ALGÈBRE. – *Sur l'algèbre associée à un code bipréfixe.* Note (*) de **Christophe Reutenauer,** transmise par Marcel Schützenberger.

Nous montrons qu'un code maximal et rationnel est bipréfixe si et seulement si son algèbre syntactique est semisimple.

We show that a maximal and rational code is biprefix if and only if its syntactic algebra is semisimple.

On se donne un monoïde libre X^* engendré par un ensemble fini non vide X et un corps commutatif K de caractéristique nulle. Un *code* est une partie C de X^* qui est la base d'un sous-monoïde libre; autrement dit de toute relation :

$$u_1 \dots u_m = v_1 \dots v_n,$$

avec des mots u_i et v_j dans C, se déduit $n=m$ et $u_i=v_i$ pour tout i ([2], chap. 5). Une partie $C \neq 1$ qui ne contient aucun de ses facteurs gauches ni droits (i.e. $u, uv \in C \Rightarrow v=1$ et $v, uv \in C \Rightarrow u=1$) est un code comme on le vérifie aisément : c'est un *code bipréfixe* (notion introduite et étudiée en [7]). Une *série formelle* est une application $S : X^* \to K$; comme X^* s'identifie à une base de la K-algèbre libre sur X (i.e. les polynômes non commutatifs en X), notée $K\langle X\rangle$, une série formelle n'est rien d'autre qu'une forme linéaire sur $K\langle X\rangle$. La dualité est notée (S, P) pour toute série formelle S et tout polynôme P. *L'idéal syntactique* [6] d'une série formelle S est le plus grand idéal de $K\langle X\rangle$ contenu dans le noyau de S; l'algèbre syntactique de S est le quotient de $K\langle X\rangle$ par cet idéal. L'*algèbre syntactique d'un code* C est l'algèbre syntactique de la *série formelle caractéristique* de C^*, le sous-monoïde engendré par C; on note encore C^* cette série et l'on a donc $(C^*, w)=1$ si $w \in C^*$ et $(C^*, w)=0$ sinon. Un code est *rationnel* si c'est une partie rationnelle de X^* [(2), chap. 6]. D'après le théorème de Kleene (*ibid.*) il est équivalent de dire que C est reconnaissable (et C rationnel $\Leftrightarrow C^*$ rationnel).

THÉORÈME 1. – *L'algèbre syntactique d'un code bipréfixe rationnel est semisimple.*

Notons qu'elle est toujours de dimension finie comme nous le verrons, et qu'un code fini est toujours rationnel.

Remarques. – 1. Ce théorème est une extension du théorème de Maschke, puisqu'à tout groupe fini G on peut associer canoniquement un code bipréfixe rationnel (qui représente en quelque sorte sa table de multiplication) dont l'algèbre syntactique est K [G].

2. En général la K-algèbre du monoïde syntactique ([2], chap. 6) d'un code bipréfixe rationnel (même fini et maximal) n'est pas semisimple. Mais il est démontré en [5] qu'un code préfixe maximal fini est bipréfixe si et seulement si son monoïde syntactique est nil-simple.

Preuve. – Soit C un code rationnel.

(i) Soit M le monoïde syntactique de C^*; il est fini d'après le théorème de Kleene. Selon que C^* est *complet* (i.e. rencontre tous les idéaux bilatères de X^*) ou non, M n'a pas de zéro ou en a un; dans le premier cas il possède un unique idéal minimal et dans le second un unique idéal 0-minimal [1]; dans les deux cas nous le notons S, et pour éviter deux démonstrations quasi identiques nous utiliserons les notations de [2], chap. 8, et dirons que S est l'idéal (0)-minimal de M. S est un semigroupe complètement (0)-simple ([2] chap. 3); soit R le radical de K_0 [S], le K-algèbre contractée de S (i.e. la K-algèbre de S, dont on a identifié le zéro à l'éventuel zéro de S). On a alors $K_0[S].R.K_0[S]=0$ (th. de Teissier-Munn *voir* [3]).

(ii) D'après le théorème de Rees-Suschkewitsch ([2], chap. 3) S s'identifie à un *semigroupe de matrices de Rees* $S=\mathscr{M}(G, I, \Lambda, P)$. On peut de surcroît supposer que $1\in I\cap\Lambda$ et $p_{1,i}$, $P_{\lambda,1}\in\{0,1\}$ pour tous $i\in I$, $\lambda\in\Lambda$ et que l'image M' de C* dans M rencontre la H-classe de coordonnées (1, 1). Nous notons $S'=S\cap M$. On déduit facilement de la condition $0\notin S'$ (puisque C* ne contient aucun idéal de X* sauf dans le cas trivial C=X) l'existence d'un sous-groupe H de G, de parties $I'\subset I$ et $\Lambda'\subset\Lambda$ telles que $S'=\{(g)_{i,\lambda}\mid g\in H, i\in I', \lambda\in\Lambda'\}$ et que $p_{\lambda,i}\in H$ pour $\lambda\in\Lambda'$, $i\in I'$ (*cf.* [8]).

