MATHÉMATIQUES ET SCIENCES HUMAINES

F. LAPSCHER

Utilisation des matrices booléennes pour l'étude des treillis de post

Mathématiques et sciences humaines, tome 49 (1975), p. 43-73

<http://www.numdam.org/item?id=MSH_1975__49__43_0>

Math. Sci. hum. (13e année, n°49, 1975, p.43-73)

UTILISATION DES MATRICES BOOLEENNES POUR L'ETUDE DES TREILLIS DE POST

par

F. LAPSCHER *

1. INTRODUCTION

S'appuyant sur l'exemple de la logique à p valeurs introduite par Post [4], plusieurs systèmes d'axiomes décrivant le modèle algébrique associé ont été formulés : Rosembloom [5], Epstein [2], Traczyk [6]. La notion abstraite ainsi dégagée se retrouve cependant dans des contextes autres que celui de la logique multivaluée : théorie des questionnaires, problèmes de choix à critères multiples, étude de réseaux construits à l'aide d'interrupteurs multipositionnels ... Elle présente un intérêt comparable à la notion de treillis de Boole, dont elle constitue d'ailleurs une généralisation ; du point de vue de leur généralité, les treillis de Post se situent en effet entre les treillis distributifs et les treillis de Boole.

A partir du système d'axiomes introduit par Epstein, et rappelé dans le paragraphe 2, nous donnons dans cet article divers résultats concernant la représentation "monotone" d'un élément dans un treillis de Post (§3). La définition, sur un treillis de Post d'ordre p, de p lois unaires "de glissement" (§4) nous conduit ensuite aux notions de matrice de glissement et de

---

* Maître de Conférence , Centre d'Informatique, Université Montpellier II, 34060 Montpellier.

matrice de multiplication définies sur un treillis de Boole (§§5 et 6). L'ensemble $\mathcal{M}$ des matrices de glissement d'ordre p définies sur un treillis de Boole donné B présente à la fois une structure d'anneau commutatif unitaire de caractéristique p (§§ 5 et 6) et une structure de module, ou d'espace vectoriel si p est premier (§ 7). Il est encore possible de retrouver sur $\mathcal{M}$ les mêmes structures, pour des lois de composition un peu plus générales (§ 8). En outre, la bijection existant entre un treillis de Post P et l'ensemble $\mathcal{M}$ des matrices de glissement associées au treillis de Boole sous-jacent B permet de traduire dans le langage de P les résultats obtenus pour $\mathcal{M}$; on retrouve ainsi, présentées sous un jour nouveau, diverses propriétés connues et on établit quelques propriétés nouvelles (§ 9). Enfin, le paragraphe 10 donne des résultats obtenus une interprétation géométrique utilisant en particulier la notion de "cycle" précédemment mise en évidence.

2. QUELQUES RAPPELS SUR LES TREILLIS DE POST

Dans un treillis, nous noterons additivement la loi de borne supérieure et multiplicativement celle de borne inférieure.

2.1. Treillis de Boole associé à un treillis distributif

Rappelons que l'ensemble des éléments complémentés d'un treillis distributif est un treillis de Boole. Nous verrons que le treillis de Boole sous-jacent à un treillis de Post joue un rôle important.

2.2. Axiomes d'Epstein pour un treillis de Post [2]

Nous énonçons ci-dessous un système d'axiomes légèrement modifié par rapport à celui d'Epstein.

Un treillis de Post est un treillis distributif P dans lequel, p étant un entier supérieur ou égal à 1, sont vérifiés les axiomes supplémentaires suivants :

1) Il existe, dans P, p éléments $0,1,\ldots,(p-1)$ avec les propriétés suivantes:

a) Ces éléments forment une chaîne avec $0 \leq 1 \leq \ldots \leq (p-1)$.

b) Si $x \in P$ et $x1 = 0$ alors $x = 0$.

c) Si $x \in P$ et si, pour un certain i, $x + (i-1) = i$ alors $x = i$.

2) Pour tout élément $x \in P$, il existe p éléments $x_{(0)}, x_{(1)}, \ldots, x_{(p-1)}$ deux à deux disjoints et dont la borne supérieure est $(p-1)$; c'est-à-dire que $x_{(i)}x_{(j)} = 0$ pour $i \neq j$ et $\sum_{i=0}^{p-1} x_{(i)} = (p-1)$.

3) Pour tout $x \in P$, $x = \sum_{i=0}^{p-1} i\, x_{(i)}$ c'est-à-dire

$$x = 0x_{(0)} + 1x_{(1)} + \ldots + (p-1)\, x_{(p-1)} \qquad (1)$$

2.3. Conséquences diverses. Représentations disjointe et monotone

Des axiomes précédents on peut déduire que 0 est élément nul et $(p-1)$ élément universel du treillis (il n'est pas nécessaire de le supposer a priori comme le fait Epstein). Epstein établit que les éléments $x_{(i)}$ appartiennent au treillis de Boole B sous-jacent à P et, pour x donné, sont uniques.

La représentation unique des éléments de P, ainsi fournie par l'axiome 3, est appelée représentation disjointe. Les éléments distingués $0,1,\ldots,(p-1)$ sont appelés constantes du treillis de Post.

Compte tenu des inégalités $0 \leq 1 \leq \ldots \leq (p-1)$, on peut encore écrire

$$x = 0(x_{(0)} + x_{(1)} + \ldots + x_{(p-1)}) + 1(x_{(1)} + x_{(2)} + \ldots + x_{(p-1)}) + \ldots$$
$$\ldots + (p-2)\,(x_{(p-2)} + x_{(p-1)}) + (p-1)\, x_{(p-1)}$$

Soit, en posant $x^{(i)} = x_{(i)} + x_{(i+1)} + \ldots + x_{(p-1)}$,

$$x = 0\, x^{(0)} + 1x^{(1)} + \ldots + (p-1)\, x^{(p-1)} \qquad (2)$$

avec d'ailleurs $x^{(0)} = (p-1)$ et $x^{(p-1)} = x_{(p-1)}$. La représentation (2) est dite monotone car les coefficients $x^{(i)}$ forment une chaîne : $x^{(0)} \geq x^{(1)} \geq \ldots \geq x^{(p-1)}$. Epstein établit de plus que cette représentation monotone est unique : toute représentation

$$x = 0x_0 + 1x_1 + \ldots + (p-1)\, x_{p-1}$$

pour laquelle les coefficients forment une chaîne : $x_0 \geq x_1 \geq \ldots \geq x_{p-1}$, coïncide avec la précédente : $x_i = x^{(i)}$.

A partir des coefficients de la représentation monotone ceux de la représentation disjointe s'obtiennent de la manière suivante :

$$x_{(i)} = x^{(i)}\, x^{(i+1)'} \qquad 0 \leq i \leq (p-2)$$

$$x_{(p-1)} = x^{(p-1)}$$

la complémentation étant prise dans le treillis de Boole B sous-jacent à P.

Rappelons enfin que pour toute représentation de la forme

$$x = 0x_0 + 1x_1 + \ldots + (p-1)\, x_{p-1}$$

on a $$x_{(i)} \leq x_i \leq x^{(i)} \qquad 0 \leq i \leq (p-1)$$

et $$x^{(i)} = x_i + x_{i+1} + \ldots + x_{p-1}$$

$$x_{(i)} = x_i (x_{i+1})' \ldots (x_{p-1})'$$

2.4. Représentation des treillis de Post. Structures d'anneau et de module

Tout treillis de Post P peut être considéré comme l'ensemble des fonctions p-valuées, continues, définies sur un certain espace de Hausdorff compact, totalement disconnecté [2]. A partir de cette définition, on peut très simplement doter P d'une structure d'anneau (pour les lois d'addition et de multiplication des fonctions) ou d'une structure de module unitaire sur Z/p. En outre, si P est fini, la structure de module permet de montrer l'isomorphisme avec $(Z/p)^n$ (pour un certain entier n), ce qui fournit une caractérisation très simple des treillis de Post finis.

2.5. Exemple

Considérons à titre d'exemple le treillis de Post $(Z/5)^2$ avec ses 5 constantes et son treillis de Boole sous-jacent $\{0, \alpha, \beta, 4\}$. Les éléments x et y de la figure, par exemple, admettent les représentations suivantes :

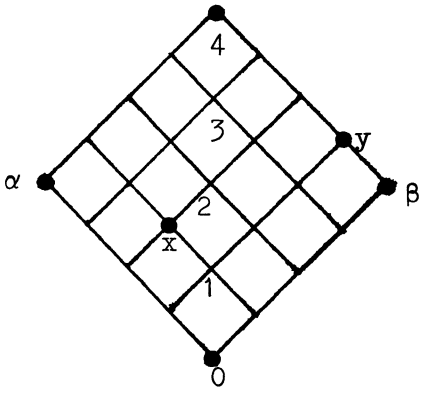


Figure 1

$$x = 1\beta + 2\alpha$$
$$= 0.0 + 1\beta + 2\alpha + 3.0 + 4.0 \quad \Big\} \text{ représentation disjointe}$$
$$= 0.4 + 1.4 + 2\alpha + 3.0 + 4.0 \quad \text{représentation monotone}$$

$$y = 1\alpha + 4\beta$$
$$= 0.0 + 1\alpha + 2.0 + 3.0 + 4\beta \quad \Big\} \text{ représentation disjointe}$$
$$= 0.4 + 1.4 + 2\beta + 3\beta + 4\beta \quad \text{représentation monotone}$$

Cet exemple sera repris et complété au paragraphe 10.

