MATHÉMATIQUES ET SCIENCES HUMAINES

A. LENTIN

Équations dans les monoïdes libres

Mathématiques et sciences humaines, tome 31 (1970), p. 5-16

<http://www.numdam.org/item?id=MSH_1970__31__5_0>

M.S.H. (8e année, no 31, 1970, p. 5-16)

ÉQUATIONS DANS LES MONOÏDES LIBRES

par

A. LENTIN [1]

RÉSUMÉ

Après une introduction de caractère historique, l'auteur expose succinctement les principaux résultats qu'il a obtenus (thèse, Paris 1969) dans le domaine jusqu'alors pratiquement inexploré des équations dans les monoïdes libres.

1. INTRODUCTION : DE LA STRUCTURE DE MONOÏDE LIBRE ET DE SON HISTOIRE

1.1. Rappelons qu'un monoïde (M, μ, *e*) est une structure algébrique définie par un ensemble support non vide M, une opération binaire associative μ et un élément distingué *e* de M, neutre pour μ. Par abus de langage, on désignera souvent à l'aide du même symbole, le monoïde et son support. D'autre part, on appellera μ la *multiplication* dans M et on dira que le composé par μ de deux ou plusieurs éléments en est le *produit.*

Une partie X de M engendre, par application répétée de μ, une certaine partie X_1. Si X_1 coïncide avec M, alors X est un *système générateur* de M. Conformément à une notion mathématique très générale, on dit que M est *libre* sur X, si, et seulement si, toute application f de X dans un monoïde quelconque A peut être prolongée par un homomorphisme Φ de M dans A. Dans le cas présent, une définition équivalente de cette liberté consiste à dire que tout élément de M admet une décomposition, et une seule, comme produit d'éléments de X.

On établit aisément que, s'il existe des monoïdes libres, alors tout monoïde peut être considéré comme image homomorphe d'un monoïde libre. La question se pose donc de savoir si, étant donné un ensemble quelconque X, il existe au moins un monoïde libre engendré par X. La réponse est qu'on en obtient un, soit X*, en prenant pour M l'ensemble des *suites finies d'occurrences d'éléments* de X, pour μ la *concaténation*, pour *e* la *suite vide.*

Il peut être commode de se représenter X* de la manière suivante. Considérons X comme un *alphabet*, fini ou infini, ses éléments comme des *lettres*. Les éléments de X* sont alors les *mots* que l'on peut écrire (sinon prononcer !) avec ces lettres. La concaténation correspond à une manipulation familière. Par exemple, X étant l'alphabet latin, le couple (los, ange) donne par concaténation « losange », tandis que le couple (ange, los) donne « angelos ».

1. Paris V.

Si X admet plus d'un élément, la concaténation n'est pas commutative (mais elle est bien associative) ; elle est commutative dans le seul cas où X ne contient qu'un élément. On observera que, dans ce cas particulier, X* est isomorphe au monoïde additif des entiers naturels ; il correspond, si l'on veut, à « l'arithmétique des bâtons ». Quine [1] a prouvé que, si X admet au moins deux éléments, par exemple si X = {0, 1}, alors on peut reconstituer *toute* l'arithmétique dans le cadre de X*. Le résultat de Quine suggère que la structure de monoïde libre est plus riche qu'elle ne le semble, peut-être, au premier abord.

1. 2. Cette structure pose à l'historien des sciences le problème, intéressant selon nous, de savoir pourquoi elle n'a été que si tardivement perçue, alors qu'elle est sous-jacente à plusieurs situations concrètes, de tous temps des plus usuelles.

Il n'est pas exagéré de dire que certains « calculs » élémentaires conduits dans le cadre des monoïdes libres relèvent d'une pratique familière à l'*Homo sapiens* dès le paléolithique supérieur : pensons à la confection des colliers. En ces temps lointains, l'ensemble X comprenait entre autres, la canine gauche (resp. droite) de renard, la perle sphérique en ivoire de mammouth, le cylindre fait de cette matière, et des coquilles variées — coquilles de cérithes, de *Dentalium badense*, de *Melanopsis vindobonensis* et de toutes espèces de mollusques alors vivants ou déjà fossiles. Les éléments de X*, mots ou *motifs* si l'on préfère ici, s'obtenaient en enfilant les exemplaires (occurrences) collectionnés par centaines de ces éléments de X sur le support linéaire approprié.

Si la nature matérielle des éléments constitutifs a varié, l'art des colliers a traversé les âges. On aurait pu s'attendre qu'il suscitât des problèmes combinatoires du fait des symétries, des répétitions auxquelles il donne lieu, des préoccupations arithmologiques, magiques ou cultuelles, auxquelles on le voit souvent lié.

