Construction des bases standard des sous-$K\langle A\rangle$-modules à droite.

Guy Melançon
Département de mathématiques et d'informatique
Université du Québec à Montréal, C.P. 8888, Succ. 'A'
Montréal, Québec, Canada H3C 3P8

1 Introduction.

On sait depuis P.M. Cohn [3] que tout idéal à droite de $K\langle A\rangle$ est libre (comme $K\langle A\rangle$-module à droite). Berstel et Reutenauer en ont donné une nouvelle preuve qui utilise les codes préfixes ([1, Chap. II, Th. 3.2]). La présence des codes préfixes dans ce contexte est liée aux résultats de Schützenberger [7] concernant les représentations minimales des séries rationelles (en variables non-commutatives) en rapport avec les récurrences linéaires que satisfont ces séries. Nous présentons des bases pour les sous-$K\langle A\rangle$-modules à droite de $K\langle A\rangle^q$, que nous appelons *bases standard* (voir paragraphes 4, 5). Dans le cas où $q = 1$, ces sous-modules (sous-$K\langle A\rangle$-modules à droite) sont des idéaux à droite de $K\langle A\rangle$ et la construction des bases standard est très proche de la construction de Schreier d'une base d'un sous-groupe du groupe libre (voir [4,5]).

Dans le but de donner une construction effective de la base standard d'un sous-module, on munit l'ensemble des mots du monoïde libre A^* d'un ordre $\leq$, satisfaisant certaines conditions de compatibilité (voir paragraphe 2). Cet ordre est un analogue non commutatif de celui imposé sur l'ensemble des monômes de $K[z_1, \ldots, z_n]$ pour le calcul des *bases de Gröbner* (ou *bases standard*) des idéaux de cet anneau (voir Rem. 2.1). Les algorithmes que nous donnons, qui permettent le calcul de la base standard d'un sous-module, sont analogues à ceux déjà existant dans le cas des bases de Gröbner de $K[z_1, \ldots, z_n]$ (voir [2]). Les calculs effectués sur les systèmes de générateurs se font tous à l'aide de *réécritures élémentaires*. Ces réécritures élémentaires sont inspirées des transformations de Nielsen (voir [4,5]) utilisées pour le calcul d'une *base réduite* d'un sous-groupe de type fini du groupe libre.

Une des principales applications de nos résultats est de rendre effectif le travail avec les sous-modules $\mathcal{M}$ de $K\langle A\rangle^q$ et les quotients $K\langle A\rangle^q/\mathcal{M}$. L'ordre $\leq$ étant fixé, on montre l'*unicité* de la base standard d'un sous-module (Th. 4.6, Th. 5.9). L'algorithme de calcul de la base standard d'un sous-module de type fini permet de tester si deux sous-modules de type fini sont égaux (Cor. 4.8, Cor. 5.11). On est aussi en mesure de tester si un élément de $K\langle A\rangle^q$ appartient à un sous-module $\mathcal{M}$ et on peut résoudre le "problème des mots" dans le quotient $K\langle A\rangle^q/\mathcal{M}$ (Cor. 4.9, Cor. 5.12).

Dans [6], Mora construit des bases de Gröbner des *idéaux bilatères de* $K\langle A\rangle$. Notre approche

est sensiblement différente et nous livre des résultats d'une autre nature. D'une part, nous considérons les idéaux à droite de $K<A>$. D'autre part, nous nous inspirons de Cohn [3] pour introduire la notion de $\leq$-dépendance à droite d'une famille de polynômes; ce faisant, nous obtenons une version adaptée à notre contexte de l'*Algorithme faible de* Cohn. Nous développons d'abord, aux paragraphes 2, 3 et 4, la théorie pour les idéaux (le cas $q = 1$); nous généralisons ensuite aux dimensions supérieures ($q \geq 1$) (paragraphe 5).

2 Recteurs des polynômes et $\leq$-Dépendance.

Dans tout ce qui suit, A désigne un ensemble qu'on appelle *alphabet*, dont les éléments sont appelés des *lettres*. Les éléments du monoïde libre sur A, A^*, seront appelés des *mots*. Une partie X de mots non vides est un *code préfixe* si aucun mot de X n'est facteur gauche d'un autre mot de X. Par exemple, $\{abc, ac, b\}$ et $\{a^n b : n \geq 0\}$ sont des codes préfixes. Dans toute la suite, K désignera un corps. On note $K<A>$ la K-algèbre associative libre sur A. C'est l'algèbre des *polynômes* non commutatifs sur A. C'est aussi le K-module libre sur A^*; les polynômes de $K<A>$ sont des combinaisons linéaires de mots de A^* à coefficients dans K. On désigne le coefficient d'un mot w dans un polynôme P par (P, w). On écrira abusivement $w \in P$ lorsque $(P, w) \neq 0$. On peut donc définir l'addition et la multiplication de deux polynômes P et Q par les égalités:

$$(P + Q, w) = (P, w) + (Q, w),$$

$$(PQ, w) = \sum_{u \in P, v \in Q, uv = w} (P, u)(Q, v).$$

Notez que les mots de A^* peuvent être considérés comme des polynômes de $K<A>$.

On se donne un *bon ordre* $\leq$ sur l'ensemble des mots. On suppose que cet ordre est *compatible avec la multiplication à droite* et qu'il est *préfixiel*, c'est-à-dire qu'il satisfait:

$$\text{Pour tous mots } u, v, w \in A^*, u \leq v \text{ implique } uw \leq vw, \tag{1}$$

$$\text{Si } u, v, w \in A^*, v \text{ est non vide et } w = uv \text{ alors } u < w. \tag{2}$$

De la deuxième condition on déduit que $1 \leq w$ pour tout $w \in A^*$.

Remarque 2.1 Soit $Z = \{z_1, \ldots, z_n\}$ un ensemble d'*indéterminées* qui commutent deux à deux; désignons par $K[Z]$ l'anneau de *polynômes commutatifs* sur Z à coefficient dans K. Dans la théorie des *Bases de Gröbner* (ou *Bases standard*) des idéaux de $K[Z]$ (voir [2]), dans le but de formuler des algorithmes qui calculent les bases standard des idéaux, on impose un *bon ordre* $<$ sur l'ensemble des monômes $z_1^{\alpha_1} \ldots z_n^{\alpha_n}$ de $K[Z]$. Ce bon ordre doit être *compatible avec la multiplication* et doit satisfaire: $1 < z_1^{\alpha_1} \ldots z_n^{\alpha_n}$, où 1 est l'élément unité de l'anneau et où $z_1^{\alpha_1} \ldots z_n^{\alpha_n}$ est un monôme quelconque de $K[Z]$. On voit donc que les conditions (1) et (2) nous

donne un analogue non commutatif des conditions imposées sur l'ensemble des monômes dans le cas commutatif. ◇

Exemple 2.2 L'ordre du dictionnaire des mots croisés est un ordre qui satisfait nos conditions. Cet ordre est construit en ordonnant d'abord les mots par longueur, puis lexicographiquement sur chacune des longueurs. Plus précisément, $u < v$ si et seulement si soit $|u| < |v|$, soit $|u| = |v|$ et $u <_{lex} v$. ◇

Soit $P \in K\langle A\rangle$; le *recteur* [1] de P est le mot le plus grand qui y apparaît: $r(P) = \max\{w : w \in P\}$. On posera $r(0) < r(P), \forall P \in K\langle A\rangle$. Nous dirons d'un polynôme qu'il est *unitaire* si le coefficient de son recteur est égal à 1. En d'autres mots, un polynôme P est unitaire s'il s'écrit sous la forme: $P = u + \sum_{v<u}(P, v)v$.

Lemme 2.3 *Soient* $P, Q, P_n, Q_n \in K\langle A\rangle$ $(n = 1, \ldots, N)$.
(i) Pour tout $w \in A^*$, *on a* $r(Pw) = r(P)w$,
(ii) $r(PQ) = \max\{r(Pw) : w \in Q\}$,
(iii) $r(\sum_{n=1}^{N} P_nQ_n) \leq \max_{n=1,\ldots,N} r(P_nQ_n)$.

