Portugal. Math. (N.S.)
Vol. 65, Fasc. 3, 2008, 339–343

Portugaliae Mathematica

Irréductibilité et spécialisation des polynômes

Salah Najib

(Communicated by Rui Loja Fernandes)

Abstract. Starting from the decomposition in base $b(X)$ (a nonconstant polynomial), we give an irreducibility criterion of the bivariate polynomials. Moreover we study a problem of specialization which has a link with Hilbert's irreducibility theorem.

Résumé. À partir de la décomposition en base $b(X)$ (un polynôme non constant), nous donnons un critère d'irréductibilité des polynômes en deux variables. Puis nous étudions un problème de spécialisation qui a un lien avec le théorème d'irréductibilité de Hilbert.

Mathematics Subject Classification (2000). 12D05, 12E25, 12E05, 11C08.

Keywords. b-basis decomposition, irreducible polynomial, hilbertian set, hilbertian field, Hilbert irreducibility theorem.

1. Introduction

Soit $b \geq 2$ un entier. Tout entier $n > 0$ s'écrit sous la forme

$$n = a_0 + a_1 b + \cdots + a_m b^m,$$

avec $a_m \neq 0$ et $0 \leq a_i \leq b-1$ pour $i = 0, \ldots, m$. Cette écriture est unique et est appelée *la décomposition de l'entier n en base b*.

Par exemple, si on prend $b = 10$ et $n = 137$, alors la décomposition de n en base b est : $137 = 7 + 3 \cdot 10 + 10^2$. De plus, il est facile de montrer que le polynôme associé $f(X) = X^2 + 3X + 7$ est irréductible dans $\mathbb{Q}[X]$.

Dans ce contexte, on a le résultat suivant.

Théorème 1. *Soit $n \geq 2$ un entier premier et $n = \sum_{i=0}^{m} a_i b^i$ sa décomposition en base b. Alors le polynôme $f(X) = \sum_{i=0}^{m} a_i X^i$ est irréductible dans $\mathbb{Z}[X]$.*

Preuve. Ce théorème a été démontré dans [1], Corollary 2. □

Le but de cette note est double. D'une part, donner une version plus générale du théorème 1 (voir le théorème 2 ci-dessous). D'autre part, étudier dans la dernière section la réciproque de la version générale (voir le théorème 3).

Nous remercions le Prof. P. Dèbes pour les discussions à propos de la formulation et de la preuve du théorème 3. Nous remercions le referee dont les commentaires nous ont permis de beaucoup améliorer le texte.

2. Version générale

Soit $b(X)$ dans $\mathbb{Q}[X]$ un polynôme de degré ≥ 1.

Pour tout polynôme non constant $f(X)$ dans $\mathbb{Q}[X]$, nous écrivons

$$f(X) = \sum_{i=0}^{m} a_i(X) b(X)^i$$

une décomposition de $f(X)$ en base $b(X)$, avec $a_m(X) \neq 0$ et $\deg(a_i) < \deg(b)$ pour $i = 0, \ldots, m$.

Nous donnons une preuve directe du théorème suivant.

Théorème 2. *Soit $f(X)$ un polynôme irréductible dans $\mathbb{Q}[X]$ tel que $f(X) = \sum_{i=0}^{m} a_i(X) b(X)^i$ est sa décomposition en base $b(X)$. Alors le polynôme $F(X, Y) = \sum_{i=0}^{m} a_i(X) Y^i$ est irréductible dans $\mathbb{Q}[X, Y]$, avec Y est une nouvelle variable qui est algébriquement indépendant avec X sur $\mathbb{Q}$.*

Preuve. Supposons que le polynôme $F(X, Y)$ possède dans $\mathbb{Q}[X, Y]$ une factorisation : $F(X, Y) = f_1(X, Y) \ldots f_r(X, Y)$, avec $f_i \in \mathbb{Q}[X, Y]$ irréductible sur $\mathbb{Q}$ pour tout $i = 1, \ldots, r$.