On prend trois motifs, on double chacun d'eux, on enchaîne les résultats ainsi obtenus. Existe-t-il un motif qui, répété cinq fois, donnerait le même collier ?

Des problèmes de ce genre sont simples à énoncer, l'usage de l'ornementation linéaire (frises) pourrait les suggérer aussi, or ils n'apparaissent jamais dans la mathématique ancienne. D'autre part, les penseurs de l'antiquité classique connaissaient l'écriture alphabétique, avec sa disposition en ligne — parfois selon deux sens *(boustrophedon)* — et pourtant les propriétés combinatoires des suites linéaires de signes n'ont pas retenu leur attention. Pourquoi ?

L'emploi d'un alphabet avait cependant provoqué, semble-t-il, sinon une combinatoire, du moins une attitude combinatoire. En effet, on a plusieurs fois remarqué que les langues des civilisations qui ont développé des théories atomiques furent des langues à écriture alphabétique. L'idée de réduire le monde à des combinaisons de particules élémentaires, dont les types sont en nombre fini, aurait pu être suggérée par la réduction de la parole à un petit nombre de signes distincts. On sait que Lucrèce, quand il argumente en faveur de la théorie atomique [2], fait à plusieurs reprises remarquer que des lettres, en petit nombre, donnent par combinaison un grand nombre de mots, de vers différents. Certes Lucrèce écrivait quelque trois ou quatre siècles après Démocrite, mais cette idée, il l'a peut-être héritée des créateurs de la théorie.

S'il en était ainsi, on saisirait deux raisons qui ont empêché le développement d'une combinatoire linéaire. D'une part, l'impossibilité de se passer du *sens* des mots, d'autre part, le saut de l'unidimensionnel (linéaire) au tridimensionnel, philosophiquement intéressant mais regrettable techniquement.

Mais les choses paraissent plus compliquées. Le mot σ τ ο ι χ ε ῖ ο ν que Démocrite [3] emploie parfois pour désigner une particule élémentaire, semble avoir eu, avant le sens bien attesté de « caractère d'écriture » le sens de *trait* avec lequel on forme les caractères. Ainsi, deux σ τ ο ι χ ε ῖ α sont nécessaires pour tracer un chi (X), trois pour un dzéta (Z) ou un nu (N), etc. Alors, dès le début, la réflexion aurait

glissé vers une combinatoire du plan. Nous sommes redevable à Roger Martin d'une très intéressante citation d'Aristote [4], propre à étayer cette thèse : « Les différences de l'être, disent-ils, [Leucippe et Démocrite] ne viennent que de la configuration, de l'arrangement et de la tournure (ῥ υ σ μ ό ς, δ ι α θ ι γ ή, τ ρ ο π ή). Or la configuration c'est la figure (σ χ ῆ μ α), l'arrangement, c'est l'ordre (τ ά ξ ι ς) et la tournure c'est la position (θ έ σ ι ς). Ainsi A diffère de N par la figure, AN de NA par l'ordre et Z de N par la position ».

Si dzéta et nu diffèrent par la *position*, c'est que nous sortons de la ligne. Adieu, monoïdes libres, adieu pour des siècles !

Il faut en effet attendre le XX^{e} siècle pour voir l'attention des mathématiciens se porter vers ces objets. S'il n'est pas question de faire ici une étude historique, peut-être convient-il cependant de citer les noms du Norvégien Axel Thue, qui a posé le *problème des mots*, de l'Américain Emil Post, créateur des systèmes combinatoires et du problème de la double correspondance.

Aujourd'hui, la branche des mathématiques qui traite des familles de parties des monoïdes libres est la théorie des langages formels. (Voir, par exemple, Chomsky et Schützenberger [5].)

2. ÉQUATIONS. SOLUTIONS PRINCIPALES

2. 0. Revenant au problème posé plus haut, si l'on désigne par a, b, c les motifs à doubler, par d le motif à répéter cinq fois, on est conduit à écrire l'équation :

$$a\ a\ b\ b\ c\ c = d\ d\ d\ d\ d,$$

ou :

$$a^2\ b^2\ d^2 = d^5.$$

2. 1. D'une façon générale, un couple de mots $f, f' \in \mathrm{X}^*$, détermine une équation que nous écrivons (f, f'), réservant le signe de l'égalité aux seules égalités non conditionnelles. Nous dirons que l'équation est *propre* si et seulement si, f et f' ne sont pas identiques : $f \neq f'$.

Les *solutions particulières* dans Y^* de cette équation sont les morphismes $\varphi : \mathrm{X}^* \to \mathrm{Y}^*$ tels que $\varphi f = \varphi f'$.

