ACTA ARITHMETICA
116.4 (2005)

Théorème d'irréductibilité de Hilbert effectif

par

Yann Walkowiak (Lille)

Introduction. Une question naturelle quand on s'intéresse à l'irréductibilité des polynômes est le problème d'hérédité par spécialisation :

Soit $F(T,Y) \in k[T,Y]$ irréductible sur un corps k, avec $\deg_Y(F) \geq 1$. Si on spécialise T en $t \in k$, le polynôme $F(t,Y)$ est-il encore irréductible sur k ?

Le théorème d'irréductibilité de Hilbert dit que pour $k = \mathbb{Q}$, la réponse est positive pour une infinité de t.

Théorème (Hilbert [H], 1892). *Soit $F(T,Y) \in \mathbb{Q}[T,Y]$ un polynôme irréductible sur $\mathbb{Q}$ tel que $\deg_Y(F) \geq 1$. Alors pour une infinité de $t \in \mathbb{Q}$, $F(t,Y)$ est irréductible sur $\mathbb{Q}$.*

Ce théorème a de nombreuses applications. La première, qui était la motivation de Hilbert, concerne le problème inverse de Galois. Il montre en effet qu'il suffit de prouver qu'un groupe fini G est groupe de Galois sur $\mathbb{Q}(T)$ pour le prouver sur $\mathbb{Q}$. Parmi d'autres applications, citons le problème de factorisation d'un polynôme à deux variables :

Soit $F(T,Y)$ un polynôme unitaire en Y et à coefficients dans $\mathbb{Z}$ dont on cherche la décomposition en irréductibles sur $\mathbb{Q}$,

$$F(T,Y) = \prod_{i=1}^{r} F_i(T,Y)^{\alpha_i}.$$

On peut spécialiser cette égalité, on obtient

$$F(t,Y) = \prod_{i=1}^{r} F_i(t,Y)^{\alpha_i}.$$

D'autre part, $F(t,Y)$ étant un polynôme à une variable, on peut le factoriser, en utilisant par exemple l'algorithme de A. K. Lenstra, H. W. Lenstra et

2000 *Mathematics Subject Classification*: Primary 12E25, 14G05; Secondary 12E05.

L. Lovász [LLL], pour obtenir

$$F(t,Y)=\prod_{i=1}^{s}\Pi_i(Y)^{\beta_i},$$

où les $\Pi_i(Y)\in\mathbb{Z}[Y]$ sont irréductibles sur $\mathbb{Q}$ et unitaires en Y. Si les $F_i(t,Y)$ sont irréductibles sur $\mathbb{Q}$, alors on peut déduire de l'unicité de la factorisation dans $\mathbb{Z}[Y]$ que $r=s$ et, quitte à renuméroter,

$$(F_i(t,Y),\alpha_i)=(\Pi_i(Y),\beta_i).$$

En faisant ce raisonnement pour un nombre suffisant de "bons" t, on aboutit à un système avec assez d'équations pour en déduire les $F_i(T,Y)$.

On est donc amené à se poser une nouvelle question : est-il possible de trouver explicitement une "bonne" spécialisation ? Et si oui, en combien de temps ?

La première réponse positive a été donnée par P. Dèbes en 1993 (voir [De]), ce qui nous fournit donc un algorithme de factorisation pour les polynômes à deux indéterminées. Cependant, si on s'intéresse à la complexité de cet algorithme, on s'aperçoit que, alors que l'algorithme de A. K. Lenstra, H. W. Lenstra et L. Lovász [LLL] pour les polynômes à une variable est polynomial, cette méthode ne fournit un algorithme polynomial que s'il est possible de trouver une "bonne" spécialisation en temps polynomial. Or le résultat de P. Dèbes ne répond pas à cette condition. Une amélioration de ce résultat a été donnée en 1995 par A. Schinzel et U. Zannier [ScZa] mais n'est toujours pas suffisante pour répondre affirmativement au problème de factorisation d'un polynôme à deux variables en temps polynomial.

La motivation de ce travail est cette dernière question : est-il possible de trouver explicitement et en temps polynomial une "bonne" spécialisation ? Un premier essai basé sur la preuve de K. Dörge ([1]) a donné une version effective du théorème de Hilbert, mais avec une borne pour une "bonne" spécialisation qui n'améliore pas les résultats existants ; une seconde tentative utilisant des méthodes de congruence et inspirée par un article de M. Fried [Fr] est en cours d'étude (voir [Wa] pour l'exposé de ces résultats). Nous allons présenter dans cet article une amélioration de la méthode utilisée par A. Schinzel et U. Zannier, utilisant des résultats récents de Heath-Brown sur les points entiers d'une courbe algébrique.

NOTATIONS. Soit $F(T,Y)\in\mathbb{Z}[T,Y]$. On supposera F primitif, c'est-à-dire que les coefficients de F sont sans facteur commun. Ceci ne change en rien le problème d'irréductibilité et permet de considérer la hauteur usuelle

([1]) Voir [Do] qui date de 1927, donc bien avant le premier résultat effectif.

$H(F)$ de F comme le maximum des valeurs absolues de ses coefficients. On notera

- d le degré total de F,
- m et n les degrés partiels de F respectivement par rapport à la première et la seconde variable,
- $H = \max\{H(F), e^e\}$.

Dans un premier temps, nous donnerons une version explicite du résultat récent de Heath-Brown sur l'étude de la quantité

$$N(F;B) = \sharp\{(t,y) \in \mathbb{Z}^2 : F(t,y) = 0, \max(|t|,|y|) \leq B\},$$

où B est un entier supérieur ou égal à 2.

THÉORÈME 1. *Soit $F(T,Y) \in \mathbb{Z}[T,Y]$ irréductible sur $\mathbb{Q}$ de degré total $d \geq 1$. On a*

$$N(F,B) \leq 2^{48} d^8 \log^5(B) B^{d^{-1}}.$$

Un des intérêts de cette version effective est que la dépendance en d est polynomiale, ce qui améliore les résultats de Bombieri et Pila [BP] et de Schinzel et Zannier [ScZa]. De plus, le résultat est indépendant de la hauteur de F.

Nous appliquerons ensuite ce résultat afin d'estimer le nombre de spécialisations entières $t \leq B$, telles que le polynôme $F(t,Y)$ ait un zéro entier. Ceci nous permettra en premier lieu de donner une borne pour les spécialisations telles que $F(t,Y)$ n'ait pas de zéro entier :

THÉORÈME 2. *Soient $s \in \mathbb{N}^*$ et $F(T,Y) \in \mathbb{Z}[T,Y]$ irréductible sur $\mathbb{Q}$, primitif et tel que $n = \deg_Y(F) \geq 2$. Il existe s entiers positifs $t_1, \ldots, t_s$ inférieurs à*

$$(s + 2^{88} d^{45} \log^{19}(H))^4$$

tels que les équations $F(t_i,Y) = 0$, $i = 1, \ldots, s$, n'aient pas de solution entière.

Cela nous permettra également, via une réduction classique du théorème de Hilbert, de donner une nouvelle forme effective du théorème de Hilbert qui améliore de façon significative les résultats existants.

THÉORÈME 3. *Soient $s \in \mathbb{N}^*$ et $F(T,Y) \in \mathbb{Z}[T,Y]$ irréductible sur $\mathbb{Q}$, primitif et tel que $n \geq 1$. Il existe s entiers positifs $t_1, \ldots, t_s$ inférieurs à*

$$(s + 2^{108} 2^{76n} m^{64} \log^{19}(H))^4$$

tels que les polynômes $F(t_i,Y)$, $i = 1, \ldots, s$, soient irréductibles sur $\mathbb{Q}$.

