ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 28, Number 2, Summer 1998

POLYNÔMES ET PUISSANCES PURES

LAURENT DENIS

1. Motivations. Plusieurs problèmes d'arithmétiques tendent à la compréhension du phénomène suivant: des conditions imposées à l'ensemble des valeurs prises par un polynôme entraînent des propriétés correspondantes sur ce polynôme. Le lecteur intéressé pourra consulter l'ouvrage de W. Narkiewicz pour de multiples illustrations [**6**].

De nombreux auteurs se sont intéressés plus particulièrement à la question suivante:

Etant donné $P \in \mathbf{Z}[X]$ et k un entier naturel ≥ 2, si l'ensemble $E = \{n \in \mathbf{Z}/P(n)$ est la puissance k-ième d'un élément de $\mathbf{Z}\}$ est suffisamment gros, alors existe-t-il un polynôme $Q \in \mathbf{Z}[X]$ tel que $P(X) = Q(X)^k$?

Il est bien connu que cette question admet une réponse affirmative dans le cas $E = \mathbf{Z}$, voir [**7**, section 8, et 190].

Un corollaire d'un résultat de H. Davenport, D.J. Lewis, A. Schinzel, confère corollaire 1 de [**1**], affirme que la même conclusion reste valable si on suppose seulement que E rencontre toute progression arithmétique contenue dans $\mathbf{Z}$.

Ces résultats peuvent aussi être obtenu rapidement comme corollaire du théorème de Hilbert.

Les possibilitiés pour la taille et la nature des ensembles E pour lesquels la conclusion $P(X) = Q(X)^k$ est encore une conséquence des hypothèses ont enfin été essentiellement complètement décrites par C. Levêque dans [**5**]. Il est ainsi en particulier prouvé, à l'aide du théorème de C.L. Siegel donnant la finitude du nombre des points entiers sur une courbe de genre ≥ 1 que si E est infini alors $P(X)$ est soit de la forme $c(X-a)^e g(X)^k$ soit de la forme $c(X^2-aX+b)^{k/2} g(X)^k$. Ainsi dès que E est de densité naturelle positive, P est une puissance k-ième, il est même possible de donner des ordres de grandeurs pour le nombre maximal de points de E de valeurs absolues $\leq T$ qu'on puisse

Received by the editors on May 7, 1996, and in revised form on June 20, 1996.

avoir sans que P soit une puissance k-ième, voir [**5**]. Notons également qu'on peut obtenir d'autres résultats en remplaçant le théorème de Siegel par celui de G. Faltings comme l'on fait les auteurs de [**2**].

La question se pose alors en dimension supérieure. Un premier énoncé se trouve dans le texte de T. Kojima [**4**] où il est démontré entre autre choses que si pour tout $(x_1, \ldots, x_n)$ élément de $\mathbf{Z}^n$ le polynôme à n variables $P(X_1, \ldots, X_n)$ prend des valeurs puissances k-èmes dans $\mathbf{Z}$ alors, il existe $Q(X_1, \ldots, X_n)$ à coefficients dans $\mathbf{Z}$ tel que $P(X_1, \ldots, X_n) = Q(X_1, \ldots, X_n)^k$. A. Schinzel est également capable de donner une version à plusieurs variables de son énoncé sur les ensembles rencontrant toutes suites arithmétiques. Dans le cadre qui nous intéresse, il prouve ainsi que si l'ensemble des $(x_1, \ldots, x_n)$ éléments de $\mathbf{Z}^n$ tels que $P(x_1, \ldots, x_n)$ prend des valeurs puisances k-èmes dans $\mathbf{Z}$ contient un produit d'ensembles rencontrant chacun une progression arithmétique arbitraire alors P est encore identiquement une puissance k-ième (l'énoncé général est donné dans [**8**, théorème 36]).

Pour le résultat qui suit, on considère k un entier naturel supérieur ou égal à 2 et E_i, $1 \leq i \leq n$, des ensembles d'entiers relatifs tels que pour chaque valeur de i, si un polynôme arbitraire à coefficients dans $\mathbf{Z}$ en une variable prend des valeurs puissances k-ième d'entiers relatifs sur E_i alors ce polynôme est la puissance k-ième d'un polynôme à coefficients dans $\mathbf{Z}$.

