (2^p +_{\mathrm{N}} m) = \underbrace{(n +_{\mathrm{N}} m)}_{< 2^p} +_{\mathrm{N}} 2^p = (n +_{\mathrm{N}} m) + 2^p$$

□

On a aussi :

$$\forall a, b \in \omega \quad a +_{\mathrm{N}} b \leq a + b \tag{8}$$

Démonstration. On a toujours $\operatorname{mex} X \leq \operatorname{card}(X)$ et comme on a évidemment $\operatorname{card}(\{a +_{\mathrm{N}} b'\}) \leq b$, $\operatorname{card}(\{a' +_{\mathrm{N}} b\}) \leq a$ et $\operatorname{card}(\{a +_{\mathrm{N}} b'\,,\, a' +_{\mathrm{N}} b\}) \leq \operatorname{card}(\{a +_{\mathrm{N}} b'\}) + \operatorname{card}(\{a' +_{\mathrm{N}} b\})$, on a le résultat voulu. □

On a aussi l'amusante propriété suivante :

Propriété 3. *Soit $\mathfrak{L}_{\mathfrak{n}}$ la somme de Nim des n premiers entiers naturels, alors on a :*

- *Si $n \equiv 0[4]$ alors $\mathfrak{L}_{\mathfrak{n}} = n$*
- *Si $n \equiv 1[4]$ alors $\mathfrak{L}_{\mathfrak{n}} = 1$*
- *Si $n \equiv 2[4]$ alors $\mathfrak{L}_{\mathfrak{n}} = n + 1$*
- *Si $n \equiv 3[4]$ alors $\mathfrak{L}_{\mathfrak{n}} = 0$*

Démonstration. On raisonne par récurrence. La phase d'initialisation se vérifie aisément. Supposons que la propriété est vraie pour tout n plus petit que $p = 4q$ pour un certain $q \in \omega$. On a alors $\mathfrak{L}_{4\mathfrak{q}+1} = 4q +_{\mathrm{N}} 4q +_{\mathrm{N}} 1 = 1$ et $\mathfrak{L}_{4\mathfrak{q}+2} = 1 +_{\mathrm{N}} (4q + 2) = 4q + 3$ et enfin $\mathfrak{L}_{4\mathfrak{q}+3} = 0$. □

2 La multiplication de Nim

2.1 Une première définition

De la même manière que $+_{\mathrm{N}}$ a été définie pour obtenir une structure de groupe, on veut définir une opération de multiplication qui donne une structure d'anneau avec l'addition de Nim, ce qui nous donne une condition nécessaire pour cette opération analogue à (1).

On doit avoir :

$$\forall a' \neq a, \forall b' \neq b \quad (a -_{\mathrm{N}} a') \times_{\mathrm{N}} (b -_{\mathrm{N}} b') \neq 0$$

$$\Leftrightarrow a \times_{\mathrm{N}} b -_{\mathrm{N}} a \times_{\mathrm{N}} b' -_{\mathrm{N}} a' \times_{\mathrm{N}} b +_{\mathrm{N}} a' \times_{\mathrm{N}} b' \neq 0$$

Note : Comme on a $a +_{\mathrm{N}} a = 0$, la « différence de Nim » est identique à l'addition de Nim, et les opérations de soustraction ont été notées $+_{\mathrm{N}}$, ce qui finalement donne :

$$\forall a' \neq a, \forall b' \neq b \quad a \times_{\mathrm{N}} b \neq a \times_{\mathrm{N}} b' +_{\mathrm{N}} a' \times_{\mathrm{N}} b +_{\mathrm{N}} a' \times_{\mathrm{N}} b' \tag{9}$$

Par analogie avec l'addition, on donne donc :

Définition 3. $a \times_{\mathrm{N}} b = \mathrm{mex}\{a \times_{\mathrm{N}} b' +_{\mathrm{N}} a' \times_{\mathrm{N}} b +_{\mathrm{N}} a' \times_{\mathrm{N}} b'\}$

On pourra remarquer qu'encore une fois les ensembles $\{a \times_{\mathrm{N}} b' +_{\mathrm{N}} a' \times_{\mathrm{N}} b +_{\mathrm{N}} a' \times_{\mathrm{N}} b'\}$ pour différents a' et b' peuvent être vus comme les termes d'une suite indexée par les couples (a', b').