Exemple.

$$\mathrm{X} = \{ a, b, c \}\ ; \quad \mathrm{Y} = \{ u, v \}\ ; \quad f = abc\ ; \quad f' = cba.$$

Soit φ tel que $a \mapsto uvu$, $b \mapsto$ v, c $\mapsto$ *uvuvuvuvu*, alors :

$$\varphi f = \varphi f' = uvuvuvuvuvuvu.$$

(Le problème général des équations dans les monoïdes libres n'avait pratiquement pas été abordé. Les seules équations considérées l'ont été en vue de résoudre tels problèmes préliminaires à l'étude des équations dans les groupes libres. Voir M. P. Schützenberger [6] ainsi que R. C. Lyndon et M. P. Schützenberger [7].)

2. 2. Y_1^* étant un autre monoïde libre, on dit que la solution φ_1 de (f, f') dans Y_1^* procède de la solution φ si, et seulement s'il existe un morphisme $\chi : \mathrm{Y}^* \to \mathrm{Y}_1^*$ tel que $\chi \varphi = \varphi_1$.

Cette relation étant un préordre, le problème se pose de chercher un ensemble minimal W ne dépendant que de l'équation $(f, f') \in \mathrm{X}^* \times \mathrm{X}^*$ et une famille privilégiée de solutions dans W^*, soit

$\Psi = \Psi(f, f'; W)$, tels que toute autre solution de (f, f') procède d'une solution privilégiée. *A priori*, ce problème admet une réponse formelle, et nous dirons que la famille Ψ est formée des *solutions principales*. Intuitivement, **Card** (W) est le nombre des mots arbitraires figurant dans les solutions de l'équation et il mesure en quelque sorte la force des contraintes qu'impose celle-ci. On prouve, par exemple, que pour les équations $(a^m\ b^n,\ c^p)$ avec $m, n, p \geqslant 2$ ou $(a^m\ b^n\ c^p,\ d^q)$ avec $m, n, p, q \geqslant 3$, on a **Card** (W) = 1 [8].

2. 3. D'une manière informelle, l'étude des solutions principales peut être présentée comme suit.

Soit t un symbole distingué. Si une équation $(f, f') \in X^* \times X^*$ admet une solution $\varphi : X^* \to Y^*$, elle admet la solution $\theta : X^* \to \{t\}^*$ obtenue en envoyant sur t tout $y \in Y$. La solution θ caractérise ce qu'on peut appeler la « longueur de φ ».

Inversement, partons d'une solution $\theta : X^* \to \{t\}^*$, solution « en longueurs pures » et représentons-nous t comme une case blanche.

Dans $\theta f = \theta f'$, chaque case reçoit un numéro, son *ordinal absolu*, qui donne sa position à partir de la gauche.

D'autre part, dans chaque mot $\theta\ x$, $x \in X$, chaque case reçoit une étiquette numérotée. On obtient ainsi, λ étant la longueur de $\theta\ x$:

$$\theta^\sharp\ x = (x, 1)\ (x, 2)\ \ldots\ (x, \lambda).$$

La relation définie par égalité des ordinaux, relation $Œ_\theta$, engendre une équivalence $\overline{Œ_\theta}$ dans l'ensemble X_θ des paires (x, i), $x \in X$. Le morphisme naturel $\theta^\natural$ de X_θ vers l'ensemble quotient : $\overline{X}_\theta = X_\theta / \overline{Œ_\theta}$ est la *solution* θ- *libre* attachée à θ.

Dans chaque $\theta^\sharp$ x est défini sur les éléments (x, i) un ordre total par les numéros croissants, d'où par produit direct un ordre partiel dans X_θ. De manière vraiment très informelle, disons que le comportement de cet ordre par rapport au morphisme $\theta^\natural$ pose le « problème des consécutions » : « quelque chose passe plus ou moins » à travers le morphisme. On atteint ce « quelque chose » en analysant la propagation des *digrammes*.

2. 4. Les solutions principales sont caractérisées par le théorème suivant.

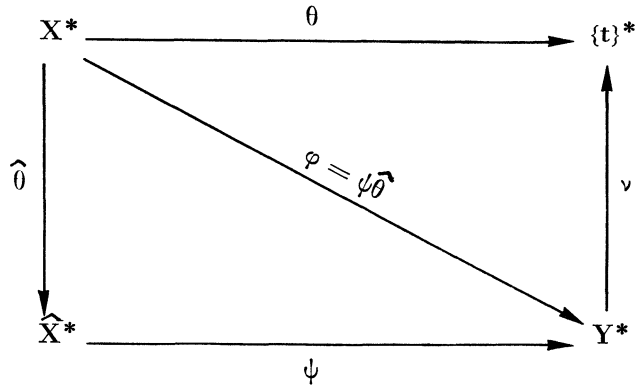
Théorème.