En substituant $b(X)$ à Y dans l'identité précédente, on obtient d'après notre hypothèse « $f(X)$ est irréductible dans $\mathbb{Q}[X]$ » que tous les polynômes $f_i\big(X, b(X)\big)$ sauf un sont constants non nuls. De plus, le facteur exceptionnel, disons $f_j\big(X, b(X)\big)$, doit être égal à $f(X)$ (à une constante non nulle près).

Or, on a $\deg_X(f_j) \leq \deg_X(F) < \deg(b)$. Par conséquent, en raison de l'unicité de l'écriture en base $b(X)$, on a nécessairement $f_j(X, Y)$ égal à $F(X, Y)$ (à une constante non nulle près). □

Remarque. La condition « $f(X)$ est irréductible dans $\mathbb{Q}[X]$ » est nécessaire. En effet, par exemple pour $b(X) = X^3$ et $f(X) = X^4 + X^6$. Ici, on a $a_0(X) = 0$, $a_1(X) = X$ et $a_2(X) = 1$. Cependant, le polynôme $F(X, Y) = XY + Y^2$ est réductible dans $\mathbb{Q}[X, Y]$.

Dans le reste de ce texte, nous considérons la réciproque du théorème 2; c'est-à-dire, étant donné un polynôme irréductible $F(X, Y) \in \mathbb{Q}[X, Y]$, existe-il un

polynôme $b(X) \in \mathbb{Q}[X]$, avec $\deg(b) > \deg_X(F)$ tel que $F\big(X, b(X)\big)$ est irréductible dans $\mathbb{Q}[X]$? Autrement dit, regarder l'irréductibilité après spécialisation de la variable Y dans $\mathbb{Q}[X]$. Ce problème a un lien avec le *théorème d'irréductibilité de Hilbert*.

Une réponse à cette question est négative par exemple si le corps $\mathbb{Q}$ est remplacé par un corps algébriquement clos. En travaillant sur un corps *hilbertien* K, nous montrons qu'il existe beaucoup de choix de tels polynômes $b(X) \in K[X]$ dont la conclusion voulue est vérifiée.

3. La réciproque du théorème 2

Commençons par quelques préliminaires.

3.1. Préliminaires. Soit K un corps. Soient m, r et d des entiers ≥ 1. Soient $\boldsymbol{T} = (T_1, \ldots, T_m)$ et $\boldsymbol{Z} = (Z_1, \ldots, Z_d)$ des indéterminées algébriquement indépendantes sur K et $P_1(\boldsymbol{T}, \boldsymbol{Z}), \ldots, P_r(\boldsymbol{T}, \boldsymbol{Z})$ r polynômes irréductibles dans $K(\boldsymbol{T})[\boldsymbol{Z}]$ de degré > 0 en $\boldsymbol{Z}$. Notons $H_K(P_1, \ldots, P_r)$ l'ensemble constitué des spécialisations $\boldsymbol{t} = (t_1, \ldots, t_m) \in K^m$ des indéterminées $\boldsymbol{T}$ pour lesquelles les polynômes $P_i(\boldsymbol{t}, \boldsymbol{Z})$, $i = 1, \ldots, r$, sont irréductibles dans $K[\boldsymbol{Z}]$. Rappelons qu'on appelle *partie hilbertienne* de K^m tout ensemble, intersection d'un ensemble du type $H_K(P_1, \ldots, P_r)$ avec un ouvert de Zariski de K^m et qu'un corps K est dit *hilbertien*[1] si pour tout entier $m \geq 1$, les parties hilbertiennes sont non vides. En ces termes, le théorème d'irréductibilité de Hilbert [3] s'énonce : *le corps* $\mathbb{Q}$ *des nombres rationnels est hilbertien*. Pour avoir plus de détails et plus de références sur ce sujet, nous renvoyons par exemple à [2] et [4].

Le but crucial de cette dernière section est de démontrer le théorème suivant.

