PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 42, Number 2, February 1974

ELEMENTS NILPOTENTS ET DIVISEURS DE ZERO DANS LES ALGEBRES LARGES

KHYRA LAMÈCHE-GÉRARDIN

ABSTRACT. On determine les polynômes (resp. les séries formelles) nilpotents ou diviseurs de zéro dans l'algèbre des polynômes (resp. dans l'algèbre large) sur un alphabet fini à coefficients dans un anneau unitaire commutatif. Ces résultats généralisent ceux de McCoy [1] et de D. E. Fields [3], qui correspondent au cas où l'alphabet est réduit à un élément.

NOTATIONS. Soit X un ensemble fini appelé alphabet; on notera X^* le monoïde libre engendré par X, e le mot vide de X^*. Si A est un anneau commutatif unitaire, on désignera par $A\langle\langle X\rangle\rangle$ l'algèbre large sur X à coefficients dans A, par $A\langle X\rangle$ la sous-algèbre des polynômes et par $A^{\mathrm{rat}}\langle\langle X\rangle\rangle$ l'algèbre des séries rationnelles sur X à coefficients dans A.

Une série formelle a de $A\langle\langle X\rangle\rangle$ est dite quasi-inversible si $(a, e)=0$ ((a, e) désignant le coefficient de e dans l'écriture de a); le quasi-inverse a^* de a vérifie la relation:

$$a^* = a + aa^* = a + a^*a.$$

Rappelons la définition et la caractérisation des séries rationnelles.

DEFINITION [4]. $A^{\mathrm{rat}}\langle\langle X\rangle\rangle$ est la plus petite sous-algèbre de $A\langle\langle X\rangle\rangle$ contenant X et stable par quasi-inversion des éléments quasi-inversibles.

CARACTERISATION [4]. Une série formelle a de $A\langle\langle X\rangle\rangle$ est rationnelle si et seulement si il existe un entier $N\geqq 1$ une matrice P de $M_N(A)$ un homomorphisme μ de X^* dans le monoïde multiplicatif $M_N(A)$ telle que l'on ait:

$$a = \sum_{f\in X^*}(a,f)f = \sum_{f\in X^*} Tr(P\mu f)f.$$

LEMME 1. *Une condition nécessaire pour qu'une série formelle a soit rationnelle est que l'idéal engendré par les coefficients de a dans l'anneau A soit de type fini.*

Received by the editors November 3, 1972.

AMS (MOS) subject classifications (1970). Primary 16A34.

Key words and phrases. Formal power series, noncommutative variables, zero divisors, nilpotent elements.

DÉMONSTRATION. On dit qu'une série formelle a vérifie la propriété (P) si l'idéal engendré par les coefficients de a dans l'anneau A est de type fini.

Il est immédiat qu'un polynôme vérifie la propriété (P).

Soit a (resp. b) une série formelle qui vérifie la propriété (P). Soit I (resp. J) l'idéal engendré par les coefficients de a (resp. b) dans A. L'idéal engendré par les coefficients de $a+b$ (resp. ab) est bien évidemment $I+J$ (resp. IJ). D'où $a+b$ (resp. ab) vérifient la propriété (P). Soit a une série quasi-inversible qui vérifie la propriété (P); soit I (resp. K) l'idéal engendré par les coefficients de a (resp. a^*) dans A; de l'égalité

$$a^* = a + aa^* = a + a^*a$$

on tire $K \subseteq I$.

De l'égalité $a=a^*-aa^*$ on tire $I \subseteq K$. D'où $I=K$, i.e. a vérifie la propriété (P) si et seulement si a^* la vérifie. L'ensemble des séries formelles qui vérifient la propriété (P) est une sous-algèbre de $A\langle\langle X\rangle\rangle$ qui contient les polynômes qui est stable par quasi-inversion des éléments quasi-inversibles d'où $A^{\mathrm{rat}}\langle\langle X\rangle\rangle \subseteq$ (séries qui vérifient la propriété (P)).