2.2 Une définition alternative

Tout comme $+_{\mathrm{N}}$ admet deux définitions différentes, $\times_{\mathrm{N}}$ admet une autre définition, non récursive. On donne tout d'abord la :

Définition 4. *On nomme puissance de Fermat un nombre s'écrivant sous la forme* 2^{2^n} *avec* $n \in \omega$.

Et la :

Définition 5. *Le produit de Nim de deux puissances de Fermat distinctes est leur produit usuel, et le carré de Nim d'une puissance de Fermat est égal à cette même puissance de Fermat multipliée par* $\frac{3}{2}$. *Les produits d'autres nombres peuvent êtres obtenus en utilisant des propriétés d'associativité et de distributivité sur l'addition de Nim.*

Je n'ai cependant pas prouvé l'équivalence des définitions 3 et 5.

2.3 Propriétés de la multiplication

On va montrer les différents résultats suivants pour la multiplication de Nim en utilisant la définition 3 :

$$\forall a \in \omega \quad 0 \times_{\mathrm{N}} a = 0 \tag{10}$$

$$\forall a \in \omega \quad 1 \times_{\mathrm{N}} a = a \tag{11}$$

$$\forall a, b \in \omega \quad a \times_{\mathrm{N}} b = a \Rightarrow b = 1 \tag{12}$$

Propriété 4. $\times_{\mathrm{N}}$ *est commutative*

Propriété 5. $\times_{\mathrm{N}}$ *est distributive sur* $+_{\mathrm{N}}$

Propriété 6. $\times_{\mathrm{N}}$ *est associative*

Ce qui permettra d'arriver au :

Théorème 2. $(\omega\,,\,+_{\mathrm{N}}\,,\,\times_{\mathrm{N}})$ *est un anneau commutatif unifère.*

Démonstration. (10). Aucun nombre ne peut être de la forme $b' \times_{\mathrm{N}} a +_{\mathrm{N}} 0 \times_{\mathrm{N}} a' +_{\mathrm{N}} b' \times_{\mathrm{N}} a'$ avec $b' < 0$, donc l'ensemble des nombres de cette forme est vide, et son mex est par conséquent 0. □

Démonstration. (11). On raisonne par récurrence sur a.

On a $1 \times_{\mathrm{N}} 0 = 0$.

On a $\{1'\} = \{0\}$, donc les nombres de la forme $1' \times_{\mathrm{N}} a +_{\mathrm{N}} 1 \times_{\mathrm{N}} a' +_{\mathrm{N}} 1' \times_{\mathrm{N}} a'$ sont exactement les nombres de la forme $0 \times_{\mathrm{N}} a +_{\mathrm{N}} 1 \times_{\mathrm{N}} a' +_{\mathrm{N}} 0 \times_{\mathrm{N}} a'$, c'est à dire les a' par récurrence, donc le mex de l'ensemble des nombres de cette forme est a. □

Démonstration. (12).

$$a \times_{\mathrm{N}} b = a \Leftrightarrow \{0 \dots a-1\} \in \{a \times_{\mathrm{N}} b' +_{\mathrm{N}} a' \times_{\mathrm{N}} b +_{\mathrm{N}} a' \times_{\mathrm{N}} b'\} \wedge a \notin \{a \times_{\mathrm{N}} b' +_{\mathrm{N}} a' \times_{\mathrm{N}} b +_{\mathrm{N}} a' \times_{\mathrm{N}} b'\}$$

Comme $1 \times_{\mathrm{N}} a = a$ la seconde condition ci-dessus implique que $1 \notin \{b'\}$ et donc que $b = 0$ ou que $b = 1$. Le seul choix possible pour vérifier la première condition est alors $b = 1$. □

Démonstration. Propriété 4.