Théorème 3. *Soit K un corps hilbertien. Soit $F(X, Y)$ un polynôme irréductible dans $K[X, Y]$. Alors il existe une infinité de polynômes $b(X) \in K[X]$, avec $\deg(b) > \deg_X(F)$ tels que $F\big(X, b(X)\big)$ est irréductible dans $K[X]$.*

La différence entre notre théorème et le caractère hilbertien d'un corps K est que la variable Y est spécialisé dans $K[X]$ au lieu de K.

3.2. Preuve du théorème 3. Considérons le polynôme

$$\mathscr{F}(X, T_1, \ldots, T_d, Y) = F(X, Y + T_1X + \cdots + T_dX^d),$$

avec $d > \deg_X(F)$ un entier et $\boldsymbol{T} = (T_1, \ldots, T_d)$ des variables.

[1] Notons par exemple qu'un corps fini n'est pas hilbertien.

Pour la preuve du théorème 3, il suffit de montrer que le polynôme $\mathscr{F}$ est irréductible dans $K(\boldsymbol{T}, Y)[X]$. Nous allons démontrer cet argument pour K un corps infini.

Supposons que $\mathscr{F}(X, \boldsymbol{T}, Y) = \mathscr{Q}(X, \boldsymbol{T}, Y) \cdot \mathscr{R}(X, \boldsymbol{T}, Y)$, avec $\mathscr{Q}, \mathscr{R} \in K[X, \boldsymbol{T}, Y] \backslash K[\boldsymbol{T}, Y]$. Soit $\boldsymbol{t} = (t_1, \ldots, t_d)$ un d-uplet dans K^d. Par spécialisation de $\boldsymbol{T}$ en $\boldsymbol{t}$, on obtient

$$F(X, Y + t_1 X + \cdots + t_d X^d) = \mathscr{Q}(X, \boldsymbol{t}, Y) \cdot \mathscr{R}(X, \boldsymbol{t}, Y)$$

Posons $\phi_{\boldsymbol{t}}(X) = t_1 X + \cdots + t_d X^d$. Le changement de (X, Y) par $\big(X, Y - \phi_{\boldsymbol{t}}(X)\big)$ dans l'identité précédente nous donne $F(X, Y) = \mathscr{Q}\big(X, \boldsymbol{t}, Y - \phi_{\boldsymbol{t}}(X)\big) \cdot \mathscr{R}\big(X, \boldsymbol{t}, Y - \phi_{\boldsymbol{t}}(X)\big)$. Puisque $F(X, Y)$ est irréductible dans $K[X, Y]$, alors l'un des deux polynômes dans le terme de droite est dans K. Mais, en changeant (X, Y) par $\big(X, Y + \phi_{\boldsymbol{t}}(X)\big)$, on obtient que $\mathscr{Q}(X, \boldsymbol{t}, Y) \in K$ ou $\mathscr{R}(X, \boldsymbol{t}, Y) \in K$. Comme ceci est vérifie pour tout d-uplet $\boldsymbol{t} \in K^d$, on obtient une contradiction avec l'hypothèse « $\mathscr{Q} \notin K[\boldsymbol{T}, Y]$ et $\mathscr{R} \notin K[\boldsymbol{T}, Y]$ ». Notons en plus que $\deg_X(\mathscr{F}) \geq 1$ (puisque $\mathscr{F}(X, 0, \ldots, 0, Y) = F(X, Y)$) pour conclure que $\mathscr{F}$ est irréductible dans $K(\boldsymbol{T}, Y)[X]$. D'òu l'ensemble des polynômes $b(X) = y + t_1 X + \cdots + t_d X^d$ de degré $\leq d$ qui vérifient la conclusion du théorème 3, vu comme sous ensemble de K^{d+1}, est une partie hilbertienne. En particulier, ce sous ensemble est Zariski-dense dans K^{d+1} (car K est supposé hilbertien). □