Soit $\theta : X^* \to \{t\}^*$ une solution dans le monoïde $\{t\}^*$ d'une équation $(f, f') \in X^* \times X^*$. Il existe un ensemble $\hat{X}$ et une solution $\hat{\theta} : X^* \to \hat{X}^*$ de cette équation, uniques aux isomorphismes près, qui satisfont les deux conditions suivantes :

1) Chaque lettre de $\hat{X}$ apparaît au moins une fois à l'initiale et au moins une fois à l'ultième dans les mots $\hat{\theta}\ x$ $(x \in X)$.

2) Toute solution $\varphi : X^* \to Y^*$, telle que θ procède de φ, procède elle-même de $\hat{\theta}$.

Ainsi, toute solution φ de « longueur » θ, procède de $\hat{\theta}$, qui ne procède que d'elle-même, et l'on a le diagramme :



Si donc nous posons : par $(f, f') = \mathbf{Max}\ \{\mathbf{Card}\ (\hat{X}) : \hat{\theta}\ \text{principale}\}$,

il est clair que l'on a :

$$\mathbf{Card}\ (W) = \text{par}\ (f, f').$$

On démontre alors le théorème suivant :

Théorème.

On a, X étant minimal, par $(f, f') < \mathbf{Card}\ (X)$ si et seulement si l'équation (f, f') est propre.

On remarquera que le maximum $-1 + \mathbf{Card}\ (X)$ peut être atteint. Il suffit de prendre pour (f, f'), $f = x_1$ et $f' \in X^*_1$ avec $X_1 = X \setminus \{x_1\}$.

2. 5. *Équations équilibrées.*

Les propriétés des solutions principales suggèrent de s'intéresser aux équations équilibrées (f et f' abéliennement équivalents) et de poser à leur sujet le problème suivant, que nous appellerons *problème aux frontières* (en abrégé *PF*).

On considère les paires $< C, \omega >$ formées d'un ensemble non vide C et d'un morphisme $\omega : X^* \to (C \times C)^*$. Si pour $x \in X$ on a $x \mapsto c'\ c''$; $C', C'' \in C$, on dira que c' (resp. c'') est l'élément initial (resp. ultième de $\omega\ x$. (*PF*) s'énonce alors :

Déterminer les paires $< C, \omega >$ telles que :

a) $f^{(1)}$ et $f'^{(1)}$ (resp. $f^{(r)}$ et $f'^{(r)}$ étant l'initiale (resp. ultième) de f et celle de f', l'élément initial de $\omega f^{(1)}$ (resp. ultième de $\omega f^{(r)}$) soit égal à l'élément initial de $\omega f'^{(1)}$ (resp. ultième de $\omega f'^{(r)}$) ;

b) quand x décrit f, l'élément initial (resp. ultième) de $\omega\ x$ décrit C entièrement ;

c) les mots formés dans ωf et $\omega f'$ par les *digrammes frontaliers* soient abéliennement équivalents.

(Pour $x_i\ x_j$, le digramme frontalier de $\omega\ (x_i\ x_j)$ est formé par l'élément ultième de $\omega\ x_i$ suivi de l'élément initial de $\omega\ x_j$.)

On voit immédiatement qu'à toute solution principale de l'équation (f, f') on peut associer canoniquement une solution de (PF). L'entier naturel (*indice frontalier*) *ifro* (f, f') :

$$ifro\ (f, f') = \text{Max}\ \{\ \textbf{Card}\ (C) : <\ C, \omega\ >\quad \text{solution}\quad \text{de}\ (PF)\ \}$$

donne donc une borne supérieure de **Card** (W).

3. *P*-OPÉRATIONS ET SYSTÈMES DE BIMOTS

3. 0. Dans l'équation $(f, f') \in X^* \times X^*$, soit y l'initiale de f, z celle de f' et soit $y \neq z$.

Si l'on suppose que la longueur $|\ y\ |$ de y est supérieure à la longueur $|\ z\ |$ de z, on peut remplacer toute occurrence de y par $z\ y_1$ et, simplifiant par z à l'initiale, on obtient une nouvelle équation. Il est loisible d'économiser un indice et de remplacer y par zy, si l'on garde mémoire de l'opération. On a le cas symétrique $|\ y\ | < |\ z\ |$ (et le cas $|\ y\ | = |\ z\ |$ qui implique $y = z$).

Il est loisible de détacher cette construction du contexte équationnel.

