ANNALES SCIENTIFIQUES
DE L'UNIVERSITÉ DE CLERMONT-FERRAND 2
Série Mathématiques

DOV TAMARI

Sur quelques problèmes d'associativité

Annales scientifiques de l'Université de Clermont-Ferrand 2, tome 24, série *Mathématiques*, n° 3 (1964), p. 91-107

<http://www.numdam.org/item?id=ASCFM_1964__24_3_91_0>

SUR QUELQUES PROBLÈMES D'ASSOCIATIVITÉ

Dov TAMARI

INTRODUCTION -

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 relation-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 exprimé par une simple identité *inconditionnelle*, notée A_2 :

$$(A_2) : x(yz) = (xy)z,$$

on démontre alors, par induction, qu'on a aussi toutes les identités inconditionnelles $A_n(P,Q)$:

$$(A_n(P,Q)) : P(x_o, \ldots, x_n) = Q(x_o, \ldots, x_n),$$

où n est un nombre naturel > 2, et $P = P^n$, $Q = Q^n$ dénotent deux parenthésages distinctes (formellement correctes) quelconques d'un mot quelconque $x_o \ldots x_n$ de longueur n + 1. Le terme "inconditionnel" veut dire "pour tous les x, y et z, respectivement pour tous les $x_o, \ldots, x_n$, appartenant au système multiplicatif considéré". Il est bien évident, que ceci n'a plus de sens dans le cas partiel, mais se laisse remédier facilement d'une manière ou d'une autre ; p.e. en ajoutant la condition "si les deux membres existent (= ont un sens) simultanément", ce qu'on peut exprimer :

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

Formellement on pourrait aussi compter comme A_1 l'uniformité de l'opération A_1 : $xy = s$, $xy = t \Longrightarrow s = t$, en admettant aussi $P = Q$. Alors on peut montrer, (et on le doit) par une induction facile, que $A_1 \Longrightarrow A_n(P,P)$ pour tout $n > 1$.

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 dans le cas, où il existe une chaîne de déplacements simples - chaque fois une seule paire de parenthèses change - de longueur $l > 1$:

$$P = P_o \longrightarrow P_1 = P' \longrightarrow P'' = P_2 \longrightarrow \ldots \longrightarrow P_i \longrightarrow P_i' \longrightarrow \ldots \longrightarrow P_{l-1}' = P_l = Q,$$

où tous les *monômes intermédiaires* $P_1, \ldots, P_{l-1}$ ont aussi un sens simultanément avec P et Q. On fabrique facilement des exemples "ad hoc" pour montrer qu'autrement les lois A_n, $n > 2$, sont effectivement indépendantes de A_2. Etant donné qu'il y a $k_n = \left(\frac{2n}{n+1}\right)/n$ parenthésages distinctes de

n paires de parenthèses, il y a $\left(\frac{k_n}{2}\right) = \frac{1}{2} k_n (k_n - 1)$ 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 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 triplets d'éléments, on doit aussi bien regarder les quadruples, quintuples, etc. 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. On remarque encore que la structure $A = \bigcup_1^\infty A_n$ satisfait l'équivalence logique $A \Longleftrightarrow \lim_{n\to\infty} A_n$ parce que, évidemment, $A_n \Longrightarrow A_{m<n}$; ici $\cup$ dénote aussi la conjonction logique.

Ceci suffira pour motiver le grand intérêt d'une recherche plus détaillée de la structure des lois associatives d'un point de vue très général, appartenant à la logique mathématique et aux fondements. Dans ce contexte, on se propose désormais des problèmes d'une apparence trompeuse de particularité étroite ; mais tout en gardant le charme d'un problème particulier assez difficile, bien que soluble, il semble s'agir d'un prototype d'une nouvelle classe d'algèbres, ou, aussi bien, de systèmes partiellement ordonnés, qui jusqu'à présent n'ont pas été objet d'une étude consciente.

Notons T_n l'ensemble de toutes les parenthésages sur des mots de longueur $n+1$ $x_o x_1 \ldots x_n$ - donc card $T_n = k_n$ - et $T = \bigcup_{n=o}^\infty T_n$ le système gradué de toutes les parenthésages. Il n'est même pas évident "a priori" que les systèmes T_n sont connexes dans ce sens qu'il existe, pour chaque couple $P, Q \in T_n$, au moins une chaîne de déplacements simples de parenthèses suivant la loi A_2 :

$$P = P_o, P_1, \ldots, P_{l-1}, P_l = Q \quad \text{avec} \quad P_{i+1} = P'_i,\ i = 0, \ldots, l,\ P_i \in T_n.$$

La réponse positive est un corollaire immédiat d'un de nos premiers résultats.

Le système T est un système multiplicatif gradué avec une composition naturelle "o" définie par $AoB \equiv (AB)$, c'est-à-dire la juxtaposition AB à l'intérieur d'une paire de parenthèses ; $\equiv$ signifie l'identité graphique. Evidemment $AoB = C$ ou $A = A^d \in T_d$, $B = B^e \in T_e$, $C = C^f \in T_f \Longrightarrow f = d + e + 1$. Inversement, chaque $C = C^f$ de dim $f > 0$ possède une et une seule décomposition en deux facteurs (directs), bien déterminés $A = A^d$, $B = B^e$ tels que $C = AoB$. Il y a une seule parenthésage vide, ou de dim 0, correspondant aux monômes (= mots pourvus de parenthésages) d'une lettre seule. Toutes les parenthésages sont obtenues par la composition canonique "o" de proche en proche, en partant de la parenthésage vide $A^o = a_o$. Ainsi on obtient, avec des notations évidentes, la seule $A^1 = A^o oA^o = (a_o a_1)$, les deux A^2 qu'on notera $A^2 = A^o oA^1 = (a_o(a_1 a_2))$ et $A'^2 = A^1 oA^o = ((a_o a_1)a_2)$, les cinq A^3, les 14 A^4, etc.

Une parenthésage C^f possède, en général, deux représentations bien déterminées comme parenthésages de parenthésages : $C^f = C^f(x_o, \ldots, x_f) = C^f(C^o, \ldots, C^o)$ et $C^f = A^d oB^e = C^1(A^d, B^e)$ la dernière seulement si $f > 0$; les deux se confondent si et seulement si $f = 1$. Si $f > 1$ il y a aussi, pour tous les i, $1 < i < f$, des représentations $C^I(C_o^{f_o}, \ldots, C_i^{f_i})$ avec $f = i + f_o + \ldots + f_i$, mais elles ne sont plus, en général, uniquement déterminées.

Le système de parenthésages T est canoniquement isomorphe au système multiplicatif complet engendré par un seul générateur libre non-associatif, c'est-à-dire à la généralisation non-associative du semi-groupe cyclique, qu'on peut identifier au système des nombres naturels. De ce point de vue T est donc la généralisation naturelle non-associative des nombres naturels. $T = (T, o)$ est muni d'une structure de préordre naturel, noté $\longrightarrow$, bien déterminé par :

1/ la loi *demi-associative* A_2 : $Ao(BC) \longrightarrow (AB)oC$, c'est-à-dire $(A(BC)) \longrightarrow ((AB)C)$, qui est la généralisation de l'opérateur successeur ou aussi $Ao(BoC) \longrightarrow (AoB)oC$;

2/ fermeture transitive : $A \longrightarrow B,\ B \longrightarrow C \Longrightarrow A \longrightarrow C$;

3/ l'invariance (= compatibilité ou homogénéité) de $\longrightarrow$ avec la composition "o", c'est-à-dire les multiplications, ou translations, gauches et droites :

$$A \longrightarrow B \Longrightarrow XoA \longrightarrow XoB,\ AoX \longrightarrow BoX, \quad \text{c'est-à-dire} \quad (XA) \longrightarrow (XB),\ (AX) \longrightarrow (BX).$$

On verra dans la suite, assez vite, que $\longrightarrow$ est, en fait, un ordre (partiel) strict.

On voit facilement, que dans la définition de la relation $\longrightarrow$ on peut remplacer les propriétés 1/ et 3/ par la propriété de substitution suivante : Si C^f possède une représentation conte-

nant A^2, c'est-à-dire au moins un de C^i, $C_o^{f_o}, \ldots,$ ou $C_i^{f_i}$ est A^2, et si $C^{f'}$ s'obtient de C^{f_1} par la substitution d'une A^2 par une $A^{2'}$, alors $C^f \longrightarrow C^{f'}$. Mais cet exposé est dédié à la démonstration du

THEOREME :

Les systèmes $T_n = (T_n, \longrightarrow)$ *sont des treillis* ; donc $(T_n, o, \longrightarrow)$ est réticulé. L'énoncé de ce théorème se trouve déjà dans la thèse de Tamari (Paris 1951), employant aussi les mêmes notations, fondamentales introduites dans le paragraphe suivant, mais sans démonstration. Les traits principaux de la démonstration donnée ici en particulier la plupart des lemmes et propositions importants, sont essentiellement dus à un travail de Madame Haya Freedman de l'année 1958. Même avec les nouveaux perfectionnements apportés ici, c'est encore une démonstration assez formidable pour un théorème d'une apparence si modeste. Mais il est à espérer, que les notions et méthodes employées ici ont une portée et une signification plus large, et qu'elles se prêtent à des généralisations importantes. Un exemple dans une direction est la généralisation de l'algorithme d'Euclide du dernier paragraphe ; mais il existe certainement aussi d'exemples d'une toute autre nature.