Démonstration. (i) Soit $w' \in Pw$. Alors $w' = uw$ pour un certain $u \in P$. Comme $u \leq r(P)$, la condition (1) entraine $uw \leq r(P)w$, d'où l'assertion.
(ii) Il est clair, selon le point (i) de la démonstration, que si le mot $\max\{r(Pw) : w \in Q\}$ a un coefficient non nul dans PQ, alors c'est le recteur de PQ. Soient $u = r(P)$ et $w_1 \in A^*$ tels que $uw_1 = \max\{r(Pw) : w \in Q\}$. Il nous faut montrer que $(PQ, uw_1) \neq 0$. Supposons qu'au contraire on ait $(PQ, uw_1) = 0$. Alors c'est qu'il existe des mots $v \in P, w_2 \in Q$ tels que $u \neq v$ et $w_1 \neq w_2$, et tels que $uw_1 = vw_2$. Comme $u = r(P)$, on a $u > v$, de sorte que la condition (1) entraine $uw_2 > vw_2 = uw_1$, ce qui contredit la maximalité de uw_1. On a donc $(PQ, uw_1) \neq 0$ et par conséquent $r(PQ) = uw_1 = \max\{r(Pw) : w \in Q\}$.
(iii) Il suffit de voir que si $w \in \sum_{n=1}^{N} P_nQ_n$ alors $w \leq \max_{n=1,\ldots,N} r(P_nQ_n)$. Mais si $u \in P_n, v \in Q_n$ alors, en vertu du point (ii) on a $uv \leq r(P_nQ_n)$; comme $r(P_nQ_n) \leq \max_{n=1,\ldots,N} r(P_nQ_n)$, le résultat est montré. ◇

Corollaire 2.4 *Soient* P *et* Q *des polynômes unitaires de recteurs respectifs* u *et* v. *S'il existe* $w \in A^*$ *tel que* $u = vw$, *alors* $r(P - Qw) < r(P)$.

Démonstration. On a, selon le Lemme 2.3 (i), $u = vw = r(Qw)$. Comme ce mot apparaît dans Qw avec coefficient 1, l'inégalité $r(P - Qw) < r(P)$ est vérifiée. ◇

[1] En grammaire française, le mot qui tient le rôle central dans un groupe de mots s'appelle le *recteur* de ce groupe de mots. Par exemple, dans *'Le célèbre algorithme faible de Cohn'*, le recteur est *'algorithme'*.

Soient maintenant N un ensemble d'indices et $\{Q_n\}_{n\in N}$, une famille de polynômes de $K<A>$. Nous ne considérerons que les cas où N est l'ensemble des entiers non nuls ou $N = \{1,\ldots,n\}$. Dans les deux cas nous noterons les familles par $\{Q_n\}_{n\geq 1}$ en précisant de quel cas il s'agit lorsque cela s'avère nécessaire; les familles finies seront parfois notées simplement $Q_1,\ldots,Q_n$. On dira que les polynômes Q_n sont *presque tous nuls* si l'ensemble $\{n : Q_n \neq 0\}$ est fini; c'est toujours le cas lorsque la famille est finie. Soient $\{P_n\}_{n\geq 1}$ et $\{Q_n\}_{n\geq 1}$ deux familles de polynômes et supposons que les polynômes Q_n sont presque tous nuls. Alors les polynômes P_nQ_n sont presque tous nuls et la somme $\sum_{n\geq 1} P_nQ_n$ est définie.

Remarque 2.5 Le résultat (iii) du Lemme 2.3 reste vrai si on multiplie une famille $\{P_n\}_{n\geq 1}$ et une famille de polynômes presque tous nuls $\{Q_n\}_{n\geq 1}$, i.e.: $r(\sum_{n\geq 1} P_nQ_n) \leq \max_{n\geq 1}\ r(P_nQ_n)$.◇

Nous nous inspirons de Cohn [3] pour introduire la notion de $\leq$-dépendance à droite dans l'algèbre $K<A>$. On dira qu'une famille de polynômes $\{P_n\}_{n\geq 1}$ est *$\leq$-dépendante à droite* si soit l'un des P_n est nul, soit il existe une famille de polynômes $\{Q_n\}_{n\geq 1}$ presque tous nuls tels que $r(\sum_{n\geq 1} P_nQ_n) < \max_{n\geq 1}\ r(P_nQ_n)$.

On dira qu'un polynôme P est *$\leq$-dépendant à droite de la famille* $\{P_n\}_{n\geq 1}$ s'il existe une famille de polynômes $\{Q_n\}_{n\geq 1}$ presque tous nuls tels que $r(P - \sum_{n\geq 1} P_nQ_n) < r(P)$, et tels que $r(P_nQ_n) \leq r(P)$, pour tout n.

Il s'agit là d'une notion beaucoup plus restrictive que celle que Cohn a introduite. A preuve, le Corollaire 2.9, qui dit qu'une relation de $\leq$-dépendance à droite d'une famille de polynômes a toujours lieu entre deux polynômes de la famille. Dans le cas de la dépendance au sens de Cohn, une relation de dépendance entre des polynômes $P_1,\ldots,P_n$, ordonnés selon le degré, implique seulement que l'un des P_i est dépendant de ses prédécesseurs (cf. [1, Chap. VII, Th. 1.1]). Par la suite, nous abrégerons l'expression '*$\leq$-dépendant à droite*' par '*dépendant*'.

Remarques 2.6 (i) Si une sous-famille de la famille $\{P_n\}_{n\geq 1}$ est dépendante alors la famille $\{P_n\}_{n\geq 1}$ est dépendante.
(ii) Si un polynôme P est dépendant d'une famille de polynômes $\{P_n\}_{n\geq 1}$ alors la famille $\{P\} \cup \{P_n\}_{n\geq 1}$ est dépendante.
(iii) Si un polynôme P est dépendant d'une sous-famille de la famille $\{P_n\}_{n\geq 1}$ alors la famille $\{P\} \cup \{P_n\}_{n\geq 1}$ est aussi dépendante. ◇

Remarque 2.7 Utilisant le (iii) du Lemme 2.3 on voit qu'une famille $\{P_n\}_{n\geq 1}$ est *indépendante à droite* si quelle que soit la famille de polynômes $\{Q_n\}_{n\geq 1}$ presque tous nuls on a:

$$r(\sum_{n\geq 1} P_nQ_n) = \max_{n\geq 1}\ r(P_nQ_n).$$

Et dans ce cas, selon les résultats du même lemme, il existe des mots $u_i \in P_i, v_i \in Q_i$ tels que $r(\sum_{n\geq 1} P_nQ_n) = u_iv_i$. ◇

Théorème 2.8 *Soit $\{P_n\}_{n\geq 1}$ une famille de polynômes non nuls et soit $u_n = r(P_n)$. La famille $\{P_n\}_{n\geq 1}$ est indépendante si et seulement si les u_n sont distincts deux à deux et forment un code préfixe.*

Démonstration. On peut supposer P_n unitaire, pour tout n. Supposons d'abord que les mots u_n ne soient pas distincts deux à deux ou ne forment pas un code préfixe. Alors il existe $i \neq j$ et un mot $w \in A^*$ tels que $u_i = u_j w$. Selon le Lemme 2.4 on a $r(P_i) = r(P_j w)$ et $r(P_i - P_j w) < r(P_i)$, c'est-à-dire que P_i est dépendant de P_j. En vertu de la Rem. 2.6 (iii), cela implique que la famille $\{P_n\}_{n\geq 1}$ est dépendante.