3. 1. Appelons *bimot* tout couple $(f, f') \in X^* \times X^*$. Si y est l'initiale de f et z celle de f' avec $y \neq z$, on considère le morphisme $\pi : X^* \to X^*$ tel que $y \mapsto zy$ et, pour $x \neq y$, $x \mapsto x$. Simplifiant $(\pi f, \pi f')$ à gauche par z, on obtient un bimot qui dérive de (f, f') par l'opération de *pivot initial gauche*, ou opération *pig*. Il y a quatre *p*-opérations de ce genre, dont deux opérations *pi* (à pivot initial). Les *p*-opérations organisent les bimots selon certains systèmes algébriques, les *p*-systèmes, lesquels peuvent être considérés en soi, indépendamment de leurs applications équationnelles, dans le cadre de l'Algèbre universelle. Une classification utile est la suivante :

p-systèmes	linéaires	non linéaires
équilibrés	bipermutationnels A	équilibrés non linéaires C
non équilibrés	linéaires non bipermutationnels B	ni linéaires ni équilibrés D

Les opérations *pi* préservent en effet d'une part l'équilibre et, d'autre part, la linéarité.

3. 2. Qualifions un bimot d'*équationnel* si et seulement s'il existe des solutions $\theta : X^* \to \{ t \}^*$ pour lesquelles $e \notin \theta\ X$ (e le mot vide).

On voit facilement que si un bimot est équationnel mais non équilibré, alors chaque membre contient au moins un *hapax*, c'est-à-dire une lettre qui ne présente qu'une occurrence unique.

Le cas B donne lieu au théorème suivant :

Théorème.

Si (f, f') est un bimot indécomposable, équationnel, linéaire mais non bipermutationnel, il existe dans le système Pi (f, f') — c'est-à-dire dans le système engendré à partir de (f, f') par les *pi*-opérations — un bimot dont un membre admet un hapax à l'initiale.

3. 3. Cas d'un bimot (f, f') équilibré.

a) A l'ensemble X nous associons deux ensembles de même cardinalité ^{-}X et ^{+}X en bijection canonique avec X.

b) A tout bimot équilibré $(f, f') \in X^* \times X^*$, nous associons deux alphabets :

$^{-}\mathscr{A}(f, f') = {}^{-}\mathscr{A}$, qui provient de ^{-}X par identification de $^{-}f^{(1)}$ et $^{-}f'^{(1)}$;

$^{+}\mathscr{A}(f, f') = {}^{+}\mathscr{A}$, qui provient de ^{+}X par identification de $^{+}f^{(r)}$ et $^{+}f'^{(r)}$; $r = |f| = |f'|$.

c) Dans l'ensemble $^{+}\mathscr{A} \times {}^{-}\mathscr{A}$, nous définissons le sous-ensemble ou *relation frontalière droite*

$$\tau_D = \{ [{}^{+}f'^{(1)}, {}^{-}f'^{(2)}], \ldots, [{}^{+}f'^{(i)}, {}^{-}f'^{(i+1)}], \ldots, [{}^{+}f'^{(r-1)}, {}^{-}f'^{(r)}] \}$$

et dans l'ensemble $^{-}\mathscr{A} \times {}^{+}\mathscr{A}$ le sous-ensemble ou *relation frontalière gauche.*

$$\tau_G = \{ [{}^{-}f^{(2)}, {}^{+}f^{(1)}], \ldots, [{}^{-}f^{(i+1)}, {}^{+}f^{(i)}], \ldots, [{}^{-}f^{(r)}, {}^{+}f^{(r-1)}] \}.$$

d) Dans l'ensemble $^{+}\mathscr{A} \times {}^{+}\mathscr{A}$, nous définissons, la *relation pi-frontalière* $\sigma(f, f') = \sigma$ attachée au bimot (f, f') par :

$$\sigma = \tau_D \tau_G.$$

On alors la proposition suivante :

Proposition.

Si le bimot (g, g') appartient à Pi (f, f'), le bimot (f, f') étant équilibré, alors la relation *pi*-frontalière de (g, g') contient celle de (f, f').

La preuve de cette proposition se fait par cas et ne présente pas de difficulté particulière.

Le calcul de *ifro* (f, f') se ramène à la détermination d'un certain Maxmin sur l'ensemble des bijections des flèches de τ_D sur les flèches de τ_G.

Dans le cas d'un *pi*-système bipermutationnel, σ peut être considéré comme une substitution de $\Sigma\,(^{+}\mathscr{A})$ et, plus précisément, comme une substitution appartenant au groupe alterné $\mathcal{A}\,(^{+}\mathscr{A})$ et elle est un invariant du *pi*-système engendré par (f, f'). De plus :

$$ifro\,(f, f') = M(\sigma) = \text{Max}\,\{\,\min(z(\sigma'), z(\sigma'')) : \sigma = \sigma'\,\sigma''\,;\ \sigma', \sigma'' \in \Sigma\,(^{+}\mathscr{A})\,\},$$

$z(\sigma)$ désignant le nombre de cycles de σ.

