Séminaire Dubreil.
Algèbre et théorie
des nombres

Dov Tamari

Le problème de l'associativité des monoïdes et le problème des mots pour les demi-groupes ; algèbres partielles et chaînes élémentaires

Séminaire Dubreil. Algèbre et théorie des nombres, tome 24, n° 1 (1970-1971), exp. n° 8, p. 1-15

<http://www.numdam.org/item?id=SD_1970-1971__24_1_A6_0>

Séminaire DUBREIL-PISOT
(Algèbre et Théorie des nombres)
24e année, 1970/71, n° 8, 15 p.

1er février 1971

LE PROBLÈME DE L'ASSOCIATIVITÉ DES MONOÏDES ET LE PROBLÈME DES MOTS POUR LES DEMI-GROUPES ; ALGÈBRES PARTIELLES ET CHAÎNES ÉLÉMENTAIRES

par Dov TAMARI

Introduction. - Comme dans notre conférence antérieure dans ce séminaire [9], on appelle monoïde $M = (|M|, .)$, un système binaire partiel : l'ensemble $|M|$, le support de M, est pourvu d'une opération binaire partielle " . " : $R_M \to |M|$, où R_M est une partie quelconque de $|M| \times |M|$; donc le "produit" n'est pas nécessairement partout défini. On peut s'imaginer un monoïde comme une table de multiplication avec des "trous".

Les problèmes et les résultats principaux apparaissent à première vue assez semblables à ceux de la conférence antérieure, laquelle a eu lieu il y a plus de huit ans. Quelles sont les différences ?

Principalement, c'est la définition de l'associativité même, donc aussi le sens précis du problème de l'associativité, qui sont différents. La présente définition est plus générale et plus simple dans sa forme existentielle ; mais elle devient plus compliquée dans sa réalisation combinatoire-constructive. La définition ancienne suffisait pour les monoïdes symétriques, en vertu du théorème "d'une seule montagne" ; elle ne suffit pas pour le cas général dans lequel ce théorème n'est plus valable. C'est la raison pour laquelle notre conférence antérieure devait partir des monoïdes symétriques, et se référait au problème plus difficile des mots pour les groupes. Si l'on voulait partir d'un monoïde quelconque, on devait le symétriser d'abord. On montrait alors que le problème de l'associativité des monoïdes symétriques finis est équivalent au problème (insoluble) des mots pour les groupes à présentation finie. Aujourd'hui, on montre directement que le problème de l'associativité des monoïdes finis quelconques est équivalent au problème (insoluble) des mots pour les demi-groupes à présentation finie. Les deux résultats sont liés par le fait que le groupe engendré par un monoïde quelconque est isomorphe au demi-groupe engendré par la symétrisation du monoïde donné, le demi-groupe engendré par un monoïde symétrique étant de soi-même un groupe.

Antérieurement, on démontrait l'équivalence logique des conditions célèbres de MAL'CEV à l'associativité de la symétrisation d'un semi-groupe, les deux étant des conditions nécessaires et suffisantes pour l'immersibilité d'un semi-groupe dans un groupe. Ici, l'expression explicite, constructive de l'associativité la plus générale

des monoïdes, est par sa définition même la condition nécessaire et suffisante pour l'immersibilité d'un monoïde quelconque dans un demi-groupe. Littéralement, les mêmes modèles géométriques, le modèle de courants et le modèle circulaire de ma thèse [8] pour les conditions de MAL'CEV proprement dites, s'interprètent maintenant directement comme diagrammes des lois de l'associativité la plus générale.

Cette conférence expose le nouveau concept général de l'associativité. On traite ce problème de monoïdes associatifs, ou, ce qui revient au même, de demi-groupes partiels, comme cas spécial du problème de transfert d'une loi ou propriété universelle aux algèbres partielles. C'est le problème de définition juste d'une algèbre partielle correspondant à une algèbre universelle, équationnellement définie, qui est au fond des problèmes de mots et d'immersion. Notre définition existentielle par l'immersibilité de l'algèbre partielle dans l'algèbre complète, et sa forme constructive par chaînes élémentaires spéciales fermées, est indépendante du choix d'un système d'axiomes particulier pour l'algèbre. C'est la différence essentielle entre notre méthode et celle d'EVANS.

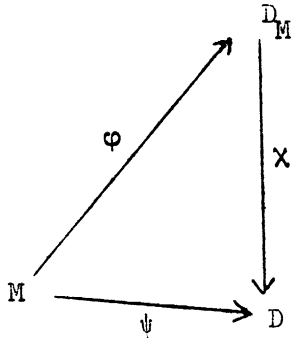
Les autres sujets, en particulier l'équivalence des deux problèmes du titre et sa nouvelle démonstration, sont seulement mentionnés. Leur exposé détaillé, avec une bibliographie plus riche, paraîtra ailleurs [10].

Le germe du développement esquissé se trouve déjà dans ma thèse [8]. C'est pour moi un devoir agréable de remercier ici les professeurs français qui m'ont aidé, il y a à peu près vingt ans, en particulier ceux qui formaient le jury de ma thèse : MM. A. CHÂTELET, H. CARTAN et P. DUBREIL. Je remercie le professeur GÖDEL, de l'Institut des Hautes Etudes de Princeton, pour ses encouragements répétés qui m'ont permis de continuer ce travail malgré les adversités extérieures extraordinaires de ma vie académique. Je remercie les mathématiciens hollandais, français et américains qui m'ont aidé quand j'étais dans le besoin. Je dois une grande reconnaissance intellectuelle aux travaux de MAL'CEV, où je puisais ma première inspiration dans cette direction ; je lui dois aussi une reconnaissance morale et personnelle pour son encouragement quand nous nous sommes rencontrés après ma communication au Congrès International, à Stockholm en 1962. Enfin je reste très obligé aux Organisateurs et Participants de la Conférence d'été qui a eu lieu en Californie en 1969 : "Sur des problèmes de décision dans la théorie des groupes", en particulier aux professeurs BOONE et CANNONITO, pour leur hospitalité, leur patience et leurs remarques critiques.

