Reprinted from

Séminaire de Théorie des Nombres, Paris 1985–86

Edited by Catherine Goldstein

Progress in Mathematics, Volume 71

Birkhäuser
Boston · Basel

RESULTATS RECENTS LIES AU THEOREME D'IRREDUCTIBILITE DE HILBERT

Pierre DEBES

Le théorème d'irréductibilité de Hilbert est un résultat de la fin du siècle dernier [17]. Le problème est le suivant : étant donnés un corps k et $P_1,\dots,P_n$ n polynômes irréductibles dans $k(X_1,\dots,X_r)[Y_1,\dots,Y_s]$, montrer que l'ensemble qu'on note classiquement $H_k(P_1,\dots,P_n)$, constitué des spécialisations $(x_1,x_2,\dots,x_r)$ des indéterminées $(X_1,\dots,X_r)$ pour lesquelles les polynômes $P_i(x_1,\dots,x_r,Y_1,\dots,Y_s)$, $i= 1,2,\dots,n$, sont irréductibles dans $k[Y_1,\dots,Y_s]$, contient beaucoup d'éléments de k^r. Précisément, on appelle partie hilbertienne de k^r tout ensemble, intersection d'un ensemble du type $H_k(P_1,\dots,P_n)$ avec un ouvert de Zariski de k^r et on dit que le corps k est hilbertien si pour tout entier $r\geq 1$, les parties hilbertiennes sont non vides. On appelle aussi ensemble mince tout ensemble dont le complémentaire contient une partie hilbertienne. En ces termes, le théorème d'irréductibilité de Hilbert s'énonce :

Théorème 0 - Le corps $\mathbb{Q}$ des nombres rationnels est un corps hilbertien.

Le théorème de Hilbert autorise dans certaines situations à spécialiser des paramètres, sans modifier la structure algébrique. Ainsi, on peut spécialiser des indéterminées d'un polynôme de telle sorte que l'irréductibilité soit conservée, mais aussi la structure de son groupe de Galois. Cela permet de construire des extensions de $\mathbb{Q}$ de groupe de Galois donné G (problème inverse de la théorie de Galois) : il suffit de savoir construire une extension d'un corps d'indéterminées $\mathbb{Q}(X_1,\dots,X_r)$ de groupe G et de spécialiser ensuite $X_1,\dots,X_r$. On trouve dans les oeuvres de Hilbert, des exemples de ce genre de construction avec $G=S_n$ et $G=A_n$ (voir [27] pour d'autres exemples).

Le théorème de Hilbert sert également à construire des courbes elliptiques de rang élevé. La stratégie est la même : on construit une courbe elliptique sur un corps d'indéterminées qu'on spécialise ensuite. D'après un théorème de Néron, en dehors d'une ensemble mince, le rang se conserve. Néron a obtenu de cette façon des courbes

elliptiques de rang sur $\mathbb{Q}$ $r=9$, 10 et même 11 [21]; sa construction pour $r=11$ a été précisée récemment par M. Fried [14]. Jusqu'aux travaux de J.-F. Mestre [20], c'était la seule méthode.

Pour montrer qu'un corps k est hilbertien, l'étude du cas $r=s=1$ (c'est-à-dire un paramètre et une indéterminée) est suffisante ([19] Ch. 9 § 3). Le problème consiste alors, via une réduction classique ([19] Ch. 9 Prop. 1.1), à compter des points sur des courbes algébriques, précisément à montrer que si $\deg_Y P_i \geq 2$ pour $i= 1,2,\ldots,n$, les ensembles

$$V'_k(P_1,\ldots,P_n)= \{x\in k / P_i(x,Y) \text{ n'a pas de racine dans } k \text{ pour } i=1,2,\ldots,n\}$$

sont infinis. Le théorème de Siegel sur la finitude des points entiers sur les courbes de genre ≥ 1 permet alors de majorer en $O(\sqrt{N})$ le nombre des entiers x qui ne sont pas dans $H_{\mathbb{Q}}(P_1,\ldots,P_n)$ et tels que $|x|\leq N$; cette estimation est d'ailleurs la meilleure possible à cause des carrés $(P_1= Y^2-X)$. On a des résultats semblables pour les x rationnels de hauteur $\leq N$ (cf. [27]).