Supposons maintenant que les mots u_n sont distincts deux à deux et forment un code préfixe. Soit $\{Q_n\}_{n\geq 1}$ une famille de polynômes presque tous nuls. Selon le Lemme 2.3 (ii), pour tout i tel que $Q_i \neq 0$, il existe un mot v_i tel que $r(P_i Q_i) = r(P_i)v_i$. Soient $u_k = r(P_k)$ et $v_k \in Q_k$ tels que $u_k v_k = \max_{n\geq 1} r(P_n Q_n)$. Ce mot est bien défini puisque les polynômes $P_n Q_n$ sont presque tous nuls. Montrons que $u_k v_k$ apparaît dans $\sum_{n\geq 1} P_n Q_n$. Sinon, c'est qu'il existe un indice j et des mots $u' \in P_j, v' \subset Q_j$ tels que $u_k v_k = u'v'$, et:
(i) soit $j = k, u' \in P_k$ et $u' < u_k$,
(ii) soit $j \neq k, u' \in P_j$ et $u' \leq u_j$.
Observons d'abord que dans le cas (ii), on ne peut avoir $u' = u_j$ puisqu'alors $u_k v = u_j v'$ et que les u_i sont distincts deux à deux et forment un code préfixe. On a donc dans tous les cas, $u_j > u'$. Mais alors, en utilisant la condition (1), on trouve que: $u_j v' > u'v' = u_k v_k$, ce qui contredit la maximalité de $u_k v_k$.

Comme le mot $u_k v_k$ apparaît dans $\sum_{n\geq 1} P_n Q_n$, on a, selon la Rem. 2.7, que $r(\sum_{n\geq 1} P_n Q_n) = u_k v_k$; c'est-à-dire $r(\sum_{n\geq 1} P_n Q_n) = \max_{n\geq 1} r(P_n Q_n)$. La famille $\{Q_n\}_{n\geq 1}$ étant arbitraire, on en conclut que la famille $\{P_n\}_{n\geq 1}$ est indépendante. ◇

La démonstration du Th. 2.8 montre aussi le corollaire suivant.

Corollaire 2.9 *Si la famille $\{P_n\}_{n\geq 1}$ est dépendante alors il existe des indices $i \neq j$ tels que P_i est dépendant de P_j.* ◇

Soient $\{P_n\}_{n\geq 1}$ une famille indépendante de polynômes. Nous dirons que le code préfixe $\{u_n\}_{n\geq 1}$, où $u_n = r(P_n)$, est le *code préfixe associé* à la famille $\{P_n\}_{n\geq 1}$.

Remarque 2.10 Dans [6], Mora suit de très près les concepts et définitions utilisés dans le cas commutatif. L'ordre qu'il utilise sur les mots de A^* diffère du nôtre. Il annonce que ses résultats restent vrais pour les idéaux à droite. Il mentionne aussi que si les générateurs d'un idéal ont tous des recteurs distincts qui forment un code préfixe alors ces générateurs forment une base de Gröbner de l'idéal. ◇

3 Idéaux à droite dans $K<A>$.

Soit $\{P_n\}_{n\geq 1}$ une famille de polynômes; on désigne par $I =< \{P_n\}_{n\geq 1} >$, ou $I =< P_1, \ldots, P_n >$ si la famille est finie, l'*idéal à droite* de $K<A>$ engendré par la famille $\{P_n\}_{n\geq 1}$. Les polynômes qui sont dans I sont tous de la forme $\sum_{n\geq 1} P_n Q_n$ où les Q_n sont des polynômes arbitraires de $K<A>$, presque tous nuls. On dit aussi que la famille $\{P_n\}_{n\geq 1}$ forme un *système de générateurs* pour l'idéal I. Dans le cas où il existe une famille finie qui engendre I on dit qu'il est de *type fini*. On désignera par $\varphi : K<A> \rightarrow K<A>/I$ le morphisme de K-module canonique.

Soit $P_1, \ldots, P_n$ un système de générateurs d'un idéal à droite. On définit trois types de *réécritures élémentaires* '$\rightarrow$' d'un tel système :

(R1) si $P_i = 0$: $P_1, \ldots, P_n \rightarrow P_1, \ldots, P_{i-1}, P_{i+1}, \ldots, P_n$

(R2) pour $\alpha \in K, \alpha \neq 0$: $P_1, \ldots, P_n \rightarrow P_1, \ldots, P_{i-1}, \alpha P_i, P_{i+1}, \ldots, P_n$

(R3) si $i \neq j$ et $r(P_j w) = r(P_j)w \leq r(P_i)$:

$$P_1, \ldots, P_n \rightarrow P_1, \ldots, P_{i-1}, P_i', P_{i+1}, \ldots, P_n \text{ où } P_i' = P_i - P_j w.$$

Remarques 3.1 (i) Ces trois règles de réécritures élémentaires permettent de remplacer, dans un système de générateurs, un polynôme P_i par le polynôme $P_i - \sum_{i\neq j} P_j Q_j$.
(ii) Bien que les réécritures élémentaires puissent être formulées pour des systèmes de générateurs infinis, nous ne le ferons pas. Nous utiliserons les règles de réécritures pour formuler des algorithmes de calculs effectifs des bases des idéaux engendrés par des familles finies. ◇

Lemme 3.2 *Soient $P_1, \ldots, P_n$ et $Q_1, \ldots, Q_m$ deux familles de polynômes. Si la seconde peut être obtenue de la première par une suite de réécritures élémentaires alors elles engendrent le même idéal: $< P_1, \ldots, P_n >=< Q_1, \ldots, Q_m >$.* ◇

Remarques 3.3 Tout idéal à droite peut être considéré comme un sous-$K<A>$-module à droite de $K<A>$. Il est connu depuis Cohn [3] qu'un tel sous-$K<A>$-module à droite est toujours libre. Notez que si une famille de polynômes $P_1, \ldots, P_n$ est indépendante alors elle est *a fortiori* $K<A>$-linéairement indépendante. Ainsi, tout idéal à droite engendré par une famille indépendante est librement engendré par elle, comme $K<A>$-module. ◇

Théorème 3.4 *Soit I un idéal de $K<A>$ engendré par une famille de polynômes $P_1, \ldots, P_n$. Il est possible de calculer une base indépendante de I en effectuant une suite de réécritures élémentaires sur la famille $P_1, \ldots, P_n$.*

Démonstration. Notre but est d'arriver à calculer, à l'aide de réécritures élémentaires, une famille $Q_1, \ldots, Q_m$ dont les recteurs sont distincts deux à deux et forment un code préfixe. Cette famille sera alors indépendante, en vertu du Th. 2.8, et formera une base de l'idéal I. On peut toujours faire en sorte que tous les polynômes de la famille $P_1, \ldots, P_n$ soient non nuls et unitaires, à l'aide de réécritures du type (R1) et (R2). On suppose donc les P_i non nuls et on pose $u_i = r(P_i)$ pour $i = 1, \ldots, n$. Soit $M = M(P_1, \ldots, P_n)$ l'ensemble qui rassemble les u_i qui possèdent comme préfixe l'un des u_j. Plus précisément: $M(P_1, \ldots, P_n) = \{w : \exists i \neq j, \exists v \in A^* \text{ tels que } w = u_i \text{ et } w = u_j v\}$. Nous allons procéder par récurrence sur $\max(M)$. Dans le cas où M est vide, c'est que les recteurs des polynômes P_i sont distincts deux à deux et forment un code préfixe. Par conséquent, en vertu du Th. 2.8, la famille est indépendante et selon la Rem. 3.3 elle forme une base de l'idéal qu'elle engendre.

Supposons donc que l'ensemble M n'est pas vide. Soit $w = \max(M)$ et $i_1, \ldots, i_k$ les indices tels que $r(P_{i_1}) = \ldots = r(P_{i_k}) = w$. Il faut distinguer deux cas.

Cas 1. Il existe un polynôme P_j dont le recteur est un préfixe propre de w. Dans ce cas $j \neq i_1, \ldots, i_k$ et il existe $v \in A^*$, non vide, tels que $w = u_j v$. On applique séquentiellement pour $p = 1, \ldots, k$, les réécritures élémentaires du type (R3): $P_{i_p} \to P_{i_p} - P_j v$. On pose soit $Q_q = P_q - P_j v$ si $q \in \{i_1, \ldots, i_k\}$ et $Q_q = P_q$, sinon. Selon le Lemme 2.4, on a $r(Q_q) < w$ pour tout $q \in \{i_1, \ldots, i_k\}$. Ecartons les Q_q qui sont nuls à l'aide de réécritures du type (R1) et ajustons les indices des polynômes de façon à ce que le nouveau système de générateurs soit $Q_1, \ldots, Q_m$, avec $m \leq n$. On a donc $< P_1, \ldots, P_n >=< Q_1, \ldots, Q_m >$ et $(M(Q_1, \ldots, Q_m)) < \max(M(P_1, \ldots, P_n))$; on peut conclure par récurrence.

