Séminaire Dubreil.
Algèbre et théorie
des nombres

DOV TAMARI

Problèmes d ’associativité des monoïdes et problèmes des mots pour les groupes

Séminaire Dubreil. Algèbre et théorie des nombres, tome 16, nº 1 (1962-1963), exp. nº 7, p. 1-29
<http://www.numdam.org/item?id=SD_1962-1963__16_1_A7_0>

17 décembre 1962

PROBLÈMES D'ASSOCIATIVITÉ DES MONOÏDES ET PROBLÈMES DES MOTS POUR LES GROUPES

par Dov TAMARI

I. Introduction

1. Généralités.

L'associativité d'un système multiplicatif signifie l'indépendance de la valeur ou du sens d'un mot, dans la mesure qu'il y en a, de la distribution des parenthèses, qui sont " a priori" indispensables pour réduire son calcul à l'opération binaire interne donnée. La complexité du concept général de l'associativité d'un monoïde ou groupoïde partiel, c'est-à-dire d'une opération binaire partielle (= incomplète = non-partout définie), est bien cachée dans le cas dégénéré de la multiplication complète (= partout définie) usuelle. Donc, en passant au cas plus général de l'opération partielle, on est conduit à la formulation d'un problème de l'associativité tout à fait fondamental, qui s'avère comme étroitement lié au problème des mots pour les groupes, et, enfin, comme équivalent à ce problème dans un sens très précis, Il en résulte que le problème de l'associativité est insoluble, même pour les monoïdes finis, ces derniers correspondants aux groupes à présentation finie (c'est-à-dire ayant un nombre fini de générateurs et de relations-définitions). En bref, en admettant des "trous" dans les tables de multiplication-même finies-on a admis "le diable de l'insolubilité".

Dans le cas traditionnel de l'opération complète, la loi de l'associativité est usuellement exprimée par une simple identité inconditionnelle, notée

$$A_2 : \ x(yz) = (xy)z \ .$$

On démontre alors, essentiellement par réduction et transitivité de l'égalité, qu'on a aussi toutes les identités inconditionnelles

$$A_n(P , Q) : \ P(x_0 , \dots , x_n) = Q(x_0 , \dots , x_n) \ ,$$

où n est un nombre naturel > 2 , et $P = P^n$, $Q = Q^n$ dénotent deux paranthésages distincts, formellement corrects, quelconques d'un mot quelconque de longueur $n + 1$: $x_0 x_1 \dots x_n$. Le terme "inconditionnel" veut dire : "pour tous les x, y, et z, respectivement, pour tous les $x_0, \ldots, x_n$ appartenant au système multiplicatif considéré". Il est bien évident, que ceci n'a plus de sens dans le cas partiel, mais se laisse remédier, par exemple en ajoutant la condition "si les deux membres éxistent (= ont un sens) simultanément".

On peut l'exprimer

$A_n(P, Q)$: $P(x_0, \ldots, x_n) = s$, $Q(x_0, \ldots, x_n) = t \Longrightarrow s = t \quad (n \geqslant 2)$.

En admettant formellement aussi les cas $P = Q$, on peut inclure le cas $n = 1$ exprimant l'uniformité de l'opération :

$$A_1 : xy = s, \; xy = t \Longrightarrow s = t .$$

Alors on montre, par une induction facile que

$$A_1 \Longrightarrow A_n(P, P) \text{ pour tout } n > 1 \text{ et pour tout } P = P^n .$$

Il est plus grave que, pour $P \neq Q$, la démonstration de $A_2 \Longrightarrow A_n(P, Q)$ s'effondre. Il est encore vrai que $A_2 \Longrightarrow A_n(P, P')$, où P et P' se distinguent par le déplacement d'une seule paire de parenthèses. Mais si P et Q ne se dérivent pas l'une de l'autre par le déplacement d'une seule paire de parenthèses, A_2 n'implique $s = t$ que s'il existe (au moins) une chaîne de déplacements simples de longueur $\ell > 1$

$$P \to P' \to P'' \to \ldots \to P^{(i-1)'} = P^{(i)} \to P^{(i)'} = P^{(i+1)} \to \ldots \to P_\ell^{(\ell)} = Q$$

où tous les monômes intermédiaires $P', \ldots, P^{(\ell-1)}$ ont un sens simultanément avec P et Q. On fabrique facilement des exemples "ad hoc", montrant qu'autrement les lois A_n, $n > 2$, sont effectivement indépendantes de A_2. Etant donné qu'il y a $k_n = \binom{2n}{n-1}/n$ parenthésages distincts de n paires de parenthèses, il y a $\binom{k_n}{2} = \frac{1}{2} k_n(k_n - 1)$ lois associatives A_n dont quelques unes dépendent de A_2 et quelques unes de plus de l'ensemble de toutes les A_i, $i < n$; mais il y aura toujours un nombre croissant (croissant avec n) de lois effectivement indépendantes des A_i, $i < n$. C'est donc que la vérification directe de l'associativité, même d'un monoïde fini, devient, en général, une tâche infinie : Il ne suffit plus de regarder les triples d'éléments ; on doit aussi bien regarder les quadruples, les quintuples, etc. ad infinitum. Le théorème de l'insolubilité du problème de l'associativité pour la classe des monoïdes finis signifie qu'on ne peut trouver aucune procédure générale, qui fera de cette tâche une tâche finie.

2. Enoncé des résultats.

Toute une éducation élémentaire de calcul non-associatif est à refaire. Après avoir franchi ce cap de notions préliminaires, indispensables, de la théorie générale de monoïdes, on est conduit à aborder plusieurs théories d'immersion :

A) Celle de la complétion d'une opération partielle à une opération complète, toujours possible d'une infinité de manières, dont quelques unes banales ; c'est donc l'immersion des monoïdes dans des monades (= groupoïdes de Ore, = monoïde complet). En considérant des complétions assujetties à des conditions diverses intéressantes et des propriétés de structure de classes de telles complétions, cette théorie englobe un vaste domaine de problèmes.

B) Celle de la symétrisation des monoïdes, c'est-à-dire de la génération de monoïdes plus particuliers possédant certaines propriétés de symétrie involutive, en partant des monoïdes quelconques. On pose le problème relativement facile de la symétrisabilité d'un monoïde, c'est-à-dire de son immersibilité dans un monoïde symétrique. De cette théorie il nous faut retenir ici deux faits assez faciles à vérifier :

a. Les semi-groupes (= demi-groupes simplifiables), et plus généralement, les monades simplifiables, sont symétrisables.

b. La symétrisation d'un monoïde fini, donc aussi la vérification de sa symétrisabilité, sont des tâches finies, donc effectivement solubles (= décidables).

Ces théories préliminaires, comme aussi les résultats suivants, dépendent essentiellement du choix judicieux des concepts de base, en particulier ceux de sous-monoïde, d'inverse, de symétrie et d'associativité.

R. 1. - Le premier théorème fondamental est un théorème d'immersibilité, et, plus exactement, de complétion spéciale :

Pour qu'on puisse compléter un monoïde symétrique M_s jusqu'à un groupe, il faut et il suffit que M_s soit associatif : $I_G M_s \iff AM_s$.

(I_G = immersibilité dans un groupe, A = associativité).

Ce théorème est, en fait, fondamental : sa démonstration est basée sur quelques propositions très générales, les résultats 2-6 ne sont que des corollaires plus ou moins immédiats. Les corollaires 2-4 concernent l'immersion de semi-groupes dans des groupes.

R. 2. - Un semi-groupe est immersible dans un groupe, si et seulement si sa symétrisation est associative.

R. 3. - L'existence de semi-groupes non-immersibles dans des groupes est équivalente à l'existence de symétrisations non-associatives de monoïdes associatifs.

R. 4. - L'explicitation de l'associativité - et de ces généralisations plus étendues encore remplaçant l'égalité par un préordre - donne le système infini des conditions de Malcev, et de leurs généralisations pour le préordre.

Supposons désormais le monoïde symétrique fini.

R. 5. - La solubilité du problème de l'associativité pour les monoïdes symétriques finis M_{sf} entraîne la solubilité du problème de trivialité (= T) pour les groupes $G(M_s)$ engendrés par des monoïdes symétriques finis :
$\text{Sol. } AM_{sf} \implies \text{Sol. } TG(M_{sf})$.

R. 6. - La solubilité du problème des mots pour les groupes $G(M_{sf})$ entraîne la solubilité du problème de l'immersibilité des M_{sf} dans $G(M_{sf})$, donc, en vertu du premier théorème fondamental, de l'associativité de M_{sf} :

$$\text{Sol. mots } G(M_{sf}) \implies \text{Sol. } I_G\, M_{sf} \iff \text{Sol. } AM_{sf}\ .$$

On appelle <u>présentation</u> Π (d'un système multiplicatif), en particulier d'un semi-groupe ou d'un groupe, la donnée d'un ensemble de générateurs Γ et d'un ensemble de relations-définitions R, $\Pi = (\Gamma, R)$, satisfaisant éventuellement à des conditions particulières plus ou moins explicitement indiquées. Π est une présentation finie, si les deux ensembles Γ et R sont finis. On se limite aux <u>groupes à présentation finie</u>, c'est-à-dire à la classe des groupes possédant une présentation-de-groupe finie. L'établissement de correspondances canoniques entre monoïdes symétriques et présentations-de-groupes conduit à la méthode de la présentation-standard monoïdale et au résultat fondamental :

R. 7. - <u>La classe</u> $\mathcal{C}G(M_f)$ <u>des groupes engendrés par des monoïdes finis</u> M_f, <u>identique à la classe</u> $\mathcal{C}G(M_{sf})$ <u>des groupes engendrés par des monoïdes symétriques finis, est identique à la classe</u> $\mathcal{C}G(\Pi_f)$ <u>des groupes à présentation finie</u> :

$$\mathcal{C}G(M_f) = \mathcal{C}G(M_{sf}) = \mathcal{C}G(\Pi_f)\ .$$

Le résultat bien connu [1], [20] que le problème $TG(\Pi_f)$ est insoluble, conduit au corollaire immédiat de 5 et de 7 :

R. 8. - Le problème de l'associativité des monoïdes symétriques finis est insoluble.

Ceci implique immédiatement l'énoncé plus faible :

R. 9. - L'insolubilité du problème de l'associativité des monoïdes finis.

Utilisant le fait qu'on a aussi $TG(\Pi_f) \iff$ mots $G(\Pi_f)$, on est conduit à :

R. 10. - Le problème de l'associativité des monoïdes symétriques finis est équivalent au problème des mots pour les groupes à présentation finie (donc, insoluble).