(iii) Si C est supposé bipréfixe, on a les deux conditions :

$$\forall\lambda\in\Lambda',\quad \forall i\in I\setminus I'\ p_{\lambda,i}=0 \qquad \text{et} \qquad \forall i\in I',\quad \forall\lambda\in\Lambda\setminus\Lambda'\ p_{\lambda,i}=0.$$

En effet, si l'on avait $p_{\lambda,i}\neq 0$ pour $\lambda\in\Lambda'$ et $i\in I\setminus I'$ alors, comme $(1)_{1,\lambda}(p^{-1}_{\lambda,i})_{i,\lambda}=(1)_{1,\lambda}\in S'$, on déduit de la préfixité de C que $(p^{-1}_{\lambda,i})_{i,\lambda}\in M'$ ([2], chap. 5) ce qui n'est pas. L'autre condition s'obtient symétriquement. (On peut montrer que les deux conditions ci-dessus impliquent la bipréfixité de C, cependant que la première seule caractérise sa préfixité.)

(iv) Soit $a=\sum_{\substack{g\in G\\ i\in I,\lambda\in\Lambda}} a_{g,i,\lambda}(g)_{i,\lambda}\in R$. Alors d'après (i) :

$$0=(1)_{1,1}\,a\,(1)_{1,1}=\sum a_{g,i,\lambda}(p_{1,i}gp_{\lambda,1})_{1,1}$$

et d'après (iii) :

$$0=\sum_{\substack{g\in G\\ i\in I',\lambda\in\Lambda'}} a_{g,i,\lambda}(g)_{1,1}$$

donc on a pour tout g dans G :

$$\sum_{i\in I',\lambda\in\Lambda'} a_{g,i,\lambda}=0.$$

(v) Soit ψ la forme linéaire sur $K_0[M]$ définie par $\psi(m)=1$ si $m\in M'$ et $\psi(m)=0$ si $m\in M\setminus M'$. D'après (ii) et (iv), $a\in R$ implique $\psi(a)=0$ donc $R\subset\operatorname{Ker}\psi$. $K_0[S]$ étant un idéal dans $K_0[M]$, R est un idéal de $K_0[M]$ contenu dans $\operatorname{Ker}\psi$.

(vi) Soit φ le morphisme syntactique $X^*\to M$; il se prolonge en un morphisme de K-algèbres $\varphi: K\langle X\rangle\to K_0[M]$. Alors la forme linéaire C* sur $K\langle X\rangle$ est égale à $\psi\circ\varphi$, donc $\operatorname{Ker}\varphi$ étant un idéal de $K\langle X\rangle$ contenu dans $\operatorname{Ker}C^*$, il est contenu dans l'idéal syntactique $\mathscr{I}$ de C*. Soit $\mathfrak{M}=K\langle X\rangle/\mathscr{I}$ l'algèbre syntactique de C et $\mu: K\langle X\rangle\to\mathfrak{M}$ le morphisme canonique; il existe donc un morphisme de K-algèbres $\nu: K_0[M]\to\mathfrak{M}$ tel que $\mu=\nu\circ\varphi$.

(vii) Alors $\varphi^{-1}(R)$ est un idéal contenu dans $\operatorname{Ker}C^*$, donc contenu dans $\mathscr{I}$ et l'on a : $\nu(R)=\nu\circ\varphi(\varphi^{-1}(R))=\mu(\varphi^{-1}(R))=0$. Par suite l'image $\mathfrak{M}'$ de $K_0[S]$ dans $\mathfrak{M}$ est une algèbre semisimple. Soit $J=X^*\cap\varphi^{-1}(S)$. Alors $\varphi(J)=S$, donc $\varphi(K[J])=K_0[S]$ et $\mathfrak{M}'=\mu(K[J])$.

(viii) Nous montrons maintenant que $\mathfrak{M}'=\mathfrak{M}$. Soit $\mathscr{A}=(Q, 1, 1)$ l'automate minimal de C*. J est exactement l'ensemble des mots induisant sur Q une application (partielle) de rang $\geqq 1$ minimum, ou l'application vide ([2], chap. 8). Par conséquent pour tout $q\in Q$ il existe $w\in J$ tel que $1.w=q$, puisque $\mathscr{A}$ est transitif. $V=K^Q$ devient naturellement un $K\langle X\rangle$-module à droite; soit $\mathscr{J}$ l'idéal à droite défini par $\mathscr{J}=\{P\in K\langle X\rangle\mid 1.P=0\}$.