Cas 2. Aucun des polynômes n'a pour recteur un préfixe propre de w. Alors $k \geq 2$ et on applique séquentiellement pour $p = 2, \ldots, k$, les réécritures élémentaires du type (R3): $P_{i_p} \to P_{i_p} - P_{i_1}$. On pose $Q_q = P_q - P_{i_1}$ si $q \in \{i_2, \ldots, i_k\}$ et $Q_q = P_q$, sinon. Selon le Lemme 2.4, on a $r(Q_{i_q}) < w$ pour tout $q \in \{i_2, \ldots, i_k\}$. Le polynôme Q_{i_1} est maintenant le seul qui a pour recteur w; aucun autre polynôme n'a pour recteur un mot qui possède w comme préfixe, en vertu de la définition de w. On écarte encore une fois les Q_q qui sont nuls à l'aide de réécritures du type (R1) et on ajuste les indices des polynômes de façon à ce que le nouveau système de générateurs soit $Q_1, \ldots, Q_m$, avec $m \leq n$. On a , encore une fois, $< P_1, \ldots, P_n >=< Q_1, \ldots, Q_m >$ et $\max(M(Q_1, \ldots, Q_m)) < \max(M(P_1, \ldots, P_n))$; on peut conclure par récurrence. ◇

La démonstration du Th. 3.4 montre que lors du calcul d'une base indépendante d'un idéal finiment engendré, le nombre de générateurs peut diminuer. On a donc le corollaire suivant.

Corollaire 3.5 *(Théorème du défaut pour les idéaux à droite de type fini.)*
Si n polynômes sont $K<A>$-linéairement dépendants à droite, alors l'idéal à droite qu'ils engendrent est libre de rang $\leq n - 1$.

4 Bases standard des idéaux à droite.

Soit maintenant un idéal à droite I, quelconque. Nous dirons qu'une famille de mots $\{w_i\}_{i\geq 1}$, finie ou infinie, est *linéairement indépendante* mod I si leurs images $\{\varphi(w_i)\}_{i\geq 1}$ sont linéairement indépendantes dans $K<A>/I$. De façon équivalente, $\{w_i\}_{i\geq 1}$ est linéairement indépendante mod I s'il est impossible de trouver des scalaires $\alpha_i \in K$, presque tous nuls (mais non tous nuls), tels que $\sum_{i\geq 1} \alpha_i w_i \in I$.

Désignons par $[u,v]$ l'*intervalle* des mots compris entre u et v. Plus précisément, $[u,v] = \{w \in A^* : u \leq w \leq v\}$. On définit une suite (finie ou infinie) de mots u_n comme suit:

$$u_1 = \inf\{w \in A^* : [1,w] \text{ est linéairement dépendant mod } I\},$$

et pour $n \geq 2$:

$$u_n = \inf\{w \in A^* - \{u_1,\ldots,u_{n-1}\}A^* : [1,w] \cap (A^* - \{u_1,\ldots,u_{n-1}\}A^*)$$
$$\text{est linéairement dépendant mod } I\}.$$

Il se peut qu'à un certain moment, la famille $\{v\}_{v\in A^*-\{u_1,\ldots,u_{n-1}\}A^*}$ soit linéairement indépendante mod I. Le mot u_n, et les suivants, ne sont alors pas définis.

Lemme 4.1 *La famille de mots $\{u_n\}_{n\geq 1}$ est un code préfixe qui satisfait $u_i < u_j$ si $i<j$.*

Démonstration. Nous montrons par récurrence sur n, que les mots $u_1,\ldots,u_n$ forment un code préfixe et que $u_1 < \ldots < u_n$. Il n'y a rien à montrer pour $n=1$.

Soit $n \geq 1$. Supposons que les mots $u_1,\ldots,u_n$ forment un code préfixe satisfaisant $u_1 < \ldots < u_n$. Comme $u_{n+1} \in (A^* - \{u_1,\ldots,u_n\}A^*)$, aucun des mots $u_1,\ldots,u_n$ n'est préfixe de u_{n+1}; en particulier, $u_n \neq u_{n+1}$. Nous allons montrer que $u_n < u_{n+1}$. On saura alors, en vertu de (2) que u_{n+1} n'est pas préfixe de $u_1,\ldots,u_n$. Supposons qu'au contraire $u_{n+1} < u_n$. On sait alors, par (2), que $[1,u_{n+1}] \cap u_n A^* = \emptyset$. Par conséquent, $[1,u_{n+1}] \cap (A^* - \{u_1,\ldots,u_n\}A^* = [1,u_{n+1}] \cap (A^* - \{u_1,\ldots,u_{n-1}\}A^*$. Or, par définition de u_{n+1}, le membre gauche de cette égalité est linéairement dépendant mod I. Un coup d'oeil au membre droit nous permet de constater que l'on contredit la minimalité du mot u_n. On a donc $u_n < u_{n+1}$ et le lemme est montré. $\diamond$

Posons pour la suite $X_n = \{u_1,\ldots,u_{n-1}\}$ et $X = \{u_n\}_{n\geq 1}$. Par définition, pour chaque n il existe une relation, qui définit un polynôme de l'idéal I: $P_n = u_n + \sum_{v<u_n, v\in A^*-X_nA^*} (P_n,v)v \in I$. En vertu du Lemme 4.1, les polynômes P_n forment une famille indépendante. Par conséquent, selon le Th. 2.8, ils forment une base de l'idéal qu'ils engendrent.

Lemme 4.2 *Soit $R \in K<A>$. Il existe une famille de polynômes $\{Q_n\}_{n\geq 1}$ presque tous nuls, et une famille de scalaires $\{\alpha_v\}_{v\in A^*-X_nA^*}$ presque tous nuls, tels que R puisse s'écrire sous la forme: $R = \sum_{n\geq 1} P_n Q_n + \sum_{v\in A^*-XA^*} \alpha_v v$.*

Démonstration. Il suffit de montrer le lemme dans le cas où R est un mot $w \notin A^* - XA^*$. On a alors $w = u_k w'$ et on procède par récurrence sur la longueur du mot w'. Le cas $|w'| = 0$ est donné par la relation qui définit P_k. Sinon, on a: $u_k w' = P_k w' + \sum_{v<u_k, v\in A^*-X_kA^*} (P_k, v)vw'$. Les mots vw' qui apparaîssent dans la somme de droite sont soit des mots de $A^* - XA^*$, soit ils sont de la forme $vw' = u_j w''$ avec $|w''| < |w'|$ et alors on conclut par récurrence. ◇

Lemme 4.3 *La famille de mots $\{v\}_{v\in A^*-XA^*}$ est linéairement indépendante mod I.*

Démonstration. Dans le cas où $X = \{u_1, \ldots, u_n\}$ est fini, le résultat est évident: le mot u_{n+1} n'est pas défini précisément parce que la famille $\{v\}_{v\in A^*-XA^*}$ est linéairement indépendante mod I.