Utilisant le fait qu'il y a des groupes particuliers (individuels) avec problème des mots insoluble, on peut même "localiser" l'insolubilité du problème de l'associativité à une sous-classe de monoïdes symétriques finis, déterminée par une présentation standardisée d'un tel groupe.

3. Connexions avec d'autres travaux.

On voit donc à la base de plusieurs problèmes fondamentaux et presque classiques de la théorie des semi-groupes et des groupes, des systèmes finis qui ne sont pas multiplicativement clos - à savoir les monoïdes finis. Ces problèmes assez difficiles se comprennent donc mieux, quand on les considère comme des problèmes d'associativité de ces monoïdes sous-jacents, qui, au fond, ne sont qu'une version standardisée des présentations. Cette standardisation diminue le caractère évasif, protéïque, des présentations. Le fait qu'une présentation peut être un monoïde associatif ou non-associatif peut servir à une systématisation du calcul des groupes jusqu'à la programmation sur des machines calculatrices. Ces calculs aboutiront seulement dans les cas solubles.

L'auteur croit qu'une démonstration directe pour l'insolubilité du problème de l'associativité des monoïdes finis, ou même des monoïdes symétriques finis, employant directement le procédé diagonal de Cantor, est faisable : on construit facilement des représentations uniques des monoïdes symétriques finis associatifs par des suites infinies en un nombre fini, fixé, de symboles, ressemblant par exemple aux développements décimaux des nombres réels. On devait donc arriver à une contradiction, en supposant une énumération de ces monoïdes-suites $M_1, M_2, \dots, M_n, \dots$ et en construisant effectivement de cette suite de suites une suite diagonale M_0 représentant aussi un monoïde symétrique fini associatif distinct de tous les M_i $(i \geqslant 1)$ de la suite. La difficulté est dans la caractérisation de ces suites pour qu'elles représentent seulement de tels monoïdes. Malheureusement, nous n'avons pas réussi à trouver une telle démonstration directe. Une démonstration directe de l'insolubilité de notre problème de l'associativité donnera immédiatement une démonstration plus significative pour l'insolubilité du problème des mots pour les groupes.

A part des liaisons évidentes avec les points de vue d'autres auteurs, dont la bibliographie rend partiellement compte [2], [3], [10], [17], ce travail repose principalement sur les travaux antérieurs de l'auteur. A un point essentiel de la démonstration du premier théorème fondamental, on fait usage d'une idée dont le principe abstrait est déjà indiqué chez NEWMAN [17], mais qui, en fait remonte au beau travail de LAMBEK [12], où elle apparaît sous une forme explicite et dans un contexte proche, mais très spécial.

Les résultats 2 et 4 ont déjà été anticipés, d'une manière plus vague, par l'auteur en 1949 [20]. En 1951, après sa thèse [21] et après la publication de [12], l'auteur a proposé à LAMBEK un travail commun, pour mettre en évidence le rôle prépondérant joué par l'associativité générale. Malheureusement, par suite de circonstances extérieures, ce travail n'a jamais été écrit. Le travail récent de BUSH [7], bien qu'essentiellement indépendant, répond partiellement à ce sujet.

Le principe de représentation-standard monoïdal des systèmes binaires, réduisant des relations-définitions de longueur quelconque à un nombre fini de relations de la forme $ab = c$, ou $ab = 1c = c1$, etc., est déjà appliqué dans la thèse [21] (voir aussi la remarque p.268 du livre de DUBREIL [9]).

Les travaux [8], [11], [24] traitent d'autres aspects des problèmes d'associativité et de symétrisation, à l'aide aussi des relations binaires ou des notions de treillis. Un travail dédié plus particulièrement à la symétrisation et les "inverses en puissance" reste encore à écrire.

En 1960, la formulation exacte et une preuve du premier théorème fondamental [23] permettaient une conclusion satisfaisante de ce travail en augmentant son envergure par les résultats 3 et 5-10. Depuis il a fait le sujet de nombreuses conférences aux Etats-Unis et ailleurs. Sous ces réserves l'auteur peut affirmer que cette conférence est, en fait, une continuation de ses conférences données dans ce même séminaire pendant l'année 1950/51.

Remarque. - Plusieurs fois on m'a dit "vous auriez avantage à vous servir du langage des catégories qui se prête particulièrement bien à votre sujet". Ces remarques venant de mathématiciens éminents à diverses occasions, aucun doute, qu'il en soit ainsi, n'est possible. Toutefois, il s'avère que la traduction en langage de catégories ne facilite la compréhension que pour ceux qui connaissent bien ce langage, mais qu'il n'apporte pas d'aide appréciable à la solution des problèmes eux-mêmes. J'ai donc préféré, au moins pour le moment, m'en tenir à un langage manquant du modernisme prestigieux, mais facilitant encore la compréhension à la grande majorité des mathématiciens. Seulement, une application plus approfondie de ce nouvel instrument, qu'est ce langage, apportera à notre sujet des lumières nouvelles, comme il l'a déjà fait dans d'autres domaines (par exemple, pour la géométrie algébrique). C'est sur trois plans de ce travail, que cet apport sera le plus appréciable : 1) les "collections", en particulier les treillis de complétions (théorie préliminaire A) ; 2) les collections ou treillis de symétrisations diverses (théorie préliminaire B);3) les rapports canoniques, triangulaires ou plus, entre présentations, présentations-standard monoïdales et les demi-groupes et groupes engendrés par elles, qui constituent une théorie assez centrale (en connexion avec les résultats 7-10 et plus). Nous nous sommes donc limités sur ces sujets à des mentions nécessaires et renvoyons le lecteur, pour l'édification détaillée, à des exposés futurs.

On expose ici des théories préliminaires, on démontre le théorème fondamental et on donne quelques indications sur les autres démonstrations dans l'espoir que le lecteur gagnera une vue d'ensemble de cette théorie.

II. Théories préliminaires.

Définitions. - On appelle monoïde (= groupoïde partiel, halfgroupoid) $M = (|M| , O_M)$ un ensemble (ou une classe) non-vide $|M|$ muni d'une opération intérieure, binaire, partielle (= incomplète ou non-partout définie) O_M, application d'une partie P_M de $|M| \times |M|$ dans $|M|$: si $a , b \in |M|$, ou bien il existe un seul $c \in |M|$ tel que $O_M : (a , b) \to c$, ce qu'on écrit aussi " $(ab) = c$ dans M ", et, alors, on dit que (ab) existe, $\exists\ (ab)$; ou bien $(a , b) \notin P_M$, (ab) n'existe pas dans M, $\nexists\ (ab)$. Le plus souvent on se permettra d'écrire M au lieu de $|M|$ et ab au lieu de (ab). Si $ab = c$, on dit aussi " ab se contracte en c ", "se réduit à c ", " ab a le sens c ", etc. ; et aussi bien " c se factorise, ou se décompose en facteurs a et b ", etc.

Un monoïde revient donc essentiellement à la donnée d'une table de multiplication incomplète, c'est-à-dire admettant des "trous" ; ou, aussi bien, à la donnée d'une relation ternaire particulière O_M telle que

$$\text{" } ab = c \text{ dans } M \text{ "} \iff \text{"}(a , b , c) \in O_M\text{"} ,$$

le couple des facteurs a et b déterminant uniquement la troisième composante, le "produit" c . Si M n'admet pas d'éléments complètement isolés, c'est-à-dire qui ne sont dans M ni facteurs, ni produit, M est complètement déterminé par O_M ; M est le champ de O_M . Comme on le verra, nous avons jugé utile d'admettre des éléments complètement isolés, jusqu'à l'admission de monoïdes avec tableau de multiplication vide $O_M = \emptyset$, correspondant aux ensembles abstraits. Par contre, on appelle monade (= groupoïde de Ore ou "épi-monoïde") un monoïde à multiplication complète : $P_M = M \times M$.

Le cas plus général d'une relation ternaire quelconque O_M s'identifie avec l'hyper-monoïde $(|M| , O_M)$, c'est-à-dire d'un ensemble muni d'une opération binaire multiforme. Au contraire, dans un monoïde simplifiable (ou de cancellation) un couple quelconque de a , b , c détermine uniquement le triple.

On note $\overline{M}$ l'opposé ou l'anti-isomorphe de M , $\overline{a}$, $\overline{b}$, ... ses éléments correspondants à a , b , ... de M :

$$\text{" } ab = c \text{ dans } M \text{ "} \iff \text{" } \overline{b}\overline{a} = \overline{c} \text{ dans } \overline{M} \text{ "} ;$$

donc aussi, en particulier, " $\exists$ ab dans M " $\iff$ " $\exists$ $\overline{b}\overline{a}$ dans $\overline{M}$ " . M est l'opposé de $\overline{M}$: $\overline{\overline{M}} = M$, et même $\overline{\overline{a}} = a$, par l'application 1 - 1 : $a \to \overline{a}$ et son inverse $\overline{a} \to a$.

Nos définitions impliquent que

$$\exists \; ab \implies (\exists \; c)(ab = c) , \qquad ab = c \implies \exists \; ab$$

$$\exists \; (ab)c \implies \exists \; ab , \qquad \exists \; a(bc) \implies \exists \; bc \quad ; \text{etc.}$$

Multiplication de complexes (= sous-ensembles de M) $A , B , C \subset M$:

$$AB = C \iff C = \{c | (\exists \; a \in A , \; \exists \; b \in B)(ab = c)\} .$$

Un monoïde N est un <u>sous-monoïde</u> de M, $N \subset M$, si $|N| \subset |M|$ et si " ab = c dans N " $\implies$ " ab = c dans M " ; autrement dit si $O_N \subset O_M$. On a une notion plus restreinte de sous-monoïde, le <u>sous-monoïde de trace</u>, si $O_N = O_M \cap |N|^3$, où $|N|^3 = |N| \times |N| \times |N|$; autrement dit, un sous-monoïde N de M est un sous-monoïde de trace de M , si

$$\text{" } (ab = c \text{ dans } M) \;\&\; (a , b , c \in N) \text{ "} \implies \text{" } ab = c \text{ dans } N \text{ "} .$$

On aura la notion encore plus restreinte du <u>sous-monoïde stable</u>, si $O_N = O_M \cap (|N|^2 \times |M|)$, c'est-à-dire si $NN \subset N$; autrement dit, si N satisfait encore

$$\text{" } ab = c \text{ dans } M \,\&\, a\,,\, b \in N \text{ "} \Longrightarrow \text{" } ab = c \text{ dans } N \text{ "} \quad .$$

Un sous-monoïde stable est un sous-monoïde de trace qui est un sous monoïde tout court. La définition du sous-monoïde est si faible, que le sous-ensemble $|N|$ ne détermine pas le sous-monoïde, mais seulement le sous-monoïde de trace ; les sous-monoïdes avec le même support $|N|$ sont des sous-monoïdes de ce sous-monoïde de trace. La notion de sous-monoïde stable est si forte qu'il n'y a pas, en général, un tel sous-monoïde pour un sous-ensemble arbitraire $|N|$, et un monoïde peut être simple dans ce sens qu'il ne possède aucun sous-monoïde stable sauf lui-même. Mais les sous-monades de monoïdes sont des sous-monoïdes stables. Les éléments idempotents sont des sous-monades réduites à un seul élément. C'est la notion du sous-monoïde (faible) qui nous sera la plus utile.