3. TREILLIS DE POST EN REPRESENTATION MONOTONE

3.1. De nouveaux axiomes de modularité

Pour chaque entier $p \geq 2$, on considère l'axiome suivant :

$$(M_p)\ x_1 \geq x_2 \geq \ldots \geq x_{p-1} \geq x_p \quad \wedge \quad y_1 \leq y_2 \leq \ldots \leq y_{p-1}$$
$$\Rightarrow x_1y_1 + x_2y_2 + \ldots + x_{p-1}y_{p-1} + x_p = x_1(y_1+x_2)(y_2+x_3)\ldots(y_{p-2}+x_{p-1})(y_{p-1}+x_p)$$

3.2. Remarque 1

(M_p) est autodual :

$$(M_p)^*\ x_1 \leq x_2 \leq \ldots \leq x_{p-1} \leq x_p \quad \wedge \quad y_1 \geq y_2 \geq \ldots \geq y_{p-1}$$
$$\Rightarrow (x_1+y_1)(x_2+y_2)\ldots(x_{p-1}+y_{p-1})x_p = x_1 + y_1x_2 + y_2x_3 + \ldots + y_{p-2}x_{p-1} + y_{p-1}x_p$$

$(M_p)^*$ coïncide avec (M_p) moyennant l'échange de x_i avec x_{p-i+1} et celui de y_j avec y_{p-j}.

3.3. Remarque 2

$$(M_2) \quad x_1 \geq x_2 \Rightarrow x_1y_1 + x_2 = x_1(y_1 + x_2)$$

coïncide avec l'axiome de modularité connu :

(M) $\quad z \leq x \Rightarrow xy + z = x(y+z)$

3.4. THEOREME Sur un treillis, M_p est équivalent à M_q

Il suffit de montrer que M_p est équivalent à M, en utilisant les axiomes d'un treillis.

1) $M_p \Rightarrow M$.

On pose $\quad x_1 = x$

$$x_2 = x_3 = \ldots = x_p = z$$

$$y_1 = y_2 = \ldots = y_{p-1} = y$$

d'où

$$xy + zy + \ldots + zy + z = x(y+z)\ (y+z) \ldots (y+z)$$

puis, compte tenu de l'hypothèse $z \leq x$,

$$xy + z = x(y+z)$$

2) $M \Rightarrow M_p$.

- On sait déjà que M coïncide avec M_2, donc entraîne M_2.

- Supposons établi que $M \Rightarrow M_{p-1}$, c'est-à-dire que

$$x_1 \geq x_2 \geq \ldots \geq x_{p-1} \ \wedge \ y_1 \leq y_2 \leq \ldots \leq y_{p-2}$$

$$\Rightarrow x_1 y_1 + \ldots + x_{p-2} y_{p-2} + x_{p-1} = x_1(y_1 + x_2) \ldots (y_{p-2} + x_{p-1})$$

et supposons de plus que $x_p \leq x_{p-1}$ et $y_{p-1} \geq y_{p-2}$. D'après $x_p \leq x_{p-1}$ on a $x_p \leq x_1 y_1 + \ldots + x_{p-2} y_{p-2} + x_{p-1}$ puis

$$(x_1y_1 + \ldots + x_{p-2} y_{p-2} + x_{p-1})(y_{p-1}+x_p) =$$

$$= (x_1y_1 + \ldots + x_{p-2}y_{p-2} + x_{p-1})\ y_{p-1} + x_p$$

D'après $y_1 \leq y_{p-1}$, $y_2 \leq y_{p-1}$,..., $y_{p-2} \leq y_{p-1}$, on a $x_1y_1 \leq y_{p-1}$, ..., $x_{p-2} y_{p-2} \leq y_{p-1}$ d'où $x_1y_1 + \ldots + x_{p-2} y_{p-2} \leq y_{p-1}$ puis

$$(x_1y_1 + \ldots + x_{p-2} y_{p-2} + x_{p-1})\ y_{p-1} = x_1 y_1 + \ldots + x_{p-2} y_{p-2} + x_{p-1}y_{p-1}$$

Ce qui donne le résultat $M \Rightarrow M_p$.

3.5. Effet de la dualité sur la représentation monotone

On part de

$$x = 1x^{(1)} + 2x^{(2)} +\ldots+ (p-2)\, x^{(p-2)} + x^{(p-1)}$$

Compte tenu de $x^{(1)} \geq x^{(2)} \geq\ldots\geq x^{(p-1)}$ et $1 \leq 2 \leq\ldots\leq (p-2)$, l'axiome M_p donne

$$x = x^{(1)}\,(1+x^{(2)})(2+x^{(3)})\ \ldots\ ((p-3) + x^{(p-2)})((p-2)+x^{(p-1)})$$

qui est une expression monotone en produit de sommes.

Par dualité

$$x^*=x^{(1)*}+1^*\, x^{(2)*} + 2^*\, x^{(3)*}+\ldots+ (p-3)^*\, x^{(p-2)*} + (p-2)^*\, x^{(p-1)*}$$

avec $(p-2)^* \leq (p-3)^* \leq\ldots\leq 2^* \leq 1^*$. Ceci est la représentation monotone de x^* car on a bien

$$x^{(1)*} \leq x^{(2)*} \leq\ldots\leq x^{(p-1)*}$$

3.6. Conséquence

La représentation monotone de x étant unique, il en est de même de celle de x^*. En utilisant l'une des définitions d'un treillis de Post données par Traczyk, on voit alors que le treillis distributif dual d'un treillis de Post est un treillis de Post.

4. TREILLIS DE POST EN REPRESENTATION DISJOINTE

4.1. Passage de la représentation monotone à la représentation disjointe

On a vu que

$$x^{(i)} = x_{(i)} + x_{(i+1)} +\ldots+ x_{(p-1)}$$

et

$$x_{(i)} = x^{(i)}\, x^{(i+1)'}$$

Donc

$$x = 1\, x^{(1)}x^{(2)'} + 2\, x^{(2)}\, x^{(3)'} +\ldots+ (p-2)\, x^{(p-2)}x^{(p-1)'} + x^{(p-1)}$$

On a aussi

$$x^* = (p-2)^*\, x^{(p-1)*}x^{(p-2)*'} + (p-3)^*\, x^{(p-2)*}x^{(p-3)*'} + \ldots$$

$$\ldots + 1^*\, x^{(2)*}x^{(1)*'} + x^{(1)*}$$

d'où, par dualité,

$$x = x^{(1)}(1+x^{(2)}+x^{(1)'})(2+x^{(3)}+x^{(2)'})\ldots((p-2)+x^{(p-1)}+x^{(p-2)'})$$

4.2. Définition des p lois de composition interne unaires de glissement

En représentation disjointe, on peut écrire

$$x = 0x_{(0)} + 1x_{(1)} + 2x_{(2)} +\ldots+ (p-2)x_{(p-2)} + (p-1)x_{(p-1)}$$

Nous posons $x^{[0]} = x$ puis

$$x^{[1]} = 0x_{(p-1)} + 1x_{(0)} + 2x_{(1)} +\ldots+ (p-2)x_{(p-3)} + (p-1)x_{(p-2)}$$

$$x^{[2]} = 0x_{(p-2)} + 1x_{(p-1)} + 2x_{(0)}+\ldots+(p-2)x_{(p-4)}+(p-1)x_{(p-3)}$$

.

.

.

$$x^{[p-1]} = 0x_{(1)}+1x_{(2)}+2x_{(3)}+\ldots+(p-2)x_{(p-1)}+(p-1)x_{(0)}$$

$x^{[p]}$ coïncide à nouveau avec $x^{[0]}$. On associe ainsi à tout $x \in P$, p-1 nouveaux éléments ce qui définit p lois de composition interne unaires :

$$x \to x^{[0]}$$

$$x \to x^{[1]}$$

.

.

.

$$x \to x^{[p-1]}$$

dites lois de glissement d'amplitudes $0,1,\ldots,p-1$.

4.3. Remarque

$$(x^{[i]})^{[j]} = x^{[i+j]}$$

i,j et i+j étant pris modulo p (c'est-à-dire étant éléments de l'anneau Z/p).