1. Définition existentielle de l'associativité.

On dit que le monoïde M est associatif, s'il peut être complété à un demi-

groupe, c'est-à-dire s'il peut être plongé dans un demi-groupe ; en d'autres termes, s'il existe un demi-groupe D et un monomorphisme (= homomorphisme injectif) $\psi : M \to D$, où $(ab = c \text{ dans } M) \Longrightarrow (a^{\psi} b^{\psi} = c^{\psi} \text{ dans } D)$. On peut choisir $D = D_M$, à savoir le demi-groupe "librement" engendré par M. D_M est l'objet universel dans la catégorie des morphismes de M dans les demi-groupes. On voit, sur le diagramme commutatif ci-contre, que, s'il existe un D et un monomorphisme ψ, alors l'homomorphisme canonique $\varphi : M \to D_M$ est aussi un monomorphisme.



Il est bien connu que $D_M \simeq F_{|M|}/E_M$, où $F_{|M|}$ est le demi-groupe libre engendré par l'ensemble des générateurs $|M|$, c'est-à-dire le demi-groupe des mots sur l'alphabet $|M|$ avec l'opération de concaténation, et E_M la relation de congruence engendrée dans l'ensemble des mots par les relations définissantes qui sont justement toutes les relations $ab = c$ valables dans M. On dit brièvement " M est une présentation monoïdale de D_M ".

L'homomorphisme canonique φ applique chaque $m \in M$ à la classe d'équivalence $m^{\varphi} \subset F_{|M|}$ contenant le mot d'une seule lettre, " m ".

M est donc associatif, si, pour chaque $m \in M$, m est le seul mot d'une seule lettre dans sa classe d'équivalence.

On a les conséquences immédiates suivantes :

(M est associatif) $\Longrightarrow$ ($\text{card } M = \text{card } M^{\varphi} \leqslant \text{card } D$) ;

(M associatif et $\text{card } M > 1$) $\Longrightarrow$ ($\text{card } D > 1$), c'est-à-dire D n'est pas trivial (= réduit à un seul élément) ;

(M effectivement non associatif) $\Longleftrightarrow$ ($\text{card } M > \text{card } M^{\varphi}$) $\Longleftrightarrow$ ($\exists\, a, b \in M$, $a \neq b$ dans M), mais $a = b$ dans $M^{\varphi} \subset D$.

M^{φ} est l'image homomorphique associative la plus grande de M, unique à des isomorphismes près.

Pourquoi cette simple définition conceptuelle et instructive de l'associativité n'a-t-elle pas été adoptée plus tôt ?

2. Définition explicite et constructive de l'associativité.

La traduction en termes explicites et constructifs de cette définition existentielle n'est simple que pour le cas trivial d'un système binaire complet, c'est-à-dire à l'opération partout définie ; c'est alors la loi associative ordinaire, une

seule identité en trois variables : $\forall\ x\ ,\ y\ ,\ z \mid (xy)z = x(yz)$.

Dans le cas général d'opération partielle, on obtient un système infini d'implications de la forme $\mathcal{C}_a^b \Longrightarrow a = b$, où les $\mathcal{C}_a^b$ sont des chaînes de longueur et de complexité toujours croissantes. Ces chaînes sont semblables aux conditions de MAL'CEV pour l'immersibilité d'un demi-groupe dans un groupe, mais d'une interprétation plus simple et plus fondamentale. Leurs chaînons sont tous de la forme $rs \to t$ ou $t \to rs$, où $rs = t$ représente une entrée dans la table de multiplication du monoïde. Pour dériver ces chaînes et les décrire plus en détail, regardons de plus près la génération de D_M .

Deux mots W_0 , $W \in F_{|M|}$ sont équivalents, $W_0 \sim W \pmod{E_M}$, si, et seulement si, ils peuvent être liés par une chaîne

$$\mathcal{C}^W_{W_0} : \quad W_0 \xrightarrow{\tau_i} W_1 \longrightarrow \ldots \longrightarrow W_{i-1} \xrightarrow{\tau_i} W_i \longrightarrow \ldots \xrightarrow{\tau_\lambda} W_\lambda \equiv W \ ,$$

de longueur finie λ ; les τ_i sont des transformations élémentaires des mots suivant les entrées de la table de multiplication de M , dites aussi substitutions élémentaires ; chaque fois, on utilise une seule relation valable de M , $rs = t$, dans une des deux manières possibles :

Ou bien comme une contraction (fusion, multiplication) $rs \to t$, remplaçant deux lettres voisines rs du mot W_{i-1} par la seule lettre t ;

Ou bien comme une expansion (fission, factorisation) $t \to rs$, remplaçant dans W_{i-1} la lettre t par le couple rs .

Chaque fois la longueur du mot change d'une unité ± 1 . Tous les mots d'une classe d'équivalence, et de cette classe seule, s'obtiennent à partir de l'un quelconque d'eux par des applications successives de telles transformations élémentaires.

Parmi les classes d'équivalence de mots $\pmod{E_M}$, nous distinguons les m^φ qui contiennent, au moins, un mot de longueur ℓ , à savoir " m ". Parmi les chaînes $\mathcal{C}^W_{W_0}$, nous distinguons les chaînes spéciales $\mathcal{C}_a^b$ liant deux mots de longueur ℓ : $a \equiv W_0$, $b \equiv W_\lambda \equiv W$, λ un nombre pair. Evidemment, " M associatif " signifie qu'une chaîne quelconque ne contient, au plus qu'un seul mot d'une seule lettre, mais, le même mot plusieurs fois est possible. Donc

$$(M \text{ associatif}) \Longleftrightarrow (\mathcal{C}_a^b \Longrightarrow a = b) \ .$$

Voilà la définition constructive de l'associativité générale. On n'avait pas encore pu établir cette définition, bien qu'on l'ait approchée souvent.

