

SÉMINAIRE DUBREIL. ALGÈBRE ET THÉORIE DES NOMBRES

JULIAN PETRESCO

Prégroupe de mots et problème des mots

Séminaire Dubreil. Algèbre et théorie des nombres, tome 21, n° 2 (1967-1968), exp. n° 17,
p. 1-11

http://www.numdam.org/item?id=SD_1967-1968__21_2_A8_0

© Séminaire Dubreil. Algèbre et théorie des nombres
(Secrétariat mathématique, Paris), 1967-1968, tous droits réservés.

L'accès aux archives de la collection « Séminaire Dubreil. Algèbre et théorie des nombres » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

PRÉGROUPES DE MOTS ET PROBLÈME DES MOTS

par Julian PETRESCO

1. Prégroupes.

On considère un ensemble E et l'ensemble $\mathcal{P}(E)$ des parties de E . E est un pré-groupe si :

(1) Deux applications $f : E \times E \rightarrow \mathcal{P}(E) - \emptyset$ et $g : E \times E \rightarrow \mathcal{P}(E)$ sont distinguées. Si $a, b \in E$, on note : $a \leftarrow b = f(a, b)$, $a \rightarrow b = g(a, b)$. Si $A, B \subseteq E$ et $\omega = \{\leftarrow, \rightarrow\}$, $A \omega B = \bigcup_{a \in A, b \in B} (a \omega b)$. Enfin :

$$\bar{\omega} = \begin{cases} \leftarrow ; & \omega = \rightarrow \\ \rightarrow ; & \omega = \leftarrow \end{cases} .$$

$$(2) \quad a' \in a \leftarrow b \iff a \in a' \rightarrow b .$$

$$(3_1) \quad a \leftarrow (b \leftarrow c) \subseteq (a \leftarrow b) \leftarrow c ;$$

$$(3_2) \quad a \leftarrow (b \rightarrow c) \subseteq (a \leftarrow b) \rightarrow c ;$$

$$(3_3) \quad (a \rightarrow b) \leftarrow c \subseteq (a \leftarrow c) \rightarrow b .$$

$(a_1 \omega_1 a_2 \omega_2 \dots \omega_{n-1} a_n)_\alpha$ est une expression comportant $n - 1$ signes $\omega_i \in \{\leftarrow, \rightarrow\}$ et les n éléments a_1, a_2, \dots, a_n dans cet ordre, associés de manière arbitraire ; en particulier

$$a_1 \omega_1 a_2 \omega_2 \dots \omega_{n-1} a_n = [\dots (a_1 \omega_1 a_2) \omega_2 a_3 \dots] \omega_{n-1} a_n$$

$$(a_1 \omega_1 a_2 \omega_2 \dots \omega_{n-1} a_n)_* = a_1 \omega_1 [\dots a_{n-2} \omega_{n-2} (a_{n-1} \omega_{n-1} a_n) \dots] .$$

Des notations analogues sont utilisées pour $A_i \subseteq E$ à la place des $a_i \in E$. On a :

$$(2') \quad a \in (a \leftarrow b) \rightarrow b, \quad a \rightarrow b \neq \emptyset \implies a \in (a \rightarrow b) \leftarrow b .$$

$$(3_2) \iff (3_2') \quad a \rightarrow (b \leftarrow c) \subseteq (a \rightarrow c) \rightarrow b .$$

$$(3_3) \iff (3_3') \quad a \rightarrow (b \rightarrow c) \subseteq (a \leftarrow c) \rightarrow b .$$

PROPOSITION 1.1 (valable pour $B_i \subseteq E$).

$$a' \in a \omega_1 b_1 \omega_2 \dots \omega_n b_n \iff a \in a' \bar{\omega}_n b_n \bar{\omega}_1 \dots \bar{\omega}_1 b_1 .$$

PROPOSITION 1.2 (valable pour $A_i \subseteq E$).

$$(a_1 \leftarrow a_2 \leftarrow \dots \leftarrow a_n)_* \subseteq (a_1 \leftarrow a_2 \leftarrow \dots \leftarrow a_n)_\alpha \subseteq a_1 \leftarrow a_2 \leftarrow \dots \leftarrow a_n .$$