Il résulte de là que l'ensemble $\{x^{[0]}, x^{[1]},\ldots,x^{[p-1]}\}$ peut être obtenu par les p glissements à partir de n'importe lequel de ses éléments.

Ceci montre que les p^n éléments d'un treillis de Post fini P (voir justifi-

cation au paragraphe 9.2)se répartissent en p^{n-1} classes disjointes dans chacune desquelles les p éléments se déduisent les uns des autres par glissement et que nous appellerons cycles. On a le cycle particulier

$$\{0,1,\ldots,(p-1)\}$$

Notons que $$i^{[j]} = i + j$$

5. MATRICES DE GLISSEMENT

5.1. Définition

Les expressions définissant les quantités $x^{[0]}, x^{[1]},\ldots, x^{[p-1]}$ peuvent se résumer sous forme matricielle :

$$\begin{Vmatrix} x^{[0]} \\ x^{[1]} \\ \cdot \\ \cdot \\ \cdot \\ x^{[p-1]} \end{Vmatrix} = \begin{Vmatrix} x_{(0)} & x_{(1)} & \cdots & x_{(p-1)} \\ x_{(p-1)} & x_{(0)} & \cdots & x_{(p-2)} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ x_{(1)} & x_{(2)} & \cdots & x_{(0)} \end{Vmatrix} \times \begin{Vmatrix} 0 \\ 1 \\ \cdot \\ \cdot \\ \cdot \\ (p-1) \end{Vmatrix}$$

(Dans la suite, nous écrirons de façon simplifiée x_i pour $x_{(i)}$). Nous désignerons par X la première matrice-colonne, par M (ou M_X) la matrice carrée d'ordre p, appelée matrice de glissement, et par C la matrice-colonne des constantes :

$$X = M\,C$$

La notion de matrice de glissement peut cependant être introduite indépendamment de celle de treillis de P_ost. Etant donné un treillis de Boole B, on appellera matrice de glissement d'ordre p sur B toute matrice carrée d'ordre p dont la première ligne constitue une partition de l'élément universel (éléments ayant deux à deux pour produit l'élément nul 0 et ayant pour somme l'élément universel u) et dont les autres lignes se déduisent chacune de la précédente par permutation circulaire d'une position vers la

droite (matrice cyclique). Nous désignerons par $\mathcal{M}$ l'ensemble des matrices de glissement définies sur B. Entre autres matrices de glissement, nous utiliserons les suivantes :

$$I=I_0=\begin{Vmatrix} u & 0 & 0 & 0 & 0 \\ 0 & u & 0 & 0 & 0 \\ 0 & 0 & u & 0 & 0 \\ 0 & 0 & 0 & u & 0 \\ 0 & 0 & 0 & 0 & u \end{Vmatrix} \quad I_1=\begin{Vmatrix} 0 & u & 0 & 0 & 0 \\ 0 & 0 & u & 0 & 0 \\ 0 & 0 & 0 & u & 0 \\ 0 & 0 & 0 & 0 & u \\ u & 0 & 0 & 0 & 0 \end{Vmatrix} \quad I_2=\begin{Vmatrix} 0 & 0 & u & 0 & 0 \\ 0 & 0 & 0 & u & 0 \\ 0 & 0 & 0 & 0 & u \\ u & 0 & 0 & 0 & 0 \\ 0 & u & 0 & 0 & 0 \end{Vmatrix} \quad \text{etc.}$$

En définitive, revenant au treillis de Post P, nous constatons l'existence d'une bijection :

$$x = 0\,x_0 + 1x_1 + \ldots + (p-1)\,x_{p-1} \longleftrightarrow M = \begin{matrix} x_0 & x_1 & \cdots & x_{p-1} \\ x_{p-1} & x_0 & \cdots & x_{p-2} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ x_1 & x_2 & \cdots & x_0 \end{matrix}$$

entre P et l'ensemble $\mathcal{M}$ des matrices de glissement définies sur B, treillis de Boole sous-jacent à P. Dans la suite de cet article, nous montrerons la possibilité d'interpréter et de préciser, au moyen des matrices de glissement, les résultats précédemment énoncés pour les treillis de Post. En particulier, nous traduirons dans le langage matriciel les diverses lois de composition relatives aux structures d'anneau et de module : ainsi, selon le théorème 1 ci-dessous, à la loi d'addition de l'anneau correspond le produit matriciel habituel ; à la loi de multiplication correspond une opération matricielle nouvelle que nous définirons au paragraphe 6.

5.2. THEOREME 1. Sur un treillis de Boole à n atomes, l'ensemble $\mathcal{M}$ des matrices de glissement d'ordre p est, pour l'opération de multiplication, un groupe commutatif fini d'ordre p^n et de caractéristique p.

Chaque matrice de glissement est caractérisée par les éléments de sa première ligne et correspond donc bijectivement à une partition de l'élément universel. Or, on obtient une telle partition en faisant figurer chaque atome du treillis de Boole une fois et une seule dans l'un des p éléments. Le nombre de partitions de l'élément universel, c'est-à-dire le nombre de matrices de glissement, est donc égal au nombre p^n d'applications de l'ensemble des n atomes dans l'ensemble des p composantes de la première ligne.

Le produit de deux matrices de glissement est une matrice de glissement. Prenons un exemple avec p = 3 :

$$\begin{vmatrix} x_0 & x_1 & x_2 \\ x_2 & x_0 & x_1 \\ x_1 & x_2 & x_0 \end{vmatrix} \times \begin{vmatrix} y_0 & y_1 & y_2 \\ y_2 & y_0 & y_1 \\ y_1 & y_2 & y_0 \end{vmatrix} = \begin{vmatrix} x_0y_0+x_1y_2+x_2y_1 & x_0y_1+x_1y_0+x_2y_2 & x_0y_2+x_1y_1+x_2y_0 \\ x_2y_0+x_0y_2+x_1y_1 & x_2y_1+x_0y_0+x_1y_2 & x_2y_2+x_0y_1+x_1y_0 \\ x_1y_0+x_2y_2+x_0y_1 & x_1y_1+x_2y_0+x_0y_2 & x_1y_2+x_2y_1+x_0y_0 \end{vmatrix}$$

Pour p quelconque, on voit que dans la première ligne de la matrice produit figurent les p^2 produits x_iy_j répartis en p sommes de p termes chacune. On en déduit que la première ligne réalise une partition de l'élément universel. On voit aussi que chaque autre ligne se déduit par permutation circulaire d'une position vers la droite de la ligne qui la précède. On a donc bien une matrice de glissement.

On sait que, pour les matrices booléennes, le produit matriciel est associatif, possède un élément neutre $I = I_0$ et que, pour des matrices cycliques (booléennes ou non), comme c'est le cas ici, il est commutatif. L'inverse d'une matrice de glissement est sa transposée : $M^{-1} = M^T$, comme on le vérifie immédiatement.

L'expression $$c_{ij} = \sum_{k=0}^{p-1} a_{ik}\, b_{kj}$$

du terme général d'une matrice produit (avec les indices variant de 0 à p-1) devient ici

$$z_k = \sum_{i+j\equiv k} x_i\, y_j$$

où $\equiv$ représente l'égalité modulo p, c'est-à-dire l'égalité dans Z/p.

Pour un produit de trois matrices de glissement, on établit sans peine que

$$t_\ell = \sum_{i+j+k\equiv \ell} x_i\, y_j\, z_k$$

expression qui se généralise et donne, pour la puissance $m^{ème}$ d'une matrice de glissement,

$$y_j = \sum_{mi\equiv j} x_i$$

puisque $x_i\, x_j = 0$ si $i \neq j$. Par suite, pour $m = p$,

$$y_0 = u(=p-1)$$

$$y_j = 0 \quad \text{si} \quad j \neq 0$$

car $pi \equiv 0$ est vrai pour tout i, $pi \equiv j \neq 0$ est faux pour tout i. Ceci exprime que

$$M^P = I$$

Enfin, p est le plus petit entier non nul pour lequel $M^P = I$ quel que soit M. On voit en effet que $(I_1)^m \neq I$ si $0 < m < p$.

6. MATRICES DE MULTIPLICATION

6.1. Définition

Considérons les p matrices du type suivant (ici p = 4) :

$$U_0 = \begin{vmatrix} u & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{vmatrix} \quad U_1 = \begin{vmatrix} 0 & 0 & 0 & 0 \\ u & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{vmatrix} \quad U_2 = \begin{vmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ u & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{vmatrix} \quad U_3 = \begin{vmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ u & 0 & 0 & 0 \end{vmatrix}$$

Pour une matrice de glissement M, la combinaison linéaire

$$\overline{M} = \sum_{i=0}^{p-1} U_i\, M^i$$

$$= U_0 I + U_1 M + U_2 M^2 + U_3 M^3$$

est appelée matrice de multiplication associée à M.