Pour les dimensions plus grandes , des estimations analogues ont été établies par S.D. Cohen dans la fin des années 70 [5], mais la méthode est différente : elle consiste à étudier la réduction modulo un idéal premier $\mathfrak{p}$ d'un ensemble mince M; grâce au théorème de Lang-Weil sur le nombre de points mod $\mathfrak{p}$ d'une variété algébrique, on montre que certaines classes ne sont pas atteintes. Le théorème du grand crible permet d'en déduire que l'ensemble M lui-même n'a pas beaucoup d'éléments. La première partie de la méthode redonne d'autre part un résultat établi par A. Schinzel [24] et de façon effective par M. Fried [13] : toute partie hilbertienne de $\mathbb{Q}$ contient une progression arithmétique d'entiers. Pour plus de détails sur cet exposé introductif, nous renvoyons à [27] et [19].

Des travaux de ces dernières années permettent de donner une autre description des parties hilbertiennes, plus qualitative : ils mettent en évidence une relation liant la structure arithmétique d'un polynôme spécialisé $P(x,Y)$ (sa décomposition en polynômes irréductibles) à celle de x (sa décomposition en nombres premiers, ou plus généralement en idéaux premiers pour x algébrique). Cette relation se trouve être contraignante et imposera que "très souvent", on ne puisse être que dans le cas le plus simple, c'est-à-dire celui où $P(x,Y)$ est irréductible. On obtiendra de cette manière de nouveaux résultats liés au théorème d'irréductibilité de Hilbert et ce qui est important des résultats complètement explicites (voir en particulier le théorème 4).

Notations. Les valeurs absolues associées aux places d'un corps de nombres F sont normalisées de telle sorte qu'elles soient égales sur $\mathbb{Q}$ aux valeurs absolues usuelles. M_F désigne l'ensemble des places de F. La formule du produit s'écrit

$$\prod_{v\in M_F} |\xi|_v^{d_v^F} = 1 \quad \text{pour} \quad \xi \in F,\ \xi \neq 0$$

et la hauteur (logarithmique) d'un nombre algébrique est définie par

$$h(\xi)= \frac{1}{[F:\mathbb{Q}]} \sum_{v\in M_F} d_v^F \log \max(1,|\xi|_v) \quad \text{pour} \quad \xi \in F,$$

où d_v^F désigne le degré local de la place $v\in M_F$ par rapport à $\mathbb{Q}$. Enfin pour $\xi\in M_F$ on note $M_F(\xi)$ l'ensemble des places $v\in M_F$ où $|\xi|_v<1$ (par exemple, si ξ est un entier rationnel, $M_{\mathbb{Q}}(\xi)$ est l'ensemble des nombres premiers divisant ξ).

Dans la suite, k désigne un corps de nombres et P un polynôme irréductible dans $k(X)[Y]$. On suppose qu'il existe une série de Laurent $\underset{\sim}{Y} = \sum_{m\geq m_0} \eta_m X^m$ à coefficients η_m dans $\overline{\mathbb{Q}}$, solution de $P(X,\underset{\sim}{Y})=0$. D'un point de vue géométrique, cette hypothèse signifie que dans un modèle projectif lisse de la courbe "$P(x,y)=0$", la fonction x possède au moins un zéro simple Q.

Soit K le corps $K=k((\eta_m)_{m\geq m_0})$. Il est facile de voir que K est un corps de nombres et que $[K:k] \leq \deg_Y P$. Géométriquement K est le corps de définition sur k de Q.