3. Identités conditionnelles.

Déjà pour les demi-groupes, l'associativité signifie, en plus de l'identité à trois variables, que le sens, ou la valeur, d'un mot est unique, indépendamment de la distribution des parenthèses binaires. Celles-ci sont, a priori, indispensables pour calculer les mots de longueur $\ell > 2$. Le parenthésage détermine ce calcul, à certaines inversions triviales de l'ordre près ; inversement, le calcul détermine le parenthésage sans aucune ambiguïté. On a donc

$$(A_\ell) : \forall\, P , Q , x_1 , \dots , x_\ell \mid P(x_1 , \dots , x_\ell) = Q(x_1 , \dots , x_\ell) ,$$

où $P \neq Q$ parcourent les couples de parenthésages binaires distincts sur des mots $x_1 , \dots , x_\ell$ de longueur ℓ . On a le théorème élémentaire bien connu :

$$(A_3) \implies (A_\ell) , \quad \forall\, \ell > 3 .$$

Dans le cas d'une opération partielle, ces formulations n'ont plus de sens. On peut obtenir un sens en remplaçant les identités universelles, inconditionnelles, ci-dessus, par des identités conditionnelles

$$(A^c_\ell) : (P(a_1 , \dots , a_\ell) = p , \ Q(a_1 , \dots , a_\ell) = q) \implies (p = q) ;$$

à savoir : Si le mot $a_1 , \dots , a_\ell$, pourvu de parenthésage P , a un sens p , c'est-à-dire qu'en calculant $P(a_1 , \dots , a_\ell)$ on ne trébuche dans aucun trou de la table de multiplication et qu'on arrive à finir avec p , et de même pour $Q(a_1 , \dots , a_\ell) = q$, alors $p = q$. Mais il n'est plus vrai, en général, que

$$(A^c_3) \implies (A^c_\ell) , \quad \forall\, \ell > 3 .$$

Ceci conduit à adopter les (A^c_ℓ) , $\forall\, \ell \geqslant 3$, comme des lois d'associativité. Elles ne sont pas toutes mutuellement indépendantes ; mais elles ne peuvent pas être réduites à un sous-ensemble fini, sauf dans les cas spéciaux. Le cas spécial bien connu est le groupoïde de Brandt et sa généralisation immédiate au demi-groupoïde, mieux connu sous son nom moderne de catégorie de morphismes, dont l'associativité peut être réduite à son expression pour les mots de longueur 3 .

4. Algèbre universelle et algèbre partielle.

En passant du cas d'opérations complètes au cas d'opérations partielles, les lois équationnelles perdent leur sens. Par contre, les reformulations implicationnelles par des identités conditionnelles ont un sens, mais sont-elles adéquates ?

Remarque. - Les lois implicationnelles ne sont pas caractéristiques pour les

algèbres partielles. Il y a des algèbres complètes implicationnellement définies, e. g. les semi-groupes (= demi-groupes simplifiables) par les lois de simplification $(ac = bc) \Longrightarrow (a = b)$ et $(ca = cb) \Longrightarrow (a = b)$. On les appelle algèbres quasi-universelles.

Soit $\mathfrak{A} = \{A \mid A \in \mathfrak{A}\}$ une classe d'algèbres équationnellement définie. Ces algèbres ont les "mêmes" opérations (dans un sens très faible, mais précis, bien connu), et satisfont les mêmes identités universelles. En pratique, on définit une telle classe par une base $(\Omega , \mathfrak{E})$: $\Omega = \bigcup \Omega_n$ est un ensemble (fini ou infini) d'opérations fondamentales $\omega : |A|^{n_\omega} \to |A|$ ($|A|$ le support de A , n_ω l'arité de $\omega \in \Omega_{n_\omega}$), d'où dérivent, par composition, les opérations dérivées, dites aussi polynômes ; $\mathfrak{E}$ est un ensemble (fini ou infini) de lois ou d'identités fondamentales

$$(L_j) : f_j(x_1 , \dots , x_{\nu_j}) = g_j(x_1 , \dots , x_{\nu_j}) \quad (f_j , g_j \text{ certains polynômes}) ,$$

d'où dérivent toutes les identités valables dans les algèbres de $\mathfrak{A}$. En principe, le choix d'une base est arbitraire ; ce qui compte, c'est l'ensemble de toutes les opérations et de toutes les identités valables, sans distinction entre fondamentales et dérivées.

D'autre part, dans les cas bien connus, ce n'est pas par tradition seulement qu'on distingue une base particulière, mais par sa simplicité extrême et évidente. Ainsi, la classe des demi-groupes a une base naturelle, constituée par une seule opération binaire et une seule identité $(xy)z = x(yz)$; ses polynômes sont les parenthésages binaires. Dans le passage aux opérations partielles, ces distinctions les plus naturelles des algèbres universelles perdent leur sens, souvent dans une mesure extrême : peu, ou presque rien, se préserve des relations logiques de dérivation et de dépendance parmi les identités. Donc, en général, on doit, au moins, remplacer une "petite" base avec identités universelles par une infinité d'opérations et de lois implicationnelles de longueur et de complexité toujours croissantes.

Il y a plus ! En général, ce remplacement nécessaire, bien que déjà assez compliqué, n'est pas encore suffisant. La rupture est plus grave. En fait, on doit remplacer non seulement les identités de l'algèbre universelle, mais aussi bien les infinités d'identités conditionnelles correspondantes, par des chaînes élémentaires implicationnelles les plus générales ; en même temps, on gagne en simplicité en se limitant aux opérations fondamentales seulement.