2 - PRELIMINAIRES -

Un mot de $n+1$ lettres $x_o, \ldots, x_n$ pourvu d'une parenthésage binaire formellement correcte est dit monôme de dimension n (dim $n \geqslant 0$). En plus des parenthèses essentielles, habituelles, on compte aussi la paire extérieure superflue (qu'on n'écrit pas souvent). En abstrayant complètement de la nature des lettres, elles ne signifient que des indications nécessaires pour localiser les parenthèses de la parenthésage. On se limite dans la suite aux parenthésages abstraites qu'on pourrait aussi appeler "patrons monômiaux". Le mot monôme signifiera ici parenthésage ou monôme de parenthésage (= parenthésage de parenthésages). L'application de cette théorie aux monoïdes quelconques (systèmes multiplicatifs partiels non-associatifs) est immédiate.

On dénote : la place immédiatement avant la lettre x_i, donc (si $i > 0$) la place immédiatement après x_{i-1} par l'indice i ; le nombre d'ouvertures de parenthèses à la place i par a_i, $b_i, \ldots,$ e_i, etc. Il est bien connu, et on peut le voir facilement, qu'une parenthésage est déjà bien déterminée par ses ouvertures, donc p.e. par la suite $E = E^n = \langle e_o, \ldots, e_i, \ldots, e_n \rangle$ avec les conditions assez évidentes :

(*)

$$\begin{array}{r} e_n = 0 \\ e_{n-1} + e_n \leqslant 1 \\ e_{n-2} + e_{n-1} + e_n \leqslant 2 \\ \ldots\ldots\ldots\ldots\ldots \\ e_i + \ldots\ldots + e_n \leqslant n - i \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ e_1 + \ldots\ldots + e_n \leqslant n - 1 \\ e_o + e_1 + \ldots\ldots + e_n = n \end{array}$$

ou aussi bien comme

$$\begin{array}{r} e_n < 1 \\ e_{n-1} + e_n < 2 \\ e_{n-2} + e_{n-1} + e_n < 3 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ e_i + \ldots\ldots + e_n < n + 1 - i \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ e_1 + \ldots\ldots + e_n < n \\ e_o + e_1 + \ldots\ldots + e_n = n. \end{array}$$

ou encore :

$$\begin{array}{r} e_o \geqslant 1 \\ e_o + e_1 \geqslant 2 \\ \ldots\ldots\ldots\ldots\ldots \\ e_o + e_1 + \ldots + e_i \geqslant i + 1 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ e_o + e_1 + \ldots + e_{n-1} = n \end{array}$$

ou

$$\begin{array}{r} e_o > 0 \\ e_o + e_1 > 1 \\ \ldots\ldots\ldots\ldots\ldots \\ e_o + e_1 + \ldots + e_i > i \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ e_o + e_1 + \ldots + e_{n-1} = n. \end{array}$$

On a donc réduit les parenthésages de dim n à certaines suites finies de nombres naturels $0, 1, \ldots, n$. Pour le moment on garde encore e_n, bien qu'étant toujours = 0, on l'abandonnera dans la suite. La composition A^d o $B^e = (A^d\, B^e) = C^{f=d+e+1}$ devient :

$$\langle a_o, \ldots, a_d \rangle \, o \, \langle b_o, \ldots, b_e \rangle = \langle c_o, \ldots, c_f \rangle,$$

où :

$$c_o = a_o + 1,\ c_i = a_i\ (0 < i < m),\ c_{m+1+j} = b_j\ (0 < j < n).$$

Aussi, inversement, *chaque telle suite de nombres naturels représente une et une seule parenthésage*. On peut le montrer "ab ovo", ou, p.e., en construisant un système isomorphe au système non-associatif libre d'un seul générateur $x = x_o$, en posant $E^o = <0>$ et appliquant la composition, notée "o" (pour cause comme au-dessus) de proche en proche :

$$<a_o, \ldots, a_m> o <b_o, \ldots, b_n> = <a_o + 1, a_1, \ldots, a_m, b_o, \ldots, b_n>,$$

l'isomorphisme étant déterminé par $x_o \longleftrightarrow <0>$. $<0>$ satisfait évidemment (*) et est sa seule solution pour $n = 0$. Si A^m, B^n satisfont (*), $A^m \circ B^n = C^{l=m+n+1}$ le fait aussi, parce que :

$$c_l = b_n = 0$$

$$c_{l-1} + c_l = b_{n-1} + b_n \leqslant 1$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$c_{m+2} + \ldots + c_l = b_1 + \ldots + b_n \leqslant n - 1 \qquad m + 2 = l - (n - 1)$$

$$c_{m+1} + \ldots + c_l = b_o + \ldots + b_n = n \qquad m + 1 = l - n$$

$$c_{m+} \quad + c_l = a_m + b_o + \ldots + b_n = 0 + n = n < n + 1 \qquad m = l - (n + 1)$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$c_1 + \ldots + c_m + \ldots + c_l = a_1 + \ldots + a_m + n \leqslant m - 1 + n < l - 1$$

$$c_o + \ldots\ldots\ldots\ldots + c_l = a_o + 1 + a_1 + \ldots + a_m + n = 1 + m + n = l.$$

Inversement donné un C^l quelconque satisfaisant (*), on peut construire une (et une seule) décomposition $C = A^m o B^n$ en déterminant parmi les indices i, $0 \leqslant i < l$, l'indice le plus grand tel, qu'on a une égalité $c_{l-i} + \ldots + c_l = i$; Il y en a toujours parce qu'on a au moins une égalité pour $i = 0$. On le note n, et on pose $m = l - 1 - n$; $0 \leqslant m < l$; $m = 0 \Longleftrightarrow n = l - 1$. On a alors :

$$c_l = 0$$

$$c_{l-1} + c_l \leqslant 1$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$c_{m+2} + \ldots + c_l \leqslant n - 1$$

$$c_{m+1} + \ldots + c_l = n,$$

ce que satisfait (*) en posant :

$$<c_{m+1}, \ldots\ldots, c_l> = <b_o, \ldots, b_n>.$$

Il reste à montrer qu'on peut aussi poser :

$$<c_o - 1, \ldots, c_i, \ldots, c_m> = <a_o, \ldots, a_m> \quad \text{satisfaisant (*).}$$

Si $m = 0 \Longleftrightarrow l = n + 1 \Longleftrightarrow l - n = 1$, on a $c_o + c_1 + \ldots + c_l = l = n + 1$, donc $c_o = l - (c_1 + \ldots + c_l) = l - n = 1$, et $<c_o - 1> = <0>$ satisfait (*). Si $m = l - n - 1 > 0 \Longleftrightarrow l > n + 1$:

$$c_m + c_{m+1} + \ldots + c_l = c_m + n < n + 1 \Longrightarrow c_m = 0$$

$$c_{m-1} + c_m + c_{m+1} + \ldots + c_l = c_{m-1} + c_m + n < n + 2 \Longrightarrow c_{m-1} + c_m \leqslant 1$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$c_1 + \ldots + c_m + n < l - 1 = m + n \Longrightarrow c_1 + \ldots + c_m \leqslant m - 1$$

$$c_o + c_1 + \ldots + c_m + n = l = 1 + m + n \Longrightarrow (c_o - 1) + c_1 + \ldots + c_m = m.$$

Naturellement, on aurait aussi bien pu choisir les suites de fermetures, ou une autre notation de parenthésage, comme, p.e., les groupes de points de Peano. Des études des relations intéressantes entre ces diverses genres de notation ont été amorcées dans la thèse [3] (voir aussi [4]).

Les n-1 paires de parenthèses essentielles d'une parenthésage se divisent en deux classes : *premières* (I) ou *gauches* et *secondes* (II) ou *droites*, suivant qu'elles enferment le facteur gauche ou droit à l'intérieur de la parenthèse immédiatement superordonnée. On peut les caractériser comme suit : les ouvertures de (I) sont immédiatement précédées sur la même place d'autres ouvertures, au moins celle de leur superordonnée, mais leur fermetures ne sont suivies d'aucune fermeture sur leur place ; les ouvertures de (II) ne sont précédées d'aucune ouverture sur la même place, mais leur fermetures sont immédiatement suivies sur la même place de la fermeture de leur superordonnée. Dans notre notation de vecteurs $E^n = \langle e_o, \ldots, e_n \rangle$ cette caractérisation s'exprime : les ouvertures (II) sont justement représentées par les premières unités du groupe des e_i, $e_i > 0$, sur la place i ; les autres $e_i - 1$, autant que $e_i - 1 > 0$, sont des ouvertures (I). P.e., on a les deux cas extrêmes : 1 toutes les parenthèses sont droites (II), c'est-à-dire $e_o = e_1 = \ldots = e_{n-1} = 1$; ou bien 0 toutes sont gauches (I), et alors $e_o = n$ et $e_1 = \ldots = e_{n-1} = 0$.