PROPOSITION 1.3 (valable pour $A_i \subseteq E$).

$$(a_0 \omega_1 a_1 \omega_2 \dots \omega_n a_n)_\alpha \subseteq a_0 \omega'_1 a_{i_1} \omega'_2 \dots \omega'_n a_{i_n} ;$$

$$a_0 \omega_1 a_1 \omega_2 \dots \omega_n a_n \subseteq a_0 \leftarrow a_{i_1} \leftarrow \dots \leftarrow a_{i_k} \rightarrow a_{j_1} \rightarrow \dots \rightarrow a_{j_h} ,$$

où $\omega_{i_1}, \dots, \omega_{i_k} = \leftarrow, \omega_{j_1}, \dots, \omega_{j_h} = \rightarrow, k + h = n$.

E est pré-groupe unitaire si :

$$(4) a \leftarrow 1 = 1 \leftarrow a = a \rightarrow 1 = a, a \neq 1 \implies 1 \rightarrow a = \emptyset, a \rightarrow a = 1 .$$

On note :

$$(5) a \leq b \iff b \rightarrow a \neq \emptyset .$$

PROPOSITION 1.4. - Si E est unitaire, $a \leq b$ est une relation d'ordre ;

$$1 \leq a ; \quad b \leq a \leftarrow b .$$

$F \subseteq E$ est sous-pré-groupe de E si :

$$(6) a, b \in F \implies awb \subseteq F .$$

L'intersection d'une famille de sous-pré-groupe est sous-pré-groupe. Si $X \subseteq E$, l'intersection (X) des sous-pré-groupe contenant X est le sous-pré-groupe engendré par X .

Si l'on considère $\omega_i, 1 \leq i \leq n-1; \omega'_j, 1 \leq j \leq m-1; \omega''_k, 1 \leq k \leq p-1, \dots,$

$$A \omega_i^n B \omega'_j^m C \omega''_k^p \dots = A \omega_1 A \dots \omega_{n-1} A \omega'_1 B \dots \omega'_{m-1} B \omega''_1 C \dots \omega''_{p-1} C \dots .$$

On convient que $A \omega_i^0 = 1, A \omega_i^1 = A, A \omega_i^n B \omega'_j^1 = A \omega_i^n$. Si $\omega_i = \omega, \omega'_j = \omega', \omega''_k = \omega'', \dots$, on écrit $A \omega^n B \omega'^m C \omega''^p \dots$. Par exemple :

$$A \overleftarrow{n} A \overrightarrow{m} = \underbrace{A \leftarrow \dots \leftarrow A}_{n} \rightarrow A \rightarrow \dots \rightarrow A .$$

$\underbrace{\hspace{10em}}_m$

Enfin :

$$A^{\omega_i} B^{\omega_j'} C^{\omega_k''} \dots = \bigcup_{n,m,p,\dots; \omega_i, \omega_j', \omega_k'', \dots} A^{\omega_i n} B^{\omega_j' m} C^{\omega_k'' p} \dots ,$$

de sorte que, par exemple, $A^{\omega_i} A^{\omega_i} = A^{\omega_i}$, et que :

$$(6') \quad X \subseteq F \implies X^{\omega_i} \subseteq F .$$

PROPOSITION 1.5. - $(X) = X^{\omega_i} = X^{\leftarrow} X^{\rightarrow}$.

PROPOSITION 1.6. - $a \in bX^{\omega_i}$ est une relation d'équivalence.

2. Prégroupes de mots.

Soient G un groupe, et $A = \{a_\alpha\}_{\alpha \in I}$ un ensemble indexé d'éléments $a_\alpha \in G$; $(r_i) = (r_1, \dots, r_n)$ avec $r_i \equiv a_{\alpha_i}^{\varepsilon_i}$, $\alpha_i \in I$, $\varepsilon_i \in \{1, -1\}$ est dite A-suite ; si $r_1 r_2 \dots r_n = r \in G$, le couple $((r_i), r)$ est dit A-mot défini par (r_i) de valeur r , qu'on note R ou encore $r_1 r_2 \dots r_n$. Si S est le mot défini par $(s_j) = (s_1, \dots, s_m)$ avec $s_j \equiv a_{\beta_j}^{n_j}$, de valeur s :

$$R \equiv S \iff (r_i) = (s_i) \iff n = m, \alpha_i = \beta_i, \varepsilon_i = \eta_i ;$$

$$R = S \iff r = s ; R \equiv S \implies R = S ;$$

$$RS \equiv r_1 \dots r_n s_1 \dots s_m ; R^{-1} \equiv r_n^{-1} \dots r_1^{-1} .$$