Enfin, nous verrons que dans le cas où l'extension définie par F est galoisienne, il est possible de modifier la réduction usuelle afin de donner, via

un résultat récent de L. Pyber de théorie des groupes, une borne polynomiale pour la plus petite spécialisation qui conserve l'irréductibilité d'un polynôme. Le résultat de L. Pyber fait intervenir une constante absolue qui sera notée c.

THÉORÈME 4. *Soient $s \in \mathbb{N}^*$ et $F(T,Y) \in \mathbb{Z}[T,Y]$ irréductible sur $\mathbb{Q}$, primitif, tel que $n \geq 1$ et définissant une extension galoisienne sur $\mathbb{Q}(T)$. Il existe s entiers positifs $t_1, \ldots, t_s$ inférieurs à*

$$(s + 2^{165} m^{64} n^{147+c} \log^{19}(H))^4$$

tels que les polynômes $F(t_i, Y)$, $i = 1, \ldots, s$, soient irréductibles sur $\mathbb{Q}$.

L'article est divisé en quatre sections, chaque section donnant la preuve d'un des théorèmes ci-dessus. L'objectif de ce travail étant centré sur l'ordre de grandeur des bornes données, nous n'avons pas cherché à obtenir les meilleures constantes possibles.

1. Théorème de Heath-Brown explicite. Dans cette section, nous allons nous intéresser à la quantité

$$N(F,B) = \sharp\{\underline{x} = (x_1, x_2) \in \mathbb{Z}^2 : F(x_1, x_2) = 0, \max(|x_1|, |x_2|) \leq B\},$$

où F est un polynôme irréductible de degré d et B est un entier strictement positif. Un théorème de Bombieri et Pila [BP] donne une majoration de $N(F;B)$ en $B^{1/d}$. Afin d'améliorer la borne pour la plus petite spécialisation qui laisse un polynôme irréductible, A. Schinzel et U. Zannier [ScZa] ont modifié la preuve de Bombieri et Pila et ont supprimé une condition contraignante sur la taille de B. Le résultat récent de Heath-Brown [HB] donne une nouvelle méthode plus générale (pour une boîte quelconque et dans l'espace projectif) que nous allons donner en explicitant les constantes et dans le cas qui nous intéresse, c'est-à-dire pour deux variables et dans l'espace affine. Le résultat principal de Heath-Brown pour les courbes algébriques est le suivant :

THÉORÈME H-B. *Soit $F(X_1, X_2) \in \mathbb{Z}[X_1, X_2]$ un polynôme irréductible sur $\mathbb{Q}$ de degré d, et soient $\varepsilon > 0$ et $B \geq 1$ donnés. Alors on peut trouver D ne dépendant que de d et ε et un entier k satisfaisant la condition*

$$k \ll_{d,\varepsilon} B^{d^{-1}+\varepsilon} (\log(H(F)))^3$$

tels qu'on ait la propriété suivante : il existe k polynômes $F_1, \ldots, F_k \in \mathbb{Z}[X_1, X_2]$, premiers avec $F(X_1, X_2)$ et de degré au plus D, tels que chaque point compté par $N(F;B)$ soit le zéro d'un des polynômes $F_j(X_1, X_2)$.

REMARQUE. On peut supposer que F est absolument irréductible. En effet, dans le cas contraire, on a une borne directement pour $N(F,B)$, qui plus est indépendante de B, de la façon suivante :

$F(x_1, x_2) = 0$ implique que $\varphi(x_1, x_2) = 0$ pour un facteur $\varphi \notin \mathbb{Q}[X_1, X_2]$ de F irréductible sur $\mathbb{C}$ unitaire en x_2, et donc $\psi(x_1, x_2) = 0$ pour un conjugué de φ sur $\mathbb{Q}$ qui est un autre facteur de F. Comme $\mathrm{Res}_{x_2}(\varphi, \psi)^2$ divise $\mathrm{disc}_{x_2}(F)$, alors le nombre de x_1 entiers tels que $\varphi(x_1, x_2) = \psi(x_1, x_2) = 0$ pour un x_2 entier est inférieur à $\frac{1}{2}\deg(\mathrm{disc}_{x_2}(F)) \leq d(d-1)$. Le même raisonnement s'applique pour x_2, et on obtient alors que le nombre total de points entiers est majoré par d^4.

Pour estimer $N(F, B)$, il suffira alors de compter le nombre d'intersections de F avec les F_j en appliquant le théorème de Bézout. Nous allons désormais donner la preuve de ce théorème en explicitant la dépendance en d et ε.

1.1. *Points singuliers.* Commençons par considérer les points singuliers. Tout point singulier de la courbe $F(\underline{X}) = 0$ satisfait

$$\frac{\partial F}{\partial X_i}(\underline{x}) = 0 \quad (i = 1, 2).$$

Comme F n'est pas constant, au moins un des polynômes $\partial F/\partial X_i$ n'est pas identiquement nul. Un tel polynôme ne peut pas être un multiple de F car son degré est $d-1$. On inclut donc les deux dérivées partielles de F parmi les polynômes F_i décrits dans le théorème H-B ci-dessus. On peut alors majorer par 2 le nombre k' de polynômes associés aux points singuliers.

En ce qui concerne les points non singuliers, nous utiliserons le résultat suivant qui nous permet de considérer les points non singuliers modulo un premier p qu'on peut choisir assez grand.

1.2. *Réduction modulo p pour les points non singuliers.* Soient

$$S(F; B, p) = \left\{ \underline{x} \in \mathbb{Z}^2 : F(\underline{x}) = 0,\ |x_i| \leq B\ (1 \leq i \leq 2),\ \exists j,\ p \nmid \frac{\partial F}{\partial X_j}(\underline{x}) \right\},$$

$$S(F; B) = \left\{ \underline{x} \in \mathbb{Z}^2 : F(\underline{x}) = 0,\ |x_i| \leq B\ (1 \leq i \leq 2),\ \exists j,\ \frac{\partial F}{\partial X_j}(\underline{x}) \neq 0 \right\}.$$

Lemme 1.1. *Soient P un entier, $P \geq 2$, et $r = [\log_2(2d^3 H(F) B^{d-1})] + 1$. Alors il existe r nombres premiers distincts $p_1, \ldots, p_r$ dans l'intervalle*

$$P \leq p_i \leq 8r^2 P \log(P)$$

tels que

$$S(F; B) = \bigcup_{i=1}^{r} S(F; B, p_i).$$

Preuve. Soient $p_1, \ldots, p_r$ les r premiers nombres premiers supérieurs à P. Soit $\underline{x} \in S(F; B)$. Alors $(\partial F/\partial X_j)(\underline{x}) \neq 0$ pour un certain j. On a la majoration

$$\left|\frac{\partial F}{\partial X_j}(\underline{x})\right| \le 2d^3 H(F) B^{d-1}$$

qui nous donne

$$\sharp\left\{p \text{ premier} : p \,|\, \left|\frac{\partial F}{\partial X_j}(\underline{x})\right|\right\} \le \log_2\left(\left|\frac{\partial F}{\partial X_j}(\underline{x})\right|\right) \le \log_2(2d^3 H(F) B^{d-1}).$$

Cette quantité étant par hypothèse strictement inférieure à r, un des p_i ne divise pas $(\partial F/\partial X_j)(\underline{x})$.

Pour majorer les p_i, il suffit de majorer p_r. Pour cela, on peut le majorer par le $(P+r)$-ième premier, soit

$$\begin{aligned} p_i &\le 2(r+P)\log(r+P) \le 8r^2 P\log(P) \\ &\le 72\log^2(2d^3 H(F) B^{d-1}) P\log(P). \ \blacksquare \end{aligned}$$

Remarque. Nous avons modifié le résultat de Heath-Brown afin d'obtenir une dépendance polynomiale en d par la suite, quitte à perdre un peu puisqu'il obtient une majoration des p_i de l'ordre de P.