La notion de sous-monoïde une fois fixée, elle détermine d'une manière évidente les notions correspondantes d'extension ou d'immersion, et, en particulier, de complétion = immersion dans une monade. Les notions moins évidentes de génération, de génération libre, etc. sont aussi entendues dans la suite, éventuellemant avec les éclaircissements du contexte. Une référence générale sur ce sujet - la seule à ma connaissance - est le chapitre I de BRUCK [6].

A. Théorie de complétion.

Chaque monoïde M , qui n'est pas une monade, peut être complété de manières diverses, par exemple en mettant sur les "trous" n'importe quels éléments de M . Mais il y a d'autre complétions plus intéressantes ; ainsi on peut rechercher s'il y a des complétions qui sont des groupes. On peut aussi considérer la structure de certaines classes de complétions ou de la classe de toutes les complétions engendrées par un monoïde donné.

La complétion universelle. - Chaque monoïde M , qui n'est pas une monade, engendre librement sa complétion universelle $\mathcal{U}_M$, qui est toujours infinie et effectivement non-associative. Toutes les autres complétions, engendrées par M sont des images homomorphes de $\mathcal{U}_M$.

Construction de $\mathcal{U}_M$. - On note $M = M_1$, et T_1 l'ensemble de ses trous (donc $T_1 = (|M| \times |M|) \setminus P_M$). On note $M_2 = M_1 \cup T_1$, et on construit la table de multiplication de M_2 en ajoutant un ensemble de nouveaux trous "d'ordre 2 " T_2 ; on pose $M_3 = M_2 \cup T_2$, etc. ad infinitum. M_2 est un monoïde contenant $M = M_1$ comme sous-monoïde, avec $M_1 M_1 = M_2$ dans M_2 . Tout en bouchant les trous de M_n par l'adjonction de l'ensemble d'éléments nouveaux T_n , l'ensemble de ses trous antérieurs, et en posant $M_{n+1} = M_n \cup T_n$, on crée toujours plus de trous nouveaux

$$T_{n+1} = (|T_n| \times |M_n|) \cup (|M_n| \times |T_n|) \cup (|T_n| \times |T_n|) \;;$$

mais en passant à la limite

$$M_\infty = \lim_{n\to\infty} M_n = \bigcup_n M_n = \mathcal{U}_M$$

on a bouché (paradoxalement) tous les trous : on obtient une monade, tous les trous ont disparu. En effet, quels que soient u, $v \in \mathcal{U}_M$, il existe des nombres naturels m, n tels que $u \in M_m$, $v \in M_n$, donc les deux $\in M_\ell$ ($\ell \geqslant m, n$). Ou bien $\exists$ uv dans M_ℓ ou bien $\nexists$ uv dans M_ℓ ; dans ce dernier cas $uv \in T_\ell$ et donc $uv \in M_{\ell+1}$. Donc dans les deux cas $uv \in \mathcal{U}_M$.

Un mot de M, de longueur $\ell = d + 1$, est une suite finie d'éléments de M $s = a_0\, a_1 \ldots a_d$ ($d = 0, 1, \ldots$; $d = -1$ peut servir pour le mot vide). Un tel mot, pourvu d'un ensemble formellement correct de d paires de parenthèses (en fait on écrit souvent seulement $d - 1$ paires et on supprime la paire extérieure), exprimant une itération de proche en proche de l'opération binaire, est un monôme formel de dimension (dim) d (ou de degré $d + 1$), indiqué par

$$A = A^d = A^d(s) = A^d(a_0, \ldots, a_d) \quad \text{ou} \quad ((a_0, \ldots, a_d)) \quad \text{seul.}$$

Pour chaque mot il y en a $\binom{2d}{d+1}/d = \binom{2d}{d}/(d+1)$ monômes formels, c'est-à-dire arrangements distincts de parenthèses. En remplaçant les éléments d'un monoïde par des symboles abstraits quelconques, distincts ou non, qu'on peut appeler variables ou indéterminés x_0, x_1, $\ldots$, x_d, on obtient des formes monômiales. En faisant encore abstraction d'éléments et d'indéterminés, on obtient le système $\mathcal{P}$ des parenthésages binaires ou patrons monômiaux. Comme le système des nombres naturels N, l'ensemble des patrons monômiaux $\mathcal{P}$ doit être regardé comme une structure catégorique (= unique) assez fondamentale et fort intéressante, bien que moins importante que celle de N à laquelle $\mathcal{P}$ se laisse réduire avec quelque peine [21], [11], [25].

Dans $\mathcal{P}$ sont définies plusieurs opérations canoniques. Ici nous traitons seulement de la composition naturelle "$\circ$" des patrons monômiaux par juxtaposition dans une nouvelle paire de parenthèses :

$$A^d \circ B^e \equiv (A^d\, B^e) = C^{d+e+1} \;,$$

c'est-à-dire

$$A^d(a_0, \ldots, a_d) \circ B^e(b_0, \ldots, b_e) = C^f(c_0, \ldots, c_f) \;,$$

où $c_0 = a_0, \ldots, c_d = a_d$, $c_{d+1} = b_0, \ldots, c_f = b_e$, $f = d + e + 1$. On obtient tous les patrons monômiaux par cette composition en partant du seul patron monomial de dim 0 : $A^0 = a_0$, donc $A^1 = A^0 \circ B^0 = (a_0\, a_1)$,

$A^2 = A^1 \circ B^0 = ((a_0\, a_1)\, a_2)$, $C^2 = A^0 \circ B^1 = (a_0(a_1\, a_2))$, etc., avec des changements de notation évidents pour l'indication des "places vides". On peut identifier ce système avec la monade non-associative libre engendrée par un seul générateur, comme on peut identifier le système des nombres naturels avec le semi-groupe cyclique = monade associative libre à un générateur.

En introduisant dans les places vides des patrons monômiaux des éléments d'un monoïde M , on obtient la monade des monômes formels sur M , qu'on peut identifier, d'une manière évidente, avec $\mathcal{U}_{|M|}$, la complétion universelle (ou libre) du monoïde $|M|$ (l'ensemble abstrait à table de multiplication vide) ; ou aussi bien, avec la <u>monade libre</u> engendrée par l'ensemble de générateurs libres $|M|$.

En $\mathcal{U}_{|M|}$ aussi "l'inverse" de la composition, la <u>décomposition</u> ou <u>factorisation directe</u> (= binaire) est une opération bien définie, faisant correspondre à chaque monôme de $\dim \geqslant 1$ un et un seul couple ordonné de monômes formels :

$$\mathcal{U}_{|M|} \setminus |M| = \mathcal{U}_{|M|}^{(1)} \to \mathcal{U}_{|M|} \times \mathcal{U}_{|M|} \ ;$$

autrement dit, chaque C^f , $f \geqslant 1$, détermine uniquement un A^d et un B^e avec $0 \leqslant d\ ,\ e \leqslant d + e + 1 = f$ tels que $A^d \circ B^e = C^f$.

On définit une relation d'équivalence $\mathcal{E}_M$ entre monômes formels de M , c'est-à-dire dans $\mathcal{U}_{|M|}$ par $A^d \sim B^e$ $(\mathcal{E}_M)$ s'il existe une chaîne (finie) d'expansions (= factorisations) et contractions (= multiplications) élémentaires, suivant la table de multiplication et respectant les parenthèses, transformant A^d en B^e . Plus explicitement :

$$A^d = A_0^{d_0}\ ,\ A_1^{d_1}\ ,\ \dots\ ,\ A_i^{d_i}\ ,\ A_{i+1}^{d_{i+1}}\ ,\ \dots\ ,\ A_n^{d_n} = B^e\ ,$$

où $d_{i+1} = d_i \pm 1$ et $A_{i+1}^{d_{i+1}}$ est obtenu de $A_i^{d_i}(c_0\ ,\ \dots\ ,\ c_k\ ,\ \dots\ ,\ c_{d_i})$ par un des deux types de transformations élémentaires suivantes :

a. Expansion élémentaire $c_k \to c_k'\, c_{k+1}'$ toujours possible, pourvu que dans M $c_k = c_k'\, c_{k+1}'$:

$$\begin{aligned} A_i^{d_i}(c_0\ ,\ \dots\ ,\ c_k\ ,\ \dots\ ,\ c_{d_i}) \to A_i^{d_i}&(c_0\ ,\ \dots\ ,\ c_k'\, c_{k+1}'\ ,\ \dots\ ,\ c_{d_i}) \\ &= A_i'^{\,d_i+1}(c_0\ ,\ \dots\ ,\ c_{k-1}\ ,\ c_k'\ ,\ c_{k+1}'\ ,\ \dots) \\ &= A_{i+1}^{d_{i+1}}(c_0'\ ,\ \dots\ ,\ c_k'\ ,\ c_{k+1}'\ ,\ \dots\ ,\ c_{d_{i+1}}') \end{aligned}$$

où $c'_j = c_j \quad (j < k)$, $c'_k\, c'_{k+1} = c_k$, $c'_{j+1} = c_j \quad (j > k)$, $d_{i+1} = d_i + 1$.

b. Contraction élémentaire $c_k\, c_{k+1} \to c'_k$, possible si et seulement si $c_k\, c_{k+1}$ sont deux composantes formellement composées dans le monôme $A_i^{d_i}$, c'est-à-dire non séparées par des parenthèses, et effectivement composables dans M suivant son tableau de multiplication :

$$A_i^{d_i}(\dots , c_{k-1} , c_k , c_{k+1} , \dots) \equiv A_i'^{\,d_i-1}(\dots , c_{k-1} , c_k\, c_{k+1} , c_{k+2} , \dots)$$

$$\to A_{i+1}^{d_i-1}(\dots , c_{k-1} , c'_k , \dots) = A_{i+1}^{d_{i+1}}(c'_0 , \dots , c'_k , \dots)$$

où $c'_j = c_j \quad (j < k)$, $c'_k = c_k\, c_{k+1}$, $c'_j = c_{j+1} \quad (j > k)$.