Rétrospectivement, la rupture apparaît moins grande. On peut remplacer chaque

équation particulière

$$P(a_1 , \dots , a_\ell) = b \quad ,$$

ou identité

$$f(x_1 , \dots , x_\nu) = g(x_1 , \dots , x_\nu) \quad ,$$

par une chaîne élémentaire dont chaque chaînon n'est qu'une seule application d'une des opérations fondamentales, complètes ou partielles, c'est-à-dire une substitution tirée des "tables de multiplications (opérations)". Au fond, cette chaîne n'est rien d'autre qu'une spécification des pas élémentaires du calcul des polynômes suivant les tables d'opérations fondamentales, en introduisant des résultats intermédiaires ou des variables "dépendantes" auxiliaires. Ainsi, l'identité $(xy)z = x(yz)$ devient

$$(xy = u \ , \ uz = v \ , \ yz = s \ , \ xs = t) \implies (y = t) \quad ,$$

qu'on écrit

$$(v \to uz \to xyz \to xs \to t) \implies (v \to t) \quad .$$

(L_j^c) devient

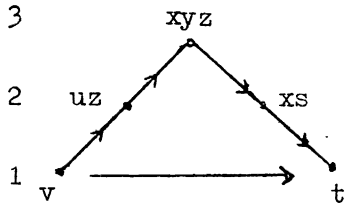
$$(p \to \dots \to f_j(x_1 , \dots , x_{\nu_j}) = g_j(x_1 , \dots , x_{\nu_j}) \to \dots \to q) \implies (p = q) \quad .$$

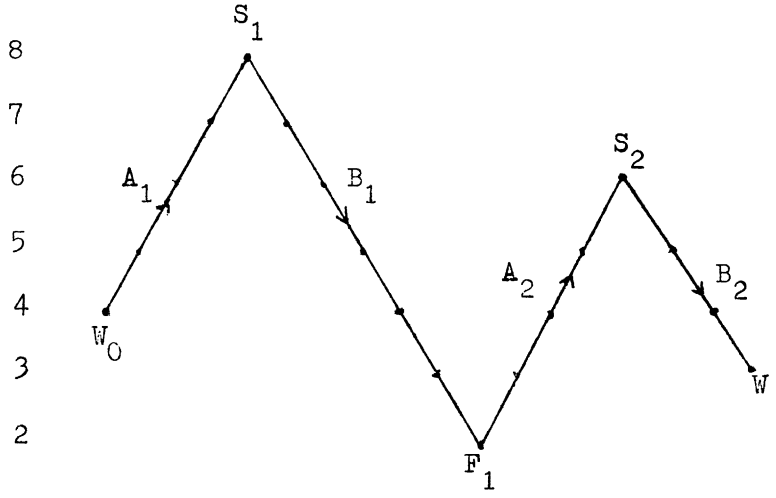
Ces chaînes élémentaires sont assez spéciales ; elles correspondent à un seul polynôme, ou à un couple de polynômes avec les mêmes variables. Ces polynômes sont une écriture abrégée de ces chaînes élémentaires. En explicitant seulement des contractions, elle tend à faire oublier les expansions $b \to \omega a_1 , \dots , a_{n_\omega}$. Pour les chaînes élémentaires générales, ce n'est plus possible. On peut encore abréger des morceaux de chaînes par des quasi-polynômes, dits aussi polynômes partiels ou plutôt partiellement complets, qui correspondent aux cîmes de la chaîne. En général, on obtient une chaîne de polynômes partiels assez compliquée, sans qu'il y ait des bornes supérieures, ni pour la longueur des chaînes, ni pour la complexité de leurs quasi-polynômes. Notre étude plus détaillée de la loi associative suffira pour éclaircir, à titre d'exemple, la situation générale.

5. Profils des chaînes élémentaires.

On arrange les mots (= éléments de $F_{|M|}$) suivant leur longueur en étages, l'étage 0 (s'il y a lieu) pour le mot vide, l'étage 1 pour les mots d'une seule lettre (les éléments de M), l'étage ℓ pour les mots de longueur ℓ . Par une

substitution élémentaire, on monte ou on descend un étage ([1]). En plus, on représente la progression dans une chaîne de mots en progressant de gauche à droite. Ainsi, la dernière chaîne ci-dessus se représente par le diagramme que voici. Dans un demi-groupe $v = t$, "le diagramme se ferme". Ce diagramme, d'une chaîne générale $C^{W}_{W_0}$, s'appelle son <u>profil</u>. Il est une suite alternante de <u>montées</u> et de <u>descentes</u> ; une montée, suivie d'une descente, est une <u>montagne</u> ; le dernier mot de sa montée, donc son mot le plus long, est son <u>sommet</u>, à partir d'où commence la descente. Une descente, suivie d'une montée, forme une <u>vallée</u> ; le dernier mot de sa descente, donc son mot le plus court, est son <u>fond</u>, à partir d'où commence sa montée. Une chaîne est donc une suite de montagnes (vallées) ; la première montée (descente) ou la dernière descente (montée) peuvent manquer (= être vides), et la chaîne commence ou finit avec une vallée (montagne). La dualité n'est pas complète. E. g. les chaînes spéciales C^{b}_{a} ne peuvent que monter au commencement, et descendre à la fin (sauf le cas trivial $C^{e_2}_{e_1}$: $e_1 = \emptyset = e_2$ l'élément d'identité unique égal au mot vide). L'asymétrie est celle des nombres naturels ; on peut monter sans borne pour la hauteur des montagnes, mais on ne peut descendre plus bas qu'à l'étage 1 (ou 0).