Si $i \leq j$, $(r_i, r_j) \equiv r_i r_{i+1} \dots r_j$ est dit segment de R . Un sous-mot S de R (on écrit $S \subseteq R$) est cosegment de R si l'on a $S \equiv (r_i, r_j)$ ou $R - (r_i, r_j)$; n est la longueur de R , notée $\lambda(R)$; $(\emptyset, 1)$ est le mot vide, noté 1 ; $\lambda(1) = 0$. Un cosegment S est majeur si $\lambda(S) \geq \frac{1}{2} \lambda(R)$.

On note $R \leftarrow S$ l'ensemble des $n+1$ A-mots

$$SR, \dots, r_1 \dots r_i S r_{i+1} \dots r_n, \dots, RS$$

obtenus par insertion de S dans R ; en particulier

$$R \xleftarrow{r_i} S \equiv r_1 \dots r_i S r_{i+1} \dots r_n .$$

Si S_1, \dots, S_p sont les segments de R avec $S_1 \equiv \dots \equiv S_p \equiv S$, on note $R \rightarrow S$ l'ensemble des A-mots

$$R - S_1, \dots, R - S_p$$

obtenus par expulsion d'un segment $\equiv S$ de R ; si de tels segments n'existent pas, $R \rightarrow S \equiv \emptyset$.

L'ensemble des A -mots avec \equiv comme égalité, muni des opérations \leftarrow et \rightarrow , est un pré-groupe unitaire (l'unité est 1) dans lequel

$$S \leq R \iff S \text{ est } \equiv \text{ à un segment de } R .$$

On note R^0 l'ensemble des n A -mots obtenus par permutations circulaires des éléments de R ; en particulier

$$R^{Or_i} = r_i \dots r_n r_1 \dots r_{i-1} .$$

Si $S \subseteq R$, S^{Or_i} est le mot de S^0 commençant par le premier élément de S après r_i , dans R . Si X est un ensemble de A -mots, $X^0 = \bigcup_{R \in X} R^0$; X est circulaire si $X^0 \equiv X$; $X^{00} = X^0$ de sorte que X^0 est circulaire.

PROPOSITION 2.1.

$$(R \leftarrow S)^0 \subseteq (R^0 \leftarrow S) \cup (S^0 \leftarrow R^0) , \quad (R \rightarrow S)^0 \subseteq R^0 \rightarrow S ,$$

$$R \in (R_1 \omega_1 R_2 \dots \omega_{n-1} R_n)^0 \iff R \in R_{i_1}^0 \omega'_1 R_{i_2}^0 \dots \omega'_{n-1} R_{i_n}^0 ,$$

$$R \in (R_1 \leftarrow R_2 \dots \leftarrow R_n)^0 \iff R \in R_{i_1}^0 \leftarrow R_{i_2}^0 \dots \leftarrow R_{i_n}^0 ,$$

$$(X^{\omega_i})^0 \subseteq (X^0)^{\omega_i} , \quad (X^{\leftarrow})^0 \subseteq (X^0)^{\leftarrow} .$$

3. Mots segmentés.

Soit ρ' un ensemble de sous-mots non vides $S' \subseteq R$. Si $S' \equiv r_{i_1} r_{i_2} \dots r_{i_p}$, on considère le segment $S \equiv (r_{i_1}, r_{i_p}) \leq R$, et l'on dit que S' est le support de S . On note ρ l'ensemble des $S \subseteq R$ supportés par les $S' \leq R$. Tout $r_i \in R$ appartient à un $S' \in \rho'$ unique, noté $(r_i)_{\rho'}$, donc au support d'un $S \in \rho$ unique, noté $(r_i)_{\rho}$.