Pour toute place v de K, notons R_v le rayon de convergence v-adique de $\underset{\sim}{Y}$ (on a $R_v>0$) et Y_v la fonction naturellement induite par $\underset{\sim}{Y}$ sur la boule ouverte épointée $B^*(0,R_v)= \{x\in K_v / 0<|x|_v<R_v\}$ du complété K_v de K pour la métrique v.

L'énoncé suivant est fondamental. Pour ξ non nul dans k, on se donne a priori un diviseur π dans $k[Y]$ du polynôme $P(\xi,Y)$; les nombres $Y_v(\xi)$ qui sont définis sont tous racines du polynôme $P(\xi,Y)$; dans le théorème 1, on s'intéresse seulement à ceux de ces nombres qui sont racines du polynôme π.

Théorème 1 - Soient $\xi\in k$, $\xi\neq 0$ et π un diviseur de $P(\xi,Y)$ dans $k[Y]$. Soit $S(\xi,\pi)$ l'ensemble des places v de K vérifiant :

$$|\xi|_v < R_v \quad \text{et} \quad \pi(Y_v(\xi)) = 0.$$

On a alors

$$\frac{1}{[K:\mathbb{Q}]} \sum_{v\in S(\xi,\Pi)} d_v^K \log \min(1,|\xi|_v) = -\frac{\deg \Pi}{\deg_Y P} h(\xi) + O(\sqrt{h(\xi)})$$

où les constantes intervenant dans le $O(\ldots)$ ne dépendent que de P.

On peut interpréter le théorème 1 comme un résultat sur la distribution des $Y_v(\xi)$ qui sont définis, à l'intérieur des racines de $P(\xi,Y)$. En effet, à cause de la formule du produit, on a

$$h(\xi) = -\frac{1}{[K:\mathbb{Q}]} \sum_{v\in M_K} d_v^K \log \min(1,|\xi|_v);$$

la relation du théorème 1 signifie donc, qu'à un $O(1/\sqrt{h(\xi)})$ près, la probabilité (selon la loi image par l'application $v \longrightarrow d_v^K \log|\xi|_v$) qu'à une place v d'appartenir à un ensemble $S(\xi,\Pi)$, c'est-à-dire la probabilité qu'à un nombre $Y_v(\xi)$ d'être une racine de Π, vaut $\deg \Pi/\deg_Y P$.

Le théorème 1 est banal dans les cas extrêmes $\Pi=1$ et $\Pi = P(\xi,Y)$. Les situations intermédiaires sont plus intéressantes : la relation du théorème 1 impose à ξ des conditions (arithmétiques) non triviales pour qu'une telle situation puisse se produire c'est-à-dire pour que le polynôme $P(\xi,Y)$ puisse être réductible. Le corollaire suivant est une bonne illustration de ce lien existant entre les structures arithmétiques de $P(\xi,Y)$.

Corollaire 1 ([10] § 2.3) - Soit $P(\xi,Y) = u P_1^{\alpha_1} \ldots P_g^{\alpha_g}$ la décomposition du polynôme $P(\xi,Y)$ en irréductibles distincts de $k[Y]$. Alors, pourvu que $h(\xi)>h_0$ où h_0 est une constante ne dépendant que de P, on a

$$g \leq \text{Card } M_K(\xi).$$

Il suffit de remarquer que si $h(\xi)$ est suffisamment grand, le terme de gauche dans la relation du théorème 1 ne peut être nul si $\deg \Pi \geq 1$; par conséquent, on a $S(\xi,P_i) \cap M_K(\xi) \neq 0$ pour $i= 1,2,\ldots,g$. D'autre part, on a $S(\xi,P_i) \cap S(\xi,P_j) = \emptyset$ si $i\neq j$. Il y a donc au moins autant de places dans $M_K(\xi)$ que de polynômes P_i □

On obtient en particulier le résultat suivant :

Corollaire 2 [29] - Soit P un polynôme irréductible dans $\mathbb{Q}(X)[Y]$. On suppose que le polynôme $P(0,Y)$ possède une racine simple dans $\mathbb{Q}$. ALors si p est un nombre premier et m un entier, le polynôme $P(p^m,Y)$ est irréductible dans $\mathbb{Q}[Y]$ dès que p^m est suffisamment grand (supérieur à une constante ne dépendant que de P).