Enfin, si (f, f') est une bipermutation indécomposable, on montre qu'à toute solution de (PF) on peut associer une solution de l'équation (f, f') et l'on en déduit que :

$$M(\sigma) = \mathbf{Card}\,(W).$$

4. CALCULS RELATIFS AUX GROUPES SYMÉTRIQUES

4. 0. Pour calculer $M(\sigma)$, il convient de développer un certain nombre de techniques dont les possibilités d'emploi débordent vraisemblablement les applications qui en sont faites ici. Pour un traitement plus développé, voir [9].

4. 1. A étant un ensemble de cardinalité quelconque, E une partie finie de A, on désigne par Φ_A et l'on appelle *fixateur* de E pour A l'opérateur qui envoie Σ_A dans lui-même de telle sorte que, si $\sigma \in \Sigma_A$ et si $\bar{\sigma} = \Phi_A^E(\sigma)$, alors :

i) pour tout $x \in E$, $x \,.\, \sigma = x$;

ii) pour $a \in A \setminus E$, $a \,.\, \bar{\sigma} = a \,.\, \sigma^n$,

où n est le plus petit entier naturel non nul, tel que $a \,.\, \sigma^n \in A \setminus E$.

Il est clair que la finitude de E assure l'existence de n et que Φ_A projette $\mathfrak{E}\Sigma_A$ sur son sous-groupe maximal qui conserve E point par point.

Dans le cas où E se réduit à un point i, on établit un lemme utile, à savoir que l'égalité $\sigma = \varphi\,\psi$ entraîne, par fixation de i, l'égalité $\bar{\sigma} = \bar{\varphi}\,\bar{\psi}$ si, et seulement si, i est point fixe de l'une des trois substitutions φ, ψ, σ.

D'autre part, on considère sous le nom de *biinvodécomposition* (en abrégé b.i.d.), les décompositions $\sigma = \alpha\,\beta$ d'une substitution σ en un produit de deux involutions α et β. On dit que la b.i.d. $\sigma = \alpha\,\beta$ est *intraorbitale* si toute orbite de α ainsi que toute orbite de β, est contenue dans quelque orbite de σ ; dans le cas contraire, on la dit *extraorbitale*. On dit encore que la b.i.d. est *équilibrée* si, et seulement si, la différence entre les nombres des points fixes des facteurs ne dépasse pas *un* en valeur absolue.

Utilisant le lemme de fixation on démontre que le Maxmin donnant $M(\sigma)$ est atteint (en particulier) pour les b.i.d. intraorbitales équilibrées, d'où enfin le résultat suivant [10] :

Théorème.

$z(\varphi)$ désignant le nombre des cycles de la substitution φ, y compris les cycles de longueur un, le nombre :

$$M(\sigma) = \mathrm{Max}\,\{\,\min(z(\alpha), z(\beta)) : z = \alpha\,\beta\,;\ \alpha, \beta \in \Sigma_n\,\}$$

est donné par :

$$M(\sigma) = [(n + \mathbf{Card}\, z(\sigma)) / 2],$$

où les crochets désignent la partie entière.

4. 2. **Card** (W) pour les équations linéaires.

Les résultats précédents permettent de calculer *a priori* **Card** (W) pour toute équation linéaire. On dira que l'équation linéaire (f, f') est *normalisée* si et seulement si, l'alphabet X est minimal et le bimot (f, f') équationnel. On obtient le théorème :

Théorème.

Pour une équation normalisée linéaire non bipermutationnelle, on a :

$$\mathbf{Card}\,(W) = -1 + \mathbf{Card}\,(X).$$

Pour une équation normalisée linéaire et bipermutationnelle, on a :

$$\textbf{Card}\,(\mathrm{W}) = \tfrac{1}{2}\,(z\,(\sigma) - 1 + \textbf{Card}\,\mathrm{X}),$$

où $z\,(\sigma)$ désigne le nombre des orbites de la substitution *pi*-frontalière.

(Il n'y a pas lieu d'indiquer la partie entière dans la formule, car σ est paire.)

Exemples.

1) (*abcdef, dbfgea*).

Équation normalisée linéaire et non bipermutationnelle (e et g sont des hapax) :

$$\textbf{Card}\,(\mathrm{X}) = 7, \quad \text{donc} \quad \textbf{Card}\,(\mathrm{W}) = 6.$$

2) (*abcdefgh, hgfedcba*).