On appelle inter-support S^k de $S \in \rho$, le segment $S^k \equiv (r_{i_{k+1}}, r_{i_{k+1}-1})$ de manière que :

$$S \equiv r_{i_1} S^1 r_{i_2} S^2 \dots S^{p-1} r_{i_p} , \quad S' \equiv r_{i_1} r_{i_2} \dots r_{i_p} .$$

R est segmenté par ρ' (ou ρ est une segmentation de R) si pour tout $S \in \rho$;

$$(1') \quad r_i \in S \implies (r_i)_{\rho'} \subseteq S,$$

$$\iff (1) \quad r_i \in S \implies (r_i)_{\rho} \subseteq S,$$

$$\iff (1^k) \quad r_i \in S^k \implies (r_i)_{\rho} \subseteq S^k,$$

$$\iff (1^0) \quad S_1 \cap S_2 \equiv 1 \text{ ou } S_1 \subseteq S_2^k \text{ ou } S_2 \subseteq S_1^k, \text{ pour tout couple } S_1, S_2 \in \rho \text{ avec } S_1 \neq S_2.$$

Si X est un ensemble de A-mots et si R est segmenté par $\rho' \subseteq X$, on dit que R est segmenté dans X.

PROPOSITION 3.1. - $\rho'_0 \subseteq \rho'$, $R_0 \equiv \bigcup_{S' \in \rho'_0} S' \implies R_0$ est segmenté par ρ'_0 . On dit que le sous-mot R_0 est permis, et que la segmentation ρ_0 est induite par dans R_0 .

PROPOSITION 3.2. - Soient R et S segmentés par ρ' et σ' . Tout élément appartenant à $R \leftarrow S$ est segmenté par $\rho' \cup \sigma'$. Si S est un segment permis et σ' induite par ρ' dans S, l'élément $R - S \in R \rightarrow S$ est segmenté par $\rho' - \sigma'$.

PROPOSITION 3.3. - Si $\rho' = \{R_q\}$, $1 \leq q \leq p$,

$$R \in R_1 \leftarrow R_2 \leftarrow \dots \leftarrow R_p \iff 1 \in R \rightarrow R_p \rightarrow \dots \rightarrow R_1$$

$$\iff R \text{ est segmenté par } \rho'.$$

X^{\leftarrow} est l'ensemble des mots segmentés dans X.

4. Mots réduits.

On note A_0 l'ensemble des A-mots de la forme $a_{\alpha}^{\varepsilon} a_{\alpha}^{-\varepsilon}$. D'après la proposition 1.6, $R \in SA_0^{\omega_i}$ est une relation d'équivalence, notée \simeq . R est réduit si $R \rightarrow A_0 \equiv R$, et circulairement réduit si $R^0 \rightarrow A_0 = R^0$.

PROPOSITION 4.1. - R réduit \iff R de longueur minimum dans sa classe $RA_0^{\omega_i}$. Toute classe $RA_0^{\omega_i}$ contient un mot réduit unique, noté R^* , et appelé le réduit de R.

PROPOSITION 4.2. - $A_0^{\omega_i} = A_0^{\leftarrow}$; $R \simeq S \iff R \in SA_0^{\omega_i} \iff S^{-1} R \in A_0^{\leftarrow}$;
 $RA_0^{\omega_i} = R^* A_0^{\leftarrow}$.

Ainsi, $R \in R^* A_0^{\leftarrow}$, donc d'après la proposition 3.3, R est segmenté par $R^* \cup \gamma'$, $\gamma' \subseteq A_0$. On dit que R est réduit par γ' (ou γ est une réduction de R); une réduction n'est pas unique. On appelle reste de R suivant γ , le sous-mot $R_\gamma = \bigcup_{S' \in \gamma'} S' \subseteq R$, et l'on a $R_\gamma \equiv R^*$ pour toute réduction γ de R .

5. Systèmes de relateurs.

On note A_1 l'ensemble des A-mots unitaires (de valeur 1), et si X est un ensemble de A-mots, $X_A = X \cup X^{-1} \cup A_0$. A est relié par X (ou X est un système de relateurs de A) si $A_1 = X_A^{\omega_i}$; A est libre s'il est relié par \emptyset , autrement dit si $A_1 = A_0^{\omega_i}$, ou encore, d'après la proposition 4.2, si $A_1 = A_0^{\leftarrow}$.