Une application élémentaire de la loi associative A_2 consiste en un déplacement simple d'une parenthèse en changeant son caractère, transformant une parenthèse droite en une gauche, ou bien une gauche en une droite. La première transformation correspond à ce que nous avons distingué comme notre demi-associativité ; la seconde transformation correspond à l'inversion de la flèche, la demi-associativité duale.

Notons σ_i l'application élémentaire de la demi-associativité sur la place i, c'est-à-dire le transport d'une ouverture (II) de la place i ($e_i > 0$) à la place i', i'< i. On peut décrire la situation par le schéma.

$$\sigma_i \downarrow \quad \overbrace{\ldots\ldots}^{i'\ldots i}(A\ (B\ C))\ldots. \qquad E = \langle e_o, \ldots, e_{i'}, \ldots, e_i, \ldots, e_{n-1}\ e_n \rangle$$

$$\overbrace{((A\ B)\ C)\ \ldots}^{i'\ldots i} \qquad E\sigma_i = E^i = \begin{cases} \langle e_o^i, \ldots, e_{i'}^i, \ldots, e_i^i, \ldots, e_{n-1}^i\ e_n \rangle \\ \langle e_o, \ldots, e_{i'}+1, \ldots, e_i - 1, \ldots, e_{n-1}\ e_n \rangle, \end{cases}$$

où le monôme $A = A^{i-1-i'}$ s'étend de la place i' jusqu'à la place i-1. On a donc comme vecteur $A = \langle a_o, \ldots, a_{i-1-i'} \rangle$, où :

$$\begin{array}{l} a_{i-1-i'} = e_{i-1} = 0 \\ \ldots\ldots\ldots\ldots \\ a_{h-i'} = e_h \\ \ldots\ldots\ldots \\ a_1 = e_{i'+1} \\ a_o < e_{i'} \end{array} \qquad \Longrightarrow \qquad \begin{array}{r} e_{i-1} < 1 \\ e_{i-2} + e_{i-1} < 2 \\ \ldots\ldots\ldots\ldots \\ e_h + \ldots + e_{i-1} < i - h \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ e_{i'+1} + \ldots + e_{i-1} < i - 1 - i' \\ e_{i'} + e_{i'+1} + \ldots + e_{i-1} \geqslant i - i' \end{array}$$

La parenthésage nouvelle E^i obtenue par l'application d'une transformation σ_i ne possède pas nécessairement une parenthèse droite en moins et une gauche en plus que E, le nombre des parenthèses droites étant le nombre des composantes $e_h^i \neq 0$. En fait, en déplaçant la première des e_i parenthèses, une droite, la première des $e_i - 1$ restantes, autant que $e_i \geqslant 2$, qui était auparavant gauche, devient droite.

Notons les opérations inverses, c'est-à-dire les applications de la demi-associativité duale $(AB)C \longrightarrow A(BC)$ par des lettres τ. Si l'on voulait les noter τ_i si elles s'appliquent à une parenthèse (gauche, ouverture) sur la place i, donc si $e_i \geqslant 2$, τ_i n'aura pas de sens unique, sauf si $e_i = 2$; si $e_i > 2$, τ_i peut s'appliquer à une quelconque des $e_i - 1$ parenthèses gauches. D'autre part, σ_i^{-1} est bien déterminée par σ_i comme l'opération τ qui reconduit une certaine ouverture de la place i' à sa place antérieure i. On notera donc les τ plutôt suivant la place du but de l'ouverture $\sigma_i^{-1} = \tau_i$.

Si l'on veut, on peut encore donner un sens à σ_i , si $e_i = 0$, comme la transformation identique qui ne change rien : transformation impropre.

On exprime le fait que i' est aussi fonction de E en écrivant i'(E). Plus exactement i' dépend de $e_{i'}$, $e_{i'+1}, \ldots, e_{i-1}$, ce que ne semble pas particulièrement utile.

De la signification de "$\longrightarrow$" comme une suite d'applications de transformations σ, c'est-à-dire de transports de parenthèses proprement vers la gauche, il s'ensuit immédiatement que le préordre "$\xrightarrow{\quad}$" est un ordre : en allant toujours vers la gauche, on ne peut revenir sur une situation antérieure, ce qui montre l'anti-symétrie.

En appliquant successivement, aussi longtemps que possible, des transformations σ, à partir d'une parenthésage quelconque, on doit forcément s'arrêter après un nombre fini de pas, à la situation extrême $\mathbf{0} = <n, 0, \ldots, 0, 0>$, qui est donc l'élément le plus petit du système partiellement ordonné T_n.

En appliquant, au contraire, aussi longtemps que possible, des transformations τ, on doit s'arrêter, après un nombre fini de pas, au cas extrême $\mathbf{1} = <1, 1, \ldots 1, 0>$. Il suffit d'appliquer à $\mathbf{1}$ justement la suite des inverses σ bien déterminés dans l'ordre inverse pour arriver de nouveau à la parenthésage d'origine voulue. $\mathbf{1}$ est donc bien l'élément le plus grand de T_n.

Désormais nous repérons les monômes de dim n *fidèlement* par des vecteurs de partitions ordonnées particulières du nombre n en n parts entières non-négatives :

$$E = < e_0, \ldots, e_{n-1} > \quad \text{avec} \quad \sum_{\nu=0}^{i-1} e_\nu = S_0^i \geqslant i \quad \text{et} \quad S_0^n = n$$

On se limite, dans la suite, à la considération de ces vecteurs E, $E \in T_n$.

Les opérations, ou transformations, σ_i s'expriment ainsi : $E \in T_n \Longrightarrow$

$$E\,\sigma_i = E^i = < e_0^i, \ldots, e_{n-1}^i > \in T_n$$

avec :

$$e_i^i = e_i - 1, \quad e_{i'}^i = e_{i'} + 1 \quad \text{et} \quad e_\nu^i = e_\nu \quad (\nu \neq i, i')$$

pourvu que $e_i \neq 0$ (transformations propres) ; si $e_i = 0$, σ_i est l'application identique (ou impropre) ; i' est bien déterminée par :

$$(i' < h < i) \quad S_h^i < i - h \quad \text{(intervalles } [h, i[\text{ } \textit{déficitaires})$$

$$h = i' \quad S_i^i \geqslant i - i' \quad \text{(intervalle } \textit{suffisant}) \text{ ;}$$

autrement dit : parmi les intervalles $[h, i[$ "immédiatement devant i" l'intervalle $[i', i[$ est le plus petit intervalle suffisant (non déficitaire). Parmi les intervalles suffisants on distingue deux cas :

$S_i^i > i - i'$ est un intervalle $[i', i[$ *abondant*

$S_i^i = i - i'$ " " " $[i', i[$ *juste* (justement suffisant)

Il est commode de penser quelque fois en langage physique, à savoir, qu'une transformation propre σ_i est une *émission* d'un quantum (= unité 1) de la place i, vers la gauche, qui sera *absorbé* à la place i'. On a donc la règle qu'un intervalle déficitaire n'absorbe jamais ; donc reste déficitaire sous les transformations σ_i, donc aussi sous des suites, ou chaînes $\sigma_{i_1}\, \sigma_{i_2}, \ldots, \sigma_{i_l}$ de telles transformations. On peut appeler i - i' le *rendement* de l'émission de i, i' la *place* de la *barrière* absorbante $e_{i'}$, et $S_{i'}^i - (i - i')$ la *hauteur* de la barrière, qui est un nombre entier non négatif si la barrière est propre. On a donc la règle : un quantum émis sera absorbé par la première barrière (propre) à gauche qu'il rencontre. En d'autres termes : les intervalles déficitaires sont *transparents*, les barrières sont *opaques* ; sous l'influence d'émissions les régions de transparence ne changent qu'en s'étendant.

On note :

$$E^{ij} = (E^i)^j = E\ \sigma_i\, \sigma_j\ ,$$

et, plus généralement :

$$E^{i_1 i_2 \cdots i_l} = E\ \sigma_{i_1} \ldots \sigma_{i_l} = F$$

le monôme *dérivé* par une chaîne de transformations σ_i. On suppose que toutes les σ_i sont des transformations propres ; c'est-à-dire qu'on supprime dans une chaîne les transformations identiques : on ne les écrit pas.