En effet, on a ici $K=\mathbb{Q}$; $M_{\mathbb{Q}}(p^m)=\{p\}$; d'après le corollaire 1, on a donc $g=1$ dès que $h(p^m)= \log p^m$ est assez grand □ (voir [10] § 2.3 pour des généralisations du corollaire 2).

Le théorème 1 généralise les travaux antérieurs sur les valeurs de fonctions algébriques de T. Schneider [25] [26], P. Bundschuh [3] et V.G. Sprindzuk [29] [30] [31] [32]. Dans ces premiers travaux qui tous ont leur source dans le célèbre article de Siegel [28], seule une place entre en jeu (une place archimédienne chez Schneider et Bundschuh, une place finie chez Sprindzuk). En 1983, Sprindzuk donnera sa forme quasi définitive au résultat, en tenant compte simultanément de toutes les places [32]. Le théorème 1 [7] [10], obtenu grâce à une méthode différente de celle de Sprindzuk, affine un peu les hypothèses de son résultat et surtout en améliore les constantes : celles de Sprindzuk dépendent de k.

Les méthodes utilisées pour démontrer ce genre de résultats proviennent de la théorie des nombres transcendants.

La méthode de Siegel. C'est la méthode utilisée par Sprindzuk. Mise en oeuvre à l'origine par Siegel pour montrer la transcendance de valeurs de E-fonctions [28], on l'applique ici à des fonctions algébriques. Schématiquement, on procède de la façon suivante (voir [32] pour un exposé précis de la méthode).

Grâce au principe des tiroirs, on construit une fonction auxiliaire non nulle $\phi(X,\underset{\sim}{Y})$ où $\phi \in k[X,Y]$ est un polynôme dont on contrôle la hauteur, vérifiant les deux conditions :

(a) $\mathrm{ord}_0\ \phi(X,\underset{\sim}{Y}) \geq M$ où M est grand (précisément, M est un paramètre qu'on fait tendre vers $+\infty$ en fin de démonstration; ord_0 désigne la valuation X-adique sur $\overline{\mathbb{Q}}((X))$).

(b) Il existe $w \in S(\xi,\Pi)$ tel que $\phi(\xi, Y_w(\xi)) \neq 0$.
Par définition de $S(\xi,\Pi)$ on a aussi

(c) $\Pi(Y_w(\xi)) = 0$.

Enfin, on peut supposer Π irréductible : le cas général s'en déduit aisément. De (b) et (c) on déduit alors que R le résultant des polynômes Π et $\phi(\xi,Y)$ est non nul dans k. On applique la formule du produit à ce nombre algébrique :

$$\prod_{v \in M_K} |R|_v^{d_v^K} = 1.$$

Le résultat découle alors de la majoration de chacun des termes $|R|_v$. Ajoutons seulement que pour $v \in S(\xi,\Pi)$, on majore $|R|_v$ en

$|\phi(\xi,Y_v(\xi))|_v$ qui est petit à cause de (a) : il varie en $|\xi|_v^M$. Cela explique comment apparaît le terme de gauche dans le théorème 1. Le terme $\frac{\deg \Pi}{\deg_Y P} h(\xi)$ provient lui de la majoration de la hauteur de ϕ donnée par le principe des tiroirs □

Il y a cependant une difficulté. Pour obtenir la condition (b), on est obligé de faire des différentiations, ce qui fait apparaître des factorielles. Quand on travaille avec des E-fonctions, par exemple l'exponentielle, ces factorielles disparaissent, se simplifiant avec ceux qui figurent au dénominateur des coefficients du développement de Taylor des E-fonctions. En revanche, ils compliquent considérablement les estimations quand il s'agit de fonctions algébriques ou plus généralement de G-fonctions dont les coefficients de Taylor varient géométriquement. C'est d'ailleurs à cause de cette difficulté que les énoncés donnés par Siegel sur les G-fonctions resteront en suspens très longtemps : ce n'est qu'en 1981 qu'un résultat général sera démontré par Bombieri [1], au prix d'arguments très fins comme le théorème de Dwork-Robba. L'analogue de ce dernier résultat chez Sprindzuk est le lemme 4.5 de [32].