Dans notre contexte, où chaque substitution dérive d'une équation, on peut parcourir la chaîne dans le sens inverse, et échanger des montées et des descentes. La même <u>pente</u> est donc une montée ou une descente, suivant le sens du parcours. Ce ne sera plus le cas si les relations de substitution dérivent d'un ordre ou, plus généralement, d'un préordre (voir [8]).

Les pentes admettent une description concise et intrinsèque par parenthésage

---

([1]) Plusieurs étages, s'il s'agit d'une opération fondamentale n-aire, $n > 2$; si $n = 1$, on reste dans le même étage.

binaire partiellement complet (= quasi-polynôme). Considérons une descente, soit une suite de ν fusions $\rho_i : a_i\ b_i \rightarrow c_i$, transformant le mot S, de longueur $\ell(S)$, en mot T, de longueur $\ell(T) = \ell(S) - \nu$. $S \equiv Ua_1\ b_1\ V$, où U ou V peuvent être vides. On indique l'application de ρ_1 en écrivant $S_1 \equiv U(a_1\ b_1)V$, où $(a_1\ b_1)$ est considéré comme la seule lettre c_1. De la même manière, on applique ρ_2 à S_1, obtenant S_2 ; et ainsi de suite. Chaque fusion ajoute une paire de parenthèses binaires, et diminue la longueur de mot d'une unité. $S_\nu = T$ est donc le mot S pourvu de ν paires de parenthèses binaires. Une descente détermine le parenthésage partiel qui sera complet si $\nu = \ell(S) - 1$, c'est-à-dire $\ell(T) = 1$. L'inverse est aussi vrai, à des inversions triviales de l'ordre près. Ces parenthésages partiels ne sont pas quelconques, mais strictement binaires, parce que les parenthèses indiquant des fusions successives de lettres voisines procèdent de l'intérieur à l'extérieur. Donc S_ν (et aussi chaque mot intermédiaire) est composé de sous-mots en parenthésage binaire complet enfermés dans des paires de parenthèses maximales, séparés par des parties (sous-mots) inertes, possiblement vides.

De même pour une montée qui est une descente en ordre inverse.

Notons donc, dans une chaîne générale $C^W_{W_0}$, les divers sommets $S_i \equiv W_{\lambda_i}$, $i = 1, \ldots, \mu$, $0 \leqslant \lambda_1 < \ldots < \lambda_\mu \leqslant \lambda$, et A_i, B_i leurs pentes, ou, ce qui revient au même, leurs parenthésages binaires partiels, et F_i, $i = 1, \ldots, \mu - 1$, les mots aux fonds des vallées. La chaîne s'écrit donc

$$W_0 = A_1(S_1),\ B_1(S_1) \equiv A_2(S_2),\ \ldots,\ B_{i-1}(S_{i-1}) \equiv A_i(S_i),\ \ldots,\ B_\mu(S_\mu) \equiv W_\lambda \equiv W,$$
$$(= F_1) \qquad\qquad (= F_i)$$

où A_1 ou B_μ peuvent être vides : $W_0 \equiv S_1$ ou $S_\mu \equiv W$.

Les identités conditionnelles sont des chaînes fermées d'une seule montagne de hauteur $\ell - 1$ avec sommet $S \equiv a_1, \ldots, a_\ell$:

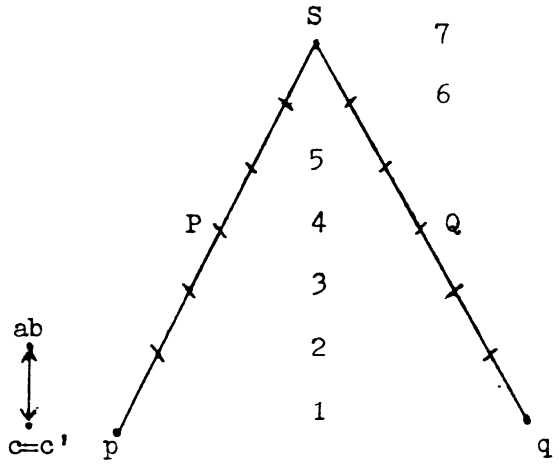
$$p \rightarrow \ldots \rightarrow a_1, \ldots, a_\ell \rightarrow \ldots \rightarrow q$$
$$\Longrightarrow\ p = q\ ,$$

qu'on peut écrire

$$p = P(S),\ Q(S) = q \Longrightarrow p = q\ .$$

Remarquons encore que le profil d'une montagne de hauteur 1, correspondant à $ab = c$, c'est-à-dire

$$(c \rightarrow ab,\ ab \rightarrow c') \Longrightarrow (c \rightarrow c')\ ,$$



est toujours fermé dans un monoïde, en conséquence de l'uniformité de l'opération $c = c'$.

6. Non-validité du théorème d'une seule montagne.

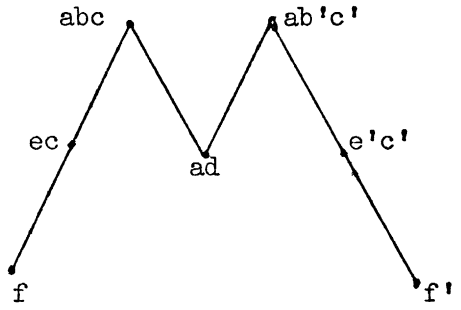
Dans notre conférence antérieure [9], on a montré que, pour un monoïde symétrique, chaque chaîne peut être transformée en une chaîne logiquement équivalente, en forme d'une seule montagne ([2]). Ce théorème admet quelque généralisation légère ; mais il n'est pas valable pour un monoïde quelconque. On le voit par l'exemple trivial ("ad hoc") d'un monoïde de 10 éléments et de 6 relations :

$$M = \{a\ ,\ b\ ,\ c\ ,\ b'\ ,\ c'\ ,\ d\ ,\ e\ ,\ e'\ ,\ f\ ,\ f'\ ;$$
$$bc = d = b'c'\ ,\quad ab = e\ ,\quad ec = f\ ,\quad ab' = e'\ ,\quad e'c' = f'\} .$$