On raisonne par récurrence double sur a et b

On a $0 \times_{\mathrm{N}} 1 = 1 \times_{\mathrm{N}} 0 = 0$

Supposons que $\forall a' < a \; \forall a'' \leq a \quad a'' \times_{\mathrm{N}} a' = a' \times_{\mathrm{N}} a''$

Supposons que $\forall b' < b \; \forall b'' \leq b \quad b'' \times_{\mathrm{N}} b' = b' \times_{\mathrm{N}} b''$.

Supposons que $a > b$.

On a alors :

$$a \times_{\mathrm{N}} b = \mathrm{mex}\{\underbrace{a' \times_{\mathrm{N}} b}_{b \times_{\mathrm{N}} a'} +_{\mathrm{N}} \underbrace{a \times_{\mathrm{N}} b'}_{b' \times_{\mathrm{N}} a} +_{\mathrm{N}} \underbrace{a' \times_{\mathrm{N}} b'}_{b' \times_{\mathrm{N}} a'}\} = \mathrm{mex}\{b \times_{\mathrm{N}} a' +_{\mathrm{N}} b' \times_{\mathrm{N}} a +_{\mathrm{N}} b' \times_{\mathrm{N}} a'\} = b \times_{\mathrm{N}} a$$

□

Démonstration. Propriété 5.

On raisonne par récurrence sur les triplets $(a\,,\,b\,,\,c)$.

Supposons que : $\forall (a'\,,\,b'\,,\,c') < (a\,,\,b\,,\,c) \quad a' \times_{\mathrm{N}} (b' +_{\mathrm{N}} c') = a' \times_{\mathrm{N}} b' +_{\mathrm{N}} a' \times_{\mathrm{N}} c'$

En prenant l'ordre lexicographique sur les triplets.

On note $d = b +_{\mathrm{N}} c$. On a alors :

$$a \times_{\mathrm{N}} (b +_{\mathrm{N}} c) = \mathrm{mex}\{\underbrace{a' \times_{\mathrm{N}} (b +_{\mathrm{N}} c)}_{a' \times_{\mathrm{N}} b +_{\mathrm{N}} a' \times_{\mathrm{N}} c} +_{\mathrm{N}} a \times_{\mathrm{N}} d' +_{\mathrm{N}} a' \times_{\mathrm{N}} d'\}$$

avec $d = \mathrm{mex}\{b +_{\mathrm{N}} c'\,,\, b' +_{\mathrm{N}} c\}$. Donc $d' \in \{b +_{\mathrm{N}} c'\,,\, b' +_{\mathrm{N}} c\}$ et $a \times_{\mathrm{N}} d'$ est de la forme $a \times_{\mathrm{N}} (b +_{\mathrm{N}} c') = a \times_{\mathrm{N}} b +_{\mathrm{N}} a \times_{\mathrm{N}} c'$ ou de la forme $a \times_{\mathrm{N}} (b' +_{\mathrm{N}} c) = a \times_{\mathrm{N}} b' +_{\mathrm{N}} a \times_{\mathrm{N}} c$. On raisonne de même pour $a' \times_{\mathrm{N}} d'$, ce qui prouve le résultat. □

Démonstration. Propriété 6.

On raisonne également par récurrence sur les triplets $(a\,,\,b\,,\,c)$.

Supposons que : $\forall(a'\,,\,b'\,,\,c') < (a\,,\,b\,,\,c) \quad a' \times_{\mathrm{N}} (b' \times_{\mathrm{N}} c') = a' \times_{\mathrm{N}} b' \times_{\mathrm{N}} c'$