La ligne d'indice i ($0 \leq i \leq p-1$) de $\bar{M}$ est la première ligne (d'indice 0) de M^i. Il en résulte que chaque matrice de multiplication ne se trouve associée qu'à une matrice de glissement unique.

6.2. Exemples

Pour p = 4 et p = 5, les matrices de multiplication sont de la forme ci-dessous :

$$\begin{vmatrix} 3 & 0 & 0 & 0 \\ x_0 & x_1 & x_2 & x_3 \\ x_0+x_2 & 0 & x_1+x_3 & 0 \\ x_0 & x_3 & x_2 & x_1 \end{vmatrix} \qquad \begin{vmatrix} 4 & 0 & 0 & 0 & 0 \\ x_0 & x_1 & x_2 & x_3 & x_4 \\ x_0 & x_3 & x_1 & x_4 & x_2 \\ x_0 & x_2 & x_4 & x_1 & x_3 \\ x_0 & x_4 & x_3 & x_2 & x_1 \end{vmatrix}$$

6.3. Remarque. Egalités diverses

1) $U_i U_0 = U_i$

$U_i U_j = 0$ si $j \neq 0$ (0 représentant la matrice nulle d'ordre p).

2) $I_h \bar{M} = \bar{M} M^h$, M étant une matrice de glissement.

3) M étant une matrice quelconque, $\sum_{i=0}^{p-1} U_i M I_i$ est une matrice de glissement dont la première ligne coïncide avec la première ligne de M.

4) $I_i I_j = I_{i+j}$

d'où $(I_i)^h = I_{hi}$

puis $(I_i)^T = (I_i)^{-1} = I_{-i}$

6.4. THEOREME 2. Le produit de deux matrices de multiplication est une matrice de multiplication.

Soit M une matrice de glissement définie par les termes $x_0, x_1, \ldots, x_{p-1}$ de sa première ligne. D'après ce qui a été vu au cours de la démonstration du théorème 1, le terme général de la première ligne de M^i est

$$u_j = \sum_{i\ell \equiv j} x_\ell$$

Le terme général de $\bar{M}$ est alors

$$\alpha_{ij} = \sum_{i\ell \equiv j} x_\ell$$

(ligne i, colonne j, i et j compris entre 0 et p-1). Pour une deuxième matrice de glissement N, $\bar{N}$ a pour terme général

$$\beta_{ij} = \sum_{im \equiv j} y_m$$

D'où le terme général du produit $\bar{M}\,\bar{N}$:

$$\begin{aligned}
\gamma_{ij} &= \sum_{k=0}^{p-1} \alpha_{ik}\, \beta_{kj} \\
&= \sum_{k=0}^{p-1} \Big(\sum_{i\ell \equiv k} x_\ell \Big) \Big(\sum_{km \equiv j} y_m \Big) \\
&= \sum_{k=0}^{p-1} \sum_{i\ell m \equiv j} x_\ell\, y_m \\
&= \sum_{i\ell m \equiv j} x_\ell\, y_m
\end{aligned}$$

Considérons la matrice P dont la première ligne a pour terme général

$$z_k = \gamma_{1k} = \sum_{\ell m \equiv k} x_\ell\, y_m$$

et dont les autres lignes se déduisent cycliquement de la première. On vérifie immédiatement que la première ligne réalise une partition de l'élément universel et, donc, que P est une matrice de glissement. La première ligne de P^i a alors pour terme général

$$t_j = \sum_{ik \equiv j} z_k = \sum_{ik \equiv j} \sum_{\ell m \equiv k} x_\ell\, y_m = \sum_{i\ell m \equiv j} x_\ell\, y_m = \gamma_{ij}$$

Elle coïncide avec la ligne d'indice i (i de 0 à p-1) du produit $\bar{M}\,\bar{N}$. On peut écrire

$$\bar{M}\,\bar{N} = \bar{P}$$

6.5. Exemples

Pour p = 4 et p = 5, on a

$$\begin{vmatrix} 3 & 0 & 0 & 0 \\ x_0 & x_1 & x_2 & x_3 \\ x_0+x_2 & 0 & x_1+x_3 & 0 \\ x_0 & x_3 & x_2 & x_1 \end{vmatrix} \times \begin{vmatrix} 3 & 0 & 0 & 0 \\ y_0 & y_1 & y_2 & y_3 \\ y_0+y_2 & 0 & y_1+y_3 & 0 \\ y_0 & y_3 & y_2 & y_1 \end{vmatrix}$$

$$= \begin{vmatrix} 3 & 0 & 0 & 0 \\ x_0+y_0+x_2y_2 & x_1y_1+x_3y_3 & x_1y_2+x_2y_1+x_2y_3+x_3y_2 & x_1y_3+x_3y_1 \\ x_0+y_0+x_2+y_2 & 0 & x_1y_1+x_1y_3+x_3y_1+x_3y_3 & 0 \\ x_0+y_0+x_2y_2 & x_3y_1+x_1y_3 & x_3y_2+x_2y_1+x_2y_3+x_1y_2 & x_3y_3+x_1y_1 \end{vmatrix}$$

$$\begin{vmatrix} 4 & 0 & 0 & 0 & 0 \\ x_0 & x_1 & x_2 & x_3 & x_4 \\ x_0 & x_3 & x_1 & x_4 & x_2 \\ x_0 & x_2 & x_4 & x_1 & x_3 \\ x_0 & x_4 & x_3 & x_2 & x_1 \end{vmatrix} \times \begin{vmatrix} 4 & 0 & 0 & 0 & 0 \\ y_0 & y_1 & y_2 & y_3 & y_4 \\ y_0 & y_3 & y_1 & y_4 & y_2 \\ y_0 & y_2 & y_4 & y_1 & y_3 \\ y_0 & y_4 & y_3 & y_2 & y_1 \end{vmatrix}$$

$$= \begin{vmatrix} 4 & 0 & 0 & 0 & 0 \\ x_0+y_0 & x_1y_1+x_2y_3+x_3y_2+x_4y_4 & x_1y_2+x_2y_1+x_3y_4+x_4y_3 & x_1y_3+x_2y_4+x_3y_1+x_4y_2 & x_1y_4+x_2y_2+x_3y_3+x_4y_1 \\ x_0+y_0 & x_3y_1+x_1y_3+x_4y_2+x_2y_4 & x_3y_2+x_1y_1+x_4y_4+x_2y_3 & x_3y_3+x_1y_4+x_4y_1+x_2y_2 & x_3y_4+x_1y_2+x_4y_3+x_2y_1 \\ x_0+y_0 & x_2y_1+x_4y_3+x_1y_2+x_3y_4 & x_2y_2+x_4y_1+x_1y_4+x_3y_3 & x_2y_3+x_4y_4+x_1y_1+x_3y_2 & x_2y_4+x_4y_2+x_1y_3+x_3y_1 \\ x_0+y_0 & x_4y_1+x_3y_3+x_2y_2+x_1y_4 & x_4y_2+x_3y_1+x_2y_4+x_1y_3 & x_4y_3+x_3y_4+x_2y_1+x_1y_2 & x_4y_4+x_3y_2+x_2y_3+x_1y_1 \end{vmatrix}$$

6.6. Définition d'une nouvelle loi de composition sur $\mathcal{M}$

La matrice P du théorème 2 étant obtenue de façon unique à partir de M et N, peut être considérée comme leur composée. Nous écrirons

$$P = M * N$$

La loi * se trouve ainsi définie par l'égalité

$$\overline{M*N} = \overline{M}\,\overline{N}$$

6.7. THEOREME 3 $\mathcal{M}$ est un anneau commutatif unitaire, de caractéristique p, pour la loi de produit matriciel notée × ou notée sans signe et la loi *.

On a déjà un groupe commutatif de caractéristique p (Théorème 1).

D'après l'expression

$$\gamma_{ij} = \sum_{i\ell m \equiv j} x_\ell \, y_m$$

du théorème 2, le produit $\overline{M}\,\overline{N}$ est commutatif :

$$\overline{M}\,\overline{N} = \overline{N}\,\overline{M}$$

Compte tenu de l'unicité de P, la loi * est donc commutative.

Dans l'égalité à démontrer

$$(\overline{M}\,\overline{N})\overline{P} = \overline{M}(\overline{N}\,\overline{P})$$

posons $\overline{M}\,\overline{N} = \overline{Q}$ et $\overline{N}\,\overline{P} = \overline{R}$. On a $Q = M*N$, $R = N*P$ et $\overline{Q}\,\overline{P} = \overline{M}\,\overline{R}$, d'où $Q*P = M*R$, c'est-à-dire

$$(M*N)*P = M*(N*P)$$

La loi * est donc associative.

Elle a pour élément neutre I_1. En effet $(I_1)^i = I_1$. D'où $\overline{I_1} = \sum_{i=0}^{p-1} U_i \, I_i = I$.