$\mathcal{E}_M$ est évidemment une <u>congruence</u> (= équivalence régulière), c'est-à-dire compatible avec la composition naturelle "$\circ$" dans $\mathcal{U}_{|M|}$, définissant ainsi une <u>monade quotient</u> ou image homomorphe de $\mathcal{U}_{|M|}$: $\mathcal{U}_M \cong \mathcal{U}_{|M|}/\mathcal{E}_M$.

Une autre manière de représenter $\mathcal{U}_M$ fidèlement est donnée par le système $\mathcal{R}$ des monoïdes formels <u>réduits</u>. Un monôme formel de M est dit réduit, s'il ne permet aucune réduction par contraction élémentaire ; en particulier, les monômes de dim 0 sont trivialement réduits. On voit facilement que chaque classe mod $\mathcal{E}_M$ de monômes formels possède un seul représentant réduit. $\mathcal{R}$ est donc un système de représentants distingués. La composition de deux monômes réduits R_1 et R_2 , est, en général, de nouveau un monôme réduit $R_1 \circ R_2 = (R_1\, R_2) = R_3$, sauf le cas particulier, où R_1 et R_2 sont les deux réduits à des éléments composables de M , dans lequel leur produit est le produit ordinaire dans M . $\mathcal{R}$, muni de cette opération induite $(\mathcal{R} , \times)$: $R_1 \times R_2 = R_1 \circ R_2 \equiv (R_1\, R_2)$ si $\dim R_1 + \dim R_2 > 0$, $a \times b = c$ si $ab = c$ dans M , $\dim R_1 = \dim R_2 = 0$ $(R_1 = a , \; R_2 = b)$, satisfait aussi à $\mathcal{U}_M \cong (\mathcal{R} , \times)$.

C'est essentiellement cette représentation de la complétion universelle de M qui a été décrite au commencement de cette section. Si l'on veut décrire d'une manière semblable, par dessin schématique, la représentation de $\mathcal{U}_M$ par $\mathcal{U}_{|M|}/\mathcal{E}_M$, on peut partir de $|M|$ au lieu de M ; c'est-à-dire on pose $T_1 = |M| \times |M|$. On engendre les classes d'équivalence d'une manière évidente, en posant :

$$(x_0 , y_0) = (a , b) \sim c = z_0$$

si dans M : $ab = c$, $(a , b) \in T_1$; $a , b , c \in M = T_0$;

$$(x_1 , y_1) \sim z_1 = (x_0 , y_0)$$

si $x_1 \sim x_0 \vee y_1 \sim y_0$, $(x_1 , y_1) \in T_2$; $x_1 , y_1 , z_1 \in T_1$; etc. ; généralement

$$z_{n+1} = (x_n , y_n) \sim z_n = (x_{n-1} , y_{n-1})$$

si $x_n \sim x_{n-1} \vee y_n \sim y_{n-1}$ et $x_n , y_n , z_n \in T_n$, $z_{n+1} \in T_{n+1}$.

Les collections de structures quelconques sont toujours munies d'un préordre naturel induit par la relation d'homomorphisme appropriée $M_2 \lesssim M_1 \iff M_2$ image homorphe de M_1 . Quand il s'agit de collections de complétions $\mathcal{C}_M$ d'un monoïde M, on se limite, naturellement, aux homomorphismes dont la restriction sur M est l'identité ; c'est-à-dire, qui sont des partitions de $\mathcal{U}_M$ telles, qu'elles séparent les éléments de M , sont compatibles avec la composition, et ont, évidemment $\mathcal{U}_M$ comme l'élément le plus grand. Alors la collection $\mathcal{C}_M$ est un sup-demi-treillis complet.

En variant des conditions diverses, on obtient d'autres treillis de complétions. Pour une théorie plus détaillée poursuivant ces points de vue, nous devons renvoyer à des exposés futurs.

B. Théorie de symétrisation.

On se limite dans ce paragraphe à quelques indications sur une théorie des éléments-unités, des éléments inverses et de la symétrisation. Un exposé plus approfondi est envisagé pour plus tard.

1. a est un inverse local de b (à gauche ou à droite, par rapport à c) dans M , si

$$(\exists\ c)[a(bc) = c \vee (cb)\ a = c]\ .$$

2. Un inverse local a de b est un inverse général (faible) de b , s'il est unique et tel que

$$(x)\{[\exists\ a(bx) \implies a(bx) = x]\ \&\ [\exists\ (xb)a \implies (xb)\ a = x]\}\ .$$

3. Un inverse local a de b est un inverse fort (ou un inverse tout court) de b si

$$(x)\{[\exists\ bx \implies a(bx) = x]\ \&\ [\exists\ xb \implies (xb)\ a = x]\}\ .$$

En langage de "multiplications" (= translations) un inverse (fort) a de b est un élément a tel que le couple de ses multiplications, la gauche et la droite, est justement le couple des opérations inverses à celles de b . Donc un élément b ne peut posséder un inverse que si ses multiplications sont biunivoques ; autrement dit, b doit être un élément régulier. Il s'ensuit qu'un inverse fort est unique et aussi un inverse général (faible) ; donc on l'appelle "a fortiori" un inverse général. Un inverse local, qui n'est pas général, est dit inverse proprement local.

Cette liste est loin d'être exhaustive ; en fait, la théorie générale de symétrisation et de symétrisabilité a besoin d'inverses généralisés qui ne sont des inverses qu'en "puissance", c'est-à-dire peuvent devenir des inverses dans certaines extensions du monoïde donné. Leur définition est trop technique pour être donnée ici, et, à la rigueur, on peut se passer d'elle.

On note $\underset{\sim}{1}$ l'élément d'identité composable avec tous les éléments de M : $\underset{\sim}{1}m = m\underset{\sim}{1} = m$; son couple de multiplications consiste donc en l'application identique de M à gauche et à droite. Si $\underset{\sim}{1} \in M$, M est dit unitaire. On peut aussi bien définir des unités locales, des unités faibles, etc. Pour simplifier, on supposera désormais tous les monoïdes unitaires. Dans ce cas aucun élément n'est isolé, et un monoïde de cancellation ne contient aucune unité $\neq \underset{\sim}{1}$.

Un monoïde unitaire est dit symétrique M_s, si chaque élément possède un inverse. Un M_s est simplifiable, l'inverse est unique et l'application $m \to m'$, où m' dénote l'inverse de m, est un anti-automorphisme involutif de M_s, ayant au moins un point fixe $\underset{\sim}{1}$ (et éventuellement d'autres d'ordre 2). Un M_s complet (monade symétrique) est une boucle avec la propriété inverse "I. P.-loop". Le M_s trivial (= réduit à un seul élément) est le M_s d'identité, qui est le groupe d'identité.

Un monoïde symétrique peut aussi être défini comme un monoïde unitaire qui est son propre opposé (= auto-dual : possédant une application intérieure $m \to m'$ qui est un anti-automorphisme involutif avec $\underset{\sim}{1}$ point fixe).

Chaque monoïde M engendre des monoïdes symétriques, et, un en particulier, qui est dit sa symétrisation $S(M) = (S(M), \circ)$. $S(M)$ est le monoïde symétrique "le plus petit" entre tous les M_s engendrés par M dans ce sens, qu'il n'impose qu'un minimum de relations d'existence et d'équivalence à son ensemble de générateurs ; on l'exprime mieux en disant que $S(M)$ est le monoïde symétrique engendré librement par M. L'ensemble de générateurs de $S(M)$ est $X_M = |M| \cup \{\underset{\sim}{1}\} \cup |\overline{M}|$, où $\overline{M}$ est l'opposé de M. Il est en même temps l'ensemble de tous les noms (= symbols représentants) d'éléments de $S(M)$. C'est donc que tous les "mots" sont de longueur $\underset{\sim}{1}$ seulement. Ils sont soumis aux règles de la multiplication "." ("relations-définitions de $(S(M), .)$:

$$a.b = c \iff ab = c \iff \overline{ba} = \overline{c} \ ; \qquad a \in M \iff \overline{a} \in \overline{M}$$

$$a.\overline{a} = \overline{a}.a = \underset{\sim}{1} \ ; \qquad x.\underset{\sim}{1} = \underset{\sim}{1}.x = x \ ; \qquad x \in X_M$$

$$a.\overline{b} = \begin{cases} a_1 \iff a = a_1 b \\ \overline{b}_1 \iff b = b_1 a \ ; \\ \nexists \ \text{autrement} \end{cases} \qquad \overline{a}.b = \begin{cases} \overline{a}_1 \iff a = ba_1 \\ b_1 \iff b = ab_1 \\ \nexists \ \text{autrement.} \end{cases}$$

Malgré notre convention concernant l'unitarité de M nous avons mentionné $\underset{\sim}{1}$ explicitement en X_M et dans les règles pour plus de clarté. D'une manière plus pédante on aurait pu, ou dû, écrire ces règles comme des équivalences "$\sim$" , au lieu d'égalités "=" , dans l'ensemble X_M , les éléments de $S(M)$ étant les classes d'équivalence modulo la congruence (= équivalence régulière) $\mathcal{E}_{sM}$ ainsi engendrée dans X_M : $S(M) = X_M/\mathcal{E}_{sM}$. Si l'on veut dériver la multiplication "." de $S(M)$ comme induite d'une multiplication dans l'ensemble X_M , c'est-à-dire si on veut poser

$$S(M) = (S(M) \ , \ .) = X_M/\mathcal{E}_{sM} \ ,$$

on doit admettre la multiformité éventuelle de cette multiplication en X_M . Bien qu'à l'encontre d'habitudes enracinées, aucune difficulté particulière n'est créée. On peut l'éviter en parlant plutôt d'une relation ternaire sur X_M au lieu d'une opération binaire, sans rien changer au fond.