On note de même $d = b \times_{\mathrm{N}} c$. On a alors :

$$a \times_{\mathrm{N}} (b \times_{\mathrm{N}} c) = \mathrm{mex}\{a \times_{\mathrm{N}} d' +_{\mathrm{N}} a' \times_{\mathrm{N}} (b \times_{\mathrm{N}} c) +_{\mathrm{N}} a' \times_{\mathrm{N}} d'\} = \mathrm{mex}\{a \times_{\mathrm{N}} d' +_{\mathrm{N}} a' \times_{\mathrm{N}} b \times_{\mathrm{N}} c +_{\mathrm{N}} a' \times_{\mathrm{N}} d'\}$$

avec $d = \mathrm{mex}\{b \times_{\mathrm{N}} c' +_{\mathrm{N}} b' \times_{\mathrm{N}} c +_{\mathrm{N}} b' \times_{\mathrm{N}} c'\}$ et donc $d' \in \{b \times_{\mathrm{N}} c' +_{\mathrm{N}} b' \times_{\mathrm{N}} c +_{\mathrm{N}} b' \times_{\mathrm{N}} c'\}$. Donc $a \times_{\mathrm{N}} d'$ est de la forme $a \times_{\mathrm{N}} (b \times_{\mathrm{N}} c') +_{\mathrm{N}} a \times_{\mathrm{N}} (b' \times_{\mathrm{N}} c) +_{\mathrm{N}} a \times_{\mathrm{N}} (b' \times_{\mathrm{N}} c')$ grâce à la distributivité, ce qui est égal à $a \times_{\mathrm{N}} b \times_{\mathrm{N}} c' +_{\mathrm{N}} a \times_{\mathrm{N}} b' \times_{\mathrm{N}} c +_{\mathrm{N}} a \times_{\mathrm{N}} b" \times_{\mathrm{N}} c'$ par hypothèse. On raisonne de même pour $a' \times_{\mathrm{N}} d'$, ce qui prouve le résultat. □

En fait, on a plus qu'une structure d'anneau. On donne le théorème suivant sans démonstration :

Théorème 3. $\forall n \in \omega \quad (2^{2^n}\,,\,\times_{\mathrm{N}})$ *est un groupe abélien, et* $(\omega\,,\,\times_{\mathrm{N}})$ *est un groupe abélien.*

Ce qui entraîne :

Théorème 4. $\forall n \in \omega \quad (2^{2^n}\,,\,+_{\mathrm{N}}\,,\,\times_{\mathrm{N}})$ *est un corps commutatif, et* $(\omega\,,\,+_{\mathrm{N}}\,,\,\times_{\mathrm{N}})$ *est un corps commutatif.*

Le second cas de ce théorème est en fait une conséquence du théorème d'extension minimale pour les corps donné plus loin.

On finit cette partie en montrant :

$$\forall a, b \in \omega \quad a \times_{\mathrm{N}} b \leq a \times b \tag{13}$$

qui est le pendant de (8) pour la multiplication.

Démonstration. $\{a \times_{\mathrm{N}} b' +_{\mathrm{N}} a' \times_{\mathrm{N}} b +_{\mathrm{N}} a' \times_{\mathrm{N}} b'\}$ est indexé par les couples $(a'\,,\,b')$ qui sont au nombre de $a \times b$. Le même argument de cardinalité que celui employé pour prouver (8) suffit donc à montrer le résultat. □

3 Les théorèmes d'extension minimale

Une série de conséquences particulièrement élégantes des défintions pour l'addition et la multiplication qui on été données est la série de théorèmes dits d'*extension minimale*. Ils ont tous la même architecture, et peuvent se résumer par la phrase suivante :

Soit a un ordinal, si a ne vérifie pas [telle propriété]*, alors a est le résultat du plus petit contre-exemple pour* [telle propriété] *fourni par des éléments de a.*

Nous allons voir un peu plus en détail ce que cela signifie.

3.1 Théorème pour le groupe

Dans ce cas, la considération générale devient :

Théorème 5. *Si un ordinal a n'est pas un groupe pour l'addition de Nim, alors $a = \alpha +_{\mathrm{N}} \beta$, avec $(\alpha\,,\,\beta)$ le plus petit couple d'éléments de a dans l'ordre lexicographique tel que la somme de ses éléments n'est pas dans a.*

Démonstration. Raisonnons par l'absurde.