L'ordre (partiel) défini par cette dérivation sera donc un ordre strict :

$$E > F \Longleftrightarrow E^{i_1 \cdots i_l} = F \qquad (l \geqslant 1) \text{ ;}$$

E > F si et seulement si F est dérivable de E par une chaîne propre.

3 - CHAINES NORMALES - REGLES DE COMMUTATION -

LEMME 1 : $j' < i < j \Longrightarrow j' \leqslant i'$.

Preuve : on doit montrer que pour tous les h, $i' < h < i$, les S^j_h sont déficitaires. En fait, S^j_i est déficitaire, car $j' < i < j$; de même tous les S^i_h ; donc aussi $S^j_h = S^i_h + S^j_i$, l'union de deux intervalles déficitaires adjacents étant déficitaire.

Le deuxième lemme est important : il caractérise les cas de non-permutabilité de deux transformations σ_i, σ_j de E, c'est-à-dire si $E^{ij} =$ ou $\neq E^{ji}$. Evidemment $E^{ij} \neq E^{ji} \Longrightarrow i \neq j$. On peut donc supposer, p.e., $i < j$.

LEMME 2 : $E^{ij} \neq E^{ji} \Longleftrightarrow j' = j'(E) = i$ & $S^j_i(E) = j - i$ (juste).

Dans ce cas $E^{ij} = E^{jii}$.

Preuve :

a) $i < j'$: les intervalles d'action des deux opérations sont séparés, et il n'y a aucune interférence :

$$E = < \ldots, \underset{+1}{e_{i'}}, \ldots\ldots, \underset{\sigma_i - 1}{e_i}, \ldots\ldots, \underset{+1}{e_{j'}}, \ldots\ldots, \underset{\sigma_j - 1}{e_j}, \ldots >$$

$$E^{ij} = E^{ji} = < \ldots, e_{i'}+1, \ldots, e_i - 1, \ldots, e_{j'}+1, \ldots, e_j - 1, \ldots >.$$

b) $j' < i$: par le lemme 1 $j' \leqslant i'$, c'est-à-dire, ou $j' < i'$, ou $j' = i'$; dans les deux cas on a :

$$E^{ij} = E^{ji}.\ E = < \ldots, \underset{+}{e_{j'}}, \ldots \underset{+}{e_{i'}}, \ldots, \underset{\sigma_i -}{e_i}, \ldots, \underset{\sigma_j -}{e_j}, \ldots > \quad \text{ou} \quad < \ldots \overset{\sigma_j}{\underset{\sigma_i}{e_{j'=i'}}} \ldots, \underset{-}{e_i} \ldots \underset{-}{e_j} \ldots >,$$

$$E^{ij} = E^{ji} = < \ldots, e_{j'}+1 \ldots, e_{i'}+1, \ldots, e_i - 1, \ldots, e_j - 1 \ldots > \quad \text{ou} \quad < \ldots e_{j'}+2, \ldots, e_i - 1 \ldots e_j - 1 \ldots >.$$

I) $S^j_i(E) > j - i$ (abondant) $\Longrightarrow S^j_i(E^i) = S^j_i(E) - 1 \geqslant j - i$ suffisant $\Longrightarrow j'(E^i) = j'(E) = i$;

c) $j' = i$:

II) $S^j_i(E) = j - i$ (juste) $\Longrightarrow S^j_i(E^i) = S^j_i(E) - 1 < j - i$ déficitaire $\Longrightarrow j'(E^i) < 1 \Longrightarrow j'(E^i) = i'(E)$.

On a donc dans le cas I) $\sigma_j(E^i) = \sigma_j(E)$ ($\sigma_i(E) = \sigma_i(E^j)$ est évident), donc $E^{ij} = E^{ji}$; mais dans le cas II) $\sigma_j(E^i) \neq \sigma_j(E)$. En résumé on a donc dans ce cas :

$$E = < \ldots, \underset{+}{e_i}, \ldots, \underset{- +}{e_{i=j'}}, \ldots, \underset{-}{e_j}, \ldots >$$

$$E^i = < \ldots, e_{i'}+1, \ldots, e_i - 1, \ldots, e_j, \ldots . > \qquad E^j = < \ldots, e_{i'}, \ldots\ldots, e_{i=j'}+1, \ldots, e_j - 1, \ldots >$$

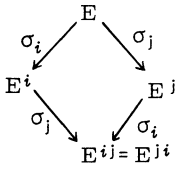
$$E^{ij} = < \ldots, e_{i'}+2, \ldots, e_i - 1, \ldots, e_j - 1, \ldots > \qquad E^{ji} = < \ldots, e_{i'}+1, \ldots, e_{i=j'}, \ldots, e_j - 1, \ldots >$$

$$E^{jii} = < \ldots, e_{i'}+2, \ldots, e_i - 1, \ldots, e_j - 1, \ldots >;$$

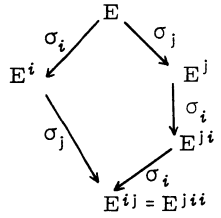
c'est-à-dire $E^{ij} = E^{jii}$, où $i < j$.

Il est commode de parler de deux sortes de relations de commutation qui épuisent, dans un certain sens, toutes les possibilités :

1) Règle du quadrangle (ou de permutabilité) $E^{ij} = E^{ji}$ aussi écrite par abus $\sigma_i\ \sigma_j = \sigma_j\ \sigma_i$ et représenté par la figure :



2) Règle du pentagone (ou de non permutabilité) $(i < j)$ $(E^{ij} \neq E^{ji})$ c'est-à-dire $E^{ij} = E^{jii} (\neq E^{ji})$ aussi écrite par abus $\sigma_i\ \sigma_j = \sigma_j\ \sigma_i^2$ et représenté par la figure :



Nous les appelons aussi règles de commutation *spéciales*

Définition de chaîne normale.

Une chaîne de transformations (propres) transformant E en $F = E^{n_1 \cdots n_r}$ (c'est-à-dire $E > F$) est dite *normale* si $n_1 \geqslant n_2 \geqslant \ldots \geqslant n_r$ est une suite descendante.

Quelques fois il est commode de réunir en "puissances" les n_i répétés dans la suite normal en écrivant :

$$F = E^{m_1^{p_1} \ldots m_s^{p_s}}$$

avec $m_1 > \ldots > m_s$ strictement descendant.

Evidemment :

$$m_1 = n_1 = \ldots = n_{p_1} > m_2 = n_{p_1+1} = \ldots = n_{p_1+p_2} > m_3 \ldots > m_s = n_{r-p_s+1} = \ldots = n_r \quad \text{et} \quad p_1 + \ldots + p_s = r$$

De même, une chaîne quelconque $I = i_1, \ldots, i_l$ peut être écrite :

$$J = j_1^{q_1}, j_2^{q_2}, \ldots, j_s^{q_s}$$

où $j_u \neq h_{u+1}$ pour tous les $u = 1, \ldots, s-1$, avec :

$$j_1 = i_1 = \ldots = i_{q_1} \neq j_2 = i_{q_1+1} = \ldots = i_{q_1+q_2} \neq \ldots \neq j_s = i_{l-q_s+1} = \ldots = i_l \quad \text{et} \quad q_1 + \ldots + q_s = l.$$

Si une chaîne n'est pas normale elle comporte au moins un couple voisin *anormal*, à savoir $i_n < i_{n+1}$; en écriture de puissances on écrira plutôt :

$$j_h^{q_h}\ j_{h+1}^{q_{h+1}} \quad \text{avec} \quad j_h < j_{h+1}.$$

En appliquant les règles de commutations exactes de proche en proche, et en raccourcissant $j_1^{q_1} \ldots j_{h-1}^{q_{h-1}}$ par J_1 on peut écrire :

$$E^{J_1\, j_h^{q_h}\, j_{h+1}^{q_{h+1}}} = E^{J_1\, j_{h+1}^{q_{h+1}}\, j_h^{q'_h}}$$

où $q_h \leqslant q'_h \leqslant q_h \cdot 2^{q_{h+1}}$.

La valeur exacte de q'_h, dépendant des circonstances de chaque cas, n'importe pas ici. Ce

qui importe c'est que le nombre des puissances distinctes ne s'accroit pas ; il peut bien se diminuer parce qu'on n'a pas nécessairement $j_{h-1} \neq j_{h+1}$ ou $j_h \neq j_{h+2}$. Aussi on n'a pas a se soucier si des transformations originalement propres ne deviennent pas identiques, parce que la suppression de transformations identiques ne peut que diminuer la chaîne.

On peut appeler règles de commutations généralisées et les écrire par abus :

$$i < j : \sigma_i^{q_i} \sigma_j^{q_j} = \sigma_j^{q_j} \sigma_i^{q_i'}$$

où $q_i \leqslant q_i' \leqslant q_i . 2^{q_j}$.

(On pourrait naturellement envisager des règles de commutation encore plus générales et plus vagues, mais nous n'avons pas besoin d'elles).

