

ALGÈBRE. — *Le problème des mots dans les treillis modulaires libres*. Note de M. MARCEL PAUL SCHÜTZENBERGER, présentée par M. Gaston Julia.

Les seuls treillis pour lesquels soit connue la solution du problème des mots sont : le treillis libre  $\mathfrak{F}$  <sup>(1)</sup> et les treillis distributifs <sup>(2)</sup> auxquels peut être ajouté le  $\mathfrak{U}$ -treillis libre <sup>(3)</sup> union subdirecte de treillis distributifs et de  $M_3$  puisque l'on connaît la forme canonique de ses éléments irréductibles.

On indiquera ici les grandes lignes de la théorie correspondante pour les treillis modulaires libres  $\mathfrak{M}$  <sup>(4)</sup>.

*Définitions :*

$E$  : un ensemble d'éléments  $e_i$  (les « générateurs »);

$\mathfrak{A} \supset E$  : le système algébrique libre constitué par toutes les expressions finies formées par récurrence à partir des  $e_i$  au moyen de deux opérations (notées ici  $+$  et  $\times$  avec les conventions habituelles d'omission du signe  $\times$ , la congruence dans  $\mathfrak{A}$  étant écrite  $\equiv$ ) *commutatives* et *associatives*;

$\mathfrak{R}$  : le quotient de  $\mathfrak{A}$  par  $\{\equiv\} = \{\rho, \rho^{-1}\}$  <sup>(5)</sup> avec  $\rho$  définie par

$$(A + B)(C + AD) \rho (A + B)C + AD \quad (A, B, C, D \in \mathfrak{A} \text{ et } C \neq \text{mot vide});$$

$\mathfrak{F}$  (le *treillis libre* engendré par  $E$ ): le quotient de  $\mathfrak{A}$  par  $\{\simeq\} = \{\sigma, \sigma^{-1}, \check{\sigma}, \check{\sigma}^{-1}\}$ , avec  $\sigma$  définie par  $(A + B)C \sigma A$  ( $A \in \mathfrak{A}$ ,  $B \in \mathfrak{A}$  ou vide);

$\mathfrak{M}$  (le *treillis modulaire libre* engendré par  $E$ ): le quotient de  $\mathfrak{A}$  par  $\{\equiv, \simeq\}$ ;

$|X|$  (la « formule » de  $X \in \mathfrak{A}$ ): le vecteur dont les composants  $\xi_+, \xi_\times, \xi_1, \xi_2, \dots, \xi_i, \dots$  sont respectivement le nombre de fois où les deux opérations et les  $e_i$  apparaissent dans l'expression  $X$ .

<sup>(1)</sup> P. WHITMAN, *Ann. Math.*, 42, 1941, p. 325-330 et 43, 1942, p. 104-105.

<sup>(2)</sup> G. BIRKHOFF, *Lattice Theory*, New-York, 1948, p. 145.

<sup>(3)</sup> M. P. SCHÜTZENBERGER, *Comptes rendus*, 221, 1945, p. 218.

<sup>(4)</sup> C'est le problème 28 de G. BIRKHOFF (*loc. cit.* p. 70).

<sup>(5)</sup> J. RIGUET, *Bull. Soc. Math.*, 76, 1948, p. 122.

On écrira  $\{\lambda, \mu, \dots\}$  pour désigner la fermeture algébrique de la fermeture d'équivalence de la réunion des relations  $\lambda, \mu, \dots$ . Le diacritique  $\check{\phantom{x}}$  symbolisera la dualité canonique échangeant entre elles les deux opérations.

Les formules seront ordonnées par  $|X| \leq |X'|$  équivalent à : tout  $i : \xi_i \leq \xi'_i$ .