Supposons que $\alpha, \beta \in a$, $\mathcal{C} = (\alpha\,,\,\beta)$ est le plus petit couple tel que $\alpha +_{\mathrm{N}} \beta \notin a$ et que $\alpha +_{\mathrm{N}} \beta \neq a$. On a donc $\alpha +_{\mathrm{N}} \beta > a$, et donc $a \in X = \{\alpha' +_{\mathrm{N}} \beta\,,\, \alpha +_{\mathrm{N}} \beta'\}$. Mais tous les éléments de X sont lexicographiquement plus petit que $\mathcal{C}$ et $a \notin a$, d'où une contradiction. □

3.2 Théorème pour l'anneau

On a le :

Théorème 6. *Si un ordinal a est un groupe mais pas un anneau, alors $a = \alpha \times_{\mathrm{N}} \beta$, avec $(\alpha\,,\,\beta)$ le plus petit couple d'éléments de a dans l'ordre lexicographique tel que le produit de ses éléments n'est pas dans a.*

Démonstration. On raisonne aussi par l'absurde.

Supposons que $\mathcal{C} = (\alpha\,,\,\beta)$ est le plus petit couple tel que $\alpha \times_{\mathrm{N}} \beta \notin a$ et que $\alpha \times_{\mathrm{N}} \beta \neq a$. On a donc au moins un élément de $X = \{\alpha \times_{\mathrm{N}} \beta' +_{\mathrm{N}} \alpha' \times_{\mathrm{N}} \beta +_{\mathrm{N}} \alpha' \times_{\mathrm{N}} \beta'\}$ qui est supérieur ou égal à a. Or tous les produits présents dans les éléments de X sont lexicographiquement plus petits que $\mathcal{C}$, et comme a est un groupe, au moins un de ces produits doit être plus grand que a pour satisfaire la condition précédente, d'où une contradiction. □

3.3 Autres théorèmes

Voici d'autres intéressants théorèmes d'extension minimale, mais leurs démonstrations sont moins simples.

Théorème 7. *Si un ordinal a est un anneau mais non un corps, alors a est l'inverse du plus petit élément non nul α de a qui n'a pas d'inverse.*

Ce qui prouve au passage le second cas du théorème 4.

Je n'ai pas démontré moi même ce théorème, mais sa démonstration n'est pas très longue. Aussi vais-je reproduire celle qu'on peut trouver dans [1].

Démonstration. On appelle $\mathfrak{A}$ le plus grand ordinal plus petit que α qui est un groupe. Alors $a \times_{\mathrm{N}} \mathfrak{A}$ ne peut pas s'écrire sous la forme $a \times_{\mathrm{N}} \mathfrak{a} +_{\mathrm{N}} a' \times_{\mathrm{N}} \mathfrak{A} +_{\mathrm{N}} a' \times_{\mathrm{N}} \mathfrak{a} = a \times_{\mathrm{N}} \mathfrak{a} +_{\mathrm{N}} a' \times_{\mathrm{N}} (\mathfrak{A} +_{\mathrm{N}} \mathfrak{a})$, $\mathfrak{a} \in \mathfrak{A}$. On pose $\alpha = \mathfrak{A} +_{\mathrm{N}} \beta$. Alors, pour tout $\mathfrak{a}$ strictement plus petit que β, $\mathfrak{A} +_{\mathrm{N}} \mathfrak{a}$ est inversible dans a, puisque $\mathfrak{A} +_{\mathrm{N}} \mathfrak{a} = \mathfrak{A} + \mathfrak{a}$ est plus petit que α. On pose alors $\underline{a'} = a' \times_{\mathrm{N}} (\mathfrak{A} +_{\mathrm{N}} \mathfrak{a})$ un ordinal quelconque de a. On a que tous les nombres $a \times_{\mathrm{N}} \beta' +_{\mathrm{N}} \underline{a'}$ plus petits que $a \times_{\mathrm{N}} \beta$ sont dans l'ensemble des nombres sous la forme desquels $a \times_{\mathrm{N}} \mathfrak{A}$ ne peut pas s'écrire. Il en va de même pour $a \times_{\mathrm{N}} \beta = a \times_{\mathrm{N}} \beta +_{\mathrm{N}} 0 \times_{\mathrm{N}} (\mathfrak{A} +_{\mathrm{N}} \beta)$, mais ce n'est pas le cas de $a \times_{\mathrm{N}} \beta +_{\mathrm{N}} 1 = a \times_{\mathrm{N}} \beta + 1$ puisqu'on devrait avoir $\mathfrak{a} = \beta$ et donc $a' \times_{\mathrm{N}} (\mathfrak{A} +_{\mathrm{N}} \beta) = 1$, c'est à dire $a' \times_{\mathrm{N}} \alpha = 1$. Donc $a \times_{\mathrm{N}} \mathfrak{A} = a \times_{\mathrm{N}} \beta +_{\mathrm{N}} 1$, et $a \times_{\mathrm{N}} \alpha = a \times_{\mathrm{N}} (\mathfrak{A} +_{\mathrm{N}} \beta) = a \times_{\mathrm{N}} \mathfrak{A} +_{\mathrm{N}} a \times_{\mathrm{N}} \beta = 1$. □