Ce résultat nous permet de considérer les points non singuliers modulo un premier p convenable pour un coût dans l'estimation finale du nombre de polynômes F_j d'un facteur $r = [\log_2(2d^3 H(F) B^{d-1})] + 1$.

Soit k'' le nombre de points $\underline{t} \in \mathbb{F}_p^2$ non singuliers avec $F(\underline{t}) = 0$. Nous allons étudier les k'' ensembles

$$S(\underline{t}) = \{\underline{x} \in S(F; B, p) : \underline{x} \equiv \underline{t} \pmod p\}.$$

Nous montrerons que, si on choisit P assez grand, alors on peut associer à chaque ensemble $S(\underline{t})$ un polynôme F_j tel que $\forall \underline{x} \in S(\underline{t}),\ F_j(\underline{x}) = 0$.

On a alors, en utilisant les inégalités de Lang–Weil (voir par exemple [FrJa]), une estimation du nombre de polynômes associés aux points non singuliers :

$$\begin{aligned} k'' &\le d(p + 1 + (d-1)(d-2)\sqrt{p}) \le 2d^3 p \\ &\le 144 d^3 \log^2(2d^3 H(F) B^{d-1}) P\log(P). \end{aligned}$$

On obtient finalement que le nombre de polynômes k décrits dans le théorème H-B est

$$k \le k' + k'' r \le 433 d^3 \log^3(2d^3 H(F) B^{d-1}) P\log(P)$$

pour un P assez grand à préciser.

1.3. *Construction d'un polynôme F_j pour un ensemble $S(t_1, t_2)$ donné.* Soit $\underline{t} = (t_1, t_2) \in \mathbb{F}_p^2$ un point non singulier de $F(\underline{t}) = 0$. Une des dérivées partielles au moins ne s'annule pas en $\underline{t}$, on peut supposer

$$\frac{\partial F}{\partial X_1}(\underline{t}) \ne 0.$$

Soit $D \geq d$; on définit une collection de monômes de degré inférieur à D par un ensemble d'exposants :

$$\mathcal{E} \subset \{(e_1, e_2) \in \mathbb{Z}^2 : e_i \geq 0 \ (i = 1, 2),\ e_1 + e_2 \leq D\}.$$

On écrira $\underline{x}^{\underline{e}} = x_1^{e_1} x_2^{e_2}$, et on notera $E = \sharp\mathcal{E}$ et $K = \sharp S(\underline{t})$.

Soient $\underline{x}_{(1)}, \ldots, \underline{x}_{(K)}$ éléments distincts de $S(\underline{t})$. Notons M_2 la matrice de taille $K \times E$ suivante :

$$M_2 = (\underline{x}_{(i)}^{\underline{e}})_{1 \leq i \leq K,\, \underline{e} \in \mathcal{E}}.$$

Nous allons montrer que, pour p bien choisi, le rang de M_2 est strictement inférieur à E, ce qui permet de trouver une solution non triviale $C \in \mathbb{Z}^E$ à l'équation $M_2 C = 0$. Les éléments de C fourniront alors les coefficients du polynôme F_j recherché.

- Si $K \leq E - 1$, alors $\mathrm{rg}(M_2) \leq E - 1$.
- Si $K \geq E$, on considère les mineurs d'ordre E : soient E éléments de $S(\underline{t})$, qu'on notera $\underline{x}_{(1)}, \ldots, \underline{x}_{(E)}$, quitte à renuméroter, et

  $$\Delta = \det[(\underline{x}_{(i)}^{\underline{e}})_{1 \leq i \leq E,\, \underline{e} \in \mathcal{E}}].$$

  Nous allons montrer que, si p est suffisamment grand, alors $\Delta = 0$.

1.3.1. *Valuation en p de Δ.* On note

$$\Delta = \begin{vmatrix} \underline{x}_{(1)}^{\underline{e}} & \underline{x}_{(1)}^{\underline{e}'} & \cdots \\ \underline{x}_{(2)}^{\underline{e}} & \underline{x}_{(2)}^{\underline{e}'} & \cdots \\ \vdots & & \\ \underline{x}_{(E)}^{\underline{e}} & & \end{vmatrix}.$$

On utilise le lemme suivant, qui est une version polynomiale du théorème des fonctions implicites :

LEMME 1.2. *Soit $F(\underline{X}) \in \mathbb{Z}_p[\underline{X}]$ un polynôme à 2 variables et soit $\underline{u} \in \mathbb{Z}_p^2$ tel que $F(\underline{u}) = 0$ et $p \nmid (\partial F/\partial X_1)(\underline{u})$. Alors pour tout $m \geq 1$, il existe $f_m(Y) \in \mathbb{Z}_p[Y]$ tel que si $F(\underline{x}) = 0$ pour un $\underline{x} \in \mathbb{Z}_p^2$ tel que $\underline{x} \equiv \underline{u} \pmod p$, alors*

$$x_1 \equiv f_m(x_2) \pmod{p^m}.$$

Preuve. Nous allons faire la preuve par récurrence sur m. On note

$$\frac{\partial F}{\partial X_1}(u_1, u_2) = \mu.$$

On définit f_m par $f_1(Y) = u_1$ et

$$f_{m+1}(Y) = f_m(Y) - \mu^{-1} F(f_m(Y), Y)$$

pour $m \geq 1$. Le cas $m = 1$ est immédiat. Pour le cas général, l'hypothèse de récurrence $x_1 \equiv f_m(x_2) \pmod{p^m}$ permet d'écrire

$$x_1 = f_m(x_2) + \lambda p^m$$

avec $\lambda \in \mathbb{Z}_p$. La formule de Taylor, tronquée modulo p^{m+1}, donne alors

$$0 = F(\underline{x}) \equiv F(f_m(x_2), x_2) + \lambda p^m \frac{\partial F}{\partial X_1}(f_m(x_2), x_2) \pmod{p^{m+1}}.$$

De plus, comme $f_m(x_2) \equiv x_1 \equiv u_1 \pmod{p}$ (car $(x_1, x_2) \equiv (u_1, u_2) \pmod{p}$), on a

$$\frac{\partial F}{\partial X_1}(f_m(x_2), x_2) \equiv \mu \pmod{p}.$$

On peut donc en conclure que

$$\lambda p^m \equiv -\mu^{-1} F(f_m(x_2), x_2) \pmod{p^{m+1}},$$

d'où

$$x_1 \equiv f_{m+1}(x_2) \pmod{p^{m+1}},$$

ce qui termine la récurrence. ∎

Ce lemme va nous permettre d'écrire le déterminant Δ en fonction d'une seule variable. En effet, on obtient que, quelque soit m,

$$\Delta \equiv \Delta_0 \pmod{p^m},$$

où

$$\Delta_0 = \det(M_0), \qquad M_0 = (\underline{w}_{(i)}^{\underline{e}})_{1 \leq i \leq E,\, \underline{e} \in \mathcal{E}}$$

avec

$$\underline{w}_{(i)} = (w_{(i),1}, w_{(i),2}) = (f_m(x_{(i),2}), x_{(i),2}).$$

En écrivant le développement p-adique de $x_{(i),2}$ comme $u_2 + y_{(i),2}$ avec $u_2 \in \mathbb{Z}_p$ indépendant de i (par définition de $S(\underline{t})$) et $y_{(i),2} \in p\mathbb{Z}_p$, on a

$$\underline{w}_{(i)}^{\underline{e}} = f_m(u_2 + y_{(i),2})^{e_1} (u_2 + y_{(i),2})^{e_2} = g_{\underline{e}}(y_{(i),2}),$$

où $g_{\underline{e}}(Y) \in \mathbb{Z}_p[Y]$.