Theoreme 1. *Soit $P(X_1, \ldots, X_n)$ un polynôme en n variables à coefficients dans $\mathbf{Z}$. Si pour tout x_i appartenant à E_i, l'entier $P(x_1, \ldots, x_n)$ est une puissance k-ième dans $\mathbf{Z}$ alors il existe un polynôme $Q(X_1, \ldots, X_n)$ à coefficients dans $\mathbf{Z}$ tel que $P(X_1, \ldots, X_n) = Q(X_1, \ldots, X_n)^k$.*

L'exemple d'un polynôme $\prod_{i=1}^n P_i(X_i)$ où chaque P_i est de la forme $c(X_i - a)^e g(X_i)^k$ ou $c(X_i^2 - aX_i + b)^{k/2} g(X_i)^k$, montre que le théorème est essentiellement optimal si on se restreint à des ensembles produits.

Comme me l'a signalé P. Dèbes, ce théorème peut aussi être avantageusement traduit en terme de parties Hilbertiennes et minces. Rappelons la définition suivante, voir [**9**, paragraphe 6.1].

On dira que H est une partie hilbertienne de $\mathbf{Q}^n$ associé à un r-

uplet de polynômes $P_i \in \mathbf{Q}(T_1, \ldots, T_n)[X_1, \ldots, X_s]$ irréductibles, si H est l'ensemble des t de $\mathbf{Q}^n$ tels que les $P_i(t, X_1, \ldots, X_s)$ restent irréductibles dans $\mathbf{Q}[X_1, \ldots, X_s]$.

Une partie sera mince si elle est contenue dans le complémentaire d'une partie hilbertienne et non mince si elle ne l'est pas. Ainsi une partie M est non mince quand pour tout r-uplet de polynômes irréductibles P_i, il existe un t dans M tels que les $P_i(t, X_1, \ldots, X_s)$ restent irréductibles.

Les ensembles apparaîssant dans notre texte motivent la définition suivante.

Définition 1. Soit $S(Y)$ un élément de $\mathbf{Z}[Y]$, on dit qu'une partie M de $\mathbf{Z}^n$ est $S(Y)$ mince s'il existe un polynôme $Q \in \mathbf{Z}[T_1, \ldots, T_n]$ qui n' est pas de la forme $S(R)$ où $R \in \mathbf{Q}[T_1, \ldots, T_n]$, tel que M est contenue dans $\{t \in \mathbf{Z}^n / S(Y) - Q(t)$ admet une racine dans $\mathbf{Q}\}$.

Dans le cas $S(Y) = Y^k$, on dira simplement que M est une partie k mince.

Il est prouvé dans [**9**, paragraphe 6], qu'étant donné un polynôme $P \in \mathbf{Q}(T_1, \ldots, T_N)[Y]$ sans racine dans $\mathbf{Q}(T_1, \ldots, T_n)$, l'ensemble des t tels que $P(t, Y)$ a une racine entière est un ensemble mince de $\mathbf{Z}^n$.

Ce résultat implique en particulier qu'une partie non mince est une partie non $S(Y)$ mince. De plus, il est relativement facile de voir par spécialisation et lemme de Gauss, que le produit de parties non minces est non mince.

Il s'en suit donc que le produit de n parties non minces de $\mathbf{Z}$ est une partie non k mince de $\mathbf{Z}^n$. Notre théorème peut alors se voir comme un raffinement de cette implication. Il est en effet équivalent à l'énoncé qui suit.

Theorem 1′. *Le produit de n parties non k minces de $\mathbf{Z}$ est une partie non k mince de $\mathbf{Z}^n$.*

2. Preuve. La preuve va se faire par récurrence sur le nombre n de variables. L'ingrédient essentiel est le lemme suivant. Nous nous aperçûmes après l'avoir prouvé qu'une version voisine de ce lemme

semblait déjà connue des auteurs de [**3**], voir p. 80, et qu'il se trouve aussi en grande partie dans [**8**, lemme 3, p. 12].

Lemme. *Soit A un anneau intègre commutatif de caractéristique nulle de corps des fractions K et soit k un entier naturel supérieur ou égal à 2. Soit encore $P \in A[X]$ un polynôme de degré $d = uk$, multiple de k, et dont le coefficient dominant est a^k avec a dans A. Il existe alors deux polynômes Q et R appartenant à $K[X]$ tels que*:

i) $P(X) = Q(X)^k + R(X)$;

ii) degré$(R) \leq uk - u - 1$;

iii) $(ka)^{k^{u+1}} Q(X) \in A[X]$, $(ka)^{k^{u+2}} R(X) \in A[X]$.