Équation bipermutationnelle. Dans ${}^{+}\mathscr{A}$, ${}^{+}a = {}^{+}h$. On supprime l'indice « + » pour simplifier l'écriture :

$$\sigma = ({}^{h}_{a}fdbgec)\,;\; z\,(\sigma) = 1\,;$$

$$\textbf{Card}\,(\mathrm{X}) = 8\,;\; \textbf{Card}\,(\mathrm{W}) = \tfrac{1}{2}\,(1 + 7) = 4.$$

3) (*abcdefgh, hdbgfcea*).

$$\sigma = ({}^{b}_{a}cd)\;(bf)\;(eg)\,;\; z\,(\sigma) = 3,$$

$$\textbf{Card}\,(\mathrm{W}) = \tfrac{1}{2}\,(3 + 7) = 5.$$

5. PROPRIÉTÉS ALGÉBRIQUES DES PI-SYSTÈMES BIPERMUTATIONNELS

5. 0. Les *pi*-systèmes engendrés par une bipermutation indécomposable, c'est-à-dire les *pi*-systèmes bipermutationnels minimaux (en abrégé : pi-sbm) possèdent des propriétés algébriques intéressantes, qui enrichissent la théorie des permutations et sont en rapport avec la théorie du groupe symétrique.

5. 1. (f, f') étant une bipermutation, l'application naturelle de f sur l'ensemble $[\mathrm{k}] = \{1, 2, \ldots, k\}, k = \textbf{Card}\,(\mathrm{X})$, définit une projection de (f, f') sur son *type*, lequel est une permutation de $[k]$. On définit aisément les *pi-sbm de types*, et tout pi-sbm se projette sur un pi-sbm de types. On démontre que le groupe des automorphismes d'un pi-sbm de types admet au plus un automorphisme non neutre qui transforme le type en le type inverse (inversotypie) et l'on montre qu'il en est ainsi lorsque le pi-sbm contient une bipermutation *involutive* (*i.e.* dont le type coïncide avec le type inverse).

5. 2. La question se pose donc de savoir si tout pi-sbm contient au moins une bipermutation involutive.

On peut y répondre de la façon suivante.

On définit un type biinvolutif spécial par les conditions :

i) commencer par k = **Card** (X), finir par 1 ;

ii) présenter entre k et 1 une suite de segments naturels dans leur ordre initial, mais individuellement retournés.

Exemples (pour $k = 9$).

9 5432 6 87 1 ;
9 3254 876 1 ;
9 5432 876 1 ; etc.

De plus, il est suffisant de considérer les *pi*-systèmes *non réductibles*, c'est-à-dire, en gros, engendrés par des bipermutations où aucune paire de lettres ne figure à la fois dans les deux membres (sinon, on pourrait « contracter »). On a alors le résultat suivant.

Théorème.

Tout pi-sbm non réductible contient au moins une bipermutation de type spécial.

Il peut arriver qu'un pi-sbm non réductible contienne plusieurs types spéciaux ; le premier exemple se rencontre pour $k = 8$. Le théorème ne permet donc pas de dénombrer, mais seulement de majorer le nombre des pi-sbm équationnellement utiles, en calculant le nombre de types spéciaux non réductibles. Celui-ci est donné par une loi « méta-fibonaccienne » :

$$u_{n+3} = u_{n+2} + u_{n+1} + u_n,$$

$$u_2 = 0,\ u_3 = 0,\ u_4 = 1.$$

5. 3. Groupe des automorphismes d'un pi-sbm.

On prouve que ce groupe est en général un groupe diédral. Cela tient au fait que les isomorphismes qui conservent le type (isotypies) conservent σ et forment en général un groupe cyclique d'une part, et qu'il y a d'autre part, la symétrie introduite par le type spécial.

5. 4. Sur les k 1 -bipermutations involutives.

Mais il est possible de s'intéresser à toutes les bipermutations involutives contenues dans un pi-sbm non réductible, ou tout au moins aux k 1 -bipermutations involutives, c'est-à-dire à celles où les lettres de rang 1 et k se correspondent. Pour ces bipermutations (qui contiennent donc en particulier les bipermutations spéciales), on peut identifier canoniquement $^{-}\mathscr{A}$ et $^{+}\mathscr{A}$.

Soit donc un pi-sbm, σ sa substitution *pi*-frontalière et $\sigma = \sigma_2\ \sigma_1$ une b.i.d. de σ. Considérons une bipermutation (f, f') du système, posons :

$$\sigma_1 = \tau_G\ \sigma_I\ \tau_G^{-1}.$$

On en déduit :

$$\sigma_2 = \tau_D\ \sigma_1\ \tau_G.$$

Pour toute (f, f') dans le pi-sbm, le décomposition se réalise donc avec un σ_1 chaque fois différent. Dans le cas d'une (k 1) bipermutation involutive, on doit avoir $\sigma_2 = \sigma_1$ (grâce à l'identification canonique).