Théorème 8. *Si un ordinal a est un corps mais n'est pas algébriquement clos, alors a est une racine du plus petit polynôme dans l'ordre lexicographique (les coefficients des degrés les plus hauts étant considérés en premier) tel que sa racine n'est pas dans a.*

Les démonstrations de ce théorème et de ceux qui suivent sont un peu compliquées et je n'en parlerai donc pas particulièrement.

Il est intéressant de noter que des formules similaires à celles données pour l'addition et la multiplication existent pour l'inverse et la racine carrée. Il est aussi intéressant de remarquer que par leur nature, ces formules sont tout à fait valides avec des ordinaux transfinis, puisqu'il ne peut pas exister de suite infinie d'ordinaux décroissants.. On donne en exemple la formule suivante pour l'inverse :

$$b = \frac{1}{a} = \text{mex}\{0, \frac{1 + (a' +_{\text{N}} a) \times_{\text{N}} b'}{a'}\} \tag{14}$$

Il faut comprendre cette formule en disant que 0 n'est l'inverse d'aucun nombre, et qu'on « remplit » la partie de gauche de l'ensemble (qui est la liste des b' possibles) au fur et à mesure. Il faut reconsidérer le nouvel ensemble des b' pour chaque a' chaque fois qu'un nouveau b' s'ajoute. L'inverse est le mex de cet ensemble quand il ne s'enrichit plus avec de nouveaux éléments.

4 Derniers théorèmes et résultats sur les ordinaux transfinis

Les résultats suivants sont aussi donnés sans démonstration, mais ils sont révélateurs de la richesse des structures permises par les opérations de Nim.

Les deux théorèmes suivants sont des conséquences directes des théorèmes 1 et 4.

Théorème 9. *Si a est un groupe abélien pour l'addition de Nim, alors il en va de même pour $2 \times a$.*

Théorème 10. *Si a est un corps commutatif pour l'addition et la multiplication de Nim, alors il en va de même pour $a \times a$.*

On peut aussi montrer le :

Théorème 11. *Soit a un ordinal fini, on a a qui est un corps commutatif pour l'addition et la multiplication de Nim si et seulement si a est un anneau commutatif unifère pour les mêmes opérations. Ce n'est plus vrai si a n'est pas fini.*

On a aussi les résultats suivants sur la clôture algébrique :

Théorème 12. $(\omega\,,\,+_{\text{N}}\,,\,\times_{\text{N}})$ *est quadratiquement clos.*

C'est à dire que tout polynôme de degré 2 à coefficients dans ω a une racine dans ω.

Théorème 13. $(\omega^{\omega^{\omega}}\,,\,+_{\text{N}}\,,\,\times_{\text{N}})$ *est le plus petit corps commutatif algébriquement clos pour les opérations de Nim.*

Le théorème suivant est plutôt surprenant :

Théorème 14. *La collection des ordinaux $\mathcal{O}n$ munie de l'addition et de la mutliplication de Nim est un corps commutatif algébriquement clos.*

Il est important de noter que $\mathcal{O}n$ n'est pas un ensemble.