REMARQUE. Généralisant à $A^{\mathrm{rat}}\langle\langle X\rangle\rangle$ la construction donnée par M. P. Schützenberger [4] dans le cas où $A=\mathbf{Z}$ de la représentation minimale associée à une série rationnelle de $Z\langle\langle X\rangle\rangle$ on peut construire une représentation minimale associée à une série rationnelle de $A\langle\langle X\rangle\rangle$. La représentation minimale montre que les coefficients d'une série rationnelle engendrent un idéal de type fini dans A.

La réciproque du Lemme 1 est bien entendu fausse; en effet si l'anneau A est noethérien tout idéal est de type fini donc l'idéal engendré par les coefficients d'une série quelconque est de type fini.

I. Éléments nilpotents.

PROPOSITION I. *Pour qu'un polynôme de $A\langle X\rangle$ soit nilpotent il faut et il suffit que chacun de ses coefficients le soit.*

DÉMONSTRATION. On raisonne par récurrence sur la longueur des mots figurant dans le support du polynôme considéré.

PROPOSITION II. *Pour qu'une série soit nilpotente il faut que chacun de ses coefficients le soit.*

DÉMONSTRATION. Soit a une série nilpotente, i.e. $a^n=0$ pour un certain n; par récurrence sur la longueur du mot f on montre que le coefficient (a,f) est nilpotent: $(a^n, e)=(a, e)^n=0$, e étant le mode vide de X^*. Do'ù

$$(a^n,f^n) = 0 = (a,f)^n + \sum_{\substack{g_1g_2g_3\cdots g_n=f^n,\\ |g_i|<|f| \text{ pour un certain } i}} (a, g_1)(a, g_2)(a, g_3)\cdots(a, g_n).$$

L'hypothèse de récurrence entraîne la nilpotence du terme général donc aussi de la somme et par suite de (a,f).

La Proposition II admet une réciproque au cas où l'idéal engendré par les coefficients de la série a est un idéal de type fini dans A, ce qui se produit si A est noethérien ou si l'anneau A étant quelconque, la série a est rationnelle.

PROPOSITION III. *Soit a une série qui vérifie la propriété* (P). *Si tous les coefficients de a sont nilpotents alors la série a est nilpotente.*

DÉMONSTRATION. Soit I l'idéal de type fini engendré par les coefficients de a. Engendré par des éléments nilpotents I est un idéal nilpotent. Soit n tel que $I^n=0$, donc: $(a^n,f)\in I^n=0$, i.e. $(a^n,f)=0$ pour tout mot f d'où $a^n=0$. Lorsque l'idéal I engendré par des éléments nilpotents n'est pas de type fini alors la série a n'est pas nécessairement nilpotente comme le montre l'exemple suivant:

Soit K un corps commutatif et A l'anneau: $A=\bigoplus_{i=0}^{\infty} K[X_i]/(X_i^i)$.

Soit $a(Y)=\sum_{i\geqq 1} X_i Y^i$ où $X_i^i=0$ $\forall i\geqq 1$.

Or la série $a(Y)$ n'est pas nilpotente, en effet si $i\neq j$ on a $X_iX_j=0$. Supposons a nilpotente; soit n tel que $a^n=0$. $a^n(Y)=\sum_{i\geqq 1} X_i^n Y^{in}=0$, i.e. $X_i^n=0$ $\forall i\geqq 1$ ce qui est faux.

II. **Diviseurs de zero.** On définit un ordre total sur le monoïde X^* en posant: $f\leqq g$ si et seulement si $|f|<|g|$, ou $|f|=|g|$ et $f\leqq g$ lexicographiquement Cet ordre est compatible avec le produit sur X^*.

PROPOSITION IV. *Pour qu'un polynôme P de $A\langle X\rangle$ soit un diviseur de zéro dans $A\langle X\rangle$, il faut et il suffit qu'il existe $r\in A-\{0\}$ tel que $rP=0$.*

DÉMONSTRATION. La condition est évidemment suffisante. Montrons qu'elle est nécessaire. Soit donc P un polynôme tel que $PQ=0$ pour un polynôme $Q\neq 0$. On a alors $P=\sum_{f\leq f_p}(P,f)f$, $Q=\sum_{g\leqq g_q}(Q,g)g$. On écrit que les coefficients du polynôme $R=PQ$ sont nuls: les relations $(R,f)=0$ pour $f\leqq f_pg_q$ fournissent un système d'équations linéaires (E) homogènes, dont les coefficients sont les (P,f) pour $f\leqq f_p$, et les $q+1$ inconnues les (Q,g), pour $g\leqq g_q$. Désignons par M la matrice du système (E). Comme ce système admet la solution non triviale fournie par Q, il existe un $k\in A-\{0\}$ qui annule tous les sous-déterminants de rang $q+1$ de M [**2**, p. 159].