Une condition nécessaire, portant sur la b.i.d. $\sigma = \sigma_2 \sigma_1$, pour qu'il puisse en être ainsi, est que l'une des lettres qui sont points fixes dans σ_1, puisse prendre le rang k — 1 dans une (k 1)-bipermutation. Appelons *adaptées* les b.i.d. qui possèdent cette propriété.

Au moyen de lemmes combinatoires assez pénibles, on montre que pour toute b.i.d. adaptée, on peut trouver dans le pi-sbm une bipermutation dans laquelle σ_1 admet une transposition (i j) qui figure dans σ_2.

A partir de là, on peut faire des récurrences en utilisant des techniques de fixation et la notion de pi-sbm *contraint* (pi-sbm pour lequel certaines lettres ne peuvent pas être utilisées comme pivots). On obtient alors le résultat suivant.

Théorème.

Pour toute biinvodécomposition adaptée $\sigma = \sigma_2 \sigma_1$ de la substitution *pi*-frontalière, un pi-sbm contient au moins une (k 1) -bipermutation involutive telle que $\sigma_2 = \sigma_1$.

6. REMARQUES DIVERSES

6. 0. On aura remarqué que le cas bipermutationnel se trouve sous la dépendance étroite du groupe symétrique et qu'il y suscite des problèmes nouveaux à traiter par des techniques nouvelles.

Ces techniques permettent d'ailleurs de résoudre des problèmes qui se posent dans le cadre de la théorie « classique » : c'est le cas d'un problème issu d'une recherche de O. Ore [11].

6. 1. Dans une note [10] publiée en collaboration, nos collaborateurs et nous-mêmes avions précisé un résultat de cet auteur en prouvant que toute substitution paire d'ordre n était au moins une fois le commutateur d'un cycle maximal et d'une involution.

On peut aller plus loin et caractériser, pour tout $\sigma \in \mathcal{A}_n$, l'ensemble des paires (γ, ε), γ cycle maximal, ε involution, pour lesquelles $\gamma \varepsilon \sigma = \varepsilon \gamma$.

6. 2. Le problème général des équations dans les monoïdes libres n'avait pratiquement pas été prospecté. Le sondage que nous avons fait prouve, croyons-nous, que ce domaine n'est pas isolé. Au terme de cheminements parfois imprévus, on débouche sur des théories classiques qui s'en trouvent enrichies.

BIBLIOGRAPHIE

[1] Quine, W. V., « Concatenation as a basis for arithmetic », *J. of Symbolic Logic*, t. 11, 1946, pp. 105-114.

[2] Lucrèce, *De la nature*, I, vers 823-826 ; II, vers 688-694 ; II, vers 1013-1018.

[3] Voir par exemple le fragment conservé par Marc-Aurèle, *Pensées*, VII-31.

[4] Aristote, *Métaphysique A*, 4, 985, 6, 14 (cité d'après la traduction Tricot).

[5] CHOMSKY, N. et SCHÜTZENBERGER, M. P., « The algebraic theory of context-free languages », in *Computer programming and formal systems*, Braffort et Hirschberg (eds.), North-Holland, 1953. On trouvera une traduction française de cet article (par G. Fauconnier) in *Langages : Les modèles en linguistique*, Maurice Gross (ed.), Didier-Larousse, mars 1968.

[6] SCHÜTZENBERGER, M. P., « Sur l'équation $a^{2+n} = b^2 + {}^m c^{2+p}$ dans un groupe libre », *C.R.A.S.*, t. 248, 1959, pp. 2435-2436.

[7] LYNDON, R. C. et SCHÜTZENBERGER, M. P., « The equation $a^M = b^N c^P$ in a free group », *Michigan Math. J.*, vol. 9, 1962, pp. 289-298.

[8] LENTIN, A., « Sur l'équation $a^M = b^N c^P d^Q$ dans un monoïde libre », *C.R.A.S.*, t. 260, 1965, pp. 3242-3244.

[9] FONTET, M. et LENTIN, A., « Fixateurs et biinvodécompositions », *C.R.A.S.*, t. 270, pp. 848-850.

[10] JACQUES, A., LENORMAND, Cl., LENTIN, A. et PERROT, J.-F., « Un résultat extrémal en théorie des permutations », *C.R.A.S.*, t. 266, 1968, pp. 446-448.

[11] ORE, O., « Some remarks on commutators », *Proc. Amer. Math. Soc.*, 2, 1951, pp. 307-314.