Chaque colonne correspond à un polynôme $g_{\underline{e}}(Y)$. On ordonne les colonnes par degré du monôme de plus bas degré croissant. Notons a le degré du monôme de plus bas degré de la première colonne. On supprime des colonnes 2 à E le monôme de degré a, s'il existe. On itère ensuite ce procédé de façon à classer les colonnes par degré du monôme de plus bas degré *strictement* croissant. Ceci est toujours possible si les colonnes sont linéairement indépendantes, et dans le cas contraire, la conclusion $\Delta = 0$ est trivialement vérifiée. Ce procédé, n'utilisant que des opérations élémentaires, ne change pas le déterminant au signe près.

Il est alors clair que la k-ième colonne est divisible par p^{k-1} car constituée de polynômes dont le premier terme est de degré supérieur à $k - 1$ et p

divise $y_{(i),2}$. Donc Δ_0 est divisible par $p^{E(E-1)/2}$. Finalement, on a montré que, si on pose $\nu := E(E-1)/2$, alors la valuation en p de Δ est supérieure à ν.

1.3.2. *Taille de Δ.* On peut estimer la taille de Δ :

$$|\Delta| \le E^E \prod_{\underline{e}\in\mathcal{E}} B^{e_1+e_2} \le E^E B^{E'},$$

où $E' = \sum_{\underline{e}\in\mathcal{E}} e_1 + e_2$. On obtient donc la conclusion suivante : Si $p^\nu > E^E B^{E'}$, alors $\Delta = 0$.

1.3.3. *Première conclusion.* On a montré que sous la condition

$$p^\nu > E^E B^{E'}, \tag{1}$$

le rang de la matrice M_2 est inférieur à $E-1$ (car tous les mineurs $E\times E$ sont nuls). On en déduit qu'il existe $C = (c_{\underline{e}}) \in \mathbb{Z}^E$, $C \neq 0$, tel que $M_2 C = 0$. Si on pose

$$F_j(\underline{X}) = \sum_{\underline{e}\in\mathcal{E}} c_{\underline{e}} \underline{X}^{\underline{e}},$$

alors F_j est un polynôme non nul de degré inférieur ou égal à D tel que $F_j(\underline{x}) = 0$ pour tout $\underline{x}$ de $S(\underline{t})$.

1.3.4. *Choix de $\mathcal{E}$.* Il reste à choisir l'ensemble d'exposants $\mathcal{E}$ afin de s'assurer que $F \nmid F_j$. On écrit

$$F(X_1, X_2) = \sum_{\underline{f}} a_{\underline{f}} X_1^{f_1} X_2^{f_2}$$

et on considère le polygône de Newton $\mathcal{P}(F)$ de F, qui est l'enveloppe convexe des points $(f_1, f_2) \in \mathbb{Z}^2$ tels que $a_{\underline{f}} \neq 0$.

On choisit un point (m_1, m_2) de $\mathcal{P}(F)$ tel que $m_1 + m_2 = d$ $(= \deg(F))$. Il suffit alors de choisir l'ensemble $\mathcal{E}$ de la façon suivante :

$$\mathcal{E} = \{(e_1, e_2) \in \mathbb{Z}^2 : e_i \ge 0 \ (i = 1, 2),\ e_1 + e_2 \le D, e_i < m_i \text{ pour un certain } i\}$$

avec $D > d$. En effet, s'il existe un G tel que $F_j = FG$, alors les propriétés des polygônes de Newton nous disent que $\mathcal{P}(F_j)$ est égal à $\mathcal{P}(F) + \mathcal{P}(G)$ (voir [Ost]) et contient donc un point du type $(m_1, m_2) + (g_1, g_2)$. Or ceci est impossible car ce point ne peut appartenir à $\mathcal{E}$.

1.3.5. *Étude de la condition* (1) : $p^\nu > E^E B^{E'}$. On a $E = \sharp\mathcal{E}_1 - \sharp\mathcal{E}_2$ avec

$$\mathcal{E}_1 = \{(e_1, e_2) \in \mathbb{Z}^2 : e_i \ge 0 \ (i = 1, 2),\ e_1 + e_2 \le D\},$$

$$\mathcal{E}_2 = \{(e_1, e_2) \in \mathbb{Z}^2 : e_i \ge 0 \ (i = 1, 2),\ e_1 + e_2 \le D,\ e_i \ge m_i \ (i = 1, 2)\},$$

donc

$$E = \binom{D+2}{2} - \binom{D-d+2}{2} = dD + 1 - \frac{(d-1)(d-2)}{2}.$$

Joint à la définition $\nu = E(E-1)/2$, cela donne

$$\frac{E}{\nu} = \frac{2}{E-1} \leq \frac{2}{dD - d^2/2} \leq \frac{2}{dD} + \frac{2}{D^2}.$$

De la même manière, on peut estimer $E' = E'_1 + E'_2$ où

$$E'_i = \sum_{\underline{e} \in \mathcal{E}} e_i = \sum_{\underline{e} \in \mathcal{E}_1} e_i - \sum_{\underline{e} \in \mathcal{E}_2} e_i.$$

En effet, les égalités

$$\begin{cases} \displaystyle\sum_{\underline{e} \in \mathcal{E}_1} e_i = \frac{D}{3}\binom{D+2}{2}, \\ \displaystyle\sum_{\underline{e} \in \mathcal{E}_2} e_i = \left(m_i + \frac{D-d}{3}\right)\binom{D-d+2}{2} \end{cases}$$

donnent l'estimation

$$E' \leq \frac{dD^2}{2} + \frac{dD}{2}.$$

On obtient ainsi, après calculs, la majoration suivante de E'/ν, valable pour $D > d$:

$$\frac{E'}{\nu} \leq \frac{1}{d} + \frac{6}{D}.$$

Il suffit donc de s'assurer que

$$p > (2dD)^{2(dD)^{-1}+2D^{-2}} B^{d^{-1}+6D^{-1}}.$$

En remarquant de plus que $(2dD)^{2(dD)^{-1}+2D^{-2}} \leq e^8$ pour $D > d$, on choisit

$$P = 1 + [e^8 B^{d^{-1}+6D^{-1}}].$$

On obtient donc, pour cette valeur de P, que le nombre k des polynômes du théorème H-B est majoré par

$$k \leq 2^{27} d^3 \log^3(2d^3 H(F) B^{d-1}) B^{d^{-1}+6D^{-1}} \log(B)$$

dès que $D > d$.

Ceci nous fournit donc une borne explicite pour le théorème H-B. Il suffit désormais d'appliquer le théorème de Bézout pour compter les intersections de F avec chaque F_j, ce qui donne une estimation totalement explicite de $N(F, B)$:

$$N(F, B) \leq 2^{27} d^4 D \log^3(2d^3 H(F) B^{d-1}) \log(B) B^{d^{-1}+6D^{-1}}$$

dès que $D > d$.

Cette estimation est optimale pour $D = \log(B)$. Afin de satisfaire la condition $D > d$, et de simplifier les calculs, on choisit la valeur $D = [d \log(B) + 1]$, ce qui donne la borne

$$N(F, B) \leq 2^{27} d^5 \log^3(2d^3 H(F) B^{d-1}) \log^2(B) B^{d^{-1}+6(d\log(B))^{-1}}$$

ou encore, en majorant $B^{6(d\log(B))^{-1}}$ par 2^9,

$$N(F,B) \leq 2^{36} d^5 \log^3(2d^3 H(F) B^{d-1}) \log^2(B) B^{d-1}.$$

1.4. *Borne indépendante de $H(F)$.* Nous allons maintenant montrer le résultat suivant qui permet de donner une borne indépendante de la hauteur de F.