L'interprétation correcte des règles "$\nexists$ autrement" signifie : "Autrement l'existence du produit des classes d'équivalence correspondantes n'est pas assurée par ce couple de représentants". La génération libre signifie, ici, que seuls existent les produits dont l'existence est imposée. Mais l'existence du produit pourrait être imposée par un autre couple de représentants ; l'existence d'un tel couple composable suffit. Il est évident, que de cette manière $S(M) = (S(M) \ , \ .)$ devient un monoïde symétrique. La construction formelle de $S(M)$ avec plus de détails explicites est remise à plus tard dans un autre travail ; quelques remarques seulement suffiront ici :

Dans les cas extrêmes $S(M)$ peut être réduit à l'identité :

$$\text{card } S(M) = 1 \ .$$

En général, pour card $M < \infty$ ou infini,

$$1 \leqslant \text{card } S(M) \leqslant 2 \text{ card } M + 1 \ ,$$

ou plutôt, parce que M est unitaire et $\underset{\sim}{1} = \underset{\sim}{\overline{1}}$,

$$1 \leqslant \text{card } S(M) \leqslant 2 \text{ card } M - 1 \ .$$

Si $S(M)$ est une immersion de M, c'est-à-dire M est <u>immersible</u> dans $S(M)$, ou autrement dit, si l'application canonique de M dans $S(M)$ est une injection, M est dit <u>symétrisable</u>. Dans ce cas on peut écrire avec un abus léger de langage $S(M) = M \cup \overline{M}$, où, naturellement, l'union n'est pas nécessairement directe :

$$\text{card } M \leqslant \text{card } S(M) \leqslant 2 \text{ card } M - 1 \;;\quad \text{card } S(M) - \text{card } M = \text{card } (M \cap \overline{M}) \;;$$

$\text{card } M = \text{card } S(M) = \text{card } (M \cap \overline{M})$ n'entraîne pas nécessairement $M = S(M)$: on peut avoir $|M| = |S(M)|$, mais $0_M \subsetneqq 0_{S(M)}$. Pour un M symétrisable la restriction de $\mathcal{E}_{sM}$ sur M est l'égalité ; c'est donc qu'une classe d'équivalence sur X_M modulo $\mathcal{E}_{sM}$ consiste au plus de deux éléments, l'un $\in M$ et l'autre $\in \overline{M}$. Si M est déjà symétrique $M = M_s$, alors $M = S(M)$. En relachant plus ou moins les règles de non-existence, on obtient d'autres symétrisations, jusqu'à la symétrisation complète, qui est une boucle I. P. Sa symétrie est compatible avec la symétrie naturelle de l'ensemble des monômes formels induite par la dualité naturelle des parenthésages : celle-ci correspond aussi bien à la dualité naturelle de l'opération opposée (anti-isomorphe) ou, plus simplement encore, à la dualité entre ouvertures et fermetures de parenthèses. Les résultats obtenus pour une symétrisation sans faire usage exprès des règles d'existence et de non-existence sont valables pour une symétrisation quelconque, donc pour toutes les symétrisations.

Il y a pourtant quelques questions fondamentales concernant les symétrisations dont les réponses nous sont indispensables : La construction de $S(M)$, pour un M donné, est-elle effective ? La réponse est positive, et pour le cas de M fini la construction aboutit toujours après un nombre fini de pas majorable d'avance. Numériquement, cette estimation dépend de conventions assez arbitraires. On sait donc, que la construction de $S(M)$ est relativement triviale et ne peut poser aucun problème insoluble.

On le voit rapidement par la description intuitive de la construction de $S(M)$, pour M quelconque, par "tableaux de multiplication". La formalisation évidente est un peu onéreuse. Une construction semblable est déjà décrite en détail, en particulier pour M un semi-groupe, dans ma thèse [21].

Le tableau obtenu représente un monoïde symétrique si et seulement s'il satisfait aux exigences de l'uniformité et de la simplifiabilité, devenues équivalentes : chaque non-simplifiabilité entraîne une multiformité et v. v. ; par exemple

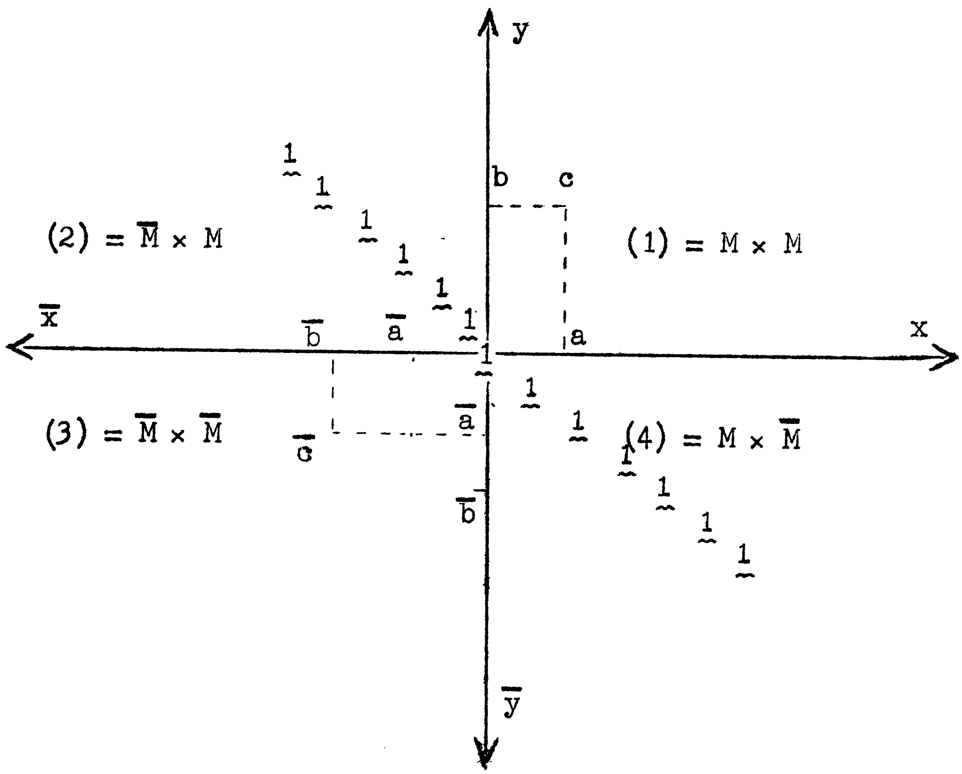
$$a_1 b = a_2 b = c \quad \text{avec} \quad a_1 \neq a_2 \iff a_1, a_2 \in c.\overline{b} .$$

Au premier échelon, l'échelon fondamental, on construit le tableau $T_1 = X_M \times X_M$, éventuellement multiforme, en suivant les règles de symétrisation ci-dessus. Il se partage en quatre quadrants comme un plan cartésien $x - y$. Le tableau $M \times M$ de M comportant toutes les relations $ab = c$ et les trous de M constitue le premier quadrant (1). On identifie la ligne et la colonne d'entrées, c'est-à-dire les axes positifs x et y, avec celles de l'élément $\underset{\sim}{1} \in X_M$, $\underset{\sim}{1} \notin M$ (*). L'origine a les coordonnées $(\underset{\sim}{1}, \underset{\sim}{1})$ et porte l'élément $\underset{\sim}{1}$. Les axes négatifs, notés $\bar{x}$ et $\bar{y}$, servent de la même manière pour le tableau $\bar{M} \times \bar{M}$ de $\bar{M}$, l'opposé de M, constituant le quadrant (3). Sur la deuxième diagonale devenue l'axe de symétrie on met partout des $\underset{\sim}{1}$. On finit T_1 en complétant les "tableaux des quotients" : chaque entrée $ab = c$ dans (1) donne lieu à deux entrées dans $(2) = \bar{M} \times M$ (quotients gauches),

$$\bar{a}c = b \,, \qquad \bar{c}a = \bar{b}$$

symétriques par rapport à l'axe des $\underset{\sim}{1}$, et, de même, deux entrées symétriques dans $(4) = M \times \bar{M}$

$$c\bar{b} = a \,, \qquad b\bar{c} = \bar{a} \,.$$



(*) Si M est unitaire on pourrait, si on le voulait, identifier $\underset{\sim}{1}_X = \underset{\sim}{1} \in M$; même sans cela on pourrait distinguer tous les éléments inverses et inversibles dans un sens plus ou moins large. Nous ne le ferons pas ici en préférant la simplicité de principe et de description à l'économie en volume des tableaux considérés. D'ailleurs en appliquant la méthode du texte on découvre nécessairement ces éléments distingués.

Si dans ce tableau T_1 deux entrées distinctes ne tombent jamais sur la même place, T_1 est déjà le tableau de $S(M)$, card $S(M) = 2$ card $M + 1$, et M est symétrisable.

Si non, c'est-à-dire s'il y a des places dans (2) (et, par dualité, de même en (4)), portant plusieurs éléments de X_M, T_1 ne présente pas un monoïde, mais un hypermonoïde (= relation ternaire) symétrique. L'identification des éléments tombant sur une même place engendre, par transitivité, une équivalence E_1 sur X_M (partition en classes disjointes) et donc un tableau induit $T_2 = X' \times X'$, $X' = X/E_1$. Si T_2 présente un monoïde, c'est-à-dire E_1 une congruence

$$a \sim a', \quad b \sim b', \quad c \in ab, \quad c' \in a'b' \implies c \sim c' \quad (\sim \bmod E_1),$$

il est tableau de $S(M)$. Si non, on définit de la même manière E_2 sur X', on pose $X'' = X'/E_2$ et on passe au tableau $T_3 = X'' \times X''$. Continuant ainsi on obtient, pour M fini, donc pour $X_M = X$ fini,

$$\infty > \text{card } X > \text{card } X' > \dots > \text{card } X^{(i-1)} > \text{card } X^{(i)} > \dots \geqslant 1 = \text{card } \{1\} .$$

On doit donc s'arrêter, après un nombre fini de pas, à un $X^{(n)} = S(M)$ par le tableau T_{n+1}. Dans le pire cas, c'est le monoïde symétrique trivial d'identité.

Il s'ensuit que la symétrisabilité d'un monoïde fini est une propriété vérifiable dans un nombre fini de pas ; on constate la non symétrisabilité de M la première fois où on doit identifier deux éléments de M entre eux (donc aussi par l'anti-isomorphie deux éléments de $\overline{M}$ entre eux). On constate la symétrisabilité si $M \subset X_M^{(n)}$ (ou plutôt $M \cup M' \subset X_M^{(n)}$; autrement dit, si aucune identification dans M n'est intervenue dans la construction de $X_M^{(n)} = S(M)$.

Nous reportons à plus tard l'énoncé explicite des théorèmes de symétrisabilité. Constatons seulement que la simplifiabilité de M est une condition nécessaire. Elle est aussi suffisante dans beaucoup des cas importants, comme, par exemple, pour les demi-groupes, les monades et les monoïdes sans inverses $\neq 1$ quelconques. Dans des cas plus généraux l'absence d'inverses proprement locaux doit être explicitée. Avec une définition appropriée d'inverses proprement locaux dans un sens généralisé d'une manière naturelle, leur absence est une condition nécessaire et suffisante pour la symétrisabilité de M la plus générale. La collection de toutes les symétrisations plus ou moins librement engendrées à partir d'un monoïde symétrisable constitue un treillis, ordonné par la relation "d'être sous-monoïde d'un monoïde". Elle possède la plus grande symétrisation, la symétrisation complète déjà mentionnée (un "I. P. - loop"), et la plus petite déjà mentionnée, $S(M)$.