M admet une chaîne élémentaire avec profil en forme de " M ", et est effectivement non associatif ; c'est-à-dire, M ne peut être plongé dans (= complété à) un demi-groupe, parce que, dans un demi-groupe,

$$f \to ec \to (ab)c = a(bc) \to ad \to a(b'c') = (ab')c' \to e'c' \to f' \implies f = f' ,$$

mais $f \neq f'$ dans M . On ne peut pas éliminer la selle de la forme M : a , b , c , b' , c' sont des éléments premiers (indécomposables) absolus ; d , e , e' se factorisent en deux tels éléments premiers ; f et f' possèdent chacun une seule factorisation en trois premiers, à savoir $f = (ab)c$, $f' = (ab')c'$. Il n'y a plus d'autres factorisations. Donc il n'y a pas de mot qui se contracte à plus d'une seule lettre bien déterminée. En particulier, il n'y a pas de mot (de longueur quelconque) qui se contracte à f et à f' .



7. Modèle des "courants".

Le profil d'une chaîne donne seulement une information fragmentaire sur la chaîne, si l'on ne le munit pas des écritures de la chaîne elle-même. On construit donc une représentation plus significative, captant et exposant toute la structure de la chaîne dans une figure à deux dimensions essentielles du plan cartésien x - y (ou t pour "temps") ou de la sphère. Essentiellement, on répète la prescription de

---

([2]) C'est-à-dire qu'on peut trouver un mot "long" V , tel qu'il y a une chaîne d'expansions $c^{V}_{W_0}$ et une chaîne de contractions $c^{W_0}_{V}$.

l'arrangement graphique des chaînes de mots, donnée dans nos travaux antérieurs, dès 1950. On peut être concis, parce que les variations sont légères, malgré la différence considérable de l'interprétation qui est maintenant la plus directe.

Ecrivons le mot $W_j = a_1^j , \dots , a_i^j , \dots , a_{\ell_j}^j$, $\ell_j = \ell(W_j)$; a_i^j représente une lettre dans la place de coordonnées (i , j) . $\tau_j : W_{j-1} \to W_j$ est :

Ou bien une fission $\sigma_j : a_{\nu_j}^{j-1} \to a_{\nu_j}^j \, a_{\nu_j+1}^j$,

Ou bien une fusion $\rho_j : a_{\nu_j}^{j-1} \, a_{\nu_j+1}^{j-1} \to a_{\nu_j}^j$.

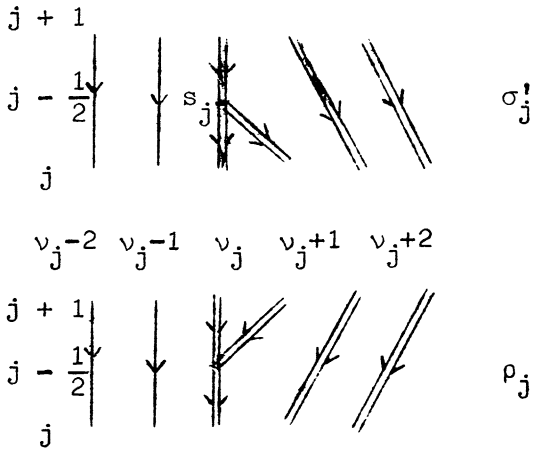
On engendre une relation d'équivalence parmi les places (i , j) par

$$a_i^j = \begin{cases} a_i^{j-1} , & i < \nu_j , \\ a_{i-1}^{j-1} , & (i > \nu_j + 1) \iff (\tau_j = \sigma_j) , \\ a_{i+1}^{j-1} , & (i > \nu_j) \iff (\tau_j = \rho_j) . \end{cases}$$

On peut imaginer chaque classe d'équivalence comme une fibre, avec la lettre commune comme nom propre, liant $(i , j - 1)$ et $(i + \delta , j)$ si, et seulement si, $a_i^{j-1} = a_{i+\delta}^j$, où δ est une valeur bien déterminée parmi $0 , -1 , +1$. On complète la figure en introduisant, pour chaque τ_j , un sommet s_j de coordonnées $(\nu_j , j - \frac{1}{2})$, et en liant chacun à trois fibres déjà construites par les places non équivalentes

$$(\nu_j , j - 1) , (\nu_j , j) \text{ et } (\nu_j + 1 , j) , \qquad \text{si } \tau_j = \sigma_j ,$$
$$(\nu_j , j - 1) , (\nu_j + 1 , j - 1) \text{ et } (\nu_j , j) , \qquad \text{si } \tau_j = \rho_j .$$

Les fibres pourvues de leur orientation naturelle sont appelées "courants".

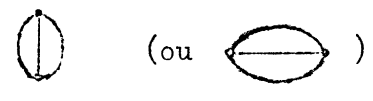


Pour les chaînes spéciales C_a^b fermées (avec conclusion $a = b$), on lie encore $W_0 \equiv a = a_1^0$ avec $W \equiv W_{2n} \equiv b = a_1^{2n}$ par un arc en dehors de la figure déjà

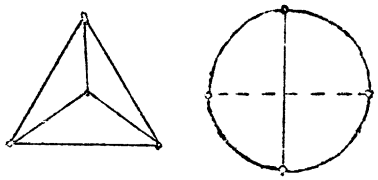
construite. (On peut le faire convenablement en passant par l'infini, soit du plan projectif, soit de la sphère des nombres complexes.) On obtient ainsi une division de la sphère, ou du plan, avec $2n$ sommets, $3n$ arêtes, et $n + 2$ faces. Chaque sommet a la multiplicité 3 ; les faces sont des polygones.