Comme mesure d'anormalité d'une chaîne C, écrite en puissance, on prend le nombre A(C) des inversions comparé à l'ordre normal voulu, c'est-à-dire le nombre de fois qu'on a $j_h < j_f$ pour tous les $h < f$ distincts possibles. En appliquant une règle de commutation généralisée à un couple anormal de puissances voisines, on diminue ce nombre A(C). Aussi longtemps que l'ordre de la chaîne n'est pas encore normal, c'est-à-dire $A(C) > 0$, on peut appliquer des règles de commutation généralisées, toujours diminuant A(C). On arrive donc de cette manière nécessairement à un stage avec $A(C) = 0$, c'est-à-dire à une chaîne normale. On a donc démontré la :

PROPOSITION 1 -

Pour chaque couple $E > F$ il existe au moins une chaîne normale dérivant F de E :

$$F = E^{n_1 n_2 \cdots n_r}, \quad n_1 \geqslant \ldots \geqslant n_r,$$

ou, si l'on veut :

$$F = E^{m_1^{p_1} \ldots m_s^{p_s}}, \quad m_1 > m_2 > \ldots > m_s.$$

Dans le paragraphe suivant, en appliquant plus à fond les données de notre théorie, on montre l'unicité de la chaîne normale qu'on construit d'une manière assez simple.

4 - L'INDICE E/F -

Définition.

Soient :

$$E = \langle e_0, \ldots, e_{n-1} \rangle$$

$$F = \langle f_0, \ldots, f_{n-1} \rangle$$

deux monômes vecteurs de la même dimension n. L'*indice* du couple ordonné (E, F) est un nombre relatif, écrit E/F et définit par :

$$E/F = \left\{ \begin{array}{l} i > 0 \iff e_i > f_i \\ -i < 0 \iff e_i > f_i \end{array} \right\}$$

et $e_\nu = f_\nu$ pour tous les $\nu > i$ s'il y en a.

Conclusions immédiates :

1/ Chaque couple $\in T_n \times T_n$ a un indice bien déterminé.

2/ $E = F \Longleftrightarrow E/F = 0$.

3/ $E/F = i > 0 \Longrightarrow e_i > f_i, \ e_{i+1} = f_{i+1}, \ldots, \ e_{n-1} = f_{n-1}$.

4/ $E/E^i = i$.

Notons le maximum de deux nombres i, j par $i \cup j$, et le maximum d'un ensemble de nombres $\{i_1, \ldots, i_l\}$ par $\bigcup_{n=1}^{l} i_n$. On a alors :

LEMME 1 -

$$E/F > 0,\ F/G > 0 \Longrightarrow E/G = E/F \cup F/G > 0$$

La démonstration s'ensuit directement des définitions :

$$E/F = i > 0 \Longrightarrow (e_i > f_i \ \&\ (\nu > i \Longrightarrow e_\nu = f_\nu)$$

$$F/G = j > 0 \Longrightarrow (f_j > g_j \ \&\ (\nu > j \Longrightarrow f_\nu = g_\nu)$$

Posant $K = i \cup j$ on a $e_K \geqslant f_K \geqslant g_K$, où une inégalité au moins est stricte, donc $e_K > g_K$ & $(\nu > K \Longrightarrow e_\nu = f_\nu = g_\nu)$ c'est-à-dire $E/G = K = E/F \cup F/G > 0$.

Ce lemme a les *corollaires* immédiats :

5/ $E/F \geqslant 0,\ F/G \geqslant 0 \Longrightarrow E/G = E/F \cup F/G$.

6/ $|E/G| \leqslant |E/F| \cup |F/G|$.

7/ $F = E^{i_1 \cdots i_l} \Longrightarrow E/F = \bigcup_{h=1}^{l} i_h$.

8/ $E > F \Longrightarrow E/F > 0$; en mots : une condition nécessaire pour $E > F$ est que l'indice E/F soit positif.

LEMME 2 -

$$E > F,\ E/F = i \Longrightarrow E^i \geqslant F.$$

Remarques.

a) On pourrait formellement affaiblir les hypothèses de ce lemme en écrivant :

$$E \geqslant F,\ E/F = i \Longrightarrow E^i \geqslant F,$$

sans rien changer au contenu ; car $E \geqslant F$, $E/F = i > 0 \Longrightarrow E > F$; si l'on admet $i = 0$, et alors σ_0 l'identité, donc $E^\circ = E$, le lemme est encore trivialement vrai.

b) On peut éliminer le i dans l'énoncé et le raccourcir :

$$E > F \Longrightarrow E^{E/F} \geqslant F.$$

Démonstration par induction.

Si F est dérivable de E par une chaîne de longueur $l = 1$ l'énoncé est évidemment vrai, parce qu'alors $E^i = F$. Supposons donc l'énoncé pour des chaînes de longueur $\leqslant l - 1$ $(l \geqslant 2)$ et soit $F = E^{i_1 i_2 \cdots i_l}$, donc $F = (E^{i_1})^{i_2 \cdots i_l}$ dérivé de E^{i_1} par une chaîne de longueur $l-1$. On a :

$$E^{i_1} > F,\ E^{i_1}/F = i^* = \bigcup_{h=2}^{l} i_h \Longrightarrow (E^{i_1})^{i^*} = E^{i_1 i^*} \geqslant F \quad \text{et} \quad E/F = i = i_1 \cup i^*.$$

Si $i_1 \geqslant i^*$ alors $i = i_1$ et $E^i = E^{i_1} \geqslant F$, et même $> F$.

Si $i_1 < i^*$ alors $i = i^*$, et l'on distingue deux cas :

a) σ_{i_1} et $\sigma_{i^*} = \sigma_i$ sont permutables par rapport à E, donc $E^{i_1 i} = E^{i i_1} \geqslant F$, donc même $E^i > F$.

b) σ_{i_1} et $\sigma_{i^*} = \sigma_i$ ne sont pas permutables par rapport à E, donc $E^{i_1 i} = E^{i i_1 i_1} \geqslant F$ donc même $E^i > F$.

PROPOSITION 2 -

Pour chaque couple $E > F$ il existe une et une seule chaîne normale transformant E en F, construite explicitement en fonction des indices seulement (d'une manière indépendante de la proposition 1).

Preuve :

$$E > F \Longrightarrow E/F = i_1 > 0 \Longrightarrow E^{i_1} \geqslant F \Longrightarrow i_2 = E^{i_1}/F \leqslant E/F = i_1.$$

Si $E^{i} = F$, donc $i_2 = 0$, la chaîne est déjà finie (chaîne normale triviale).

Si :

$$E^{i} > F : \Longrightarrow E^{i_1}/F = i_2 > 0 \Longrightarrow E^{i_1 i_2} \geqslant F \Longrightarrow i_3 = E^{i_1 i_2}/F \leqslant E^{i_1}/F = i_2 ;$$

plus généralement :

$$E^{i_1 \cdots i_{n-1}} > F \Longrightarrow E^{i_1 \cdots i_{n-1}}/F = i_h > 0 \Longrightarrow E^{i_1 \cdots i_{n-1} i_n} \geqslant F \Longrightarrow i_{h+1} = E^{i_1 \cdots i_h}/F \leqslant i_h.$$

Enfin il doit exister un dernier tel h = l avec :

$$E^{i_1 \cdots i_{l-1}} > F \Longrightarrow E^{i_1 \cdots i_{l-1}}/F = i_l > 0 \Longrightarrow E^{i_1 \cdots i_{l-1} i_l} = F,$$

parce que le nombre d'éléments de T_n est fini. $\sigma_{i_1} \sigma_{i_2} \ldots \sigma_{i_l}$ est une chaîne normale.

L'unicité de la chaîne normale $i_1 \geqslant \ldots \geqslant i_l$ s'ensuit immédiatement de la signification de i_h : le premier i_1 est bien déterminé parce que pour chaque chaîne normale $i_1 = E/F$ est l'indice bien déterminé du couple E/F. Aussi $i_h = E^{i_1 \cdots i_{h-1}}/F$ est bien déterminé en fonction de $i_1, \ldots, i_{h-1}$. Donc i_2 est bien déterminé (en fonction de i_1 bien déterminé) ; et ainsi de suite par induction : si les $i_1, \ldots, i_{h-1}$ sont déjà bien déterminés, il en est de même de i_h.

Remarque.

Sachant que T_n à un élément qui est le plus grand à savoir $\mathbf{1}_n = <1, \ldots, 1>$, il y a une seule chaîne normale conduisant de $\mathbf{1}_n$ à chaque élément de T_n. C'est donc une nouvelle méthode de représenter (ou repérer) fidèlement les éléments de T_n, à savoir par leurs chaînes normales les dérivant de $\mathbf{1}_n$, qui est lui même repéré par la chaîne vide considérée aussi comme chaîne normale.