III. L'associativité et le premier théorème fondamental.

Un monôme formel $A^d(a_0, \dots, a_d)$ d'un monoïde M est dit élémentaire s'il peut contracté par une suite de contractions élémentaires, respectant les parenthèses, à un seul élément $a \in M$; on dit aussi que A^d a un sens dans M, à savoir le sens ou la valeur a, et on l'écrit $A^d(a_0, \dots, a_d) = a$. Ceci revient à dire qu'on peut effectuer toutes les multiplications prescrites dans A^d sans "tomber dans un trou" du tableau de la multiplication de M. Bien que la suite exacte des opérations binaires successives à effectuer, c'est-à-dire la suite des contractions, n'est pas, en général, bien déterminée, le résultat, s'il existe, est unique. C'est d'ailleurs un cas particulier d'un énoncé plus général antérieur, à savoir que chaque classe mod $\mathcal{E}_M$ dans $\mathcal{U}_{|M|}$ possède un seul représentant réduit ; car le résultat (= sens) d'un monôme élémentaire est un monôme de dim 0, donc réduit.

Si a est une contraction de A^d, on dit aussi que $A^d(a_0, \dots, a_d)$ est une factorisation, expansion ou décomposition de a dans M.

Parmi les $\binom{2d}{d+1}/d$ monômes formels appartenant à un mot formel, aucun, quelques-uns, ou tous, peuvent être élémentaires, c'est-à-dire avoir un sens dans M. "A priori", ces sens, dans la mesure où ils existent, peuvent être distincts. Un mot est dit associatif s'il a au plus un seul sens (c'est-à-dire qu'il ne possède pas deux monômes élémentaires ayant deux sens distincts). Un monoïde, dont tous les mots sont associatifs, est dit un monoïde associatif. Si l'on note $[a]$ l'ensemble, fini ou infini, des mots appartenant à toutes les factorisations-expansions de l'élément $a \in M$, l'associativité s'exprime par

$$[a] \cap [b] \neq \emptyset \implies a = b .$$

Un monoïde est donc non-associatif s'il possède (au moins) un mot possédant deux sens distincts. L'ensemble des mots d'un monoïde fini ou dénombrable est effectivement énumérable (= d'une manière récurrente) ; le nombre des monômes formels appartenant à chaque mot est fini ; la réduction de chaque monôme à un monôme réduit, en particulier le calcul des monômes élémentaires, se fait en un nombre fini de pas. Il n'est pas difficile d'élaborer une méthode d'examen systématique pour trouver dans un monoïde non-associatif quelconque un mot non-associatif, c'est-à-dire ayant deux sens distincts, donc mettant la non-associativité de M en évidence. Au contraire, l'associativité d'un monoïde étant une propriété négative, l'absence de mots non-associatifs, ne peut être mise en évidence, en général, par cette inspection successive. On aurait besoin d'un moyen permettant l'inspection simultanée de toute l'infinité des mots et monômes possibles. On verra dans la suite, qu'en fait, il ne peut exister aucune méthode générale de mettre l'associativité de monoïdes en évidence ; c'est encore ainsi, si l'on se limite à la classe des monoïdes finis, même à la sous-classe de monoïdes symétriques finis seulement, et même à des sous-classes encore plus étroites.

R. 1. – Le premier théorème fondamental : Un monoïde symétrique M_s se laisse compléter jusqu'à un groupe, si et seulement s'il est associatif.

Esquisse de démonstration. – La nécessité de l'associativité est évidente. Démontrons la suffisance.

a. Un monoïde symétrique M_s engendre un groupe $G(M_s) = W_{M_s}/E_{M_s}$, où W_{M_s} est le semi-groupe de tous les mots w sur M_s avec son opération naturelle de concaténation (juxtaposition), et E_{M_s} la congruence engendrée dans W par l'ensemble des relations dans M_s (comme exprimé par son tableau de multiplication), c'est-à-dire des contractions et des expansions élémentaires de M_s déjà mentionnées auparavant. Mais à la différence de $\mathcal{E}_M$, les transformations élémentaires engendrant E_{M_s} n'ont pas à respecter de parenthèses, qui n'existent pas dans ce cas : les transformations élémentaires ne s'appliquent pas à des monômes, mais à des mots ; donc les contractions élémentaires peuvent s'appliquer à des couples voisins quelconques, pourvus qu'il soient contractibles suivant le tableau de la multiplication donnée. $G(M_s)$ est un groupe, parce qu'il est un demi-groupe avec identité $(\underset{\sim}{1})$ et des inverses $(\bar{w})$ pour chaque élément (w), où (w) dénote la classe mod E_{M_s} contenant le mot w, et $\bar{w}$ le mot formellement inverse de w : les lettres inverses de celles de w dans l'ordre inverse.

b. On voit aussi facilement que l'application canonique f de M_s dans G,

$$f : a \to (a), \qquad a \in M_s, \qquad (a) \in G(M_s)$$

est un homomorphisme de monoïdes symétriques.

Les constructions (a) et (b) sont toujours possibles, et les propriétés correspondantes vraies pour un monoïde symétrique M_s quelconque ; en particulier, elles ne dépendent pas de l'associativité de M_s. On peut les regarder comme "standard" pour des monoïdes, respectivement des monoïdes symétriques.

c. La partie principale de la démonstration est de montrer qu'en vertu de l'associativité l'homomorphisme f est une injection (application 1-1 dans), donc un isomorphisme. Cette partie est basée sur l'application de la proposition suivante, qui est importante pour elle-même.

PROPOSITION. - <u>Si</u> A <u>et</u> B <u>sont deux mots équivalents</u> mod E_{M_s} <u>d'un monoïde symétrique</u> M_s , <u>alors il existe un mot</u> $C \in W_{M_s}$ <u>tel que</u> A <u>et</u> B <u>sont deux contractions de</u> C .

En formules on peut écrire

$$A \sim B \pmod{E_{M_s}} \implies (\exists\ C)(C \searrow A\ ,\ C \searrow B)\ ,$$

ou plus brièvement

$$A \sim B \implies A \nearrow C \searrow B\ .$$

Ici $C \searrow A$ signifie que A se dérive de C par une chaîne de contractions élémentaires ; évidemment

$$C \searrow A \iff A \nearrow C$$

aussi C se dérive de A par une chaîne d'expansions élémentaires. On peut encore indiquer le nombre de chaînons (= transformations élémentaires) de la chaîne, $A \overset{(n)}{\searrow} D$, par exemple, signifiant que D se dérive de A par n contractions élémentaires successives.

En admettant cette proposition, on peut l'appliquer au cas particulier où A et B sont des mots de longueur 1 , disons a , $b \in M_s$:

$$(a) = (b) \iff a \sim b \pmod{E_{M_s}} \implies (\exists\ C)(C \searrow a\ ,\ C \searrow b)\ .$$

En vertu de l'associativité supposée de M_s , le mot C ne peut avoir qu'au plus un seul sens ; donc $a = b$; c'est-à-dire que

$$(a) = (b) \implies a = b\ ,$$

ce qu'il fallait démontrer.

<u>Démonstration de la proposition par double induction</u>. - Le contenu de la proposition peut se mettre sous une forme plus imagée que deux mots équivalents A et B , c'est-à-dire liés par une chaîne en "zig-zag" de contractions et d'expansions quelconques, se laissent aussi lier par un chemin plus standardisé qui est une chaîne constituée par une seule chaîne d'expansions (= ascension sur une montagne) $A \nearrow C$, où C est le "sommet", suivie d'une seule chaîne de contractions (= descente) $C \searrow B$.

Appelons <u>vallée de profondeur</u> n une chaîne de n contractions élémentaires suivies d'une suite d'expansions élémentaires quelconque : $A \overset{(n)}{\searrow} D \nearrow B$.

Base de la première induction : montrons d'abord que la proposition est vraie pour les vallées de profondeur 1. Soit $A = A_1\, a_1\, a_2\, A_2$ et $a_1\, a_2 = a_0$ dans M_s, donc

$$A = A_1\, a_1\, a_2\, A_2 \overset{(1)}{\searrow} A_1\, a_0\, A_2 = D \nearrow B_1\, B_0\, B_2 \quad \text{où} \quad A_1 \nearrow B_1 ,\quad a_0 \nearrow B_0 ,\quad A_2 \nearrow B_2 .$$

$$C = B_1\, a_1\, \bar{a}_1\, B_0\, B_2$$

répond au problème parce que

$$C = B_1\, a_1\, \bar{a}_1\, B_0\, B_2 \begin{cases} \overset{(1)}{\searrow} B_1\, \underset{\sim}{1}\, B_0\, B_2 \overset{(1)}{\searrow} B_1\, B_0\, B_2 = B \text{ , mais aussi} \\ \searrow A_1\, a_1\, \bar{a}_1\, a_0\, A_2 \overset{(1)}{\searrow} A_1\, a_1\, a_2\, A_2 = A \text{ , parce que} \end{cases}$$

$$a_1\, a_2 = a_0 \implies \bar{a}_1\, a_0 = a_2 \text{ ; donc } C \searrow A ,\quad C \searrow B .$$

Si $A \overset{(n)}{\searrow} D \nearrow B$ est une vallée de profondeur n, c'est-à-dire une pente

$$A = A^0 \overset{(1)}{\searrow} A^1 \overset{(1)}{\searrow} A^2 \overset{(1)}{\searrow} \cdots \overset{(1)}{\searrow} A^{n-1} \overset{(1)}{\searrow} A^n = D ,$$

on a, en particulier, une vallée de profondeur 1 :

$$A^{n-1} \overset{(1)}{\searrow} D \nearrow B \text{ , donc } (\exists\ C = C^1)(A^{n-1} \nearrow C^1 \searrow B) .$$

En somme, on a remplacé la chaîne d'une vallée de profondeur n entre A et B par une chaîne $A \overset{(n-1)}{\searrow} A^{n-1} \nearrow C^1 \searrow B$ ne contenant qu'une vallée de profondeur $n - 1$ pour laquelle on suppose la proposition comme hypothèse d'induction ; on a donc

$$A \nearrow C \searrow C^1 \searrow B \text{ , c'est-à-dire } A \nearrow C \searrow B .$$

En somme, on a remplacé une route de vallée par une route de montagne. Ceci nous sert de base d'induction suivant le nombre des vallées. Une chaîne quelconque mettant en évidence $A \sim B \pmod{E_{M_s}}$ est composée d'une suite finie de vallées propres $V_1 , V_2 , \ldots , V_\ell$ $(\ell = 0 , 1 , \ldots)$, éventuellement précédée d'une "ascension" de A (= vallée de profondeur 0), et/ou suivie d'une descente à B (= vallée dégénérée). En remplaçant, disons la dernière vallée propre V_ℓ par une montagne, on a remplacé le chemin de ℓ vallées propres par un chemin de $\ell - 1$ vallées propres, pour lequel on suppose la proposition comme hypothèse de l'induction. C'est donc qu'on arrive, enfin, à une chaîne constituée d'une seule montagne ; mais c'est l'énoncé général de la proposition.