La méthode de Gel'fond. Il y a une alternative à la méthode de Siegel : la méthode de Gel'fond, que celui-ci élabora pour montrer la transcendance de a^b (septième problème de Hilbert). Adaptée au problème considéré, elle conduit d'une part au théorème 1 [6], d'autre part, dans le cadre plus général des G-fonctions, à une nouvel énoncé [10] tout à fait analogue à celui de Bombieri, et cela sans rencontrer l'écueil de la méthode précédente. Le principe de la démonstration est le suivant.

Grâce au principe des tiroirs, on construit une fonction auxiliaire non nulle $\phi(X,\underset{\sim}{Y})$ où $\phi \in k[X,Y]$ est un polynôme dont on contrôle la hauteur, vérifiant la condition
(a) pour toute place $v \in S(\xi,\Pi)$, la fonction $\phi(X,Y_v)$ a un zéro d'ordre élevé (supérieur à un paramètre M) au point ξ.
(Ici aussi, Π est supposé irréductible dans $k[Y]$ et la condition (a), en fait, ne dépend pas de $v \in S(\xi,\Pi)$, les valeurs des fonctions Y_v en ξ (ainsi que leur dérivées) étant conjuguées sur k pour $v \in S(\xi,\Pi)$).

Ensuite, on applique la formule du produit tout simplement au premier terme non nul τ du développement de $\phi(X,\underset{\sim}{Y})$ en 0 de $\phi(X,\underset{\sim}{Y})$, la condition (a) conduisant à des majorations de $|\tau|_v$ en $|\xi|_v^M$ pour $v \in S(\xi,\Pi)$ □

Signalons pour clore ce chapitre que D.V et G.V Chudnovsky ont récemment obtenu, grâce à une méthode basée sur la théorie des approximants de Padé du second type, de nouveaux résultats sur la nature arithmétique des valeurs de G-fonctions $f_1,\ldots,f_n$ vérifiant des équations différentielles linéaires [4]. Leurs conclusions sont comparables à celles de [1] et [10], (à ceci près qu'ils ne travaillent

qu'avec une seule place), mais au contraire de ces derniers travaux, ils se dispensent de toute hypothèse sur l'opérateur différentiel linéaire dont est supposé être solution le n-uple $(f_1,\dots,f_n)$; dans [1], on suppose que cet opérateur est fuchsien de type arithmétique, dans [10] que c'est un G-opérateur. Ils démontrent d'autre part ([4] th. III) que si, de plus, $f_1,\dots,f_n$ sont linéairement indépendantes sur $\overline{\mathbb{Q}}(X)$, alors le n-uple $(f_1,\dots,f_n)$ est nécessairement solution d'un opérateur différentiel vérifiant la condition de Galočkin [16], une troisième hypothèse classique dans ce genre de problème.

En 1983, Bombieri a donné une troisième démonstration du théorème 1 [2]. Sa nouvelle approche montre que le théorème 1, obtenu jusque là par des voies arithmétiques, a en fait une origine algébrique. La formulation de son résultat est plus géométrique, mais les énoncés sont équivalents (voir [8] Ch. 7).

Soit C une courbe projective irréductible lisse définie sur le corps de nombre k. Pour $Q\in C(k)$ un point k-rationnel sur C, on note λ_Q la fonction de Weil associée au diviseur Q (précisément, λ_Q désigne un représentant fixé de la classe, modulo les fonctions M_k-bornées sur C, des fonctions de Weil associées au diviseur Q (cf. [19] Ch. 10)). A v fixé, il faut voir $\lambda_Q(.,v)$ comme une valuation sur C : $\lambda_Q(M,v)$ grand signifie que "M est proche de Q pour la place v".