Une autre manière de profiter de la proposition 2 s'exprime dans un :

COROLLAIRE 9 -

Les chaînes normales sortant de la "racine" $\mathbf{1}_n$ de T_n constituent l'ensemble $|T_n|$ comme "arbre" (dans le sens de la théorie des graphes).

On a aussi le :

COROLLAIRE 10 -

Soit $\sigma_{i_1} \ldots \sigma_{i_l}$ une chaîne quelconque dérivant F de E (E > F), $F = E^{i_1 \cdots i_l}$. En utilisant les relations de commutation exactes applicables, dans un ordre quelconque, on arrive toujours, après un nombre fini de pas, à la même chaîne normale (réduite, c'est-à-dire sans transformations identiques).

Dans le paragraphe suivant on se pose une tâche contraire : de transformer une chaîne normale donnée à une autre chaîne, naturellement anormale, mais satisfaisant une propriété voulue comme, p.e., de commencer avec un indice particulier i. Les transformations considérées n'introduisent jamais un indice nouveau, on peut déjà conclure que tous les indices, apparaissant dans la chaîne normale, doivent aussi apparaître dans des chaînes équivalentes quelconques.

LEMME 3 -

$$E/F = i,\ j > i > 0 \Longrightarrow E^j/F^j = i.$$

Remarques.

1/ En supposant seulement $i \geqslant 0$, on ajoute seulement le cas trivial :

$$E = F \Longrightarrow E^j = F^j.$$

2/ On suppose naturellement que σ_j est propre ; mais, si l'on supprime cette hypothèse, on ajoute rien, parce que σ_j est simultanément propre ou impropre dans E et dans F ; le cas impropre est évidemment trivial.

3/ Une véritable généralisation sera d'écrire :

$$E/F = i,\ j > |i| \Longrightarrow E^j/F^j = i,$$

ou d'une manière équivalente :

$$j > |E/F| \Longrightarrow E/F = E^j/F^j$$

Mais ceci sera une conséquence immédiate du lemme 3 en l'appliquant pour $E/F = i < 0$ à $F/E = -i > 0$:

$$F/E = -i,\ j > -i,\ i| > 0 \Longrightarrow F^j/E^j = -i \Longleftrightarrow E^j/F^j = i.$$

Démonstration.

Notons les places des barrières de σ_j

dans E par $j_E = j'(E)$,

dans F par $j_F = j'(F)$.

La situation générale se présente donc de la manière suivante :

$$e^j_\nu = e_\nu \ (\nu \neq j, j_E),\ = e_j - 1 \ (\nu = j),\ = e_{j_E} + 1 \ (\nu = j_E),$$

$$f^j_\nu = f_\nu \ (\nu \neq j, j_F),\ = f_j - 1 \ (\nu = j),\ = f_{j_F} + 1 \ (\nu = j_F),$$

$$e_\nu = f_\nu \ (\nu > i),\ e_i > f_i.$$

Notons encore $j^* = j_E \cup j_F$, et distinguons les cas suivants :

a) $j^* > i$: A cause de l'identité des "champs" de E et de F à droite de i, cela entraîne $j^* = j_E = j_F > i$, parce qu'une barrière rencontrée à droite de i dans E l'est aussi dans F et vice versa.

Donc :

$$\nu > i \Longrightarrow e^j_\nu = f^j_\nu$$

$$\nu = i \Longrightarrow e^j_i = e_i > f_i = f^j_i \Longrightarrow e^j_i > f^j_i,$$

c'est-à-dire $E^j/F^j = i$.

b) $j^* \leqslant i$: l'identité des champs de E et de F à droite de i et $e_i > f_i$ entraînent que si f_i est une barrière dans F, e_i l'est davantage ("a fortiori") dans E. On a donc les cas possibles :

b_1) $\quad j^* = i = j_E = j_F \quad$ donc $\quad e^j_i = e_i + 1 > f_i + 1 = f^j_i$;

b_2) $\quad j^* = i = j_E > j_F \quad$ donc $\quad e^j_i = e_i + 1 > f_i + 1 > f_i = f^j_i$;

b_3) $\quad j^* < i$; $\quad$ donc $\quad e^j_i = e_i \quad > f_i = f^j_i$;

donc dans tous les cas $e^j_i > f^j_i$, mais $e^j_\nu = f^j_\nu$ $(\nu > i)$, c'est-à-dire $E^j/F^j = i$.

5 - LE LEMME FONDAMENTAL -

PROPOSITION 3 (le lemme fondamental.

$$E > G,\ F \geqslant G,\ E/F = i > 0 \Longrightarrow E^i \geqslant G.$$

Remarques.

1/ On peut formellement affaiblir les hypothèses en écrivant plus symétriquement :

$$E \geqslant G,\ F \geqslant G,\ E/F = i \geqslant 0 \Longrightarrow E^i \geqslant G,$$

sans rien changer au contenu. En fait :

$$E \geqslant G,\ F \geqslant G,\ E/F = i > 0 \Longrightarrow E > E^i \geqslant G \Longrightarrow E > G\ ;$$

pour i = 0 la proposition est trivialement vraie.

2/ En posant F = G, au lieu F ⩾ G, on met en évidence que cette proposition est une généralisation du lemme 2.

Démonstration

Soit $G = E^{m_1 \cdots m_p} = F^{n_1 \cdots n_q}$, et soient $m_1 \geqslant \ldots \geqslant m_p$ et $n_1 \geqslant \ldots \geqslant n_q$ les deux chaînes normales dérivant G de E et de F, donc :

$$m_1 = E/G > 0,\ n_1 = F/G \geqslant 0, \quad \text{et} \quad m_1 = i \cup n \geqslant i.$$

Si $m_1 = i$ il n'y a rien à démontrer, car par le lemme 2 $E^i \geqslant G$. Reste donc le cas $m_1 > i$. On note, pour abréger, la suite $m_1 \ldots m_h = (h)$ et m_r le dernier m avec $m_r > i$; r est donc un nombre bien défini parmi $1, \ldots, p$. On conduit la suite de démonstration en montrant plusieurs lemmes.

LEMME 4 (lemme auxiliaire) -

$$m_1 = n_1, \ldots,\ m_r = n_r,\ E^{(r)}/F^{(r)} = i,\ m_{r+1} = i \quad (r < p), \quad \text{et} \quad n_{r+1} \leqslant i.$$

Preuve.

$$m_1 > i \Longrightarrow m_1 = i \underset{n}{\cup} n_1 \Longrightarrow m_1 = n_1 > i \Longrightarrow E^{n_1}/F^{n_1} = i$$

(lemme 3) ; de même :

$$m_2 > i \Longrightarrow m_2 = E^{n_1}/G = E^{n_1}/F^{n_1} \cup F^{n_1}/G = i \cup n_2 \Longrightarrow m_2 = n_2 > i \Longrightarrow E^{n_1 n_2}/F^{n_1 n_2} = i\ ;$$

Supposons qu'on a déjà montré :

$$m_1 = n_1, \ldots,\ m_{h-1} = n_{h-1} \quad \text{et} \quad E^{(h-1)}/F^{(h-1)} = i\ ;$$

alors :

$$m_h > i \Longrightarrow m_h = E^{(h-1)}/G = E^{(h-1)}/F^{(h-1)} \cup F^{(h-1)}/G = i \cup n_h \Longrightarrow m_h = n_h > i \Longrightarrow E^{(h)}/F^{(h)} = E^{(h-1)n_h}/F^{(h-1)n_h} = i.$$

Donc, enfin, par récurrence, $m_1 = n_1, \ldots,\ m_r = n_r$ et $E^{(r)}/F^{(r)} = i$, mais :

$$r < p \quad \text{et} \quad m_{r+1} = E^{(r)}/G = E^{(r)}/F^{(r)} \cup F^{(r)}/G = i \cup n_{r+1} \leqslant i \Longrightarrow m_{r+1} = i,\ n_{r+1} \leqslant i.$$

On retient de ce lemme la partie la plus importante par le :

COROLLAIRE 11 -

Sous les hypothèses de la proposition 3 au moins un σ_i fait partie de la chaîne normale de E à G, donc même de chaque chaîne de E à G.

Grosso modo on peut dire, que le reste de la démonstration est basé sur l'idée suivante : La chaîne normale de E à G est de la forme :

$$m_1 \geqslant \ldots \geqslant m_r > i \geqslant \ldots \geqslant m_p$$

On peut toujours la transformer en une autre chaîne (anormale cette fois) commençant avec i, en utilisant de proche en proche des relations de commutation exactes, convenables, pour enfin pousser le i jusqu'en tête.

LEMME 5 -

$$k \geqslant j > i,\ E^{ji} = E^{ij} \Longrightarrow E^{kji} = E^{kij}.$$

Remarque :

Le lemme étant trivialement vrai pour j = i on peut lui donner une forme plus symétrique :

$$k \geqslant i \cup j,\ E^{ij} = E^{ji} \Longrightarrow E^{kji} = E^{kij}.$$

Preuve (par l'absurde) :

Supposons $E^{kji} \neq E^{kij}$, donc :

$$(h)\ (i < h < j)\ (S_h^j\ (E^k) < j - h) \quad \& \quad S_i^j\ (E^k) = j - i\ (h = i).$$

Comparons les $S_h^j\ (E^k)$ avec les $S_h^j(E)$ pour tous les h, $i \leqslant h < j$.