IV. Les corollaires du premier théorème fondamental.

De la théorie de symétrisation on sait qu'un semi-groupe S est toujours symétrisable :

$$S \subset \Sigma(S) = S \cup \{\underset{\sim}{1}\} \cup \bar{S} .$$

Si S est immersible dans un groupe, $S \subset G(S)$ où G est le groupe engendré par S, aussi

$$\bar{S} = S^{-1} \subset G(S) \text{ , donc } \Sigma(S) \subset G(S) \quad ;$$

le monoïde symétrique $\Sigma(S)$ est complété jusqu'au groupe $G(S)$. On a donc :

R. 2. - THÉORÈME 2 : Un semi-groupe est immersible dans un groupe si et seulement si sa symétrisation est associative.

R. 3. - THÉORÈME 3 : L'existence de semi-groupes non-immersibles dans des groupes est équivalente à l'existence de symétrisations non-associatives de monoïdes associatifs.

Dans le théorème 2 on peut prendre une symétrisation quelconque. Au lieu de S on peut aussi prendre chaque sous-monoïde M engendrant S,

$$M \subset S = S(M) .$$

De même $\Sigma(M)$, la symétrisation de M engendre le même

$$G = G(S) = G(\Sigma(M)) = G(M) .$$

L'exemple célèbre de MALCEV d'un semi-groupe non-immersible dans un groupe engendré par les huit lettres a, b, c, d, x, y, u, v et les trois relations-définitions $ax = by$, $cx = dy$, $au = bv$, naturellement infini, conduit, d'une manière évidente, au monoïde fini suivant de treize éléments

$$\{a , b , c , d , x , y , u , v ,$$
$$f = ax = by , \quad g = cx = dy , \quad h = au = bv , \quad k = cu , \quad \ell = dv\}$$

et de huit places occupées dans sa table de multiplication (8 sur $13^2 = 169$). Aucun mot de trois lettres n'ayant de sens, ce monoïde est trivialement associatif. Il est symétrisable : sa symétrisation peut être construite directement et consiste en $2 \times 13 + 1 = 27$ éléments

$$\{a , b , \ldots , u , v , \ldots , k , \ell , \underset{\sim}{1} , \bar{a} , \ldots , \bar{\ell}\}$$

avec $6 \times (13+8)+1 = 127$ places occupées (sur $27^2 = 729$). Mais cette symétrisation est non-associative parce que

$$k = cu = (g\bar{x})(\bar{a}(bv))$$

et

$$\ell = dv = (g((\bar{x}\bar{a})\ b))\ v$$

sont deux sens distincts du mot $g\bar{x}\bar{a}bv$. L'inspection directe assurant $k \neq \ell$ étant trop onéreuse pour cet exemple (par son volume), on recherche des images homomorphes plus réduites possédant encore les mêmes propriétés. En effet, en posant $x = a$, $y = b$, $u = c$, $v = d$, on obtient un monoïde associatif symétrisable de neuf éléments et huit places occupées

$\{a\ , b\ , c\ , d\ , f = aa = bb\ , g = ca = db\ , h = ac = db\ , k = cc\ , \ \ell = dd\}$,

dont la symétrisation consistant en $2 \times 9 + 1 = 19$ éléments et $6 \times (8+9)+1 = 103$ places occupées (sur $19^2 = 361$) est non-associative :

$$k = (g\bar{a})(\bar{a}(bd))\ , \quad \ell = (g((\bar{a}\bar{a})\ b))\ d\ .$$

Ici encore l'inspection directe de $k \neq \ell$ par construction de la table de multiplication présente quelque travail ; mais en posant $h = g$, $k = a$, $\ell = b$, on obtient un monoïde associatif symétrisable de six éléments et huit places occupées

$\{a\ , b\ , c\ , d\ , \ f = aa = bb\ , \ g = ac = bd = ca = db\ , \ a = cc\ , \ b = dd\}$

dont la symétrisation consiste en $2 \times 6 + 1 = 13$ éléments et en $6 \times (8+6)+1 = 85$ places occupées sur $13^2 = 169$. Ici $a = (g\bar{a})(\bar{a}(bd))$, $b = (g((\bar{a}\bar{a})\ b))\ d$ comme ci-dessus, et $a \neq b$ comme on voit directement du tableau construit

$\underset{\sim}{1}$		b	a	d	c	g						
	$\underset{\sim}{1}$			b	a	f						
$\bar{b}$		$\underset{\sim}{1}$		$\bar{d}$		d		g		b		
$\bar{a}$			$\underset{\sim}{1}$		$\bar{c}$	c	g		a			
$\bar{d}$	$\bar{b}$	d		$\underset{\sim}{1}$		b		f		g		
$\bar{c}$	$\bar{a}$		c		$\underset{\sim}{1}$	a	f		g			
$\bar{g}$	$\bar{f}$	$\bar{d}$	$\bar{c}$	$\bar{b}$	$\bar{a}$	$\underset{\sim}{1}$	a	b	c	d	f	g
			$\bar{g}$		$\bar{f}$	$\bar{a}$	$\underset{\sim}{1}$		$\bar{c}$		a	c
		$\bar{g}$		$\bar{f}$		$\bar{b}$		$\underset{\sim}{1}$		d	b	d
			$\bar{a}$		$\bar{g}$	$\bar{c}$	c		$\underset{\sim}{1}$			a
		$\bar{b}$		$\bar{g}$		$\bar{d}$		d		$\underset{\sim}{1}$		b
						$\bar{f}$	$\bar{a}$	$\bar{b}$			$\underset{\sim}{1}$	
						$\bar{g}$	$\bar{c}$	$\bar{d}$	$\bar{a}$	$\bar{b}$		$\underset{\sim}{1}$

Dans un certain sens précis ces exemples sont les plus simples possibles [8].

R. 4. - Dans un monoïde symétrique M_s on peut exprimer la condition d'associativité

$$A(c_1 , \dots , c_n) = a , \quad B(c_1 , \dots , c_n) = b \implies a = b$$

aussi bien comme

$$I(x_0 , x_1 , \dots , x_n) = \underset{\sim}{1} = J(y_0 , y_1 , \dots , y_n)$$

$$\text{et} \quad x_1 = y_1 , \dots , x_n = y_n \implies x_0 = y_0 .$$

La généralisation au préordre s'écrit

$$I(x_0 , x_1 , \dots , x_n) = 1 = J(y_0 , y_1 , \dots , y_n)$$

$$\text{et} \quad k_1 \to y_1 , \dots , x_n \to y_n \implies y_0 \to x_0 .$$

Si M_s est une symétrisation de M, chaque élément de $M_s = \Sigma(M)$ est un quotient à gauche et un quotient à droite. On peut poser

$$x_i \to y_i \iff \bar{s}_i\, t_i \to u_i\, \bar{v}_i \iff t_i\, v_i \to s_i\, u_i .$$

En explicitant l'associativité de la symétrisation, on obtient une déduction, directe et en forme close, du système des conditions nécessaires et suffisantes de MAL'CEV pour l'immersibilité des demi-groupes S dans des groupes G, resp. les conditions généralisées de TAMARI pour l'immersibilité des demi-groupoïdes préordonnés S dans des groupoïdes préordonnés G sous la forme $(H) \implies (C)$

$$(H) : \quad \begin{cases} (1) \quad t_i\, v_i \to s_i\, u_i \quad (i = 1 , \dots , d) \quad \text{dans } S , \text{ où} \\ (2) \quad \prod_{g=0}^{d} \bar{s}_j\, t_j \equiv \underset{\sim}{1} \equiv \prod_{j=0}^{d} u_j\, \bar{v}_j \end{cases}$$

est une identité formellement valable dans chaque groupe qui entraîne

$$(C) : \qquad s_0\, u_0 \to t_0\, v_0 \quad \text{dans } S \quad (d = 1 , 2 , \dots) .$$

"$\to$" signifie le préordre de S ; (2) signifie qu'il y a deux permutations $j \to j'$, $j \to j''$ de $\{0 , 1 , \dots , d\}$ telles que $s_j = t_{j'}$, $u_j = v_{j''}$ et donc

$$\Pi \bar{s}_j\, t_j = \Pi \bar{t}_{j'}\, t_j \quad \text{et} \quad \Pi u_j\, \bar{v}_j = \Pi v_{j''}\, \bar{v}_j$$

sont deux mots formellement "a priori" identiques au mot vide (= l'identité $\underset{\sim}{1}$). On obtient une nouvelle connexion du modèle circulaire de Tamari avec les quotients de Lambek et des réinterprétations intéressantes. Pour les détails on renvoie à un exposé à paraître.

R. 5. - THÉORÈME 5 : Sol. $AM_{sf} \Longrightarrow$ Sol. $TG(M_{sf})$.

La solubilité du problème de l'associativité (A) pour les monoïdes symétriques finis M_{sf} entraîne la solubilité du problème de trivialité (T) pour les groupes $G(M_{sf})$ engendrés par des monoïdes symétriques finis.

Les notations suivantes signifient :

M_{sf} : de monoïdes symétriques finis non-triviaux, c'est-à-dire $\neq \underset{\sim}{I} = \{\underset{\sim}{1}\}$;

AM : le problème " M est-il associatif ou (effectivement) non-associatif ?" ;

TG : le problème " G est-il trivial, c'est-à-dire $= \underset{\sim}{I}$, ou $\neq \underset{\sim}{I}$?".

On remarque que $\underset{\sim}{I}$ est trivialement symétrique et associatif.

Démonstration : On pose $M_{sf} = M = M_0$ et on suppose la solubilité du problème de l'associativité. On a donc l'alternative :

M associatif $\Longrightarrow G(M) \supset M \neq \underset{\sim}{I} \Longrightarrow G \neq \underset{\sim}{I}$.