Vérifions enfin la distributivité, ce qui revient à vérifier l'égalité

$$M^* (NP) = (M*N)\,(M*P)$$

En posant $\overline{M}\,\overline{N} = \overline{Q}$, $\overline{M}\,\overline{P} = \overline{R}$, on est ramené à vérifier que

$$\overline{M}\,(\overline{N\,P}) = (\overline{Q\,R})$$

Pour cela, il suffit de constater que la deuxième ligne de la matrice $\overline{M}(\overline{NP})$ coïncide avec la deuxième ligne de la matrice $(\overline{QR})$. En désignant respectivement par x_i, x_j, $z_{j'}$ le terme général de la première ligne de M,N,P, le terme général de la première ligne de Q est de la forme

$$\alpha_k = \sum_{ij \equiv k} x_i \, y_j$$

le terme général de la première ligne de R est de la forme

$$\beta_{k'} = \sum_{i'j' \equiv k'} x_{i'} z_{j'}$$

le terme général de la première ligne de QR est de la forme

$$\gamma_\ell = \sum_{k+k'\equiv\ell} \alpha_k \beta_{k'}$$

$$= \sum_{k+k'\equiv\ell} \Big(\sum_{ij\equiv k} x_i y_j \Big) \Big(\sum_{i'j'\equiv k'} x_{i'} z_{j'} \Big)$$

$$= \sum_{ij+i'j'\equiv\ell} x_i y_j x_{i'} z_{j'}$$

(terme nul pour $i \neq i'$)

$$= \sum_{i(j+j')\equiv\ell} x_i y_j z_{j'}$$

le terme général de la première ligne de NP est de la forme

$$t_k = \sum_{j+j'\equiv k} y_j z_{j'}$$

le terme général de la matrice $\overline{M}(\overline{NP})$ est de la forme

$$\delta_{h\ell} = \sum_{hik\equiv\ell} x_i t_k$$

$$= \sum_{hik\equiv\ell} x_i \sum_{j+j'\equiv k} y_j z_{j'}$$

$$= \sum_{hi(j+j')\equiv\ell} x_i y_j z_{j'}$$

Pour $h = 1$, on obtient le terme général de la deuxième ligne de $\overline{M}(\overline{NP})$.

On voit qu'il coïncide avec γ_ℓ.

6.8. Remarque. Généralisation de l'égalité $I_1 * M = M$

$$I_h * M = M^h$$

Pour cela on montre que

$$\overline{I_h * M} = \overline{M}^h$$

Or

$$\overline{I_h * M} = \overline{I_h}\ \overline{M}$$

$$\overline{I_h} = \sum_{i=0}^{p-1} U_i (I_h)^i = \sum_{i=0}^{p-1} U_i\, I_{hi}$$

6.9. Exemples

Pour p = 4,h = 2, $\overline{I_2} = \begin{vmatrix} 3 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 3 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 \end{vmatrix}$. Pour P = 5,h = 2, $\overline{I_2} = \begin{vmatrix} 4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 \\ 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4 & 0 \end{vmatrix}$

$\overline{I_{h*M}}$ étant une matrice de multiplication est connue dès que sa deuxième ligne (ligne de rang 1) est connue. On cherche donc le coefficient de U_1 dans le produit

$$\overline{I_h}\ \overline{M} = \left(\sum_{i=0}^{p-1} U_i\ I_{hi}\right)\left(\sum_{j=0}^{p-1} U_j\ M^j\right)$$

c'est-à-dire que l'on cherche i et j tels que

$$U_i I_{hi} U_j = U_1$$

On voit facilement que

$$i = 1 \qquad \text{car} \quad 0 \le i \le p-1$$

$$j \equiv h$$

D'où $$\overline{I_h * M} = \overline{M^h}$$

6.10. THEOREME 4 Si p est premier, $p_M = M$ (p_M désignant la puissance $p^{ème}$ de M pour la deuxième loi).

Pour la composition de h matrices égales

$$y_j = \sum_{i^h \equiv j} x_i \qquad 0 \le j \le p-1$$

car les x_i sont disjoints. Pour h = p, on a l'équation en i :

$$i^p \equiv j$$

p étant premier et j non divisible par p, on sait, d'après un théorème d'arithmétique connu, que j est solution : $j^p - j$ est divisible par p, soit $j^p \equiv j$. Si i est une autre solution, $i^p \equiv j$ on a aussi $i^p \equiv i$ donc $i \equiv j$. On a donc une solution unique et

$$y_j = x_j$$

7. STRUCTURE DE MODULE SUR $\mathcal{M}$

7.1.THEOREME 5. $\mathcal{M}$ est un module unitaire libre avec une base d'ordre n, un espace vectoriel si p est premier, pour les deux lois de composition suivantes

$$\forall\ M,N \in \mathcal{M} \qquad (M,N) \to MN$$

$$\forall\ \lambda \in Z/p \qquad \forall\ M \in \mathcal{M} \quad (\lambda,M) \to M^{\lambda}$$

On a déjà obtenu un groupe commutatif (théorème 1). M^{λ} étant bien une matrice de glissement, la deuxième application définit une loi de composition externe. On vérifie immédiatement les axiomes d'un module unitaire :

$$(\lambda,(\mu,M)) = (M^{\lambda})^{\mu} = M^{\lambda\mu} = (\lambda\mu,M)$$

$$(\lambda+\mu,M) = M^{\lambda+\mu} = M^{\lambda}M^{\mu} = (\lambda,M)\ (\mu,M)$$

$$(\lambda,MN) = (MN)^{\lambda} = M^{\lambda}N^{\lambda} = (\lambda,M)\ (\lambda,N)$$

$$(1,M) = M^{1} = M$$

Soient $\alpha_1,\alpha_2,\ldots,\alpha_n$ les n atomes de B. Considérons les n matrices de glissement de la forme

$$A_i = \begin{vmatrix} \alpha_i' & \alpha_i & 0 & 0 & 0 \\ 0 & \alpha_i' & \alpha_i & 0 & 0 \\ 0 & 0 & \alpha_i' & \alpha_i & 0 \\ 0 & 0 & 0 & \alpha_i' & \alpha_i \\ \alpha_i & 0 & 0 & 0 & \alpha_i' \end{vmatrix} \qquad 1 \le i \le n$$

Elles sont linéairement indépendantes. En effet, partons de

$$(A_1)^{\lambda_1}\ (A_2)^{\lambda_2}\ \ldots\ (A_n)^{\lambda_n} = I$$

Pour le terme général de la première ligne du produit, on a

$$\sum_{\lambda_I i_1+\lambda_2 i_2+\ldots+\lambda_n i_n \equiv k} (\alpha_1)_{i_1}\ (\alpha_2)_{i_2}\ \ldots\ (\alpha_n)_{i_n} = \begin{cases} p-1 = u & \text{si } k\equiv 0 \\ 0 & \text{si } k\not\equiv 0 \end{cases}$$

avec

$$(\alpha_i)_0 = \alpha_i'$$

$$(\alpha_i)_1 = \alpha_i$$

$$(\alpha_i)_j = 0 \quad \text{si} \quad 2 \le j \le p-1$$

Pour $k \equiv 0$, le premier membre est une somme de monômes canoniques qui, pour être égale à u, doit les contenir tous. L'égalité $\lambda_1 i_1 + \ldots + \lambda_n i_n \equiv 0$ est donc vérifiée pour tout jeu de valeurs $(i_1, \ldots, i_n) \in \{0,1\}^n$. En posant $i_1 = 1$, $i_2 = \ldots = i_n = 0$, on obtient $\lambda_1 \equiv 0$ et, de même, $\lambda_i \equiv 0$ pour tout i.

Les n matrices A_i forment un système de générateurs. Soient une matrice de glissement M et x_i le terme général de sa première ligne. Chacun des p termes x_i $(0 \leq i \leq p-1)$ est une somme d'atomes de B :

$$x_i = \sum_{j \in J_i} \alpha_j$$

On a alors $$M = \prod_{i=1}^{p-1} \prod_{j \in J_i} (A_j)^i$$

Considérons en effet une matrice N de terme général y_k, telle que y_0 majore l'atome α_j et formons le produit $N(A_j)^i$. On voit sans difficulté que le terme général a_ℓ de la première ligne de $(A_j)^i$ est tel que $a_0 = \alpha'_j$, $a_i = \alpha_j$ et $a_\ell = 0$ pour $\ell \neq 0$ et $\ell \neq i$. La première ligne du produit $N(A_j)^i$ a donc pour terme général

$$z_m = \sum_{k+\ell \equiv m} y_k \, a_\ell$$

$$= \alpha'_j \, y_m + \alpha_j \, y_{m-1}$$

D'où, puisque $\alpha_j \not< y_k$ si $k \not\equiv 0$,

$$z_0 = \alpha'_j \, y_0$$

$$z_i = y_i + \alpha_j$$

$$z_m = y_m \quad \text{si} \quad m \not\equiv 0 \text{ et } m \not\equiv i$$

Le produit $N(A_j)^i$ se déduit donc de N en déplaçant α_j de y_0 à y_i. En partant de la matrice I que l'on multipliera successivement par les matrices $(A_j)^i$ convenables, on obtiendra M. Notons qu'on peut encore écrire

$$M = \prod_{i=0}^{p-1} \prod_{j \in J_i} (A_j)^i$$

puisque $(A_j)^0 = I$.