Evidemment :

$$(h)\ (h < j)\ (S_h^j(E) \leqslant S_h^j\ (E^k)).$$

Donc :

$$(h)\ (i < h < j)\ (S_h^j\ (E) \leqslant S_h^j(E^k) < j - h)$$

et pour h = i :

$$S_i^j(E) \leqslant S_i^j\ (E^k) = j - i.$$

Mais $S_i^j\ (E) < j - i$ est impossible, parce qu'il entraîne $S_i^j\ (E^k) < j - i$ en conséquence du caractère conservatif du déficit ; on a donc $S_i^j\ (E) = j - i$, donc $E^{ij} \neq E^{ji}$ en contradiction à notre hypothèse.

En appliquant le lemme de nouveau à $E^k = E^{k_1}$ (au lieu de E) on obtient pour $k_2 > j$:

$$E^{k_1 k_2 j i} = E^{k_1 k_2 i j},$$

et, plus généralement, le

COROLLAIRE 12 -

Soit $E^{ij} = E^{ji}$, c'est-à-dire σ_i et σ_j permutables par rapport à E. Soit $K = k_1 k_2 \ldots k_t$ où tous les $k \geqslant i \cup j$. Alors σ_i et σ_j sont aussi permutables par rapport à E^K : $E^{ij} = E^{ji} \Longrightarrow E^{Kji} = E^{Kji}$; ou d'une manière équivalente $E^{Kij} \neq E^{Kji} \Longrightarrow E^{ij} \neq E^{ji}$.

Revenant à notre proposition, constatons, que dans les cas particuliers, où σ_i est permutable par rapport à E avec tous les σ_{m_h}, h = 1,..., r le précédant dans la chaîne normale de E à G, on a :

$$E^{(r)i} = E^{(r-1)im_r} = \ldots = E^{m_1 i \ldots m_r} = E^{i(r)},$$

et aussi :

$$E^{(r)im_{r+2}\cdots m_p} = E^{(r-1)im_r\, m_{r+2}\cdots m_p} = \ldots = E^{i(r)m_{r+2}\cdots m_p},$$

donc $E^i \geqslant G$.

Il reste donc seulement à envisager des cas, où il y a des $m_h > i$ tels que σ_{m_h} n'est pas permutable avec σ_i par rapport à E. C'est ici l'occasion naturelle de se demander combien de tels m_h peuvent exister pour un E donné.

LEMME 6 -

Pour un i donné il y a au plus un seul $j > i$ tel que σ_j et σ_i ne soient pas permutables par rapport à E.

Preuve (par l'absurde).

Soient $k > j > i$ tels que $E^{ji} \neq E^{ij}$ et $E^{ki} \neq E^{ik}$, donc $k' = j' = i$, $S_i^j = j - i$, $S_j^k < k - j$ et $S_i^k = k - i$. On reçoit la contradiction :

$$S_i^k = k - i = S_i^j + S_j^k < j - i + k - j = k - i.$$

LEMME 7 -

σ_{m_h} et σ_i non permutables par rapport à $E \Longrightarrow E^{(r)i}/G = i$.

Preuve.

On montre d'abord que :

$$E^{(r)i}/F^{(r)} = i.$$

$e_i^{(r)} - e_i$, resp $f_i^{(r)} - f_i$, dénotent les nombres des quanta absorbés à la place i dans E, resp dans F, par les émissions de (r). $E/F = i$ signifie que les champs à droite de i sont identiques dans E et dans F, mais aussi que $e_i > f_i$; c'est-à-dire que e_i est une barrière plus efficace que f_i dans le sens qu'une émission absorbée par f_i l'est certainement aussi par e_i ; donc :

$$c_i^{(r)} - e_i \geqslant f_i^{(r)} - f_i \Longleftrightarrow e_i^{(r)} - f_i^{(r)} \geqslant e_i - f_i \ (\geqslant 1).$$

Supposons qu'il y ait en (r) (au moins) un $m_h = n_h = j$ (> i), dont σ_j soit non permutable avec σ_i par rapport à E. Ceci signifie qu'il y a (au moins) une émission σ_j telle qu'elle est justement absorbée à la place i de E sur la barrière e_i, mais dont le rendement dans F est plus long ; à savoir $m_h^!(E) = i$, mais $n_h^!(F) < i$. En fait :

$$(h)\ (i < h < j)\ (S_h^j\ (E) = S_h^j\ (E) < j - h),$$

$$h=i \qquad S_i^j\ (E) = S_{i+1}^j(E) + e_i = j - i,$$

$$S_i^j\ (F) = S_{i+1}^j(F) + f_i < j - i.$$

On a donc :

$$e_i^{(r)} - f_i^{(r)} > e_i - f_i \geqslant 1 \Longrightarrow e_i^{(r)} - f_i^{(r)} \geqslant 2,$$

donc, pour $\nu > i$:

$$e_\nu^{(r)i} = e_\nu^{(r)} = f_\nu^{(r)},$$

pour $\nu = i$:

$$e_i^{(r)i} - 1 > f_i^{(r)} \Longrightarrow E^{(r)i}/F^{(r)} = i$$

$$m_{r+2} = E^{(r)i}/G = E^{(r)i}/F^{(r)} \cup F^{(r)}/G = i \cup n_{r+1} \lesseqgtr i \Longrightarrow m_{r+2} = i$$

car $n_{r+1} \leqslant i$ (lemme 4) ou, aussi, bien, car $E^{(r)i}/G = m_{r+2} \leqslant m_{r+1} = i$.

Revenant sur notre proposition, on peut maintenant conclure sa démonstration. Soit $m_h = j$ tel que $\sigma_{m_{h+1}} \ldots \sigma_{m_r}$ (s'il y en a $\Longleftrightarrow h < r$) soient permutables avec σ_i. On peut donc supposer les transformations de chaîne normale (rectangles) :

$$E^{(r+2)} = E^{(r)ii} = E^{(r-1)iim_r} = \ldots = E^{(h)iim_{h+1}\cdots m_r} = E^{(h-1)jiim_{h+1}\cdots m_r}$$

Appliquons la règle du pentagone à $E^{(h-1)jii} = E^{(h-1)ij}$. En conséquence du lemme 6 j est unique, et on peut de nouveau appliquer le rectangle :

$$E^{(h-1)ij} = \ldots = E^{i(h-1)j} \Longrightarrow E^{(p)} = E^{i(h-1)jm_{h+1}\cdots m_r m_{r+3}\cdots m_p} = G \Longrightarrow E^i \geqslant G.$$

6 - DEMONSTRATION DU THEOREME. L'ALGORITHME DE LA LIMITE INFERIEURE (E,F). (Algorithme d'Euclide).

Le théorème est un corollaire assez immédiat de la proposition fondamentale (proposition 3), par son application itérée. Le procédé en question donne un algorithme pour le calcul de la limite inférieure d'un couple donné quelconque $(E,F) \in T_n \times T_n$, qui ressemble à l'algorithme d'Euclide pour le calcul du P.G.C.D.

La proposition dit qu'un minorant commun quelconque G d'un couple (E,F), disons avec $E/F = i = i_1 > 0$, est aussi minorant du couple (E^i,F) ; autrement dit, le couple (E,F) détermine le même ensemble de minorants communs comme le couple (E^i,F), bien que E^i est strictement inférieure à E. $E^i/F \geqslant 0$ ou $F/E^i > 0$: $E^i/F > 0 \Longrightarrow E^i/F = i_2 \leqslant i_1$ et $(E^{i_1 i_2},F)$ détermine encore le même ensemble de minorants communs, de même $E/E^i = j_1 > 0 \Longrightarrow (E^{i_1}, F^{j_1})$ détermine le même ensemble de minorants communs. Aussi longtemps que l'indice du couple précédemment obtenu est $\neq 0$, on peut continuer ce procédé que remplace à chaque pas une composante du couple par une composante strictement inférieure, et le procédé ne s'arrête qu'au moment quand les deux

composantes sont égales (H,H) ; donc H est un minorant commun, majorant tous les minorants communs, c'est-à-dire H est *la* limite inférieure de E et de F. D'autre part ce procédé ne peut continuer qu'un nombre fini de pas à cause du cardinal fini de T_n. Il est assez naturel de noter H comme le P.G.C.D. : H = (H,H)=...=(E,F). Mais un système ordonné fini avec limite inférieure pour chaque couple est un treillis.