M non-associatif $\Longrightarrow \exists$ un mot w_1 sur M (même pour M infini dénombrable) avec deux sens distincts $a_1 \neq b_1$ dans M $\Longrightarrow$ génération d'une relation de congruence E_1 sur M à partir de l'identification $a_1 \sim b_1$ (mod E_1) $\Longrightarrow$ construction d'un monoïde symétrique fini $M_1 = M_0/E_1$ avec card $M_1 <$ card M_0 . De nouveau on a l'alternative décidable " M_1 associatif ou non-associatif". On répète ce processus jusqu'à l'apparition, pour la première fois, d'un $M_n = M_{n-1}/E_n$ $(n \geqslant 1)$ associatif, donc

$$M_{n-1} \neq M_n = M_{n+1} = M_{n+2} = \dots$$

Un tel n existe certainement puisque

$$\infty > \text{card } M_0 > \text{card } M_1 > \dots > \text{card } M_i \geqslant 1 = \text{card } \underset{\sim}{I}$$

$$G(M_0) = G(M_1) = \dots = G(M_i) = \dots = G(M_n) \supset M_n$$

et donc

$$M_n = \underset{\sim}{I} \Longleftrightarrow G = \underset{\sim}{I} \text{ ou aussi bien } M_n \neq \underset{\sim}{I} \Longleftrightarrow G \neq \underset{\sim}{I} .$$

R. 6. - THÉORÈME 6 : Sol. mots $G(M_{sf}) \Longrightarrow$ Sol. $I_G\, M_{sf} \Longleftrightarrow$ Sol. AM_{sf} .

Démonstration. - Sol. mots G $\Longrightarrow$ si $a \neq b$ dans M , a et b sont des mots distincts (d'une seule lettre) dans G(M) , et on peut résoudre pour le nombre fini de paires $a \neq b$ dans M le problème si toutes ces paires sont aussi distinctes comme éléments de G : $a \neq b$ dans G ou $a = b$ dans G . Donc on peut résoudre, si $M \subset G$ ou $M \not\subset G$, et, de même, si M est associatif ou non-associatif.

R. 7. – THÉORÈME 7 : $\mathcal{CG}(M_f) = \mathcal{CG}(M_{sf}) = \mathcal{CG}(\Pi_f)$.

$\mathcal{CG}(M_f) = \mathcal{CG}(M_{sf})$ est évident, puisque $M_{sf} = \Sigma(M_f)$ et $G(M_f) = G(\Sigma(M_f))$. Aussi $\mathcal{CG}(M_f) \subset \mathcal{CG}(\Pi_f)$ est évident, parce que l'ensemble fini d'éléments et de relations $ab = c$ de la table de multiplication d'un monoïde fini M_f est un cas particulier d'une présentation finie Π_f . Il faut montrer aussi qu'inversement $\mathcal{CG}(\Pi_f) \subset \mathcal{CG}(M_f)$. En fait, chaque présentation finie Π_f est équivalente à une présentation monoïdale, ou même monoïdale symétrique par la standardisation suivante :

soit $\Pi = (\Gamma , R)$, où l'alphabet

$$\Gamma = \{g_1 , \dots , g_n\} \text{ et } R = \{A_1 = B_1 ; \dots , A_r = B_r\}$$

où A_i , B_i sont des mots en $g_1 , \dots , g_n$. On introduit pour tous les couples distincts $g_{i_1} g_{i_2}$ de lettres voisines apparaissant effectivement dans les mots A_i , B_j de nouveaux symboles ou lettres, par exemple avec double indice : $g_{i_1 i_2} = g_{i_1} g_{i_2}$ et ces relations de simple multiplication ; de même pour tous les triples de voisins effectivement distincts et apparaissant dans les A_i , B_j : $g_{i_1 i_2 i_3} = g_{i_1} g_{i_2 i_3} = g_{i_1 i_2} g_{i_3}$ avec ces relations de simple multiplication ; de même pour des quadruples etc. jusqu'à l'épuisement du plus long mot parmi les A_i , B_j . On obtient ainsi un monoïde avec éléments $\{g_1 , \dots , g_n , g_{i_1 i_2} , \dots , g_{i_1 i_2 i_3} , \dots\}$ et une table de multiplication dans laquelle on tient encore compte des relation $A_i = B_i$. Ce monoïde bien déterminé est la présentation monoïdale standard de $G(\Pi_f)$.

Ce qui vient d'être dit suffit pour justifier $\mathcal{CG}(\Pi_f) \subset \mathcal{CG}(M_f)$; donc $\mathcal{CG}(\Pi_f) = \mathcal{CG}(M_f)$.

R. 8, 9, 10. – Les résultats 8, 9 et 10 mentionnés sont maintenant des conséquences presqu'immédiates. Mais en liaison avec des applications plus poussées ou plus spéciales, par exemple programmation des calculs de groupes pour calculatrices électroniques, on a besoin de plus de rigueur, et on doit fixer minutieusement les détails par des conventions.

Remarquons encore la généralisation naturelle étendant la notion usuelle de présentation : on préservit l'existence de certains mots, ou, plus généralement, de certains monômes pour la présentation de monoïdes généraux (non-associatifs). Le cas spécial des mots n'est qu'une abbréviation pour les cas où tous les monômes correspondants à un même mot sont admis. Ainsi l'existence du mot

$g_{i_1} g_{i_2} \dots g_{i_k}$ seul, sans être membre d'une relation, introduit les éléments et relations monoïdales standards :

$$g_{i_1} g_{i_2} = g_{i_1 i_2} \; ; \; \dots , \; g_{i_{k-1}} g_{i_k} = g_{i_{k-1} i_k} \; ;$$

$$g_{i_1 i_2} g_{i_3} = g_{i_1} g_{i_2 i_3} = g_{i_1 i_2 i_3} , \dots , g_{i_{k-2} i_{k-1}} g_{i_k} = g_{i_{k-2}} g_{i_{k-1} i_k} = g_{i_{k-2} i_{k-1} i_k} \; ;$$

$$g_{i_1 i_2 i_3} g_{i_4} = g_{i_1 i_2} g_{i_3 i_4} = g_{i_1} g_{i_2 i_3 i_3} = g_{i_1 i_2 i_3 i_4} , \dots$$

$$g_{i_1 \dots i_{k-1}} g_{i_k} = g_{i_1 \dots i_{k-2}} g_{i_{k-1} i_k} = \dots = g_{i_1} g_{i_2 \dots i_k} = g_{i_1 \dots i_k} .$$

Chaque combinaison reçoit à sa première apparition (suivant un ordre lexicographique strict) un et un seul symbole ; aucune répétition n'est permise. De la même manière on procède pour des ensembles de mots, inclus les mots apparaissant dans les relations-définitions. On ajoute simplement les relations supplémentaires imposées diminuant le nombre de nouveaux symboles.

BIBLIOGRAPHIE

[1] ADJAN (S. I.). - Algoritmičeskaja nerazrešimost' problem raspoznavanija nekotorykh svojstv grupp, Doklady Akad. Nauk SSSR, t. 103, 1955, p. 533-535.

[2] BAER (Reinhold). - Free sums of groups and their generalizations, I., Amer. J. of Math., t. 71, 1949, p. 706-742 ; II., t. 72, 1950, p. 625-646 ; III., t. 72, 1950, p. 647-670.

[3] BATES (Grace E.). - Free loops and nets and their generalizations, Amer. J. of Math., t. 69, 1947, p. 499-550.

[4] BOONE (William W.). - The word problem, Annals of Math., Series 2, t. 70, 1958, p. 207-265.

[5] BRITTON (J. L.). - The word problem for groups, Proc. London math. Soc., t. 8, 1958, p. 493-506.

[6] BRUCK (Richard H.). - A survey of binary systems. - Berlin, Springer-Verlag, 1958 (Ergebnisse der Mathematik ..., 20, Reihe : Gruppentheorie).

[7] BUSH (George C.). - The embedding theorems of Malcev and Lambek, Canad. J. of Math., t. 15, 1963, p. 49-58.

[8] CARVALHO (J. B. de) et TAMARI (D.). - Sur l'associativité partielle des symétrisations de semi-groupes, Portug. Math., t. 21, 1962, p. 157-169.

[9] DUBREIL (Paul). - Algèbre, Tome 1, 2e édition. - Paris, Gauthier-Villars, 1954 (Cahiers scientifiques, 20).

[10] EVANS (Trevor). - The word problem for abstract algebras, J. London math. Soc., t. 26, 1951, p. 64-71 ; Embeddability and the word problem, J. London math. Soc., t. 28, 1953, p. 76-80.

[11] FREEDMAN (Haya) and TAMARI (Dov). - A finite lattice structure induced by an associative law (à paraître).

[12] LAMBEK (J.). - The immersibility of a semigroup into a group, Canad. J. of Math., t. 3, 1951, p. 34-43.

[13] MAL'CEV (A.). - On the immersion of an algebraic ring into a field, Math. Annalen, t. 113, 1937, p. 686-691.

[14] MAL'CEV (A.). - O vključenii assocativnykh sistem v gruppy, I., Mat. Sbornik, N. S., t. 6, 1939, p. 331-336 ; II., t. 8, 1940, p. 251-263.

[15] MAL'CEV (A.). - Kvaziprimitivnye klassy abstraktnykh algebr, Doklady Akad. Nauk SSSR, t. 108, 1956, p. 187-189.

[16] NEUMANN (Hanna). - Generalized free products with amalgamated subgroups, Amer. J. of Math., t. 70, 1948, p. 590-625.

[17] NEWMAN (M. H. A.). - On theories with a combinatorial definition of "equivalence", Annals of Math., Series 2, t. 43, 1942, p. 223-243.

[18] NOVIKOV (N. S.). - Ob algoritmičeskoj nerazrešimosti problemy toždestva slov v teorii grupp, Trudy Mat. Instit. Steklova, t. 44, 1955, 143 p.

[19] RABIN (Michael O.). - Recursive unsolvability of group theoretic problems, Annals of Math., Series 2, t. 67, 1958, p. 172-194.

[20] TAMARI (Dov). - Les images homomorphes des groupoïdes de Brandt et l'immersion des semi-groupes, C. R. Acad. Sc. Paris, t. 229, 1949, p. 1291-1293.

[21] TAMARI (Dov). - Monoïdes préordonnés et chaînes de Malcev, Thèse Sc. math. Paris. 1951, partiellement multigraphiée, IV + 81 p. et partiellement publiée dans Bull. Soc. math. France, t. 82, 1954, p. 53-96.

[22] TAMARI (Dov). - Une contribution aux théories modernes de communication : Machines de Turing et problèmes de mots, Synthèse, Amsterdam, t. 9, 1954, p. 205-227.

[23] TAMARI (Dov). - Imbeddings of partial (incomplete) multiplicative systems (monoïds), associativity and word problem, Amer. math. Soc. Notices, t. 7, 1960, p. 760 ; Families of binary relations and the theory of analytic functions of a complex variable, Amer. math. Soc. Notices, t. 7, 1960, p. 982.

[24] TAMARI (Dov). - The algebra of bracketings and their enumeration, Nieuw Arch. Wiskunde, Série 3, t. 10, 1962, p. 131-146.

[25] TAMARI (Dov). - Some mutual applications of logic and mathematics, Applications scientifiques de la logique mathématique, Actes du 2e colloque international de Logique mathématique [1952. Paris], p. 89-90. - Paris, Gauthier-Villars, 1954.