La condition précédente implique que $K\langle X\rangle=\mathscr{J}+K[J]$. Nous appelons idéal syntactique droit de C* le plus grand idéal à droite de $K\langle X\rangle$ contenu dans $\operatorname{Ker}C^*$ et le notons $\mathscr{I}^d$. Comme il existe une forme linéaire θ sur V telle que $(C^*, P)=\theta(1.P)$, $\mathscr{J}$ est contenu dans $\operatorname{Ker}C^*$ donc dans $\mathscr{I}^d$. On a donc $K\langle X\rangle=\mathscr{I}^d+K[J]$.

(ix) Soit $(\lambda, \bar{\mu}, \gamma)$ une représentation linéaire réduite de C*, de dimension n [4]. On a les propriétés suivantes : (*a*) $\mathscr{I} = \operatorname{Ker} \mu$ [6]; (*b*) $\mathscr{I}^d = \{P \mid \lambda \bar{\mu} P = 0\}$ [4]; (*c*) $K^n = \lambda \bar{\mu} (K \langle X \rangle)$. D'après (*a*) on peut identifier μ et $\bar{\mu}$, $\mathfrak{M}$ et $\mu (K \langle X \rangle)$. $\mathfrak{M}'$ étant une algèbre semisimple, elle admet un élément unité, soit E. On a d'après (*c*), (viii), (*b*) et (vii) :

$$K^n = \lambda\mu (K \langle X \rangle) = \lambda\mu (\mathscr{I}^d + K [J]) = \lambda\mu (K [J]) = \lambda \mathfrak{M}' = \lambda \mathfrak{M}' E,$$

donc E étant de rang n et idempotent est la matrice unité de $\mathscr{M}_n (K)$. On a $E = \mu (P)$ pour un $P \in K [J]$ donc $\mathfrak{M} = \mu (K \langle X \rangle P) \subset \mu (K [J]) = \mathfrak{M}'$, car $K [J]$ est un idéal dans $K \langle X \rangle$.

Sous une hypothèse supplémentaire, le théorème 1 admet une reciproque. Rappelons qu'un code rationnel est *maximal* (comme code) si et seulement s'il est complet ([2], chap. 6).

THÉORÈME 2. – *Si l'algèbre syntactique d'un code rationnel complet est semisimple, ce code est bipréfixe.*

Preuve. – Nous reprenons les notations de (i), (ii) et (vi). Comme C* est complet M n'a pas de zéro et les $p_{\lambda, i}$ sont tous dans G. Soit $i, j \in I, \lambda \in \Lambda'$ et $a = \sum_{g \in G} (g)_{i, \lambda} - (g)_{j, \lambda}$. On a alors pour tout $s \in S$, $s = (h)_{k, \mu}$:

$$sa = \sum_{g \in G} (hp_{\mu, i} g)_{k, \lambda} - (hp_{\mu, j} g)_{k, \lambda} = 0,$$

puisque $hp_{\mu, i} G = hp_{\mu, j} G = G$.

Donc a est dans le radical de K_0 [S], d'après [3]. Par suite, d'après l'hypothèse, $\psi (a) = 0$ et l'on en déduit que i et j sont simultanément dans I'. Donc $I' = I$ et de même $\Lambda = \Lambda'$. C est donc bipréfixe.

COROLLAIRE. – *Un code rationnel complet est bipréfixe si et seulement si son algèbre syntactique est semisimple.*

Remarques. – 1. Les deux théorèmes sont encore vrais si l'on suppose que K est un corps dont la caractéristique ne divise pas l'ordre du groupe de Suschkewitsch du code.

2. Le code incomplet $\{a, ab\}$ a une algèbre syntactique simple mais il n'est pas bipréfixe.

(*) Remise le 15 décembre 1980.

[1] A. DE LUCA, D. PERRIN, A. RESTIVO et S. TERMINI, *Discrete Math.*, 27, 1979, p. 297-308.
[2] G. LALLEMENT, *Semigroups and Combinatorial Applications*, John Wiley, New York.
[3] G. LALLEMENT et M. PETRICH, *Trans. Amer. Math. Soc.*, 139, 1969, p. 404.
[4] M. FLIESS, *J. Math. pures appl.*, 53, 1974, p. 206.
[5] D. PERRIN, *Theor. Comput. Sc.*, 9, 1979, th. 3.1, p. 236.
[6] C. REUTENAUER, *J. Algebra*, 66, 1980, p. 448-483.
[7] M. P. SCHÜTZENBERGER, *Annals Math. Stat.*, 32, 1961, p. 1201-1213.
[8] M. P. SCHÜTZENBERGER, *Bull. Soc. math. Fr.*, 93, 1965, p. 213.

Institut de Programmation, 4, place Jussieu, 75230 Paris Cedex 05.