Notons un couple (E,F) = α ; son couple inverse (F,E) = α' ; la partie non négative de son indice i = E/F par $\overline{\alpha} = \begin{cases} i \text{ si } i \geqslant 0 \\ 0 \text{ si } i < 0 \end{cases}$; et encore $|\alpha| = \overline{\alpha} \cup \overline{\alpha}'$ son "indice absolu" (on a toujours $\overline{\alpha} \cap \overline{\alpha}' = 0$). On reçoit ainsi, en décrivant le procédé au-dessus, la suite de couples :

$$\alpha = \alpha_0 = (E,F) \quad (|\alpha| = |\alpha_0| > 0) \; ; \; \alpha_1 = (E^{\overline{\alpha}}, F^{\overline{\alpha}'}) \; (|\alpha| \geqslant |\alpha_1| > 0) \; ;$$

$$\alpha_2 = (E^{\overline{\alpha}\,\overline{\alpha}_1}, F^{\overline{\alpha}'\overline{\alpha}_1'}) \; (|\alpha_1| \geqslant |\alpha_2| > 0) \; ; \; \ldots \; \alpha_{\nu+1} = (E^{\overline{\alpha}\overline{\alpha}_1 \cdots \overline{\alpha}_\nu}, F^{\overline{\alpha}'\overline{\alpha}_1' \cdots \overline{\alpha}'_\nu}) \; (|\alpha_\nu| \geqslant |\alpha_{\nu+1}| > 0);$$

$$\ldots ; \alpha_r = (E^{\overline{\alpha}\cdots\overline{\alpha}_{r-1}}, F^{\overline{\alpha}'\cdots\overline{\alpha}'_{r-1}}) \; (|\alpha_{r-1}| \geqslant |\alpha_r| > 0) \; ; \; \alpha_{r+1} = (H,H) \; |\alpha_{r+1}| = 0,$$

où $H = E^{\overline{\alpha}\overline{\alpha}_1 \cdots \overline{\alpha}_r} = F^{\overline{\alpha}'\overline{\alpha}_1' \cdots \overline{\alpha}'_r}$. En supprimant tous les $\overline{\alpha}_\nu$, $\overline{\alpha}'_\nu = 0$ correspondant à des transformations identiques (impropres), on obtient deux chaînes normales complémentaires $\overline{\alpha} \geqslant \overline{\alpha}_{k_1} \geqslant \ldots \geqslant \overline{\alpha}_{k_s}$ et $\overline{\alpha}'_{\lambda_1} \geqslant \ldots \geqslant \overline{\alpha}'_{\lambda_t}$ tels que $K_1 \ldots K_s \; ; \lambda_1, \ldots, \lambda_t$ n'est qu'une décomposition de la suite $1, \ldots, r$. La chaîne $\overline{\alpha} \geqslant \alpha_{K_1} \geqslant \ldots \geqslant \overline{\alpha}_{K_s}$ est identique avec la chaîne normale $m_1 \geqslant \ldots \geqslant m_p$ du p précédent pour un G tel que $m_1 = \overline{\alpha} = i = E/F$.

Perfectionnons la notation et le procédé de "division", qui, pour le moment, est encore au stade de soustractions itérées. On associe à chaque indice i un "exposant" ou une "multiplicité" p_i ; on appelle ce couple l'*indice posé* E//F, qu'on écrit sous forme de puissance $E//F = i^{p_i}$ indiquant $|E/F| = i$ et $p_i = e_i - f_i$. On remplace l'indice négatif par l'indice absolu avec exposant négatif : $E = F \Longleftrightarrow E/F = 0 \Longleftrightarrow E//F = 1 = i^0$. On a déjà partiellement utilisé cette notation au § 2 pour les chaînes normales $m_1^{p_1} \ldots m_s^{p_s}$ avec $m_1 > \ldots > m_s > 0$.

On appelle *quotient* et l'on note $Q_1 = E \div F$ la chaîne normale bien déterminée :

$$i_1^{p_{i_1}} \quad \ldots \quad i_k^{p_{i_k}}$$

où :

$$i_1^{p_{i_1}} = E//F_{p_{i_1}}, \; i_2^{p_{i_2}} = E^{i_1^{p_{i_1}}}//F, \ldots, \; i_k^{p_{i_k}} = E^{i_1^{p_{i_1}} \cdots i_{k-1}^{p_{i_{k-1}}}} // F,$$

mais :

$$E^{i_1^{p_{i_1}} \cdots i_k^{p_{i_k}}}//F = E^{Q_1}//F = i_{k+1}^{-p_{i_{k+1}}},$$

où tous les $p_{i_1}, \ldots p_{i_k} > 0$, $p_{i_{k+1}} \geqslant 0$.

Supposons $p_{i_{k+1}} > 0$ et posons :

$$k = k_1, \; E^{Q_1} = R_1, \; Q_2 = F \div R_1 = F \div E^{Q_1} = i_{k_1+1}^{p_{i_{k_1+1}}} \ldots i_{k_1+k_2}^{p_{i_{k_1+k_2}}}$$

avec les conditions correspondantes :

$$p_{i_{k_1+1}}, \ldots p_{i_{k_1+k_2}} > 0,$$

mais :

$$F^{Q_2}//E^{Q_1} = i_{k_1+k_2+1}^{-p_{i_{k_1+k_2+1}}} \quad \text{avec} \quad p_{i_{k_1+k_2+1}} \geqslant 0.$$

Posons encore $F^{Q_2} = R_2$, $Q_3 = R_1 \div R_2$, plus généralement :

$$R_\nu = R_{\nu-2}^{Q_\nu}, \; Q_{\nu+1} = R_{\nu-1} \div R_\nu,$$

et enfin, introduisons une "multiplication extérieure purement formelle" écrite $Q_{\nu+1} \, R_\nu$, et un symbol "d'addition purement formelle" $\perp$. On écrit au lieu de :

$$Q_1 = E \div F, \quad R_1 = E^{Q_1} \Longleftrightarrow E = Q_1\, F \perp R_1$$

$$Q_2 = F \div R_1, \quad R_2 = F^{Q_2} \Longleftrightarrow F = Q_2\, R_1 \perp R_2$$

$$Q_3 = R_1 \div R_2, \quad R_3 = R_1^{Q_3} \Longleftrightarrow R_1 = Q_3\, R_2 \perp R_3$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$Q_{\nu+1} = R_{\nu-1} \div R_\nu, \quad R_{\nu+1} = R_{\nu-1}^{Q_{\nu+1}} \Longleftrightarrow R_{\nu-1} = Q_{\nu+1}\, R_\nu \perp R_{\nu+1}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

On s'arrête au moment où apparaît :

$$R_{n+1} = R_n = (E,F) = (R_{\nu-1}, R_\nu)\ ;\ R_n = R_{n+1} = E^{Q_1 Q_3 \cdots Q_2 \left|\frac{n+1}{2}\right|^{-1}} = F^{Q_2 Q_4 \cdots Q_2 \left|\frac{n+1}{2}\right|} = R_\nu^{Q_{\nu+2}\, Q_{\nu+4} \cdots}$$

Même cette seule différence formelle à la fin des deux algorithmes est moindre qu'elle apparaît. Une modification triviale de l'algorithme d'Euclide ordinaire fait disparaître la différence ; au lieu de restreindre les restes par $0 \leqslant r_\nu < r_{\nu-1}$, on pourrait le faire aussi bien par $0 < r_\nu \leqslant r_{\nu-1}$; alors l'algorithme d'Euclide s'arrêtera convenablement au moment où apparaît $r_{n+1} = r_n$ (au lieu de $r_{n+1} = 0$).

BIBLIOGRAPHIE

[1] CARVALHO, J.B. et TAMARI, DOV - sur l'associativité partielle des symétrisations de semi-groupes. Portugaliae Mathematica 21 (1962), pp. 157-169.

[2] TAMARI, DOV - Monoïdes préordonnés et chaînes de Malcev. Thèse, Paris 1951 (non-publiée ; plusieurs parties en stencil. Le texte polycopié répété dans les Math Reviews n'est qu'une partie de la thèse. Un extrait de cet extrait est publié dans le Bull. Soc. Math. France *82* (1954), pp. 53-96, mais il ne contient pas des références directes à notre sujet ici).

[3] TAMARI, DOV - some mutual applications of logic and mathematics ; applications scientifiques de la logique mathématique, Coll. Inter. Paris 1952 ; ed. Gauthiers Villars Paris, p. 89.

[4] TAMARI, DOV - Imbeddings of partial multiplicative systems (monoïdes) associativity and word problems (N. 6) p. 760.

[5] TAMARI, DOV - The Algebra of bracketings and their enumeration. Nieuw Archief voor Wiskunde (3), *10* (1962), pp. 131-146.

[6] TAMARI, DOV - Theoria dos Monoïdes, O problema das Palavras ("word problem") e a Imersao de semi-grupos en grupos. Alas 3° Col. Brasil Mat. 1961 (sous presse).

[7] TAMARI, DOV - The theory of monoïdes and the word problem por groups (en cours de publication).