PROPOSITION 1. *Soit $F(T,Y) \in \mathbb{Z}[T,Y]$ un polynôme de degré d dont les coefficients sont sans facteur commun. Alors*

$$N(F,B) \leq d^2 + 3 \quad ou \quad H(F) \leq 625 d^8 B^{4d}.$$

Preuve. Posons $N = d^2 + 4$ et $M = (d+1)(d+2)/2$. Si $F(X_1, X_2) = 0$ a au moins $N = d^2 + 4$ solutions $\underline{x}^{(1)}, \ldots, \underline{x}^{(N)}$ telles que $|x_j^{(i)}| \leq B$ $(1 \leq i \leq N,\ j = 1, 2)$, on considère la matrice $C = (c_{i,j})_{i,j}$ de taille $N \times M$ dont la i-ème ligne est formée des M monômes possibles de degré d en les variables $x_1^{(i)}, x_2^{(i)}$. On note $f \in \mathbb{Z}^M$ le vecteur dont les composantes sont les coefficients de F de sorte que $Cf = 0$. D'après le lemme de Siegel (voir par exemple [Sch]), comme $N > M$, ce système admet une solution $g \in \mathbb{Z}^M$ non nulle vérifiant la majoration :

$$\max_{k=1,\ldots,M} |g_k| \leq (NA)^{M/(N-M)}$$

où A est choisi supérieur aux $|c_{i,j}|$. On prend $A = B^d$ et on construit un polynôme G dont les coefficients sont les éléments de g (en gardant l'ordre des monômes choisi pour F) ; il s'ensuit que G est un polynôme non nul à coefficients entiers, de degré inférieur à d, s'annulant en les N points $\underline{x}^{(1)}, \ldots, \underline{x}^{(N)}$ et vérifiant

$$\max_{k=1,\ldots,M} |g_k| \leq (NB^d)^{M/(N-M)}.$$

Par construction, $G(\underline{X})$ et $F(\underline{X})$ ont $d^2 + 4$ zéros communs et sont de degré inférieur à d. Ceci contredit le théorème de Bézout, à moins que F et G soient proportionnels. Mais comme F est irréductible et que ses coefficients n'ont pas de facteur commun, on a $G = aF$ avec $a \in \mathbb{Z}$ et

$$H(F) = \max_{k=1,\ldots,M} |f_k| \leq \max_{k=1,\ldots,M} |g_k| \leq (NB^d)^{M/(N-M)}.$$

Après calculs, on obtient la majoration suivante de $H(F)$ en fonction de d et B :

$$H(F) \leq 625 d^8 B^{4d}. \ \blacksquare$$

Le lemme précédent nous permet de donner une borne totalement explicite et indépendante de H pour $N(F,B)$:

$$N(F,B) \leq 2^{36} d^5 \log^3(1250 d^{11} B^{5d-1}) \log^2(B) B^{d-1},$$

qui peut être présentée sous la forme moins précise mais plus compacte donnée dans le théorème 1.

2. Borne pour la plus petite spécialisation sans zéro entier. Le résultat précédent va nous permettre d'estimer le nombre de spécialisations $t \in \mathbb{N}$, $t \leq B$, telles que, étant donné un polynôme $F(T,Y) \in \mathbb{Z}[T,Y]$ irréductible sur $\mathbb{Q}$, le polynôme spécialisé $F(t,Y)$ ait un zéro entier. On en déduira d'une part une borne pour trouver s spécialisations telles que le polynôme $P(t,Y)$ n'ait pas de zéro entier (théorème 2) et d'autre part une nouvelle version effective du théorème d'irréductibilité de Hilbert (section 3).

On notera toujours m et n les degrés partiels de F en T et Y respectivement. On supposera $m > 0$, le résultat étant trivial sinon.

2.1. *Estimation des solutions entières de* $F(t,Y) = 0$. On écrit F sous la forme

$$F(T,Y) = a_0(T)Y^n + \cdots + a_n(T).$$

L'inégalité de Liouville nous permet de majorer une telle solution y de $F(t,Y) = 0$ pour un entier positif t tel que $a_0(t) \neq 0$ et $t \leq B$:

$$|y| \leq 2 \max_{i=0,\ldots,n} |a_i(t)| \leq 2(m+1)H(F)B^m \leq 2(m+1)HB^m$$

où $H = \max\{H(F), e^e\}$. On peut donc se ramener à compter les points entiers sur la courbe algébrique définie par F dans le carré de côté $2B'$ avec $B' = 2(m+1)HB^m$. Afin d'obtenir une borne strictement inférieure à B, nous allons distinguer deux cas. On notera pour plus de lisibilité $L_1 = \log(H)$ et $L_2 = \log(\log(H))$. Notons que $H \geq e^e$ et donc $L_2 \geq 1$.

2.2. Cas 1 : $d \geq 2mL_1/L_2$. On applique la version effective du résultat de Heath-Brown donnée par le théorème 1 au polynôme F avec $B' = 2(m+1)HB^m$. L'hypothèse sur d nous permet de majorer efficacement les termes en H et B provenant de $B'^{1/d}$. En effet, pour H, la majoration $1/d \leq L_2/L_1$ donne

$$H^{1/d} \leq H^{L_2/L_1} = \log(H),$$

et pour B, la majoration $1/d \leq 1/2m$ donne

$$B^{m/d} \leq B^{1/2}.$$

On obtient, après calculs, que le nombre d'entiers positifs t inférieurs à B tels que $a_0(t) \neq 0$ et que $F(t,Y) = 0$ ait une solution entière est majoré par

$$2^{58} d^{18} \log^6(H) B^{1/2} \log^5(B).$$

2.3. Cas 2 : $d < 2mL_1/L_2$. On applique cette fois-ci le théorème de la section précédente au polynôme

$$G(T,Y) = F(T, T^E + Y)$$

où $E = [2mL_1/L_2] + 1 \leq 4mL_1$ (ce polynôme est alors de degré d' compris entre nE et $nE + m$). Tout zéro entier (t, y) de G correspond à un zéro de la forme $(t, t^E + y)$ de F.

On sait alors que pour tout zéro (t, y) de G tel que $|t| \leq B$, on a

$$|y| \leq B^E + 2(m+1)HB^m \leq 2(m+1)HB^E.$$

On peut alors appliquer le théorème 1 au polynôme G en choisissant $B' = 2(m+1)HB^E$. Notons également que la hauteur $H(G)$ est majorée par $2^n H(F)$. Le même type de calculs que pour le cas 1 nous donne une majoration en B de l'ordre de $B^{1/n}$ qui est bien strictement inférieur à B puisqu'on a supposé $n \geq 2$. Le nombre d'entiers positifs t inférieurs à B tels que $a_0(t) \neq 0$ et que $F(t, Y) = 0$ ait une solution entière est majoré par

$$2^{87} d^{45} \log^{19}(H) B^{1/2} \log^5(B).$$

2.4. *Conclusion.* On en déduit que dans tous les cas, en tenant compte du nombre de solutions de $a_0(t) = 0$, le nombre de spécialisations $t \geq 0$ inférieures à B telles que $F(t, Y) = 0$ ait une solution entière est plus petit que

$$2^{88} d^{45} \log^{19}(H) B^{1/2} \log^5(B). \tag{2}$$

Pour trouver s valeurs de $t \geq 0$ inférieures à B telles que $F(t, Y) = 0$ n'ait pas de solution entière, il suffit que cette quantité soit inférieure à $B - s$, ce qui est le cas si

$$B \geq (s + 2^{88} d^{45} \log^{19}(H))^4.$$

Notons qu'ainsi B est assez grand pour que la majoration $\log^5(B) \leq B^{1/4}$ soit valable. Un tel choix de B nous fournit alors la borne donnée par le théorème 2.