Il reste donc à considérer le cas où X est infini. Supposons qu'au contraire il existe des scalaires α_v, presque tous nuls, tels que $\sum_v \alpha_v v = 0 \bmod I$. Soit: $u_i = \inf\{u_n : u_n > v$ pour tout v tel que $\alpha_v \neq 0\}$. Les mots $v \in \sum_v \alpha_v v$ sont donc des mots de $A^* - X_iA^*$, plus petits que u_i, de sorte que la relation $\sum_v \alpha_v v = 0 \bmod I$ contredit la minimalité de u_i. ◇

Proposition 4.4 *La famille de polynômes $\{P_n\}_{n\geq 1}$ engendrent l'idéal I.*

Démonstration. Soit R un polynôme de I. Selon le Lemme 4.2, il existe une famille de polynômes $\{Q_n\}_{n\geq 1}$ presque tous nuls, et une famille de scalaires $\{\alpha_v\}_{v\in A^*-X_nA^*}$ presque tous nuls, tels que $R = \sum_{n\geq 1} P_n Q_n + \sum_{v\in A^*-XA^*} \alpha_v v$. Par conséquent, $0 = \varphi(R) = \sum_{v\in A^*-XA^*} \alpha_v \varphi(v)$. On en déduit que $\alpha_v = 0$ pour tout v, en vertu du Lemme 4.3. Donc, $R = \sum_{n\geq 1} P_n Q_n$ et la famille $\{P_n\}_{n\geq 1}$ engendrent l'idéal I. ◇

Corollaire 4.5 *L'idéal I est de type fini si et seulement si le code préfixe X est fini.*

Démonstration. La proposition montre que si l'ensemble X est fini alors I est finiment engendré. Nous serons en mesure de montrer la réciproque plus loin (Th. 4.7). Cela découle aussi des théorèmes de Cohn [3]. ◇

Nous allons maintenant montrer que la famille $\{P_n\}_{n\geq 1}$ est unique.

Théorème 4.6 *Soit $\{P'_n\}_{n\geq 1}$ une famille indépendante de polynômes, de recteurs respectifs $\{u'_n\}_{n\geq 1}$, satisfaisant $u'_i < u'_j$ si $i < j$. Posons $X'_n = \{u'_1, \ldots, u'_{n-1}\}, X' = \{u'_n\}_{n\geq 1}$ et supposons que: $P'_n = u'_n + \sum_{v<u'_n, v\in A^*-X'_nA^*} (P'_n, v)v$. Si la famille $\{P'_n\}_{n\geq 1}$ engendre le même idéal I que la famille $\{P_n\}_{n\geq 1}$ alors $P'_n = P_n$, pour tout n.*

Démonstration. On procède par récurrence sur k pour montrer que $u_k = u'_k$ et que $P_k = P'_k$.

Le polynôme P'_1 nous donne une relation linéaire (mod I) dans l'intervalle de mots $[1, u'_1]$. On doit donc avoir $u_1 \leq u'_1$ en vertu de la définition de u_1. Comme $\{P'_n\}_{n\geq 1}$ engendre I, il

existe des polynômes Q'_n, presque tous nuls, tels que $P_1 = \sum_{n\geq 1} P'_n Q'_n$. Selon la remarque 2.7, $r(\sum_{n\geq 1} P'_n Q'_n) = u'_i v'_i$ pour un certain i et un certain $v'_i \in Q'_i$. On a donc $u_1 = r(P_1) = u'_i v'_i$. On en tire $u'_i \leq u_1$. Par suite, on a $u_1 \leq u'_1 \leq u'_i \leq u_1$; donc $u_1 = u'_1$. On peut en conclure que $P'_1 = P_1$ puisque la famille de mots $[1, u_1] - \{u_1\}$ est linéairement indépendante mod I.

Supposons qu'on ait montré que $u_1 = u'_1, \ldots, u_{k-1} = u'_{k-1}$ et que $P_1 = P'_1, \ldots, P_{k-1} = P'_{k-1}$. On a donc $X_{k-1} = X'_{k-1}$ et le même argument que dans le cas $k = 1$ montre qu'on doit avoir $u_k \leq u'_k$. Comme $P_k \in I$ il existe des polynômes Q'_n, presque tous nuls, tels que $P_k = \sum_{n\geq 1} P'_n Q'_n$. Mais alors $u_k = r(P_k) = r(\sum_{n\geq 1} P'_n Q'_n)$. Selon la remarque 2.7, $r(\sum_{n\geq 1} P'_n Q'_n) = u'_i v'_i$ pour un certain i et un certain $v'_i \in Q'_i$. On a donc $u_k = u'_i v'_i$ et on en tire $u'_i \leq u_k \leq u'_k$. Maintenant, soit $i = k$ et alors $u_k = u'_k$; soit $i < k$ de sorte que, par récurrence, $u'_i = u_i$. Mais alors c'est que $u_k = u_i v'_i$ ce qui contredit le fait que $\{u_n\}_{n\geq 1}$ est un code préfixe. On doit donc avoir $u_k = u'_k$.

Cela entraîne $X_k = X'_k$ et par conséquent, les mots $v < u'_k$ qui apparaîssent dans P'_k sont des mots de $A^* - X_k A^*$. Donc $P'_k = P_k$ puisque les mots de $A^* - X_k A^*$ sont linéairement indépendants mod I. ◇

La base $\{P_n\}_{n\geq 1}$ de l'idéal I sera appelé *la base standard de* I. On dira aussi qu'une famille est standard si elle est la base standard de l'idéal qu'elle engendre. Un raisonnement similaire à celui fait à la démonstration du Th. 3.4 nous donne le résultat suivant.

Théorème 4.7 *Soit $P_1, \ldots, P_n$ une famille indépendante. Il est possible de calculer, à l'aide d'une suite de réécritures élémentaires, la base standard de l'idéal $I = < P_1, \ldots, P_n >$. De plus, le code préfixe associé à la base standard de I est égal au code préfixe associé à $P_1, \ldots, P_n$.* ◇

Le Th. 4.6 et le Th. 4.7 s'unissent pour nous donner le corollaire suivant.

Corollaire 4.8 *Il est possible de tester si deux ensembles finis de polynômes engendrent le même idéal.* ◇

Corollaire 4.9 *Soient Q et $P_1, \ldots, P_n \in K<A>$ tels que $P_1, \ldots, P_n$ est la base standard de l'idéal I qu'ils engendrent. Il est possible de calculer l'image de Q, dans le quotient $K<A>/I$. En particulier, il est possible de tester si $Q \in < P_1, \ldots, P_n >$.*

Démonstration. On suppose P_i unitaire, pour tout i. On pose, comme plus haut, $u_i = r(P_i)$ et $X = \{u_1, \ldots, u_n\}$. φ désigne le morphisme canonique $K<A> \to K<A>/I$. On procède par récurrence sur le recteur de Q.

Cas 1. Si $Q = 0$, alors $\varphi(Q) = 0$ et $Q \in I$.
Sinon, soit $w = r(Q)$.
Cas 2. Si $w \in (A^* - XA^*)$, on a: $\varphi(Q) = (Q, w)w + \varphi(Q - (Q, w)w)$. Par récurrence, on peut

calculer l'image de $Q-(Q,w)w$ et terminer le calcul de l'image de Q.

Cas 3. Si $w \in XA^*$, il existe $u_i \in X$ et $v \in A^*$ tel que $r(Q-(Q,w)P_iv) < r(Q)$, d'après le Lemme 2.4. Comme: $\varphi(Q-(Q,w)P_iv) = \varphi(Q) - \varphi((Q,w)(P_i,u)^{-1}P_iv)) = \varphi(Q)$, on peut calculer l'image de $Q-(Q,w)P_iv$ et terminer le calcul.

L'algorithme décrit ci-dessus fait bien le travail souhaité, puisque les mots de $A^* - XA^*$ sont linéairement indépendants mod I, selon le Lemme 4.3. Si à aucun moment lors du calcul de l'image, on ne visite le **Cas 2** on sait alors que $Q \in I$. ◇

5 $K<A>$-modules à droite et $\leq$-dépendance à droite.

Nous considérons maintenant le $K<A>$-module à droite $K<A>^q$, où q est un entier positif, $q \geq 1$. Les éléments de $K<A>^q$ sont des *vecteurs colonnes* V formés de q polynômes de $K<A>$:

$$V = \begin{pmatrix} P_1 \\ \vdots \\ P_q \end{pmatrix}.$$

Pour cette raison, nous appellerons les éléments de $K<A>^q$ des *vecteurs de polynômes*, ou simplement des *vecteurs*. Nous allons nous intéresser aux *sous-$K<A>$-modules à droite* de $K<A>^q$. Par la suite, nous abrégerons l'expression '*sous-$K<A>$-module à droite*' simplement par *sous-module*. Dans le cas où $q=1$, un sous-module de $K<A>^q$ n'est rien d'autre qu'un idéal à droite de $K<A>$. Nous serons donc en mesure d'utiliser une récurrence sur q afin d'étendre les résultats des paragraphes précédents.