8. Le modèle circulaire.

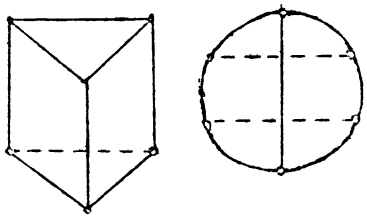
En cheminant sur les arêtes, sans nécessairement garder leur orientation naturelle (d'ailleurs ce n'est pas toujours possible), on peut visiter chaque sommet une seule fois en parcourant la circonférence d'un cercle composé de $2n$ arêtes comme arcs et laissant d'un côté ou de l'autre une arête à chaque sommet. En aplatissant la sphère à un disque avec cette circonférence, on obtient justement le modèle circulaire avec les n arêtes non parcourues devenues deux classes de cordes. Dans notre thèse [8], le circuit était bien déterminé par l'axe central de la chaîne, et l'orientation se préservait. Ce n'est plus le cas ici. Voici les configurations les plus simples (jusqu'à $n = 4$) en forme de polyèdres et de modèles circulaires.



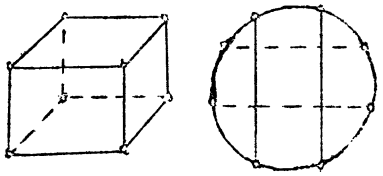
n = 1

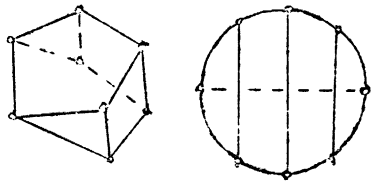


n = 2



n = 3





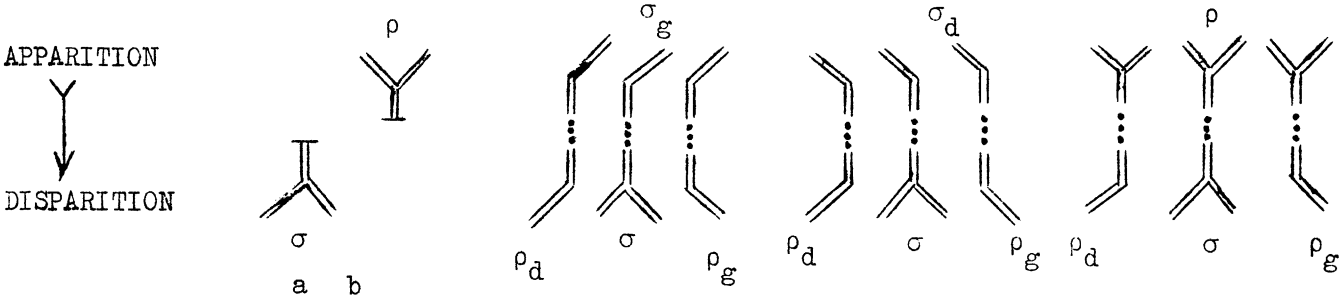
n = 4

En plus de la perte d'orientation, mentionnons d'autres différences entre l'interprétation présente du modèle circulaire et celle de ma thèse [8]. Ici, les $2n$ sommets représentent les $2n$ substitutions de l'hypothèse C_a^b , sans spécifier d'ailleurs leur caractère expansif ou contractif qui dépend d'un certain choix d'orientation pour les arêtes (= arcs et cordes). Les $3n$ arêtes représentent les $3n$ lettres des chaînes fermées (= "associatives"), respectivement les $3n + 1$ lettres des chaînes ouvertes (= "non associatives") par choix d'une arête et sa coupure en deux demi-arêtes.

Polyèdres, prototypes, questions ouvertes. - Les polyèdres sont les prototypes de ma thèse [8] avec un changement correspondant d'interprétation. L'analyse de ces

situations pose des questions appartenant à la théorie des graphes et à l'analyse combinatoire. L'analyse analogue dans ma thèse n'est même pas encore achevée.

Types des lettres dans une chaîne. - L'analyse des types des $3n$, respectivement $3n + 1$ lettres (arêtes et demi-arêtes), diffère un peu de celle de ma thèse où elle s'appliquait aux lettres barrées (inverses formels) seulement. A l'exception de a et b de C_a^b , les autres $3n - 1$ lettres sont nées et disparaissent dans la chaîne. Elles se divisent en $3 \times 3 = 9$ types suivant les circonstances de leur apparition et disparition. Notons les apparitions, soit à gauche ou à droite du produit d'une fission σ_g , σ_d , soit par fusion ρ , et les disparitions, soit à gauche ou à droite d'une fusion ρ_g , ρ_d , soit par fission σ .



Dans les chaînes générales de mots C_X^Y , il y a aussi des lettres commençant dans X et des lettres finissant dans Y . Le type existant pendant toute la chaîne peut être ignoré : une telle chaîne est une juxtaposition de chaînes plus courtes. Plus généralement, on peut ignorer des juxtapositions de chaînes, avec ou sans lettres séparant. L'étude de ces configurations, réduites à celles des chaînes connexes, et des transformations des chaînes équivalentes ayant certaines formes normales, est encore à faire.

La non-associativité d'un monoïde M demande l'existence d'au moins une chaîne non associative C_a^b , $a \neq b$, dans M . $\exists\, C_a^b \iff a^\varphi = b^\varphi$. On appelle (a , b) , un couple non associatif de M .

Si M est fini ou dénombrable (on ne considère pas d'autres monoïdes), on peut énumérer l'ensemble de ses chaînes de mots suivant, e. g. r , $r \geqslant \lambda$, ℓ_m , i_m , ou $r = \lambda + \ell_m + i_m$, etc., où λ est la longueur de la chaîne, ℓ_m la longueur maximale des mots de la chaîne, i_m l'indice maximal des lettres apparaissant dans la chaîne ; car le nombre des chaînes avec r donné est fini. Pour les chaînes commençant avec une seule lettre, chaînes demi-spéciales, il suffit d'énumérer suivant s , $s \geqslant \lambda$, i_m , ou $s = \lambda + i_m$; a fortiori, pour les chaînes spéciales. Si on

sait que M est non associatif, on est sûr de rencontrer une première chaîne non associative, donc un premier couple non associatif, même chaque chaîne et chaque couple non associatifs.