Pour chaque i, $0\leqq i\leqq p$, soit M_i la sous-matrice de M qui correspond aux équations des mots $f_ig_0,\cdots,f_ig_j,\cdots,f_ig_q$. Appelons I_i l'idéal engendré dans A par les éléments $(P,f_0),\cdots,(P,f_i)$. Notons également $I_{-1}=(0)$. On a alors le lemme suivant, dont la démonstration figure plus loin.

LEMME. *Pour tout i, on a* $\det M_i \equiv (P,f_i)^{q+1} \pmod{I_{i-1}}$.

Il est immédiat que $\det M_0=(P,f_0)^{q+1}$, et donc $k(P,f_0)^{q+1}=0$. Soit $n(0)$ le plus grand entier$\geqq 0$ tel que $k(P,f_0)^{n(0)}\neq 0$. On définit successivement des entiers $n(i)$ tels que $k(P,f_0)^{n(0)}\cdots(P,f_i)^{n(i)}\neq 0$, et $k(P,f_0)^{n(0)}\cdots(P,f_i)^{n(i)+1}=0$: pour $i=1$, $\det M_1=(P,f_1)^{q+1}+a(P,f_0)$, par le lemme, où $a\in A$; or $k\det M_1=0=k(P,f_1)^{q+1}+ak(P,f_0)$, d'où $k(P,f_0)^{n(0)}\det M_1=k(P,f_0)^{n(0)}(P,f_1)^{q+1}$ est nul; soit $n(1)$ le plus grand entier$\geqq 0$ tel que $k(P,f_0)^{n(0)}(P,f_1)^{n(1)}\neq 0$; ayant défini $n(i-1)$, on définit $n(i)$ en remarquant que, d'après le lemme, on a:

$$\det M_i = (P,f_i)^{q+1} + a_0(P,f_0) + \cdots + a_{i-1}(P,f_{i-1})$$

d'où

$$k\det M_i = 0 = k(P,f_i)^{q+1} + ka_0(P,f_0) + \cdots + ka_{i-1}(P,f_{i-1}),$$

d'où

$$k(P,f_0)^{n(0)}\cdots(P,f_{i-1})^{n(i-1)}\det M_i = k(P,f_0)^{n(0)}\cdots(P,f_{i-1})^{n(i-1)}(P,f_i)^{q+1} = 0.$$

On introduit alors le plus grand entier $n(i)\geqq 0$ tel que $k(P,f_0)^{n(0)}\cdots(P,f_i)^{n(i)}\neq 0$. Si on prend alors $r=k(P,f_0)^{n(0)}\cdots(P,f_p)^{n(p)}$, on a $r\neq 0$ et $r(P,f_i)=0$ pour tout i entre 0 et p, et donc $rP=0$, la proposition est démontrée.

PREUVE DU LEMME. La ligne de la matrice M_i qui correspond à l'equation du mot f_ig_j est:

$$(R,f_ig_j) = a_0(P,\bar f_0)(Q,g_0) + a_1(P,\bar f_1)(Q,g_1) + \cdots + (P,\bar f_i)(Q,g_j) + a_{j+1}(P,\bar f_{j+1})(Q,g_{j+1}) + \cdots + a_q(P,\bar f_q)(Q,g_q)$$

où a_n est 0 ou 1 selon que l'équation $\bar f_ng_n=f_ig_j$ a ou n'a pas de solution $\bar f_n\in\{f_0,f_1,\cdots,f_p\}$. Les éléments diagonaux de M_i sont tous égaux à (P,f_i), et les éléments qui figurent au-dessus de la diagonale sont ou bien 0 ou bien (P,f_n) pour un $n<i$. En developpant le déterminant de M_i par rapport à la première ligne, on en déduit le lemme.