Nous désignons par π_i, pour $i = 1,\ldots,q$, la projection canonique des vecteurs sur leur $i^{\text{ème}}$ composante, i.e. $\pi_i : K<A>^q \to K<A>, \pi_i(V) = P_i$. Nous introduisons aussi les projections π (resp. $\bar{\pi}$) : $K<A>^q \to K<A>^{q-1}$ qui oublient la première (resp. dernière) composante des vecteurs:

$$\pi(V) = \begin{pmatrix} P_2 \\ \vdots \\ P_q \end{pmatrix}, \bar{\pi}(V) = \begin{pmatrix} P_1 \\ \vdots \\ P_{q-1} \end{pmatrix}.$$

La multiplication à droite d'un vecteur V par un polynôme $Q \in K<A>$ s'exprime donc par $\pi_i(VQ) = \pi_i(V)Q$. Nous désignerons par ι le plongement $K<A>^{q-1} \to K<A>^q$ qui ajoute une première composante nulle, i.e. $\pi_1(\iota(V)) = 0, \pi_{k+1}(\iota(V)) = \pi_k(V)$, pour $k = 1,\ldots,q-1$. On a donc $\pi \circ \iota = id$ et $\iota \circ \pi(V) = V$ si $\pi_1(V) = 0$. Ces applications sont toutes $K<A>$-linéaires. Soient N un ensemble d'indices et $\{V_n\}_{n\in N}$ une famille de vecteurs. Nous dirons qu'une famille de q sous-ensembles $E_1,\ldots,E_q$ est une *partition en q blocs* de la famille $\{V_n\}_{n\in N}$ si: $\forall i \in N, \exists k$ unique tel que $i \in E_k$; i.e. $E_{k_1} \cap E_{k_2} = \emptyset$ $(k_1 \neq k_2)$ et $\cup_{k=1}^q E_k = N$. Prenons $N = \{n : n \geq 1\}$ et soit $\{Q_n\}_{n\geq 1}$ une famille de *polynômes* presque tous nuls. Alors les vecteurs V_nQ_n sont presque tous nuls et on peut former la somme $\sum_{n\geq 1} V_nQ_n$. Par la suite, nous abrégerons l'expression

'*partition en q blocs*' à *partition*. Notez que certains blocs de la partition peuvent être vides. Etant donné une famille de vecteurs $\{V_n\}_{n\geq 1}$ il existe une unique partition $E_1, \ldots E_q$ telle que $i \in E_k$ implique: $\pi_j(V_i) = 0$ pour $j = 1, \ldots, k-1$ et $\pi_k(V_i) \neq 0$. Cette partition sera appelée *la partition associée à la famille* $\{V_n\}_{n\geq 1}$.

Remarques 5.1 Soit $\{V_n\}_{n\geq 1}$ une famille de vecteurs de $K\!<\!A\!>^q$ et $E_1, \ldots, E_q$ sa partition associée.
(i) Alors $E'_k = E_{k+1}$ $(k = 1, \ldots, q-1)$, est la partition associée à la famille $\{\pi(V_n)\}_{n\geq 1, n\notin E_1}$.
(ii) La partition $E_1, \ldots, E_{q-1}$ est la partition associée à la famille $\{\bar{\pi}(V_n)\}_{n\geq 1, n\notin E_q}$.
(iii) La famille $\{\iota(V_n)\}_{n\geq 1}$, a pour partition associée $E'_1 = \emptyset, E'_k = E_{k-1}$ $(k = 2, \ldots, q+1)$. ◇

Soit $\{V_n\}_{n\geq 1}$ une famille de vecteurs et $E_1, \ldots, E_q$ la partition qui lui est associée. Nous dirons que cette famille est $\leq$-*indépendante à droite* si chacune des familles de *polynômes* $\{\pi_k(V_i)\}_{i\in E_k}$ est $\leq$-indépendante à droite. Par la suite, nous abrégerons l'expression '$\leq$-*indépendante à droite*' simplement par *indépendante*.

Remarques 5.2 Soit $\{V_n\}_{n\geq 1}$ une famille indépendante de vecteurs de $K\!<\!A\!>^q$.
(i) Alors on constate facilement, à l'aide des Rem. 5.1 que les familles $\{\pi(V_n)\}_{n\geq 1, n\notin E_1}$, $\{\bar{\pi}(V_n)\}_{n\geq 1, n\notin E_q}$ et $\{\iota(V_n)\}_{n\geq 1}$ sont indépendantes.
(ii) Soit $\{U_n\}_{n\geq 1}$ est une famille indépendante de $K\!<\!A\!>^{q+1}$, tels que $\pi_1(U_n) \neq 0$ pour tout $n \geq 1$. Alors on vérifie que la famille $\{U_n\}_{n\geq 1} \cup \{\iota(V_n)\}_{n\geq 1}$, est indépendante. ◇

Proposition 5.3 *Soit* $\{V_n\}_{n\geq 1}$ *une famille indépendante de vecteurs. Alors elle est* $K\!<\!A\!>$-*linéairement indépendante.*

Démonstration. On procède par récurrence sur q. On a vu à la Rem. 3.3 qu'une famille indépendante de *polynômes* est une famille $K\!<\!A\!>$-linéairement indépendante de $K\!<\!A\!>$. Par conséquent, le résultat est vrai pour $q = 1$. On suppose donc $q \geq 2$.

Imaginons qu'au contraire les vecteurs V_n ne soient pas $K\!<\!A\!>$-linéairement indépendants. Il existe alors des polynômes $\{Q_n\}_{n\geq 1}$ presque tous nuls (mais non tous nuls) tels que: $\sum_{n\geq 1} V_n Q_n = 0$. On déduit de la relation précédente, par application de π, la relation: $\sum_{n\geq 1} \pi(V_n) Q_n = 0$. Soit $E_1, \ldots, E_q$ la partition associée à la famille de vecteurs $\{V_n\}_{n\geq 1}$. Les vecteurs de $K\!<\!A\!>^{q-1}$, $\{\pi(V_n)\}_{n\geq 1, n\notin E_1}$, sont indépendants, en vertu de la Rem. 5.2. Par récurrence, ils sont aussi $K\!<\!A\!>$-linéairement indépendants. Par conséquent, les polynômes $\{Q_n\}_{n\geq 1, n\in E_1}$ ne peuvent être tous nuls. Mais alors on obtient, par application de π_1, une relation de dépendance $K\!<\!A\!>$-linéaire en première composante: $\pi_1(\sum_{n\geq 1} V_n Q_n) = \sum_{n\in E_1} \pi_1(V_n) Q_n = 0$. On contredit là l'indépendance des polynômes $\{\pi_1(V_n)\}_{n\geq 1, n\in E_1}$. La famille $\{V_n\}_{n\geq 1}$ est donc $K\!<\!A\!>$-linéairement indépendante. ◇

On peut définir des *réécritures élémentaires* de systèmes de vecteurs, analogues à celles décrites au paragraphe 3. Soient $V_1, \ldots, V_n$ une famille de vecteurs. On définit trois types de réécritures élémentaires '$\rightarrow$':

(R_q1) si $V_i = 0$: $V_1, \ldots, V_n \rightarrow V_1, \ldots, V_{i-1}, V_{i+1}, \ldots, V_n$,

(R_q2) pour $\alpha \in K, \alpha \neq 0$: $V_1, \ldots, V_n \rightarrow V_1, \ldots, V_{i-1}, \alpha V_i, V_{i+1}, \ldots, V_n$

(R_q3) s'il existe k ($1 \leq k \leq q$, $i \neq j$, et $r(\pi_k(V_j w)) = r(\pi_k(V_j))w \leq r(\pi_k(V_i))$:

$$V_1, \ldots, V_n \rightarrow V_1, \ldots, V_{i-1}, V_i', V_{i+1}, \ldots, V_n, \text{ où } V_i' = V_i - V_j w.$$

Remarques 5.4 (i) Les Rem. 3.1 que nous avons faites dans le cas $q = 1$ s'appliquent aussi au cas $q \geq 2$ (en remplaçant *polynôme* par *vecteur*).
(ii) Les règles ($R_q i$) et ($R_{q-1} i$) sont liées (les règles ($R_1 i$) ne sont autres que celles introduites au paragraphe 3). En effet, soient $V_1, \ldots V_n$ des vecteurs de $K\langle A\rangle^{q-1}$. Alors on peut, de façon équivalente, soit appliquer une règle ($R_{q-1} i$) à ce système, soit plonger les vecteurs dans $K\langle A\rangle^q$: $\iota(V_1), \ldots \iota(V_n)$, appliquer la règle correspondante ($R_q i$), et revenir à $K\langle A\rangle^{q-1}$ à l'aide de π, puisqu'on a $\pi \circ \iota = id$. ◇

On obtient évidemment un analogue du Lemme 3.2.