Images homomorphes. - Chaque couple non associatif c, et chaque ensemble C de couples non associatifs de M, engendre une congruence E_c, respectivement E_C, sur M, telle que M/E_c, M/E_C engendrent le même demi-groupe

$$D = D_M = D_{M/E_c} = D_{M/E_C} .$$

En particulier, l'ensemble de tous les couples non associatifs engendre $E_{M|M}$, la trace sur M de la congruence E_M sur $F_{|M|}$. $M/E_{M|M} \simeq M^\varphi$ est l'image homomorphe associative la plus grande de M. $D_M \simeq D_{M^\varphi}$. M^φ peut être identifié avec un extrait (une partie) de la table de multiplication de D.

Présentations standards monoïdales. - Chaque présentation Π d'un demi-groupe peut être standardisée à un monoïde, une présentation finie à un monoïde fini. Inversement, chaque monoïde M est une présentation standard du demi-groupe D_M.

Les extensions d'un monoïde fini par adjonction successive de mots engendrent une classe récursivement énumérable (r. e.) de monoïdes finis, chacune extension de son prédécesseur, tous engendrant le même demi-groupe D_M.

Réduction du problème des mots de D_Π au problème de l'associativité des monoïdes d'une classe r. e. $\mathfrak{M}_\Pi$. - L'existence d'une "épreuve d'associativité", c'est-à-dire d'un algorithme résolvant le problème d'associativité, pour les monoïdes d'une classe $\mathfrak{M}_\Pi$ (obtenue par extensions successives en joignant des mots, et fermée par rapport aux images homomorphes), au moins ceux qui engendrent le même demi-groupe, permet de construire (trouver) les images homomorphes associatives les plus grandes M^φ (parmi les M) appartenant à $\mathfrak{M}$. Ceci revient à construire des parties aussi grandes que l'on veut de la table de multiplication de D, ce qui résout le problème des mots de D.

L'insolubilité du problème de l'associativité des monoïdes, même pour une classe r. e. assez restreinte de monoïdes $\mathfrak{M}_\Pi$, est établie par l'existence bien connue de demi-groupes individuels à présentation finie Π avec problème des mots insoluble [POST, TURING, MARKOV, CEJTIN, SCOTT].

La réduction inverse : Le raisonnement précédent se laisse évidemment inverser. En partant d'un monoïde fini quelconque M, l'existence d'une "épreuve des mots" pour D_Π entraîne la solution du problème de l'associativité pour les monoïdes de $\mathfrak{M}_M$. C'est ainsi, parce que les éléments des monoïdes de $\mathfrak{M}_M$, extensions de la

présentation monoïdale M , s'expriment finalement comme des mots de D_M .

On peut donc conclure à l'équivalence des deux problèmes dans le sens précis expliqué ci-dessus.

Des questions ouvertes concernent le problème de l'associativité pour une classe r. e. quelconque de monoïdes finis, en particulier pour la classe de "tous" les monoïdes finis. On doit préciser que cette dernière signifie la classe des monoïdes finis en notation standard $|M| = \{a_1 , \ldots , a_n\}$, $n \in \underline{N}$. Cette classe $\mathfrak{M}$ contient des représentants de chaque type d'isomorphisme de monoïdes finis, donc aussi des copies fidèles de toutes les classes r. e. $\mathfrak{M}_M$ considérées ci-dessus. Nous savons seulement que le degré d'insolubilité du problème de l'associativité des monoïdes des $\mathfrak{M}$ est $\geqslant$ au degré d'insolubilité du problème des mots des demi-groupes à présentation finie.

BIBLIOGRAPHIE

[1] COHN (P. M.). - Universal algebra. - New York, Harper and Row, 1965 (A Harper international Student Reprint).

[2] EVANS (T.). - The word problem for abstract algebras, J. of London math. Soc., t. 26, 1951, p. 64-71.

[3] EVANS (T.). - Embeddability and the word problem, J. of London math. Soc., t. 28, 1953, p. 76-80.

[4] GRÄTZER (G.). - Universal algebra. - Princeton, D. Van Nostrand, 1968 (University Series in higher Mathematics).

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

[6] MAL'CEV (A.). - Über die Einbettung von assoziativen Systemen in Gruppen [en russe, avec sommaire en allemand], Mat. Sbornik, N. S., I, t. 6, 1939, p. 331-336 ; II, t. 8, 1940, p. 251-264.

[7] MAL'CEV (A.). - Sur les groupes topologiques locaux et complets, Doklady Akad. Nauk SSSR, N. S., t. 32, 1941, p. 606-608.

[8] TAMARI (D.). - Monoïdes préordonnés et chaînes de Mal'cev, Bull. Soc. math. France, t. 82, 1954, p. 53-96 (Thèse Sc. math. Paris, 1951).

[9] TAMARI (D.). - Problèmes d'associativité des monoïdes et problèmes des mots pour les groupes, Séminaire Dubreil-Pisot : Algèbre et théorie des nombres, 16e année, 1962/63, n° 7, 29 p.

[10] TAMARI (D.). - Associativity problems and word problems, in "Decision problems in group theory". - Amsterdam, North-Holland publishing Company (sous presse).

(Texte reçu le 12 juillet 1971)

Dov TAMARI
Dept of Mathematics
State University of New York
4246 Ridge Lea Road
BUFFALO, N. Y. 14226 (Etats-Unis)