Preuve. Il s'agit de trouver une solution au système à u équations obtenu en identifiant les termes de degré supérieur dans l'identité: $P(X) = a^k X^{ku} + a_1 X^{ku-1} + \cdots + a_u X^{ku-u} + \cdots + a_0 = (aX^u + b_1 X^{u-1} + \cdots + b_u)^k + R(X)$. Pour $0 \leq v \leq u$, le terme en X^{ku-v} fait apparaître d'un coté, a_v, de l'autre des produits d'au plus k termes en b_j avec $j \leq v$ et le terme en b_v est exactement $ka^{k-v}b_v$. D'où l'on tire l'existence et l'unicité de Q puis de R. Si d_{v-1} est un dénominateur commun aux b_j, $j \leq v-1$, alors d'après l'écriture précédente $ka^k(d_{v-1})^k$ est un dénominateur commun aux b_j, $j \leq v$. D'où l'assertion sur les dénominateurs de $Q(X)$ puis $R(X)$. □

Il est maintenant possible de procéder à la preuve du théorème.

Preuve du théorème. Le cas $n = 1$ vient de la définition de E_1. Supposons donc l'énoncé établit pour tout polynôme à r variables et r inférieur ou égal à $n - 1$. Considérons un polynôme P possèdant exactement n variables. Notons d_n le degré de P en la n-ième variable (qui est donc non nul) et regardons P comme élément de $A[X_n]$ où $A = \mathbf{Z}[X_1, \ldots, X_{n-1}]$, appelons Y son coefficient dominant. Soit $(x_1, \ldots, x_{n-1})$ un élément de $E_1 X \cdots X E_{n-1}$ tel que $Y(x_1, \ldots, x_{n-1})$ est non nul, alors le polynôme en une variable $P(x_1, \ldots, x_{n-1}, X_n)$ prend des valeurs puissances k-ièmes sur E_n et est donc une puissance k-ième d'un élément de $\mathbf{Z}[X_n]$. En particulier, ceci implique que d_n est un multiple de k et aussi que l'entier $Y(x_1, \ldots, x_{n-1})$ est une puissance

k-ième dans $\mathbf{Z}$. Or si $(x_1, \ldots, x_{n-1})$ un élément de $E_1 X \cdots X E_{n-1}$ tel que $Y(x_1, \ldots, x_{n-1})$ est nul, cet élément est encore une puissance k-ième égale à 0^k. Le polynôme non nul Y est donc par hypothèse de récurrence la puissance k-ième d'un polynôme également non nul, possèdant au plus $n-1$ variables et dont les coefficients sont dans $\mathbf{Z}$.

Ecrivons alors $d_n = ku$ et $Y = Z^k$.

D'après le lemme ci-dessus, on peut donc écrire:

$$(kZ)^{k^{u+2}} P(X_1, \ldots, X_n) = [(kZ)^{k^{u+1}} Q(X_1, \ldots, X_n)]^k + (kZ)^{k^{u+1}} R(X_1, \ldots, X_n);$$

où $(kZ)^{k^{u+1}} Q(X_1, \ldots, X_n)$ et $(kZ)^{k^{u+1}} Q(X_1, \ldots, X_n)$ sont des polynômes à coefficients dans $\mathbf{Z}$.

Maintenant, et comme expliqué dans l'introduction, chacun des ensembles E_i est de cardinal infini. En se souvenant du fait que Z est non nul et possède moins de $n-1$ variables, si R n'est pas le polynôme nul, il existe un élément $(z_1, \ldots, z_{n-1})$ de $E_1 X \cdots X E_{n-1}$ tel que le degré en X_n de $R((kZ)^{k^{u+2}} P)(z_1, \ldots, z_{n-1}, X_n)$ soit encore le degré en X_n du polynôme en n variables $E((kZ)^{k^{u+2}} P)$. Il s'en suit que d_n est le degré du polynôme en une variable $((kZ)^{k^{u+2}} P)(z_1, \ldots, z_{n-1}, X_n) = S(X_n)$, que le degré de $((kZ)^{k^{u+1}} Q)(z_1, \ldots, z_{n-1}, X_n) = T(x_n)$ est u, celui de $((kZ)^{k^{u+1}} R)(z_1, \ldots, z_{n-1}, X_n) = U(X_n)$ étant toujours inférieur ou égal à $ku - u - 1$.