PROPOSITION V. *Soient deux séries de $A\langle\langle X\rangle\rangle$ a et b qui vérifient la propriété* (P), *et telles que $b\neq 0$ et $ab=0$; alors il y a un $r\in A-\{0\}$ tel que $ra=0$.*

DÉMONSTRATION. Soit I (resp. J) l'idéal de type fini qu'engendrent les coefficients de a (resp. b): I est donc engendré par les coefficients (a,f_i) pour $f_i\leqq f_p$, et J par les coefficients (b,g_j) pour $g_j\leqq g_q$. Les mots $g\in X^*$ tels que $g>g_q$ et $f_ig\leqq f_pg_q$ pour un $i\leqq p$, sont en nombre fini; désignons les par $g_{q+1},\cdots,g_{q+t}$. Remarquons que si $f_rg_{q+s}=f_ig_j$ pour un couple (s,j) où $1 \leqq s \leqq k$ et $1 \leqq j \leqq q$, alors $f_r \lneqq f_i$, ce qui entraîne l'appartenance de (a,f_r) à I_{i-1}.

Appelons c la série ab: les conditions $(c,f)=0$ pour tout $f \leqq f_p g_q$ fournissent un système d'equations linéaires (E'), dont les coefficients peuvent être exprimés en termes des (a,f) pour $f \leqq f_p$, et dont les inconnues sont les (b,g) pour $g \leqq g_q$. Soit M la matrice du système (E'); l'existence d'une solution non triviale pour le système (E') implique **[2]** l'existence d'un $k \in A-\{0\}$ qui annule tous les sous-déterminants de rang $q+1$ de M. Désignons par M_i la matrice d'ordre $q+1$ extraite de M en prenant les équations relatives aux mots $f_i g_0, \cdots, f_i g_q$. Appelons I_i l'idéal engendré dans A par les éléments $(a,f_0), \cdots, (a,f_i)$, et posons $I_{-1}=(0)$. Comme dans la démonstration précédente, il suffit de prouver le lemme suivant, le reste étant analogue.

LEMME. *Pour tout i, on a* $\det M_i \equiv (a,f_i)^{q+1} \pmod{I_{i-1}}$.

PREUVE DU LEMME. Il suffit de remarquer que les éléments diagonaux de M_i sont tous congrus à (a,f_i) mod I_{i-1}, et que les éléments au-dessus de la diagonale appartiennent à I_{i-1}; on développe alors le déterminant de M_i par rapport à la première ligne.

REMARQUE. Considérons l'anneau A introduit en [**3**, Exemple 3]:

$$A = B[T, (X_n)_{n \geqq 0}]/(X_0 T, (X_n - X_{n+1}T)_{n \geqq 0})$$

où B désigne un anneau commutatif unitaire, et $T, X_0, X_1, \cdots$ est un système d'indéterminées sur B. On définit deux séries a et b de $A\langle\langle X\rangle\rangle$ par

$$(a,f) = X_n \quad \text{si } |f| = n, \quad \text{et} \quad b = T - \sum_{x \in X} x.$$

On a $ab=ba=0$, bien que l'annulateur de b dans A soit réduit à 0.

Je remercie le referee dont les remarques ont permis la correction de quelques imperfections qui figuraient dans le texte initial.

BIBLIOGRAPHY

1. Neil H. McCoy, *Remarks on divisors of zero*, Amer. Math. Monthly **49** (1942), 286–295. MR **3**, 262.

2. ———, *Rings and ideals*, Carus Monograph Series, no. 8, Open Court Publishing Company, LaSalle, Ill., 1948. MR **10**, 96.

3. David E. Fields, *Zero divisors and nilpotent elements in power series rings*, Proc. Amer. Math. Soc. **27** (1971), 427–433. MR **42** #5983.

4. M.-P. Schützenberger, *Definition of a family of automata*, Information and Control **4** (1961), 245–270. MR **24** #B1725.

, 7 RUE BARRAULT, 75 013 PARIS, FRANCE