Parmi les réduits des A-mots de R^0 , il en existe de cycliquement réduit, soit par exemple R_1 . On note $R^{*0} = R_1^0$ (qui ne dépend pas du choix de R_1), et $X^{*0} = \bigcup_{R \in X} R^{*0}$.

PROPOSITION 5.1. - A relié par $X \implies A$ relié par X^{*0} .

Dans la suite, on peut donc supposer que $X = X^{*0}$, c'est-à-dire que X est un ensemble circulaire de A-mots circulairement réduits.

PROPOSITION 5.2. - $X_A^{\omega_i} = X_A^{\leftarrow} A_0^{\rightarrow}$; $R = S \iff R \in SX_A^{\omega_i} \iff S^{-1} R \in X_A^{\leftarrow} A_0^{\rightarrow}$.

6. Mots propres.

A étant relié par X , on considère $R \in X_A^{\leftarrow}$, ce qui revient à dire, d'après la proposition 3.3, que R est segmenté par $\rho' \subseteq X_A$. On suppose que R est réduit par γ' , que le couple $r_i r_j \in \gamma'$ et, en permuttant au besoin i et j , on peut supposer que $(r_i)_\rho \cap (r_j)_\rho \equiv 1$ ou $(r_j)_\rho \subseteq (r_i)_\rho^k$, d'après la formule (1°) du paragraphe 3. Si σ est la segmentation induite par ρ dans $(r_j)_\rho = (r_{j_1}, r_{j_2})$ et δ la réduction induite par γ dans (r_{i+1}, r_{j-1}) , on note

$$\bar{R} \equiv R - (r_j)_\rho \xleftarrow{r_i} (r_j)_\rho^{Or_j} \equiv R - (r_{i+1}, r_{j-1}) \xleftarrow{r_{j_2}} (r_{i+1}, r_{j-1})^{Or_{j_1}},$$

$$\bar{\rho}' = (\rho' - \sigma') \cup \{S' \}_{S' \in \sigma'}^{Or_{j_1}}, \quad \bar{\gamma}' = (\gamma' - \delta') \cup \{S' \}_{S' \in \delta'}^{Or_{j_1}}.$$

PROPOSITION 6.1. - \bar{R} est segmenté par $\bar{\rho}'$ et réduit par $\bar{\gamma}'$; $\bar{R} \simeq R$.

Parmi les supports $S' \in \rho' \subseteq X_A = X \cup X^{-1} \cup A_0$, on distingue les A_0 -supports $S' \in A_0$ et les $X \cup X^{-1}$ -supports $S' \in X \cup X^{-1}$.

Le couple $r_i r_j \in R$ est dit propre si les trois relations suivantes sont incompatibles :

$$(1) \quad \begin{cases} r_i r_j \simeq 1, & (r_i, r_j) \simeq 1, \\ (r_i)_{\rho'} \xleftarrow{r_i} (r_j)_{\rho'} \text{ Or }^j \simeq 1 \text{ ou } (r_i)_{\rho'} \text{ ou } (r_j)_{\rho'} \text{ Or }^j. \end{cases}$$

R est propre si tous les couples $r_i r_j \in R$ sont propres.

PROPOSITION 6.2. - R propre \iff Pour toute réduction γ de R , un couple de réduction $r_i r_j \in \gamma'$ est tel que $(r_i)_{\rho'}$, et $(r_j)_{\rho'}$, sont des $(X \cup X^{-1})$ -supports avec $(r_i)_{\rho'} \xleftarrow{r_i} (r_j)_{\rho'} \text{ Or }^j \neq 1$.

On considère maintenant dans X_A^{\leftarrow} , les classes d'équivalence $RA_0^{\omega_i} \cap X_A^{\leftarrow}$, suivant \simeq .

PROPOSITION 6.3. - R de longueur minimum dans sa classe $RA_0^{\omega_i} \cap X_A^{\leftarrow} \implies R$ propre.