Et enfin, en guise de conclusion on donne la très curieuse propriété suivante :

Propriété 7. *La racine cubique de 2 pour la multiplication de Nim est ω : $\omega \times_{\text{N}} \omega \times_{\text{N}} \omega = 2$.*

A Exemples de calculs

A.1 Addition

$1 +_{\mathbb{N}} 3 = \text{mex}\{1 +_{\mathbb{N}} 3' \, , \, 1' +_{\mathbb{N}} 3\}$
$3' \in \{0, 1, 2\} \quad 1' = \{0\}$
$\{1 +_{\mathbb{N}} 3'\} = \{1 +_{\mathbb{N}} 0, 1 +_{\mathbb{N}} 1, 1 +_{\mathbb{N}} 2\}$
$1 +_{\mathbb{N}} 2 = \text{mex}\{1 +_{\mathbb{N}} 2' \, , \, 1' +_{\mathbb{N}} 2\}$
$\{1 +_{\mathbb{N}} 2'\} = \{1 +_{\mathbb{N}} 0, 1 +_{\mathbb{N}} 1\} = \{1, 0\}$
$\{1' +_{\mathbb{N}} 2\} = \{0 +_{\mathbb{N}} 2\} = \{2\}$
$1 +_{\mathbb{N}} 2 = \text{mex}\{0, 1, 2\} = 3$
$\{1 +_{\mathbb{N}} 3'\} = \{1, 0, 3\}$
$\{1' +_{\mathbb{N}} 3\} = \{0 +_{\mathbb{N}} 3\} = \{3\}$
$1 +_{\mathbb{N}} 3 = \text{mex}\{0, 1, 3\} = 2$

A.2 Multiplication

[mex]

$2 \times_{\mathbb{N}} 2 = \text{mex}\{2 \times_{\mathbb{N}} 2' +_{\mathbb{N}} 2' \times_{\mathbb{N}} 2 +_{\mathbb{N}} 2' \times_{\mathbb{N}} 2'\}$
$\to (0\,,\,0)\ (0\,,\,1)\ (1\,,\,0)\ (1\,,\,1)$
$\{2 \times_{\mathbb{N}} 0 +_{\mathbb{N}} 0 \times_{\mathbb{N}} 2 +_{\mathbb{N}} 0 \times_{\mathbb{N}} 0\} = 0$
$\{2 \times_{\mathbb{N}} 0 +_{\mathbb{N}} 1 \times_{\mathbb{N}} 2 +_{\mathbb{N}} 0 \times_{\mathbb{N}} 1\} = 2$
$\{2 \times_{\mathbb{N}} 1 +_{\mathbb{N}} 1 \times_{\mathbb{N}} 2 +_{\mathbb{N}} 1 \times_{\mathbb{N}} 1\} = 1$
$2 \times_{\mathbb{N}} 2 = \text{mex}\{0, 1, 2\} = 3$

[Puissances de Fermat]