$\mathfrak{C}^* \mathfrak{C}$  : l'ensemble des expressions *semi réduites*, c'est-à-dire telles que  $X' \simeq X \in \mathfrak{C}^*$  entraîne  $|X| \leq |X'|$ ;

$\mathfrak{M}^* \mathfrak{C} \mathfrak{C}^*$  : l'ensemble des expressions *réduites*, c'est-à-dire telles que  $Y \simeq X' \equiv X \in \mathfrak{M}^*$  entraîne  $|X| \leq |Y|$ .

On sait que  $\mathfrak{C}$  est isomorphe à  $\mathfrak{C}^*$  et  $\mathfrak{M}$  à une image  $\overline{\mathfrak{M}^*}$  de  $\mathfrak{M}^*$ .

La démonstration repose sur les remarques suivantes :

1° Quand les relations telles que  $\rho$  et  $\sigma$  ne sont pas permutables (\*), les expressions figurant dans l'énoncé où elles interviennent peuvent être mises sous une forme canonique.

2° La formule d'une expression ne peut pas s'accroître par application de  $\rho$  ou de  $\sigma$ .

LEMME I. — Si  $X \equiv X'$  alors  $|X| = |X'|$  et  $X \in \mathfrak{C}^*$  entraîne  $X' \in \mathfrak{C}^*$  (on peut se limiter à vérifier le résultat pour  $\rho$ ).

LEMME II. — Si  $X \equiv X' \simeq YX'$  où  $Y \not\sim X$  et  $X'$ , alors  $X \simeq YX''$  (on peut se limiter à  $X \rho X' \sigma YX'$ ).

LEMME III. — Si  $X \sigma^{-1} Y \rho Z \rho Z'$  il existe  $Y'$  et  $X'$  avec  $Z' \rho Y' \sigma X'$  et  $|X| = |X'|$ .

Le seul cas non trivial est celui où la relation précédente (notée  $\theta$ ) entre  $X$  et  $X'$  se réduit à celle entre

$$X = U(V + (U + U')V') \quad \text{et} \quad X' = U((U + U')V + V').$$

Par conséquent  $\theta$  et  $\check{\theta}$  qui sont strictement plus faibles que  $\rho$  et  $\rho^{-1}$  laissent comme elles les formules invariantes. D'autre part

$$\{\rho, \check{\rho}, \sigma, \check{\sigma}, \sigma^{-1}, \check{\sigma}^{-1}\} = \{\theta, \check{\theta}, \rho, \rho^{-1}, \sigma, \check{\sigma}\}.$$

Donc :

LEMME IV. — Si  $X \simeq Y \equiv Y'$  il existe  $X' \simeq Y'$  avec  $|X| = |X'|$ . D'où enfin :

THÉORÈME. —  $\mathfrak{M}^*$  est le quotient de  $\mathfrak{C}^*$  par  $\{\theta, \check{\theta}, \rho, \rho^{-1}, \sigma, \check{\sigma}\}$ .

COROLLAIRE 1. — Si deux expressions de  $\mathfrak{A}$  ont des formules finies, il est possible en un nombre fini d'opérations de les ramener à une forme réduite et de déterminer si elles sont ou non modulairement équivalentes.

COROLLAIRE 2. — Une condition nécessaire (mais non suffisante si la puissance de  $E$  dépasse 3) pour que deux expressions réduites soient modulairement équivalentes est qu'elles aient même formule.

(\*) P. DUBREIL et M. DUBREIL-JACOTIN, *J. Math. pures et appl.*, 18, 1939, p. 63.

( 3 )

On remarquera que cette dernière propriété n'est plus vraie dans le treillis modulaire  $\mathcal{M}'$  quotient de  $\mathcal{M}$  par les identités latticielles vérifiées dans tous les treillis de sous-groupes distingués (<sup>3</sup>).

Nous pouvons cependant annoncer qu'elle subsiste dans le cas où tous les éléments du groupe sont d'ordre 2.

(Extrait des *Comptes rendus des séances de l'Académie des Sciences*,  
t. 237, p. 507-508. séance du 7 septembre 1953.)