3.3. Remarques. 1) Notre argument (juste-avant) montre actuellement que $\mathscr{F}$ est irréductible dans $K(\boldsymbol{T})[X, Y]$, et en fait, il est irréductble dans $K[X, \boldsymbol{T}, Y]$. Pour cela, nous devons montrer que $\mathscr{F}$ ne possède pas une factorisation de la forme $\mathscr{F} = \mathscr{Q}(\boldsymbol{T}) \cdot \mathscr{R}(X, \boldsymbol{T}, Y)$, avec $\mathscr{Q} \in K[\boldsymbol{T}] \backslash K$ et $\mathscr{R} \in K[X, \boldsymbol{T}, Y]$. Supposons le contraire, alors en prenant $Y = 0$ et les $T_j = 0$ sauf pour un indice i, on obtient $F(X, T_i X^i) = \mathscr{Q}(0, \ldots, 0, T_i, \ldots, 0) \cdot \mathscr{R}(X, 0, \ldots, 0, T_i, \ldots, 0)$. Posons $Z = T_i X^i$ pour la réécrire comme $F(X, Z) = \mathscr{Q}(0, \ldots, 0, Z/X^i, \ldots, 0).\mathscr{R}(X, 0, \ldots, 0, Z/X^i, \ldots, 0)$. L'irréductibilité de F dans $K[X, Z]$ donne alors que $\deg_{T_i} \mathscr{Q} = 0$ pour tout $i = 1, \ldots, d$.

2) Pour démontrer le théorème 3, on peut aussi utiliser cette approche : par une application de notre théorème de [4] au polynôme $\mathscr{F}(X, T, Y) = F(X, Y + T)$ qui est irréductible dans $K[X, T, Y]$ (d'après l'argument ci-dessus et la remarque 1)), on montre qu'il existe une infinité de polynômes $t(X) \in K[X]$ de degré d donné à l'avance, en partculier $d > \deg_X(F)$ tels que le polynôme $\mathscr{F}\big(X, t(X), Y\big) = F\big(X, Y + t(X)\big)$ est irréductible dans $K(Y)[X]$. De plus, en supposant le corps K hilbertien, on en déduit que l'ensemble des polynômes $b(X) = y + t(X)$ qui vérifient la conclusion du théorème 3 est infinie.

3) Il serait intéressant de trouver (sur un corps de caractéristique ≥ 0) des analogues des théorèmes 2 et 3 dans le cas où le terme « *irréductible* » sera remplacé

par « *non composé* ». Pour cette dernière notion, nous renvoyons par exemple à [5], Chapitre 1.

Note. L'auteur veut remercier tout le staff du centre « Abdus Salam » ICTP, Trieste (Italy) pour leur accueil et leur encouragement.

Références

[1] J. Brillhart, M. Filaseta, and A. Odlyzko, On an irreducibility theorem of A. Cohn. *Canad. J. Math.* **33** (1981), 1055–1059. Zbl 0481.12006 MR 638365

[2] P. Dèbes, Résultats récents liés au théorème d'irréductibilité de Hilbert. In *Séminaire de Théorie des Nombres, Paris 1985–1986*, Progr. Math. 71, Birkhäuser Boston, Boston 1987, 19–37. Zbl 0632.12004 MR 1017901

[3] D. Hilbert, Ueber die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten. *J. Reine Angew. Math.* **110** (1892), 104–129. JFM 24.0087.03

[4] S. Najib, Un raffinement du caractère hilbertien du corps $K(X)$. *Manuscripta Math.* **120** (2006), 415–418. Zbl 05057655 MR 2245892

[5] S. Najib, Factorisation des polynômes $P(X_1, \ldots, X_n) - \lambda$ et théorème de Stein. Thèse de Doctorat, Université de Lille 1, Villeneuve d'Ascq 2005.

Received November 30, 2006; October 25, 2007

Mathematics Section, ICTP, The Abdus Salam International Centre for Theoritical Physics, Strada Costiera 11, 34014 Trieste, Italy
E-mail: najibm@voila.fr; snajib@ictp.it