Soit $m \in \mathbf{Z}$, il est possible d'écrire $S(m) = a^k m^{ku}(1 + e_m)$ et $T(m) = b m^u (1 + f_m)$ où si m est de valeur absolue assez grande alors e_m et f_m tendent vers zéro a et b étant dans $\mathbf{Z}$. Si de plus m est un élément de E_n alors il existe un entier relatif V_m tel que $P(z_1, \ldots, z_{n-1}, m) = V_m^k$, on peut alors supposer que l'on choisit cet entier de sorte que $V_m = a m^u (1 + g_m)$ oú g_m tend vers zéro.

On dispose de l'égalité $S(m) - T(m)^k = U(m)$ d'où nous tirons:

$$(V_m - T(m)) \prod_{\zeta^k = 1, \zeta \neq 1} (V_m - \zeta T(m)) = U(m).$$

Le terme de droite de cette égalité est majoré par $c m^{(k-1)u-1}$. Quand au terme de gauche il est minoré par $(V_m - T(m)) m^{(k-1)u}(1 + h_m)$ où

h_m tend vers zéro. Comme $(V_m - T(m))$ est un entier, si m est assez grand, cet entier est nécessairement nul. Enfin un polynôme n'ayant plus de racines que son degré, le fait que E_n soit infini entraîne une contradiction avec le fait que U et donc R est non nul.

Nous avons donc $(kZ)^{k^{u+2}} P(X_1, \dots, X_n) = [(kZ)^{k^{u+1}} Q(X_1, \dots, X_n)]^k$, ou encore: $P(X_1, \dots, X_n) = [(Q(X_1, \dots, X_n)]^k$ ce qui était le but recherché. □

Problème. La première extension naturelle de ce résultat serait de savoir si dans notre théorème la fonction Y^k peut-être remplacée par un polynôme $Q(Y)$ quelconque de $\mathbf{Q}[Y]$. On s'attend ainsi à ce que si les E_i sont des ensembles tels que si un polynôme P en une variable prenne des valeurs de la forme $Q(m)$ sur E_i alors $P(X) = Q(W(X))$ pour un certain polynôme W à coefficients rationnels; alors un polynôme en n variables prenant des valeurs en $Q(m)$ sur le produit $E_1 X \cdots X E_n$ devrait encore être fonctionnellement de la forme $Q(W(X_1, \dots, X_n))$. Avec la formulation de la définition 1, il s'agit donc de voir si le produit de parties non $Q(Y)$ minces est encore non $Q(Y)$ mince. Notons qu'il est facile d'établir un analogue à notre lemme sur l'approximation par des puissances k-ièmes, en approximant $P(X)$ par un $Q(Y(X))$, cependant les dénominateurs apparaîssant dans les coefficients du polynôme Y ne nous ont pas permis d'aboutir par un récurrence similaire à celle utilisée dans notre théorème.

RÉFÉRENCES

1. H. Davenport, D.J. Lewis and A. Schinzel, *Polynomial of certain special types*, Acta Arith. **9** (1964), 107–116.

2. H. Darmon and A. Granville, *On the equations* $z^m = F(x, y)$ *and* $Ax^p + By^q = Cz^r$, Bull. London Math. Soc. **27** (1995), 513–543.

3. E. Fried and J. Suranyi, *New proof of a number theoretic theorem on polynomials*, Mat. Lapok **11** (1960), 75–84.

4. T. Kojima, *Note on number-theoretical properties of algebraic functions*, Tohôku Math. J. **8** (1915), 24–37.

5. C. Leveque, *On the equation* $y^m = f(x)$, Acta Arith. **9** (1964), 209–219.

6. W. Narkiewicz, *Polynomial mapping*, Lect. Notes in Math., **1600** (1995).

7. G. Polya und G. Szego, *Aufgaben und Lehrsätze aus des analysis* II, Julius Springer, Berlin.

8. A. Schinzel, *Selected topics on polynomials*, The University of Michigan Press, 1982.

9. J.P. Serre, *Autour du théorème de Mordell-Weil* II, Prépublication de Paris **6**, 1983.

Université P. et M. Curie, Institut de Math., Case 247, 5 Place Jussieu, 75006 Paris

Current address: Université des Sciences et Technologies de Lille, Département de Mathématiques, 59655 Villeneuve D'Ascq Cedex, France
E-mail address: ladenis@ccr.jussieu.fr