7.2. Remarque

D'après une remarque du paragraphe 4, on peut définir la loi externe à l'aide de la loi * puisque

$$M^h = I_h * M$$

et vérifier sous cette forme les axiomes relatifs à la loi externe.

8. GENERALISATION

8.1. Rappel

Sur un ensemble E muni de deux lois de composition interne + et ., on définit (par "changement d'origine"), pour chaque élément $a \in E$, les nouvelles lois $\underset{a}{+}$ et $\underset{a}{.}$ telles que

$$(x \underset{a}{+} y) - a = (x - a) + (y - a)$$

$$(x \underset{a}{.} y) - a = (x - a) . (y - a)$$

- étant l'opération inverse de +, supposée exister. On vérifie immédiatement que $(A \underset{a}{+} .)$ possède le même type de structure que $(E + .)$: groupe avec élément neutre a et 2a - x pour opposé de x, si $(E +)$ est un groupe ; anneau si $(E + .)$ est un anneau ; anneau unitaire d'élément unité 1 + a, si $(E + .)$ est unitaire ; corps avec $a + (x - a)^{-1}$ pour inverse de x, si $(E + .)$ est un corps. D'autres propriétés de $(E + .)$ telles que $px = 0$ (caractéristique p) ou $x^p = x$ (avec p premier) se transportent également.

De la même façon, sur un ensemble E muni de deux lois de composition l'une interne l'autre externe, + et ., on définit de nouvelles lois $\underset{a}{+}$ et $\underset{a}{.}$ telles que

$$(x \underset{a}{+} y) - a = (x - a) + (y - a)$$

$$(\lambda \underset{a}{.} x) - a = \lambda(x - a)$$

Si $(E + .)$ est un module, $(E + .)_a$ en est un ; $(E + .)_a$ est unitaire ou libre si $(E + .)$ l'est. Si $(E + .)$ est un espace vectoriel, $(E + .)_a$ en est un.

8.2. Autres structures d'anneau sur $\mathcal{M}$

D'après le rappel, les opérations $\times_H$ et $*_H$ telles que

$$M \times_H N = H\,(H^{-1}\,M)\,(H^{-1}\,N) \qquad (1)$$

$$M *_H N = H\,((H^{-1}\,M) * (H^{-1}\,N)) \qquad (2)$$

définissent, pour chaque matrice de glissement $H \in \mathcal{M}$, une structure d'anneau sur $\mathcal{M}$, avec élément neutre H, élément unité I_1 H, caractéristique p et, si p est premier, tel que la puissance $p^{\text{ème}}$ de M pour la deuxième loi $*_H$ coïncide avec M.

8.3. Expressions des termes généraux des matrices composées par les lois $\times_H$ et $*_H$

Partons de la définition

$$M \times_H N = H\,(H^{-1}\,M)\,(H^{-1}\,N)$$

Désignons par x_i, y_j, z_k, u_h, $\xi_{i'}$, $\eta_{j'}$, $\zeta_{k'}$ les termes généraux des premières lignes de M, N, $M \times_H N$, H, $H^{-1}M$, $H^{-1}N$ et $(H^{-1}M)\,(H^{-1}N)$. On a

$$\xi_{i'} = \sum_{h'+i\equiv i'} u_{-h'}\, x_i$$

$$\eta_{j'} = \sum_{h''+j\equiv j'} u_{-h''}\, y_j$$

$$\zeta_{k'} = \sum_{i'+j'\equiv k'} \xi_{i'}\, \eta_{j'}$$

$$z_k = \sum_{h+k'\equiv k} u_h\, \zeta_{k'}$$

$$= \sum_{h+k'\equiv k} u_k \sum_{i'+j'\equiv k'} \Big(\sum_{h'+i\equiv i'} u_{-h'}\, x_i \Big) \Big(\sum_{h''+j\equiv j'} u_{-h''}\, y_j \Big)$$

Les termes u_h étant deux à deux disjoints on n'a un produit non nul que si $-h' \equiv h$ et $-h'' \equiv h$, c'est-à-dire si $i \equiv i' + h$ et $j \equiv j' + h$. Dans ces conditions

$$z_k = \sum_{h+h' \equiv k} u_h \sum_{i'+j' \equiv k'} x_{i'+h}\, y_{j'+h}$$

$$= \sum_{h+i'+j' \equiv k} u_h\, x_{i'+h}\, y_{j'+h}$$

En posant $i'+h=i$, $j'+h=j$, on a finalement

$$z_k = \sum_{(i-h)+(j-h) \equiv k-h} u_h\, x_i\, y_j$$

Le calcul précédent aurait pu être conduit plus simplement mais le calcul fait présente l'avantage de pouvoir être repris textuellement pour la deuxième loi. Il suffit, dans $\zeta_{k'}$, de remplacer la somme $i'+j'$ par le produit $i'j'$. On arrive ainsi finalement à

$$z_k = \sum_{(i-h)(j-k) \equiv k-h} u_h\, x_i\, y_j$$

8.4. Autres structures de module sur $\mathcal{M}$

Le rappel précédent permet encore d'affirmer que les opérations

$$M \underset{H}{\times} N = H\,(H^{-1}M)\,(H^{-1}\,N)$$

$$\lambda \underset{H}{\cdot} M = H(H^{-1}\,M)^{\lambda}$$

$$= M^{\{\lambda\}_H} \quad \text{(puissance } \lambda^{\text{ème}} \text{ de M pour la loi } \underset{H}{\times})$$

définissent sur $\mathcal{M}$, pour chaque matrice de glissement H, une structure de module unitaire libre avec une base d'ordre n, d'espace vectoriel si p est premier. Les n matrices $H A_i$ (A_i définie au paragraphe 7.1) constituent une base d'ordre n.

9. APPLICATION A L'ETUDE DES TREILLIS DE POST

9.1. Bijection entre P et $\mathcal{M}$

Etant donné un treillis de Post P fini, à p constantes, $\mathcal{M}$ désigne mainte-

nant à nouveau l'ensemble des matrices de glissement d'ordre p associé au treillis de Boole B, à n atomes, sous-jacent à P.

Dans la bijection :

$$x = 0x_0 + 1x_1 + \ldots + (p-1)x_{p-1} \longleftrightarrow M = \begin{vmatrix} x_0 & x_1 & \cdots & x_{p-1} \\ x_{p-1} & x_0 & \cdots & x_{p-2} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ x_1 & x_2 & & x_0 \end{vmatrix}$$

entre P et $\mathcal{M}$, la constante h correspond à la matrice I_h. Ainsi qu'il a été suggéré au paragraphe 5.1, cette bijection peut être prolongée en divers isomorphismes.

9.2. Structures d'anneau sur P

Pour chaque matrice de glissement H, c'est-à-dire pour chaque élément $u = 0u_0 + 1u_1 + \ldots + (p-1)\, u_{p-1}$, on définit sur P les lois de composition interne $\underset{u}{\oplus}$ et $\underset{u}{\odot}$ suivantes :

$$(x \underset{u}{\oplus} y)_k = \sum_{(i-h)+(j-h)\equiv k-h} u_h\, x_i\, y_j$$

$$(x \underset{u}{\odot} y)_k = \sum_{(i-h)(j-h)\equiv k-h} u_h\, x_i\, y_j$$

P muni des lois $\underset{u}{\oplus}$ et $\underset{u}{\odot}$, étant isomorphe à $\mathcal{M}$ muni des lois $\underset{H}{\times}$ et $\underset{H}{*}$, est un anneau commutatif unitaire, d'ordre p^n, d'élément neutre u, d'élément unité $u^{[1]}$, de caractéristique p : $\{p\}_u\, x = u$ (avec la notation $\{\lambda\}_u\, x$ pour représenter la somme $x \underset{u}{\oplus} x \underset{u}{\oplus} \ldots \underset{u}{\oplus} x$ de λ termes). Pour p premier, $x^{\{p\}_u} = x$ (avec la notation $x^{\{\lambda\}_u}$ pour représenter le produit $x \underset{u}{\odot} x \underset{u}{\odot} \ldots \underset{u}{\odot} x$ de λ facteurs). Pour u = 0, on retrouve bien les lois d'anneau citées au paragraphe 2.