3. Théorème de Hilbert effectif – cas général. Nous allons ici exposer rapidement la réduction classique du théorème d'irréductibilité de Hilbert qui permet de réinterpréter le problème en terme de zéros entiers de certains polynômes. On précisera la taille de ces polynômes afin d'utiliser les estimations de la section précédente. Nous obtiendrons ainsi une nouvelle forme effective de ce théorème (théorème 3) améliorant celles existant.

3.1. *Réduction à la recherche de points entiers sur une courbe algébrique.* Cette section va rappeler les résultats obtenus par A. Schinzel et U. Zannier afin de réduire le problème à la recherche de points entiers sur une courbe algébrique dans un carré. Nous apporterons quelques précisions à ce résultat classique en estimant le degré et la hauteur des nouveaux polynômes issus de cette réduction.

Soit $F(T,Y) \in \mathbb{Z}[T,Y]$. On écrit sa décomposition dans $\overline{\mathbb{Q}(T)}[Y]$

$$F(T,Y) = a_0(T)\prod_{i=1}^{n}(Y - y_i)$$

et soit $D(T)$ le discriminant de F par rapport à Y. Pour tout sous-ensemble ω de $\{1,\dots,n\}$, et pour tout entier positif $j \le \sharp\omega$, on note $P_{\omega,j}(T,Y)$ le polynôme minimal de $a_0(T)\tau_j(y_i : i \in \omega)$ sur $\mathbb{Q}(T)$, où τ_j est la j-ième fonction symétrique élémentaire. On sait alors que $a_0(T)\tau_j(y_i : i \in \omega)$ est entier sur $\mathbb{Z}[T]$ et donc $P_{\omega,j}$ est un polynôme à coefficients entiers, unitaire en Y.

Lemme 3.1. *Soit $t \in \mathbb{Z}$ tel que $a_0(t)D(t) \neq 0$ et $F(t,Y)$ soit réductible sur $\mathbb{Q}$. Alors il existe un sous-ensemble ω de $\{1,\dots,n\}$ de cardinal $l \le n/2$ et un $j \le l$ tels que $\deg_Y(P_{\omega,j}) \ge 2$ et $P_{\omega,j}(t,Y)$ ait un zéro entier. On notera P_ω ce polynôme et d_ω son degré en Y. On a de plus les majorations*

$$\begin{cases} \deg(P_\omega) \le m d_\omega \le m\binom{n}{l}, \\ H(P_\omega) \le (2^{n+1}(m+1)H(F))^{d_\omega}. \end{cases}$$

Preuve. Nous détaillons seulement l'estimation de la hauteur de P_ω car elle n'est pas utilisée par A. Schinzel et U. Zannier. Pour la preuve du lemme et l'estimation du degré, nous renvoyons à leur article [ScZa] ou aux sections 4.1 et 4.2 où des estimations similaires sont détaillées.

D'après les inégalités de Cauchy, on a

$$H(P_\omega) \le \sup_{|z|\le 1} \|P_\omega(z,Y)\|,$$

où $\|P_\omega(z,Y)\|$ désigne le maximum des modules des coefficients de $P_\omega(z,Y) \in \mathbb{C}[Y]$. En effet, si $P_\omega = \sum_{i=0}^{d_\omega} p_i(Z)Y^i$ avec $p_i(Z) = \sum_j p_{i,j}Z^j$, alors pour tout i, j on a

$$|p_{i,j}| = |p_i^{(j)}(0)/j!| \le \sup_{|z|\le 1} |p_i(z)| \le \sup_{|z|\le 1} \|P_\omega(z,Y)\|.$$

On introduit la mesure de Mahler de $P_\omega(z,Y)$:

$$M(P_\omega(z,Y)) = \prod_{i=1}^{d_\omega} \max(1, |\alpha_i(z)|),$$

où $d_\omega = \deg_Y(P_\omega)$ et les $\alpha_i(z)$ sont les zéros de $P_\omega(z,Y)$.

On a alors la majoration classique des coefficients en fonction de la mesure de Mahler (voir [HiSi] par exemple) :

$$\|P_\omega(z,Y)\| \le 2^{d_\omega} M(P_\omega(z,Y)).$$

Il reste à estimer $|\alpha_i(z)|$ pour $|z| \le 1$. On utilise pour cela le fait que $\alpha_i(z)$ est une fonction symétrique élémentaire de zéros de $F(z,Y)$ pour écrire

$$|\alpha_i(z)| \le 2^l |a_0(z)| \prod_{i=1}^{n} \max(1, |y_i(z)|)$$

où $l = \sharp\omega$ et les $y_i(z)$ sont les zéros de $F(z, Y)$, vu comme polynôme en Y. On majore alors classiquement la mesure de Mahler de $F(z, Y)$ (voir encore [HiSi]) :

$$|a_0(z)| \prod_{i=1}^{n} \max(1, |y_i(z)|) = M(F(z, Y)) \le \sqrt{n+1} \max_i(|a_i(z)|)$$

où les $a_i(z)$ sont les coefficients de $F(z, Y)$ vu comme polynôme en Y. Cela, joint aux majorations

$$|a_i(z)| \le (m+1)H(F) \max(1, |z|^m), \quad i = 1, \dots, n,$$

conduit à l'estimation suivante pour $|\alpha_i(z)|$, $|z| \le 1$:

$$|\alpha_i(z)| \le 2^l \sqrt{n+1}\,(m+1)H(F) \le 2^n (m+1)H(F).$$

On obtient donc l'estimation voulue :

$$H(P_\omega) \le (2^{n+1}(m+1)H(F))^{d_\omega}. \ \blacksquare$$

On note $S(B)$ le nombre d'entiers positifs $t \le B$ tels que $a_0(t)D(t) \ne 0$ et $F(t, Y)$ soit réductible sur $\mathbb{Q}$, et $S_\omega(B)$ le nombre d'entiers positifs $t \le B$ tels que $a_0(t)D(t) \ne 0$ et $P_\omega(t, Y)$ ait un zéro entier. On a alors l'inégalité

$$S(B) \le \sum_\omega S_\omega(B).$$

Pour estimer $S(B)$, il suffit donc d'estimer chaque $S_\omega(B)$ en utilisant l'estimation (2) de la section précédente.

3.2. *Estimation de $S_\omega(B)$.* Connaissant le degré et la hauteur des polynômes P_ω (voir lemme 3.1), on applique l'estimation (2) de la section 2.4, ce qui donne

$$S_\omega(B) \le 2^{107} 2^{75n} m^{65} \log^{19}(H) B^{1/2} \log^5(B).$$

D'autre part, la somme sur ω fait intervenir au plus 2^n termes. On a donc

$$S(B) \le 2^{107} 2^{76n} m^{64} \log^{19}(H) B^{1/2} \log^5(B).$$

En prenant en compte le nombre de solutions de $a_0(T)D(T) = 0$, ce qui ne change que la constante, on en déduit que le nombre d'entiers positifs t inférieurs à B tels que la spécialisation $F(t, Y)$ soit réductible sur $\mathbb{Q}$ est plus petit que

$$2^{108} 2^{76n} m^{64} \log^{19}(H) B^{1/2} \log^5(B).$$

Pour trouver s spécialisations t qui ne satisfont pas à cette condition, il suffit alors de rendre cette quantité strictement inférieure à $B - s$, ce qui est le cas si on choisit

$$B \ge (s + 2^{108} 2^{76n} m^{64} \log^{19}(H))^4.$$

On obtient donc la nouvelle version effective du théorème d'irréductibilité de Hilbert donnée par le théorème 3.