De la sorte, tout mot de X_A^{\leftarrow} a une présentation propre, en ce sens que :

$\forall R \in X_A^{\leftarrow}, \exists R^{\text{pr}} \text{ propre} \in X_A^{\leftarrow} : R \simeq R^{\text{pr}}$. On a :

$$R = 1 \iff R \in A_1 \iff R \in X_A^{\omega_i} \iff R^* \in X_A^{\omega_i} \quad (\text{proposition 4.2})$$

$$\iff R^* \in X_A^{\leftarrow} A_0^{\rightarrow} \quad (\text{proposition 5.2})$$

$$\iff R^* \simeq S \in X_A^{\leftarrow} \iff R^* \simeq S^{\text{pr}} \in X_A^{\leftarrow} \quad (\text{proposition 6.3}) .$$

On note $X_A^{\leftarrow \text{pr}}$ l'ensemble des mots propres de X_A^{\leftarrow} .

Problème des mots : A étant relié par X et B un A -mot réduit :

Décider si $B = 1 \iff$ Décider si B est le réduit d'un $R \in X_A^{\leftarrow \text{pr}}$.

7. Résidu. Mots simples.

On considère $R \in X_A^{\leftarrow}$, donc segmenté par $\rho' = \{R_1, \dots, R_q, \dots, R_p\} \subseteq X_A$; p est le degré de R , noté $\delta(R)$. Si p est une réduction de R , le sous-mot $R_q \cap R_p \subseteq R$ est dit γ -résidu de R_q . Le γ -résidu $R_q \cap R_p$ est simple s'il est

cosegment de R_q , R_γ et R (ce qui implique qu'il est, soit segment, soit complément de segment des trois). R est γ -simple si tous les γ -résidus sont simples ; il est simple s'il est γ -simple pour toute réduction γ .

Soient U et U_q les segments supportés par $R_q \cap R_\gamma$ dans R et R_q ; r_i le premier élément de U ; V_q tel que $U_q V_q \in R_q^0$. On considère

$$S \equiv UV_q, \quad T \equiv R - U \xleftarrow{r_{i-1}} U_q,$$

ainsi que σ' , $\tau' \subseteq \rho'$ définis par

$$\sigma' = \{S'\}_{R_q \not\subseteq S' \subseteq U}, \quad \tau' = \{S'\}_{R_q \not\subseteq S' \subseteq R-U}.$$

PROPOSITION 7.1. - S , T sont segmentés par $R_q^{i-1} \cup \sigma'$, $R_q \cup \tau'$.

PROPOSITION 7.2. - R propre $\implies S$, T propres.

Il s'ensuit que :

$$\left. \begin{array}{l} R \in X_A^{\leftarrow pr} \\ R_q \cap R_\gamma \text{ multiple} \end{array} \right\} \iff S, T \in X_A^{\leftarrow pr} \text{ avec } \delta(S), \delta(T) < \delta(R),$$

de sorte que, si M est l'ensemble comprenant $X \cup X^{-1}$, et les $R \in X_A^{\leftarrow pr}$ ayant, pour une certaine réduction γ , deux γ -résidus simples majeurs, on a la proposition suivante :

PROPOSITION 7.3. - Un mot $R \in X_A^{\leftarrow pr} - M$ de degré minimum (qu'on appellera primitif) est simple, n'ayant que des $(X \cup X^{-1})$ -supports.

On remarque que $R \in M$ a de toute façon un γ -résidu simple majeur qui est segment de $(X \cup X^{-1})$ -support.

Un mot simple $R \in (X \cup X^{-1})^{\leftarrow pr} - M$ est singulier. Le système de relateurs X est régulier, si :

$$\begin{aligned} X_A^{\leftarrow pr} = M &\iff (X \cup X^{-1})^{\leftarrow pr} \text{ ne contient pas de mots primitifs (prop. 7.3) ;} \\ X_A^{\leftarrow pr} = M &\iff (X \cup X^{-1})^{\leftarrow pr} \text{ ne contient pas de mots singuliers (prop. 7.3).} \end{aligned}$$

8. Relateurs progressifs et réguliers.

$R \in X_A^{\leftarrow \text{pr}}$ est progressif si $\lambda(R^*) \geq \lambda(R_q)$, $1 \leq q \leq p$; X est progressif, si :

Tout $R \in X_A^{\leftarrow \text{pr}}$ est progressif \iff Tout $R \in (X \cup X^{-1})^{\leftarrow \text{pr}}$ est progressif (proposition 6.2).