9.3. Interprétation des matrices de multiplication

En posant

$$X = \begin{vmatrix} x^{[0]} \\ x^{[1]} \\ \cdot \\ \cdot \\ \cdot \\ x^{[p-1]} \end{vmatrix} \qquad C = \begin{vmatrix} 0 \\ 1 \\ \cdot \\ \cdot \\ \cdot \\ (p-1) \end{vmatrix}$$

on a déjà montré que pour la matrice de glissement M associée à x,

$$X = MC$$

Considérons maintenant la matrice de multiplication $\bar{M} = \sum_{i=0}^{p-1} U_i M^i$ associée à M. Sa ligne d'indice i $(0 \leq i \leq p-1)$ est la ligne d'indice 0 de la matrice M^i, correspondant à l'élément ix de P. On a donc

$$\begin{vmatrix} 0x \\ 1x \\ \cdot \\ \cdot \\ \cdot \\ (p-1)x \end{vmatrix} = \bar{M} \times \begin{vmatrix} 0 \\ 1 \\ \cdot \\ \cdot \\ \cdot \\ (p-1) \end{vmatrix}$$

ce que nous écrivons encore

$$Cx = \bar{M}\, C$$

9.4. Egalités diverses

1) A $I_i\, I_j = I_{i+j}$ correspond $i \underset{0}{\oplus} j = (i+j)$, le signe + représentant l'addition dans Z/p.

2) A $(I_i)^h = I_{hi}$ correspond trivialement hi = hi.

3) A $I_i * M = M^i$ correspond $i \underset{0}{\otimes} x = ix$, ix représentant

$\{i\}_0 x = x \underset{0}{\oplus} x \underset{0}{\oplus} \ldots \underset{0}{\oplus} x$, somme de i termes.

4) D'après les égalités de définition 1 et 2 du paragraphe 8.2,

$$(x \underset{u}{\oplus} y) \underset{0}{\ominus} u = (x \underset{0}{\ominus} y) \underset{0}{\oplus} (y \underset{0}{\ominus} u)$$

$$(x \underset{u}{\otimes} y) \underset{0}{\ominus} u = (x \underset{0}{\ominus} u) \underset{0}{\otimes} (y \underset{0}{\ominus} u)$$

où $\underset{0}{\ominus}$ représente la loi inverse (soustraction) de $\underset{0}{\oplus}$, sur l'anneau P.

5) De $M = I_h \; M \; I_{-h}$ on déduit les égalités

$$x \underset{0}{\ominus} 0 = x \underset{1}{\ominus} 1 = \ldots = x \underset{p-1}{\ominus} (p-1)$$

qui permettent de relier les unes aux autres les p lois de groupe.

6) De $M = (I_h \; M) \; (I_h)^{-1}$ on déduit les égalités

$$(x=)\; x^{[0]} \underset{0}{\ominus} 0 = x^{[1]} \underset{0}{\ominus} 1 = \ldots = x^{[p-1]} \underset{0}{\ominus} (p-1)$$

qui, à partir d'un élément $x^{[i]}$, permettent de connaître les p-1 autres.

9.5. Structure de module ou d'espace vectoriel sur P

Pour la loi de groupe commutatif $\underset{u}{\oplus}$ et pour la loi externe associée à la loi

$$(\lambda, M) \rightarrow M^{\{\lambda\}_H}$$

de $\mathcal{M}$, à savoir

$$(\lambda, x) \rightarrow \{\lambda\}_u \; x$$

P est un module ou un espace vectoriel isomorphe à $\mathcal{M}$. A la base $\{H\,A_1, \ldots, H\,A_n\}$ de $\mathcal{M}$ correspond la base $\{u \underset{0}{\oplus} 1\;\alpha_1, \ldots, u \underset{0}{\oplus} 1\;\alpha_n\}$ de P.

9.6. Cas particulier : p = 2

P coïncide avec B.

$$x^{[0]} = 0x' + 1x = x$$

$$x^{[1]} = 0x + 1x' = x'$$

Les matrices de glissement sont de la forme suivante

$$\begin{vmatrix} x^{[0]} \\ x^{[1]} \end{vmatrix} = \begin{vmatrix} x' & x \\ x & x' \end{vmatrix} \times \begin{vmatrix} 0 \\ 1 \end{vmatrix}$$

et les matrices de multiplication de la forme

$$\begin{vmatrix} 1 & 0 \\ 0 & 0 \end{vmatrix} \times \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} + \begin{vmatrix} 0 & 0 \\ 1 & 0 \end{vmatrix} \times \begin{vmatrix} x' & x \\ x & x' \end{vmatrix} = \begin{vmatrix} 1 & 0 \\ x' & x \end{vmatrix}$$

On a quatre lois sur $\mathcal{M}$:

$$\begin{vmatrix} x' & x \\ x & x' \end{vmatrix} \overset{\times}{6} \begin{vmatrix} y' & y \\ y & y' \end{vmatrix} = \begin{vmatrix} x'y' + xy & x'y + xy' \\ x'y + xy' & x'y' + xy \end{vmatrix} = \begin{vmatrix} x \odot y & x \oplus y \\ x \oplus y & x \odot y \end{vmatrix}$$

$$\begin{vmatrix} x' & x \\ x & x' \end{vmatrix} \overset{\times}{1} \begin{vmatrix} y' & y \\ y & y' \end{vmatrix} = \begin{vmatrix} x \oplus y & x \odot y \\ x \odot y & x \oplus y \end{vmatrix}$$

$$\begin{vmatrix} x' & x \\ x & x' \end{vmatrix} \overset{*}{0} \begin{vmatrix} y' & y \\ y & y' \end{vmatrix} = \begin{vmatrix} x' + y' & xy \\ xy & x'+y' \end{vmatrix}$$

$$\begin{vmatrix} x' & x \\ x & x' \end{vmatrix} \overset{*}{1} \begin{vmatrix} y' & y \\ y & y' \end{vmatrix} = \begin{vmatrix} x'y' & x+y \\ x+y & x'y' \end{vmatrix}$$

les signes $\oplus$ et $\odot$ <u>ayant ici leur sens habituel en algèbre de Boole</u> (disjonction et conjonction). Ceci donne sur $P = B$ les deux structures connues d'anneau de Boole, avec pour lois

$$0\ (x \odot y) + 1\ (x \oplus y) = x \oplus y$$

$$0\ (x'+y') + 1\ xy = xy$$

telles que $x \oplus x = 0$ et $x\ x = x$, puis

$$0\ (x \oplus y) + 1\ (x \odot y) = x \odot y$$

$$0\ x'y' + 1\ (x+y) = x+y$$

telles que $x \odot x = 1$ et $x + x = x$.

Les égalités 6 ci-dessus deviennent

$$x \oplus 0 = x' \oplus 1$$

soit $$x' = x \oplus 1$$

9.7. <u>Etude des cycles</u>

<u>Classes de matrices de glissement</u>. $\mathcal{J} = \{I_0, I_1, \ldots, I_{p-1}\}$ est un sous-groupe distingué de $\mathcal{M}$. On a donc le groupe quotient $\mathcal{M}/\mathcal{J}$, d'ordre p^{n-1}. Dans chaque classe d'équivalence de $\mathcal{M}$, les matrices se déduisent les unes des autres par permutation circulaire de lignes (ou de colonnes), c'est-à-dire

par produit à gauche (ou à droite) par l'un des I_h.

Classes de cycles. A $\mathcal{Y}$ correspond le cycle $C = \{0,1,\ldots,(p-1)\}$. A chaque classe de matrices correspond un cycle $X = \{x^{[0]}, x^{[1]},\ldots, x^{[p-1]}\}$.

A $\mathcal{M}/\mathcal{Y}$ correspond le groupe quotient P/C. Enfin on peut écrire

$$X = MC$$

où X et C sont des cycles et M une classe de matrices (comparer à l'écriture du paragraphe 5.1.).

On peut passer d'un cycle

$$X = M_X C$$

à un autre $Y = M_Y C$

par $C = (M_X)^T X$

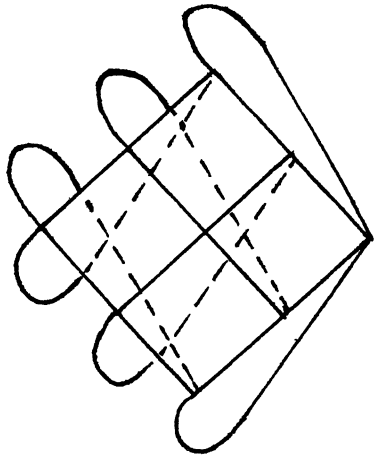
$$Y = (M_Y (M_X)^T)X$$

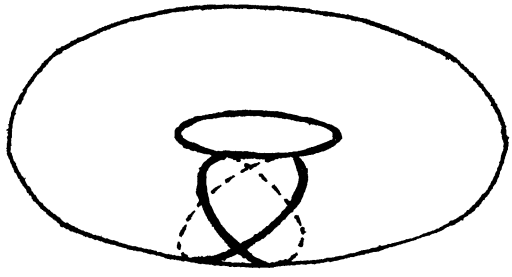
En particulier, on peut retrouver C à partir de tout X.