Remarques. (a) Ce résultat améliore les dépendances en le degré et en la hauteur de F par rapport à la borne donnée par Schinzel et Zannier. On n'obtient toujours pas de borne polynomiale en le degré, ceci en raison du nombre et du degré des polynômes issus de la réduction. Il semble qu'il soit difficile d'améliorer ce résultat dans le cas général sans éviter cette réduction. Cependant, nous allons voir dans la section suivante que dans le cas où l'extension définie par le polynôme F est galoisienne, une modification de cette réduction va nous permettre d'obtenir une borne polynomiale.

(b) Le résultat de la section précédente nous permet également de donner directement une borne polynomiale pour les polynômes unitaires en Y et dont le degré en Y vaut 2 ou 3. En effet, dans ce cas, il y a équivalence pour un polynôme à une variable entre être irréductible sur $\mathbb{Q}$ et ne pas avoir de racine dans $\mathbb{Z}$.

4. Théorème de Hilbert effectif – cas galoisien. Si on analyse la provenance des termes exponentiels dans la borne fournie par le théorème 3, on voit deux origines : le degré des polynômes issus de la réduction et leur nombre. Sous l'hypothèse que F définit une extension galoisienne de $\mathbb{Q}(T)$, nous allons voir qu'il est facile de baisser le degré de ces polynômes. D'autre part, une modification de la réduction va nous permettre, *via* un résultat récent de théorie des groupes, de contrôler également le nombre de polynômes à considérer et donner ainsi une borne polynomiale pour le théorème d'irréductibilité de Hilbert (théorème 4). Nous terminerons par une remarque sur la possibilité de généraliser cette méthode sous des conditions plus faibles sur l'extension définie par F.

4.1. *Nouvelle réduction.* Nous allons modifier la réduction habituelle afin de ne considérer que des polynômes définissant des extensions minimales parmi les extensions intermédiaires entre $\mathbb{Q}(T)$ et la clôture galoisienne de F. Nous verrons que les degrés et hauteurs restent d'un ordre de grandeur convenable.

On note N la clôture galoisienne de F. Comme pour la réduction classique, on note P_ω le polynôme minimal d'un élément $\theta_\omega = a_0(T)\tau_j(y_i : i \in \omega)$ appartenant à $N \setminus \mathbb{Q}(T)$. Soit maintenant un corps k_ω minimal satisfaisant $\mathbb{Q}(T) \subsetneq k_\omega \subseteq \mathbb{Q}(T, \theta_\omega)$, et $p_\omega(Y) \in k_\omega[Y]$ le polynôme minimal de θ_ω sur k_ω. Un des coefficients de p_ω est dans $k_\omega \setminus \mathbb{Q}(T)$ car sinon $p_\omega = P_\omega$ et k_ω serait $\mathbb{Q}(T)$. On note η_ω ce coefficient. Il s'écrit comme fonction symétrique élémentaire des racines de p_ω, donc de conjugués de θ_ω. On a alors par minimalité $k_\omega = \mathbb{Q}(T, \eta_\omega)$. Soit alors $R_\omega(T, Y)$ le polynôme minimal de η_ω sur $\mathbb{Q}(T)$. On sait que η_ω est entier sur $\mathbb{Z}[T]$, et donc R_ω est dans $\mathbb{Z}[T, Y]$, et est unitaire en Y.

Soit désormais $t \in \mathbb{Z}$ tel que $F(t,Y)$ soit réductible sur $\mathbb{Q}$ et vérifiant $a_0(t)D(t) \neq 0$. Dans ces conditions, on peut définir un morphisme de spécialisation $\mathbb{Q}[T, y_1, \ldots, y_n] \to \overline{\mathbb{Q}}$ qui prolonge la spécialisation $T \to t$. Pour $z \in \mathbb{Q}[T, y_1, \ldots, y_n]$, on notera $z(t)$ l'image de z par ce morphisme, i.e. la "valeur de z en t". Il existe un sous-ensemble ω de $\{1, \ldots, n\}$ tel que $\theta_\omega(t)$ soit un zéro entier de $P_\omega(t,Y)$ (il s'agit de la réduction classique), et $\eta_\omega(t)$ est alors un zéro entier de $R_\omega(t,Y)$. On peut donc énoncer un analogue du lemme 3.1 en remplaçant les P_ω par ces polynômes R_ω, lesquels sont en nombre inférieur ou égal au nombre d'extensions minimales entre $\mathbb{Q}(T)$ et N.

LEMME 4.1. *Pour tout $t \in \mathbb{Z}$, si $a_0(t)D(t) \neq 0$ et $F(t,Y)$ est réductible sur $\mathbb{Q}$, alors un des polynômes $R_\omega(t,Y)$ a un zéro entier.*

Supposons désormais que l'extension définie par F est galoisienne. Ceci va nous permettre de majorer de façon efficace le degré et le nombre des extensions k_ω construites ci-dessus. On discutera ensuite dans une remarque des conditions plus générales que doit vérifier l'extension définie par F pour que cette méthode donne une borne polynomiale.

4.2. *Estimation du degré et de la hauteur de R_ω.* Par construction, l'extension k_ω est une sous-extension de l'extension galoisienne $\mathbb{Q}(T, y_1) = N$. Donc le degré en Y de R_ω, qui est égal au degré $[k_\omega : \mathbb{Q}(T)]$, est majoré par le degré en Y de F. C'est-à-dire, $\deg_Y(R_\omega) \leq n$.

Afin d'estimer le degré en T, il suffit d'estimer le degré en T de chaque coefficient de R_ω vu comme polynôme en Y :

$$R_\omega(T,Y) = Y^k + \sum_{i=1}^{k} R_i(T) Y^{k-i}.$$

Pour chaque $t \in \mathbb{C}$ fixé, $R_i(t)$ est, au signe près, la i-ème fonction symétrique élémentaire en les zéros de $R_\omega(t,Y)$. Ceux-ci sont les conjugués de $\eta_\omega(t)$, qui est lui-même fonction symétrique élémentaire de conjugués de $\theta_\omega(t)$. Or, on a l'estimation suivante, due au fait que $\theta_\omega(t)$ est encore fonction symétrique élémentaire d'un ensemble de zéros de F et obtenue à l'aide de comparaisons classiques entre mesure de Mahler et hauteur usuelle :

$$|\theta_\omega(t)| \leq 2^n (m+1) H \max(1, |t|^m).$$

On obtient donc, pour $|t| \geq 1$,

$$|R_i(t)| \leq 2^i (2^{2n^2} (m+1)^n H^n |t|^{mn})^i = O(|t|^{mni})$$

et donc $\deg(R_i) \leq mni$ et $\deg_T(R_\omega) \leq mn^2$.

On peut également donner une majoration du degré total $\deg(R_\omega) \leq 2mn^2$.