Lemme 5.5 *Soient $U_1, \ldots, U_n$ et $V_1, \ldots, V_m$ deux familles de vecteurs de $K\langle A\rangle^q$. Si la famille $V_1, \ldots, V_m$ peut être obtenue de la famille $U_1, \ldots, U_n$ par une suite de réécritures élémentaires alors elles engendrent le même sous-module de $K\langle A\rangle^q$.* ◇

Théorème 5.6 *Soit $\mathcal{M}$ un sous-module de $K\langle A\rangle^q$ engendré par les vecteurs $V_1, \ldots, V_n$. Il est possible de calculer une base indépendante de $\mathcal{M}$ en effectuant une suite de réécritures élémentaires sur la famille $V_1, \ldots, V_n$.*

Démonstration. Soit $E_1, \ldots, E_q$ la partition associée aux générateurs de $\mathcal{M}$. On procède par récurrence sur q, le cas $q = 1$ ayant été traité au Th. 3.4.

Par récurrence, il est possible de calculer, à l'aide de réécritures ($R_1 i$), une base indépendante du sous-module engendré par les polynômes $\{\pi_1(V_i)\}_{i \in E_1}$ (Th. 3.4). Ces règles de réécritures peuvent être simulées sur les vecteurs $\{V_i\}_{i \in E_1}$, en appliquant les règles de réécritures ($R_q i$) correspondantes. Ces réécritures donnent lieu à une famille indépendante de vecteurs $\{V_i'\}_{i \in E_1'}$, ($E_1' \subset E_1$), tels que $\pi_1(V_i) \neq 0$, et à d'autres vecteurs $\{U_j\}_{j \in E_1 \setminus E_1'}$ tels que $\pi_1(U_j) = 0$. Soient $\mathcal{M}_1$ le sous-module de $\mathcal{M}$ de base $\{V_i'\}_{i \in E_1'}$ et $\mathcal{M}_2$ le sous-module de $\mathcal{M}$ engendré par la famille de vecteurs $\{U_j\}_{j \in E_1 \setminus E_1'} \cup \{V_i\}_{i \notin E_1}$. Chacun des vecteurs V de cette famille satisfait $\pi_1(V) = 0$ et par conséquent, on a:

$$\iota \circ \pi(\mathcal{M}_2) = \mathcal{M}_2. \tag{3}$$

De plus, $\mathcal{M}_1$ et $\mathcal{M}_2$ sont complémentaires: $\mathcal{M} = \mathcal{M}_1 \oplus \mathcal{M}_2$. Par récurrence, on peut calculer une base indépendante $\{U'_j\}_{j\in E'}$ du sous-module $\pi(\mathcal{M}_2)$ engendré par la famille de vecteurs $\{\pi(U_j)\}_{j\in E_1\setminus E'_1} \cup \{\pi(V_i)\}_{i\notin E_1}$, à l'aide de réécritures élémentaires $(\mathrm{R}_{q-1}i)$.

Par application de ι on obtient une base indépendante de $\mathcal{M}_2$, $V'_j = \iota(U'_j)$ $(j \in E')$, en vertu de (3) et de la Rem. 5.2 (i). De plus, cette base de $\mathcal{M}$ peut être calculée par une suite de réécritures élémentaires $(\mathrm{R}_q i)$, en vertu de la Rem. 5.4 (ii). La réunion des bases indépendantes des sous-modules $\mathcal{M}_1$ et $\mathcal{M}_2$ nous donne une base de $\mathcal{M}$. Cette base est indépendante, en vertu de la Rem. 5.2 (ii). ◇

Soit $\{V_n\}_{n\geq 1}$ une famille de vecteurs indépendants de $K\langle A\rangle^q$, de partition associée $E_1, \ldots, E_q$. Il correspond à cette famille q codes préfixes $X_1, \ldots, X_q$, le code X_k étant le *code associé* à la famille de polynômes $\{\pi_k(V_i)\}_{i\in E_k}$. Nous dirons que les codes préfixes X_k sont les *codes préfixes associés* à la famille $\{V_n\}_{n\geq 1}$ (voir Th. 2.8). Un raisonnement similaire à celui fait dans la démonstration du Th. 5.6, utilisant le calcul des bases standard des idéaux (Th. 4.7), montre le corollaire suivant.

Corollaire 5.7 *Soit $V_1, \ldots, V_n$ une famille de vecteurs indépendants, $E_1, \ldots, E_q$ sa partition associée et $X_1, \ldots, X_q$ ses codes préfixes associés. Il est possible, à l'aide de réécritures élémentaires, de calculer une base indépendante $V'_1, \ldots, V'_n$ telle que $\{\pi_k(V'_i)\}_{i\in E_k}$ soit une famille standard de polynômes, pour $k = 1, \ldots, q$. De plus, la partition associée et les codes associés à cette famille sont respectivement $E_1, \ldots, E_q$ et $X_1, \ldots, X_k$.* ◇

Comme dans le cas $q = 1$, bien que les bases indépendantes d'un sous-module aient toutes les mêmes codes préfixes associés (Cor. 5.7), il n'y a pas unicité de la base. On ne gagne pas l'unicité en exigeant que chacune des familles de polynômes associées à chacun des blocs de la partition soit standard. Il faut demander un peu plus. Soit $\{V_n\}_{n\geq 1}$ une famille de vecteurs indépendants de partition associée $E_1, \ldots, E_q$ et de codes préfixes associés $X_1, \ldots, X_q$. On dira que cette famille est *standard* si de plus, pour tout $k = 1, \ldots, q$:

(i) la famille de polynômes $\{\pi_k(V_i)\}_{i\in E_k}$ est une base standard de l'idéal qu'elle engendre,

(ii) si $i \in E_k$ et $j > k$ alors la condition suivante est satisfaite: pour tout $w \in A^*$, si $w \in \pi_j(V_i)$ alors $w \in A^* - X_j A^*$.

Remarque 5.8 Soit $\{V_n\}_{n\geq 1}$ une famille standard de vecteurs de $K\langle A\rangle^q$. Alors on vérifie (comme à la Rem. 5.2 (i)) que les familles de vecteurs $\{\pi(V_n)\}_{n\geq 1, n\notin E_1}$, $\{\bar{\pi}(V_n)\}_{n\geq 1, n\notin E_q}$ et $\{\iota(V_n)\}_{n\geq 1}$ sont standard. ◇

Théorème 5.9 *Soit $\mathcal{M}$ un sous-module de $K\langle A\rangle^q$. S'il existe une base standard de $\mathcal{M}$ alors elle est unique.*

Démonstration. On procède par récurrence sur q. Le théorème a déjà été montré pour $q = 1$ (Th. 4.6). Supposons qu'il existe deux bases standard de $\mathcal{M}$, $\mathcal{F} = \{V_n\}_{n\geq 1}$ et $\mathcal{F}' = \{V'_n\}_{n\geq 1}$ avec partition associée et codes préfixes associés respectifs $E_1, \ldots, E_q$, $X_1, \ldots, X_q$, et $E'_1, \ldots, E'_q$, $X'_1, \ldots, X'_q$. Les familles $\{\bar{\pi}(V_n)\}_{n\geq 1, n\notin E_q}$ et $\{\bar{\pi}(V'_n)\}_{n\geq 1, n\notin E'_q}$ sont deux bases du même sous-module de $K\langle A\rangle^{q-1}$. De plus, selon la Rem. 5.8 elles sont toutes deux standard. Par récurrence, elles sont égales. On peut donc supposer pour la suite, que $E_k = E'_k, X_k = X'_k$ $(k = 1, \ldots, q-1)$ et $\bar{\pi}(V_n) = \bar{\pi}(V'_n)$ $(n \geq 1, n \notin E_q)$.