10. INTERPRETATION GEOMETRIQUE DES RESULTATS PRECEDENTS

10.1. Représentation sur un hypertore

Pour n = 2, on met en évidence les propriétés de glissement en représentant P sur un tore à l'aide de cercles à plan oblique. Le glissement se traduit alors par une rotation du tore autour de son axe.



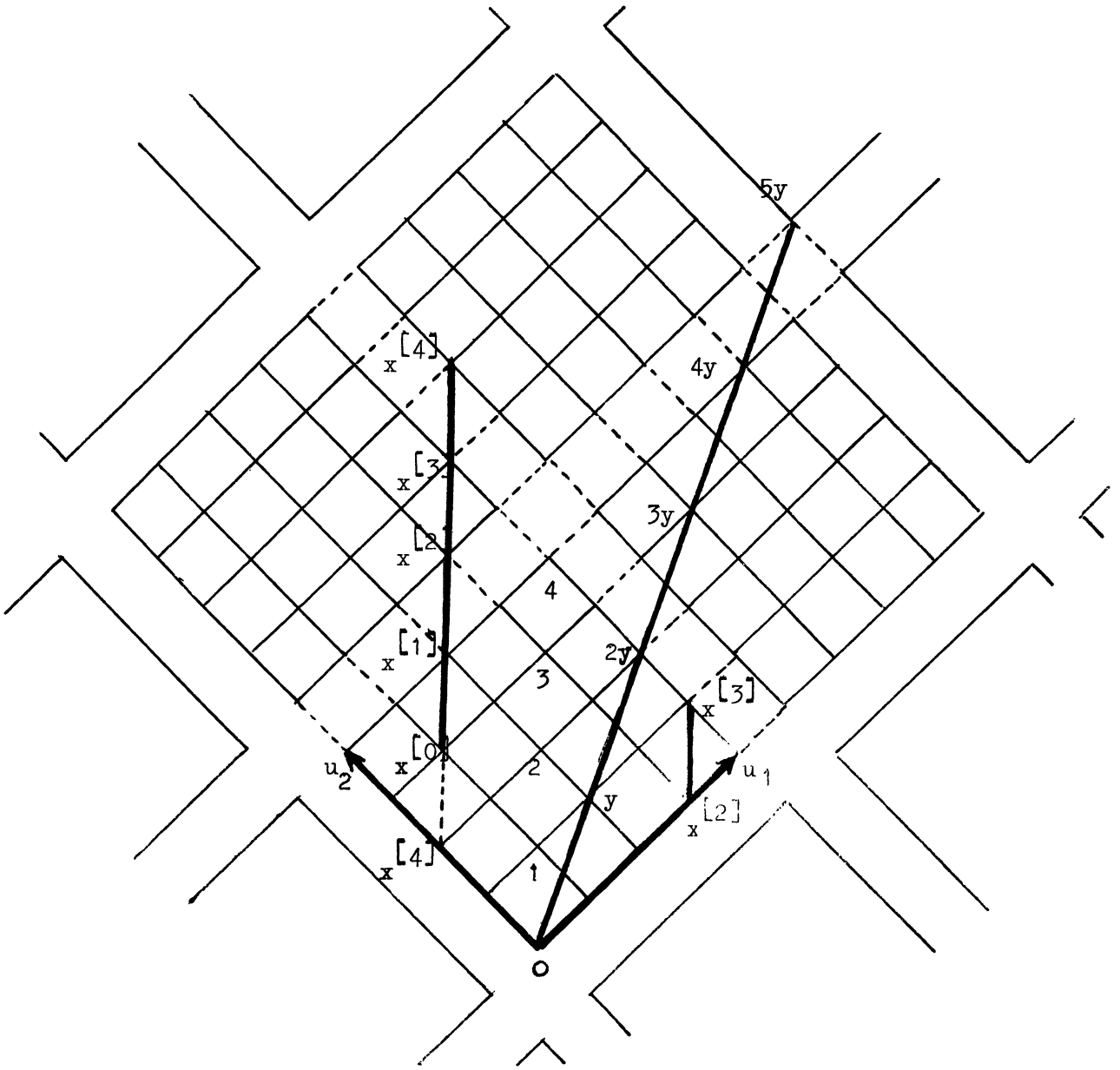


Dans cette représentation la structure d'ordre disparaît.

Pour $n > 2$, on utilisera un hypertore. La valeur de p est indifférente pour le choix de la surface.

10.2. Représentation développée

Il s'agit d'un développement infini de la représentation torique. Nous allons voir qu'elle est adaptée à la structure de module ou d'espace vectoriel. On revient à la structure de treillis en superposant toutes les figures partielles. Ici, les figures seront faites pour $n = 2$ et $p = 5$.



Interprétation de $\underset{0}{\oplus}$. Il correspond à cette opération l'addition vectorielle d'origine 0 : si à x et y correspondent les vecteurs $\sum_i \alpha_t \tau_i$ et $\sum_i \beta_i \tau_i$, à $x \underset{0}{\oplus} y$ correspond $\sum_i (\alpha_i + \beta_i) \tau_i$, où α_i et β_i sont éléments de Z et $\alpha_i + \beta_i$ leur somme dans Z. On voit que la représentation disjointe introduite par Epstein est en fait associée à la structure de module : les τ_i correspondent aux x_j et les α_i sont les constantes.

Interprétation du glissement. D'après $x^{[i]} = x \underset{0}{\oplus} i$, le glissement d'amplitude i correspond à l'addition du vecteur $\overrightarrow{0i}$.

Eléments d'un cycle. Les éléments du cycle associé à x se déduisent de x par addition de $\overrightarrow{01}$, $\overrightarrow{02}$, ..., $\overrightarrow{0(p-1)}$. Ils sont donc situés sur une même verticale.

Multiples d'un élément. 0,y, 2y, 3y,..., (p-1)y, ... sont alignés. py coïncide avec une copie de 0, car selon chaque vecteur τ_i, $p\beta_i$ est divisible par p.

Interprétation de $\underset{0}{\ominus}$. A partir de la représentation disjointe de $x \underset{0}{\ominus} y$, on voit qu'il lui correspond $\sum_i (\alpha_i\ \beta_i)\ \tau_i$, $\alpha_i\ \beta_i$ étant le produit de α_i et β_i dans Z.

Puissances d'un élément. Si p est premier, x^p coïncide avec x car, pour chaque composante, α_i, inférieur à p, n'est pas divisible par p et α_i^p a donc pour reste α_i dans la division par p.

Interprétation de $\underset{u}{\oplus}$. On a

$$(x \underset{u}{\oplus} y) \underset{0}{\ominus} u = (x \underset{0}{\ominus} u) \underset{0}{\oplus} (y \underset{0}{\ominus} u)$$

Après glissement de l'ensemble, du vecteur $\overrightarrow{u0}$, on est ramené à l'addition vectorielle d'origine 0. $\underset{u}{\oplus}$ représente donc l'addition vectorielle d'origine u.

Interprétation de $\underset{u}{\ominus}$. De la même façon, on a ici un produit composante à composante, mesurées à partir de l'origine u.

Remarque. La figure faite qui représente Z^2 convient pour toute valeur de p : il suffit de placer les pointillés différemment.

BIBLIOGRAPHIE

[1] BATBEDAT A., "p^m-Anneaux", Revue roumaine de Mathématiques pures et appliquées, tome XVII, n° 7 (1972), 987-1000.

[2] EPSTEIN G., "The lattice theory of Post algebras", Trans. Amer. Math. Soc., 95,(1960),300-317.

[3] EPSTEIN G., "An equational axiomatization for the disjoint system of Post algebras", IEEE Trans. Comput., C-22,(1973),422-423.

[4] POST E.L., "Introduction to a general theory of elementary propositions", Amer. Journal of Mathematics, 43, (1921), 163-185.

[5] ROSEMBLOOM P.C., "Post algebras I. Postulates and general theory", Amer. Math. Month., vol. 64,(1942), 167-188.

[6] TRACZYK T., "Axioms and some properties of Post algebras", Colloq. Math., 10, (1963), 193-209.

[7] TRACZYK T., "An equational definition of a class of Post algebras", Bull. Acad. Polon. Sci., Sér. Sci. math., astr. et Phys., vol. XII, n° 3, (1964), 147-149.

[8] SERFATI M., *Introduction aux algèbres de Post et à leurs applications*, Cahiers du Bureau Universitaire de Recherche Opérationnelle, Paris, Institut de Statistique des Universités de Paris, 1973.