Pour estimer la hauteur, on utilise la même méthode que pour la hauteur de P_ω. Les inégalités de Cauchy nous permettent d'écrire

$$H(R_\omega) \leq \sup_{|z|\leq 1} \|R_\omega(z,Y)\|$$

où $\|R_\omega(z,Y)\|$ est le maximum des modules des coefficients de $R_\omega(z,Y) \in \mathbb{C}[Y]$. Puis chaque $\|R_\omega(z,Y)\|$ est majoré en utilisant la mesure de Mahler, ce qui nous donne, pour $|z| \leq 1$,

$$\|R_\omega(z,Y)\| \leq 2^n(2^{2n^2}(m+1)^n H^n)^n$$

soit

$$H(R_\omega) \leq 2^{3n^3}(m+1)^{n^2} H^{n^2}.$$

4.3. *Estimation de $S_\omega(B)$.* Nous allons refaire les estimations de $S_\omega(B)$ dans le cas galoisien. Connaissant le degré et la hauteur des polynômes R_ω, il suffit d'appliquer une nouvelle fois l'estimation (2) de la section 2.4, ce qui donne

$$S_\omega(B) \leq 2^{164} m^{64} n^{147} \log^{19}(H) B^{1/2} \log^5(B).$$

D'autre part, la somme sur ω correspond au nombre d'extensions minimales non triviales entre $\mathbb{Q}(T)$ et $\mathbb{Q}(T, y_1)$, qui est, par la théorie de Galois, égal au nombre de sous-groupes maximaux d'un groupe fini d'ordre n. Or, on trouve une telle estimation dans [LuSe] (Th. 11.3.4 de L. Pyber) :

Théorème (L. Pyber). *Il existe une constante absolue c telle que pour tout groupe fini G, le nombre de sous-groupes maximaux de G soit au plus $(\sharp G)^c$.*

En prenant en compte également le nombre de solutions de $a_0(T)D(T) = 0$, on en déduit que le nombre d'entiers positifs t inférieurs à B tels que la spécialisation $F(t,Y)$ soit réductible sur $\mathbb{Q}$ est plus petit que

$$2^{165} m^{64} n^{147+c} \log^{19}(H) B^{1/2} \log^5(B).$$

Pour trouver s spécialisations t qui ne satisfont pas à cette condition, il suffit alors de rendre cette quantité strictement inférieure à $B - s$, ce qui est le cas si on choisit

$$B \geq (s + 2^{165} m^{64} n^{147+c} \log^{19}(H))^4.$$

On obtient ainsi la nouvelle version effective du théorème d'irréductibilité de Hilbert sous l'hypothèse que l'extension définie par le polynôme F soit galoisienne donnée par le théorème 4.

Remarques. (a) De façon générale (c'est-à-dire sans condition sur l'extension définie par F), on peut voir $\deg_Y(R_\omega)$ comme l'indice $[G : M]$ d'un sous-groupe maximal M de $G = \mathrm{Gal}(N/\mathbb{Q}(T))$.

En notant $\Gamma = \mathrm{Gal}(N/\mathbb{Q}(T, y_1))$, qui est d'indice n, la condition suivante est alors suffisante pour obtenir une borne polynomiale :

(∗) Il existe une constante A telle que

$$\sum_{\substack{M<G\\ M \text{ maximal}}} [G:M] \leq [G:\Gamma]^A.$$

On voit ainsi que si N est de degré une puissance de n sur $\mathbb{Q}(T)$ d'exposant borné par une constante absolue, cette condition est vérifiée grâce au théorème de Pyber et la borne obtenue par la méthode reste donc polynomiale.

(b) On peut également énoncer une condition de pure théorie des groupes qui, si elle était vraie, donnerait une borne polynomiale pour le cas général :

(∗∗) Il existe une constante a absolue telle que pour tout groupe G fini,

$$\sum_{\substack{M<G\\ M \text{ maximal}}} [G:M] \leq \Big(\min_{\substack{\Gamma<G,\,\Gamma\neq G\\ \bigcap_{g\in G}\Gamma^g=\{1\}}} [G:\Gamma]\Big)^a$$

où la condition sur les $\Gamma^g = g\Gamma g^{-1}$ assure que N est la clôture galoisienne de $\mathbb{Q}(T, y_1)$.

Cette condition revient à dire que l'action de G par translation sur les classes de G modulo Γ est fidèle. Le membre de droite est donc égal à une puissance du plus petit degré $n > 1$ d'une représentation transitive et fidèle $G \to S_n$. On peut alors citer deux types de contre-exemples :

- Il peut exister un sous-groupe maximal d'indice trop élevé : c'est le cas si G est représenté par A_n. Il existe alors (voir [DM]) des sous-groupes maximaux d'indice supérieur à toute puissance de n.
- Il peut y avoir trop de sous-groupes maximaux. C'est le cas par exemple si G est un 2-groupe transitif qui ne peut être engendré par moins de $n/\sqrt{\log n}$ éléments (l'existence de tels groupes est prouvée dans [KN]). Le groupe G possède alors $2^{n/\sqrt{\log n}}$ sous-groupes maximaux d'indice 2, ce qui rend impossible la condition (∗∗).

Remerciements. Ce travail est une partie de ma thèse. Je voudrais remercier mes directeurs de thèse P. Dèbes et U. Zannier pour m'avoir fait découvrir ce sujet ainsi que pour les discussions à propos de ce travail. Je remercie également le professeur P. Corvaja pour sa relecture attentive et ses précieux conseils, ainsi que les professeurs D. R. Heath-Brown et L. Pyber qui m'ont apporté de très intéressantes suggestions.

Références

[BP] E. Bombieri and J. Pila, *The number of integral points on arcs and ovals*, Duke Math. J. 59 (1989), 337–357.

[De] P. Dèbes, *Hilbert subsets and s-integral points*, Manuscripta Math. 89 (1996), 107–137.
[DM] J. D. Dixon and B. Mortimer, *Permutation Groups*, Springer, 1996.
[Do] K. Dörge, *Einfacher Beweis des Hilbertschen Irreduzibilitätssatzes*, Math. Ann. 96 (1927), 176–182.
[Fr] M. Fried, *On Hilbert's irreducibility theorem*, J. Number Theory 6 (1974), 211–231.
[FrJa] M. Fried and M. Jarden, *Field Arithmetic*, Springer, 1986.
[HB] D. R. Heath-Brown, *The density of rational points on curves and surfaces*, Ann. of Math. 155 (2002), 553–595.
[H] D. Hilbert, *Ueber die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten*, J. Reine Angew. Math. 110 (1892), 104–129 = Gesammelte Abhandlungen, Bd. II, Springer, 1970, 264–286.
[HiSi] M. Hindry and J. H. Silverman, *Diophantine Geometry: An Introduction*, Springer, 2000.
[KN] L. G. Kovács and M. F. Newman, *Generating transitive permutation groups*, Quart. J. Math. Oxford Ser. (2) 39 (1988), 361–372.
[LLL] A. K. Lenstra, H. W. Lenstra Jr. and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. 261 (1982), 515–534.
[LuSe] A. Lubotzky and D. Segal, *Subgroup Growth*, Progr. Math. 212, Birkhäuser, 2003.
[Ost] A. M. Ostrowski, *Über die Bedeutung der Theorie der konvexen Polyeder für formale Algebra*, Jahresber. Deutsch. Math. Verein. 30 (1921), 98–99.
[ScZa] A. Schinzel and U. Zannier, *The least admissible value of the parameter in Hilbert's Irreducibility Theorem*, Acta Arith. 69 (1995), 293–302.
[Sch] W. M. Schmidt, *Diophantine Approximations and Diophantine Equations*, Lecture Notes in Math. 1467, Springer, 1991.
[Wa] Y. Walkowiak, thèse en préparation.

U.F.R. de Mathématiques Pures et Appliquées
Université des Sciences et Technologies de Lille
U.M.R. au C.N.R.S. 8524
59655 Villeneuve d'Ascq Cedex, France
E-mail: yann.walkowiak@math.univ-lille1.fr

Reçu le 23.12.2003
et révisé le 14.9.2004 (4683)