PROPOSITION 8.1. - X progressif $\implies \lambda(S^*)$, $\lambda(T^*) \leq \lambda(R^*)$.

Algorithme de Dehn. - Soient B un A -mot réduit, X un système de relateurs de A et $R_i \in X \cup X^{-1}$. On détermine les couples (R_1, B_1) tels que B_1 soit réduit d'un élément de $B \leftarrow R_1$ avec $\lambda(B) \geq \lambda(B_1)$. Pour chaque couple (R_1, B_1) , on détermine les couples (R_2, B_2) tels que B_2 soit réduit d'un élément de $B_1 \leftarrow R_2$ avec $\lambda(B_1) \geq \lambda(B_2)$, etc.

Si X est progressif, cet algorithme est fini, en ce sens que pour un certain n : soit $\nexists B_n$ (l'algorithme est néгатif), soit $B_n \equiv 1$ (l'algorithme est positif). B est un mot de Dehn si l'algorithme relatif à B est positif, et alors $B \simeq R \in X_A^{\leftarrow}$, donc $B = 1$.

Si R est simple, on a pour toute réduction $\gamma : R^* \equiv S_1 S_2 \dots S_m$; S_j γ -résidus simples de $R_{q_j} \in \rho' \subseteq X \cup X^{-1}$, en remplaçant au besoin R par un autre mot de R^0 . On suppose de plus que parmi les présentations simples de R^* , R comporte un γ -résidu S_j de R_{q_j} de longueur maximum. Si r_{i_j} est le premier élément de S_j et T_j tel que $S_j T_j \in R_{q_j}^0$, on note

$$P \equiv R - S_j \xleftarrow{r_{i_j}^{-1}} T_j^{-1},$$

et alors

$$P_j^* \equiv S_1 \dots S_{j-1} T_j^{-1} S_{j+1} \dots S_m.$$

PROPOSITION 8.2. - P_j est segmenté par $\{R_{q_1}^c, \dots, R_{q_{j-1}}^c, R_{q_{j+1}}^c, \dots, R_{q_m}^c\}$ où $R_q^c \in R_q^0$, de sorte que $\delta(P_j) < \delta(P)$.

PROPOSITION 8.3. - R propre $\implies P_j$ propre.

PROPOSITION 8.4. - Un mot non-progressif de degré minimum est singulier, de sorte que : X régulier $\implies X$ progressif.

PROPOSITION 8.5. - X régulier $\iff X$ tel que le problème des mots est résoluble par l'algorithme de Dehn.

9. Mots primitifs.

On suppose maintenant que parmi les présentations primitives (donc simples) de R^* , R comporte un nombre de γ -résidus $S_j \neq \emptyset$ minimum. Puisque, d'après les propositions 8.2 et 8.3, $P_j \in (X \cup X^{-1})^{\leftarrow pr}$ avec $\delta(P_j) < \delta(R)$, P_j a deux γ -résidus simples majeurs, qui, étant donné la forme de P_j^* , sont nécessairement :

$$S_{j-1} V_j^{-1} \quad \text{et} \quad U_j^{-1} S_{j+1} \quad \text{où} \quad T_j = U_j Q_j V_j .$$

PROPOSITION 9.1. - On a, à une permutation circulaire près :

$$(2) \quad R_{q_1} \equiv S_1 U_2 Q_1 U_1^{-1}, \quad R_{q_2} \equiv S_2 U_3 Q_2 U_2^{-1}, \quad \dots,$$

$$R_{q_j} \equiv S_j U_{j+1} Q_j U_j^{-1}, \quad \dots, \quad R_{q_m} \equiv S_m U_j Q_m U_m^{-1},$$

avec $S_j U_{j+1}$, $U_{j+1} Q_j U_j^{-1}$, $U_j^{-1} S_j$ segments majeurs de R_{q_j} , sauf peut-être $U_{j+1} Q_j U_j^{-1}$ pour un certain j .