Nous montrons maintenant que les sous-familles $\{V_n\}_{n\in E_q}$ et $\{V'_n\}_{n\in E'_q}$ sont égales. Les idéaux I et I' respectivement engendrés par les familles de polynômes $\{\pi_q(V_n)\}_{n\in E_q}$ et $\{\pi_q(V'_n)\}_{n\in E'_q}$ sont égaux. En effet, soit $\{Q_n\}_{n\in E_q}$ une famille de polynômes presque tous nuls. Alors, puisque $\mathcal{F}$ et $\mathcal{F}'$ sont toutes deux des bases de $\mathcal{M}$, il existe une famille $\{Q'_n\}_{n\geq 1}$ de polynômes presque tous nuls tels que $\sum_{n\in E_q} V_n Q_n = \sum_{n\geq 1} V'_n Q'_n$. On en tire, par application de $\bar{\pi}$, la relation $0 = \sum_{n\notin E'_q} \bar{\pi}(V'_n) Q'_n$, d'où $Q'_n = 0$ pour tout $n \notin E_q$. Par conséquent, $\sum_{n\in E_q} V_n Q_n = \sum_{n\in E'_q} V'_n Q'_n$. Par application de π_q on obtient $\sum_{n\in E_q} \pi_q(V_n) Q_n = \sum_{n\in E'_q} \pi_q(V'_n) Q'_n$, ce qui montre que les deux familles de polynômes $\{\pi_q(V_n)\}_{n\in E_q}$ et $\{\pi_q(V'_n)\}_{n\in E'_q}$ engendrent le même idéal (puisque le raisonnement est symétrique en $\mathcal{F}$ et $\mathcal{F}'$); on a donc $I = I'$. Par hypothèse, ces familles sont toutes deux des bases standard de l'idéal qu'elles engendrent. Par récurrence, elles sont égales. On peut donc supposer que $E_q = E'_q$, $X_q = X'_q$ et $\pi_q(V_n) = \pi_q(V'_n)$ $(n \in E_q)$, d'où $V_n = V'_n$ pour $n \in E_q$.

Il reste à montrer que $\pi_q(V_i) = \pi_q(V'_i)$ pour $i \notin E_q$. Soit $i \geq 1, i \notin E_q$. Alors, comme $\mathcal{F}$ et $\mathcal{F}'$ sont toutes deux des bases de $\mathcal{M}$, il existe des polynômes $\{Q'_n\}_{n\geq 1}$ presque tous nuls, tels que $V_i = \sum_{n\geq 1} V'_n Q'_n$. A l'aide de $\bar{\pi}$ on trouve $\bar{\pi}(V_i) = \sum_{n\notin E'_q} \bar{\pi}(V'_n) Q'_n$. On a montré plus haut que $\bar{\pi}(V_n) = \bar{\pi}(V'_n)$ $(n \geq 1, n \notin E_q)$ et que la famille $\{\bar{\pi}(V_n)\}_{n\notin E_q}$ est la base standard du sous-module qu'elle engendre. Par conséquent, on a $Q'_n = 0$ si $n \notin E'_q$ et $n \neq i$, et $Q'_i = 1$. La relation initiale est donc $V_i = V'_i + \sum_{n\in E'_q} V'_n Q'_n$. Donc, par application de π_q on trouve $\pi_q(V_i) = \pi_q(V'_i) + \sum_{n\in E'_q} \pi_q(V'_n) Q'_n$. On fait passer cette dernière égalité au quotient en appliquant la projection $\varphi : K\langle A\rangle \to K\langle A\rangle/I$, pour obtenir $\pi_q(V_i) \equiv \pi_q(V'_i)$ mod I (car $I = I'$ est engendré par les polynômes $\{\pi_q(V'_n)\}_{n\in E'_q}$). On en conclut que $\pi_q(V_i) = \pi_q(V'_i)$ puisque ces polynômes sont des somme de mots de $A^* - X_q A^*$ et que cette famille de mots est indépendante mod I (Lemme 4.3). ◇

Pour montrer l'existence de la base standard d'un sous-module, on peut faire un raisonnement analogue en tout point à celui fait au paragraphe 4. On ordonne lexicographiquement l'ensemble des vecteurs de mots. Nous admettons les vecteurs W dont certaines composantes sont nulles; on a donc $W \in (A^* \cup \{0\})^q$. Nous posons $0 < w$, pour tout $w \in A^*$. Ainsi, on a $W' < W''$ s'il existe un indice k tel que pour $j = 1, \ldots, k-1$, $\pi_j(W') = \pi_j(W'')$ et $\pi_k(W') < \pi_k(W'')$. En particulier, $W' < W''$ si $i > j$ et $W' \in \{0\}^i \times (A^*)^{q-i}, W'' \in \{0\}^j \times (A^*)^{q-j}$. Etant donné un sous-module

$\mathcal{M}$ de $K<A>^q$, on définit une suite croissante de vecteurs de mots $U_n^{(k)} \in \{0\}^{k-1} \times (A^*)^{q-k}$ $(k = 1, \ldots, q)$, qui donne lieu à des éléments de $\mathcal{M}$ dont on peut montrer qu'ils forment une base standard de $\mathcal{M}$. On obtient des analogues, pour les sous-modules de $K<A>^q$, des Th. 4.7, Cor. 4.8 et Cor. 4.9, dont nous donnons les énoncés.

Théorème 5.10 *Soit $V_1, \ldots, V_n$ une famille indépendante de partition associée $E_1, \ldots, E_q$ et de codes préfixes associés $X_1, \ldots, X_q$. Il est possible de calculer, à l'aide d'une suite de réécritures élémentaires, la base standard du sous-module $\mathcal{M} =< V_1, \ldots, V_n >$. De plus, la partition associée et les codes préfixes associé à la base standard de $\mathcal{M}$ sont $E_1, \ldots, E_q$ et $X_1, \ldots, X_q$.* ◇

Corollaire 5.11 *Il est possible de tester si deux ensembles finis de vecteurs engendrent le même sous-module de $K<A>^q$.* ◇

Corollaire 5.12 *Soient V un vecteur et $\mathcal{M}$ un sous-module finiment engendré de $K<A>^q$. Il est possible de calculer l'image de V, dans le quotient $K<A>^q/\mathcal{M}$. En particulier, il est possible de tester si $V \in \mathcal{M}$.*

Références.

[1] Berstel J., Reutenauer C., *Rational Series and Their Languages*, Springer, Berlin Heidelberg New York (1988).

[2] Buchberger B., Gröbner Bases: an Algorithmic Method in Polynomial Ideal Theory, *in N. K. Bose Ed. Recent Trends in Multidimensional System Theory*, Reidel, (1985).

[3] Cohn P. M., Free Associative Algebras, *Bull. London Math. Soc.* 1 (1969), 1-39.

[4] Lyndon R. C., Schupp P. E., *Combinatorial Group Theory*, Springer, Berlin Heidelberg New York (1977).

[5] Magnus W., Karass A., Solitar D., *Combinatorial Group Theory*, Dover Publications ($2^{\text{ième}}$ Ed.) (1976).

[6] Mora F., Groebner Bases for Non-commutative Polynomial Rings, *Lectures Notes in Computer Science* **229**, 3^{rd} *International Conference AAECC-3* Proceedings, Grenoble, France, (1985), 353-362.

[7] Schützenberger M. P., On the Definition of a Family of Automata, *Information and Control* 4 (1961), 245-270.