$10 \times_{\mathbb{N}} 7.$
$10 = 2^3 +_{\mathbb{N}} 2^1 = 2^{2+1} +_{\mathbb{N}} 2^1 = 2^2 \times_{\mathbb{N}} 2 +_{\mathbb{N}} 2 = 2^{2^1} \times_{\mathbb{N}} 2^{2^0} +_{\mathbb{N}} 2^{2^0}$
$7 = 2^2 +_{\mathbb{N}} 2 +_{\mathbb{N}} 1 = 2^{2^1} +_{\mathbb{N}} 2^{2^0} +_{\mathbb{N}} 1$
$10 \times_{\mathbb{N}} 7 = (4 \times_{\mathbb{N}} 2 +_{\mathbb{N}} 2) \times_{\mathbb{N}} (4 +_{\mathbb{N}} 2 +_{\mathbb{N}} 1) = 4 \times_{\mathbb{N}} 4 \times_{\mathbb{N}} 2 +_{\mathbb{N}} 4 \times_{\mathbb{N}} 2 \times_{\mathbb{N}} 2 +_{\mathbb{N}} 4 \times_{\mathbb{N}} 2 +_{\mathbb{N}} 2 \times_{\mathbb{N}} 4 +_{\mathbb{N}} 2 \times_{\mathbb{N}} 2 +_{\mathbb{N}} 2$
$= 4 \times_{\mathbb{N}} 4 \times_{\mathbb{N}} 2 +_{\mathbb{N}} 4 \times_{\mathbb{N}} 2 \times_{\mathbb{N}} 2 +_{\mathbb{N}} 2 \times_{\mathbb{N}} 2 +_{\mathbb{N}} 2$
$= 6 \times_{\mathbb{N}} 2 +_{\mathbb{N}} 4 \times_{\mathbb{N}} 3 +_{\mathbb{N}} 3 +_{\mathbb{N}} 2$
$6 = 4 +_{\mathbb{N}} 2 \to 6 \times_{\mathbb{N}} 2 = (4 +_{\mathbb{N}} 2) \times_{\mathbb{N}} 2 = 8 +_{\mathbb{N}} 3 = 11$
$3 = 2 +_{\mathbb{N}} 1 \to 3 \times_{\mathbb{N}} 4 = (2 +_{\mathbb{N}} 1) \times_{\mathbb{N}} 4 = 8 +_{\mathbb{N}} 4 = 12$
$10 \times_{\mathbb{N}} 7 = 11 +_{\mathbb{N}} 12 +_{\mathbb{N}} 1 = 8 +_{\mathbb{N}} 8 +_{\mathbb{N}} 3 +_{\mathbb{N}} 4 +_{\mathbb{N}} 1 = 6$

B Tables des opérations

B.1 Addition

$+_N$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	0	3	2	5	4	7	6	9	8	11	10	13	12	15	14
2	2	3	0	1	6	7	4	5	10	11	8	9	14	15	12	13
3	3	2	1	0	7	6	5	4	11	10	9	8	15	14	13	12
4	4	5	6	7	0	1	2	3	12	13	14	15	8	9	10	11
5	5	4	7	6	1	0	3	2	13	12	15	14	9	8	11	10
6	6	7	4	5	2	3	0	1	14	15	12	13	10	11	8	9
7	7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8
8	8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7
9	9	8	11	10	13	12	15	14	1	0	3	2	5	4	7	6
10	10	11	8	9	14	15	12	13	2	3	0	1	6	7	4	5
11	11	10	9	8	15	14	13	12	3	2	1	0	7	6	5	4
12	12	13	14	15	8	9	10	11	4	5	6	7	0	1	2	3
13	13	12	15	14	9	8	11	10	5	4	7	6	1	0	3	2
14	14	15	12	13	10	11	8	9	6	7	4	5	2	3	0	1
15	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

B.2 Multiplication

$\times_N$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	0	2	3	1	8	10	11	9	12	14	15	13	4	6	7	5
3	0	3	1	2	12	15	13	14	4	7	5	6	8	11	9	10
4	0	4	8	12	6	2	14	10	11	15	3	7	13	9	5	1
5	0	5	10	15	2	7	8	13	3	6	9	12	1	4	11	14
6	0	6	11	13	14	8	5	3	7	1	12	10	9	15	2	4
7	0	7	9	14	10	13	3	4	15	8	6	1	5	2	12	11
8	0	8	12	4	11	3	7	15	13	5	1	9	6	14	10	2
9	0	9	14	7	15	6	1	8	5	12	11	2	10	3	4	13
10	0	10	15	5	3	9	12	6	1	11	14	4	2	8	13	7
11	0	11	13	6	7	12	10	1	9	2	4	15	14	5	3	8
12	0	12	4	8	13	1	9	5	6	10	2	14	11	7	15	3
13	0	13	6	11	9	4	15	2	14	3	8	5	7	10	1	12
14	0	14	7	9	5	11	2	12	10	4	13	3	15	1	8	6
15	0	15	5	10	1	14	4	11	2	13	7	8	3	12	6	9

Références

[1] John H. Conway. *On numbers and Games*. Academic Press, 1977.

[2] Hendrik W. Lenstra. Nim multiplication, 1978.

[3] David A. Madore. Consum v0 : An Experimental Cipher, 2007.