Si

$$P \equiv R - S_1 \xleftarrow{r_{i_1-1}} T_1^{-1} - \dots - S_m \xleftarrow{r_{i_m-1}} T_m^{-1},$$

on a

$$P^* \equiv (Q_1^{-1} \dots Q_m^{-1})^* \simeq T_1^{-1} \dots T_m^{-1}, \quad \delta(P) < \delta(R) .$$

PROPOSITION 9.2. - L'algorithme de Dehn relatif à P^* est positif. En particulier, P^* contient deux cosegments majeurs de $R_q \neq R_{q_j}$, $1 \leq j \leq m$.

D'après les propositions 9.1 et 9.2 :

X régulier \iff Pour toute suite (2) de mots de $X \cup X^{-1}$, l'algorithme de Dehn relatif à $(Q_1^{-1} \dots Q_m^{-1})^*$ est négatif.

Si la condition est vérifiée pour tout $m \leq \nu$, on peut décider par l'algorithme de Dehn relatif à B si :

$$B \simeq R \in Y_A^{\leftarrow} \quad \text{ou} \quad Y \in (X \cup X^{-1})^{\leftarrow \nu}$$

(par exemple si B s'écrit comme produit de $\leq v$ conjugués de mots de $X \cup X^{-1}$).

On a

$$(R_{q_i}^{-1} \xleftarrow{U_{i+1}^{-1}} R_{q_{i+1}}^{-1} \xleftarrow{U_{i+2}^{-1}} \dots \xleftarrow{U_i^{-1}} R_{q_j}^{-1})_* \simeq U_i Q_i^{-1} \dots Q_j^{-1} U_j^{-1} S_j^{-1} \dots S_j^{-1} ,$$

et d'après la proposition 9.2, $\exists i, j, R_q, x$:

$$(R_{q_i}^{-1} \xleftarrow{U_{i+1}^{-1}} \dots \xleftarrow{U_i^{-1}} R_{q_j}^{-1} \xleftarrow{x} R_q)_*^* \equiv V_i^{-1} Q V_j^{-1} S_j^{-1} \dots S_i^{-1} ,$$

où $V_i^{-1} S_i^{-1}, V_j^{-1} S_j^{-1}, Q$ sont γ -résidus simples de $R_{q_i}^{-1}, R_{q_j}^{-1}, R_q$ avec $\lambda(V_i^{-1} S_i^{-1}) \geq \lambda(R_{q_i}), \lambda(V_j^{-1} S_j^{-1}) \geq \lambda(R_{q_j}), \lambda(Q) \leq \lambda(R_q)$. On remarque que $Q_i, \dots, Q_j \neq \emptyset \implies j - i + 1 \leq \lambda(R_q)$, et l'on note $\lambda = \sup_{R \in X} \lambda(R)$. D'autre part $(R_1 \leftarrow \dots \leftarrow)_*^S$ est un mot simple appartenant à $(R_1 \leftarrow \dots \leftarrow R_i)_*$ avec $R_i \in X \cup X^{-1}$. On considère les conditions finies (en ce sens qu'on peut les vérifier par un nombre fini d'essais) :

(C) Pour tout $i \leq \lambda + 1$, $(R_1 \leftarrow \dots \leftarrow R_i)_*^S$ a trois γ -résidus majeurs (dont un strictement majeur).

(C_n) Il existe $n \leq \lambda$ tel que $(R_1 \leftarrow \dots \leftarrow R_i)_*^S$ ait trois γ -résidus majeurs (dont un strictement pour $i \leq n - 1$, et quatre γ -résidus majeurs pour $i = n$).

(C₄) $(R_1 \leftarrow R_2 \leftarrow R_3 \leftarrow R_4)_*^S$ n'a que des γ -résidus majeurs.

Soient maintenant S, S_i des segments de $R, R_i \in X \cup X^{-1}$ tels que $\{S_i\}$ n'est pas une partition de S , et les conditions :

$$(C'_4) S \equiv S_1 S_2 S_3 \implies \lambda(S) \leq \frac{1}{2} \lambda(R) ,$$

$$(C'_3) S \equiv S_1 S_2 \implies \lambda(S) \leq \frac{1}{4} \lambda(R) ,$$

$$(C'_2) S \equiv S_1 \implies \lambda(S) \leq \frac{1}{6} \lambda(R) .$$

PROPOSITION 9.3. - (C'_2) ou $(C'_3) \implies (C'_4) \implies (C_4)$.

$(C_n) \implies (C) \implies X$ régulier.