Théorème 2. - Soit $\mathcal{P}$ une fonction rationnelle sur C définie sur k. Il existe une famille de nombres réels δ_v, $v\in M_k$, nuls pour toutes les places sauf un nombre fini ayant la propriété suivante : si $Q\in C(k)$ est un pôle de $\mathcal{P}$ k-rationnel, alors pour tout point M dans $C(k)$, on a

$$\frac{1}{[k:\mathbb{Q}]} \sum_{\substack{v\in M_k \\ \lambda_Q(M,v)>\delta_v}} d_v^k \log \max\left(1,\left|\mathcal{P}(M)\right|_v\right) = -\frac{\mathrm{ord}_Q \mathcal{P}}{\deg \mathcal{P}}\, h(\mathcal{P}(M)) + O\left(\sqrt{h(\mathcal{P}(M))}\right)$$

où les constantes intervenant dans le $O(\dots)$ dépendent de C et $\mathcal{P}$ seulement.

La démonstration de Bombieri s'appuie sur deux résultats fondamentaux : le théorème de décomposition de Weil ([33], [19] Ch. 10) et la quadraticité de la hauteur sur les variétés abéliennes ([22], [19] Ch. 5). Son principe est le suivant (cf. [2] [9]).

En utilisant les propriétés standards des fonctions de Weil, notamment le théorème de décomposition de Weil, on montre l'existence d'une famille de nombres réels δ_v, $v\in M_k$, nuls pour presque tout v, telle que si $Q\in C(k)$ est un pôle de $\mathcal{P}$, alors pour tout $M\in C(k)$, on ait

$$\frac{1}{[k:\mathbb{Q}]} \sum_{\substack{v\in M_k \\ \lambda_Q(M,v)>\delta_v}} d_v^k \log \max(1, |\mathcal{P}(M)|_v) = - \operatorname{ord}_Q \mathcal{P}\ h_Q(M) + O(1)$$

où h_Q désigne la hauteur associée à la classe du diviseur Q dans le groupe de Picard de C.

Ensuite, on fait varier Q parmi les pôles de $\mathcal{P}$ et on somme les égalités ainsi obtenues : cela donne

$$h(\mathcal{P}(M)) = \sum_{Q' \text{pôle de } \mathcal{P}} (-\operatorname{ord}_{Q'}\mathcal{P}) h_{Q'}(M) + O(1).$$

Mais à cause de la quadraticité de la hauteur, on a (cf. [19] Ch. 5 § 5)

$$h_{Q'} = h_Q + O(\sqrt{h_Q}) \qquad \text{pour tout } Q'.$$

L'égalité précédente donne alors

$$h(\mathcal{P}(M)) = \deg \mathcal{P}\ h_Q(M) + O(\sqrt{h(\mathcal{P}(M))})$$

ce qui, reporté dans la première égalité, fournit le résultat désiré □

Comme pour le théorème 1, notons que le terme de gauche dans la relation du théorème 2 ne peut être nul si la hauteur de $\mathcal{P}(M)$ est suffisamment grande. Supposons tous les pôles de $\mathcal{P}$ rationnels sur k. La famille $(\delta_v)_{v\in M_k}$ du théorème 2 peut être choisie de telle sorte que les ensembles $\{v\in M_k / \lambda_Q(M,v)>\delta_v\}$ où Q varie dans l'ensemble des pôles de $\mathcal{P}$ soient disjoints deux à deux. De ces deux remarques, on déduit que, dès que $h(\mathcal{P}(M))$ est assez grand, le nombre de places v de k où $|\mathcal{P}(M)|_v > 1$ est minoré par le nombre de pôles de $\mathcal{P}$. Dans le cas général, on peut faire le raisonnement précédent sur une extension de k et redescendre sur k grâce à des arguments galoisiens (cf. [10] § 2.4). On obtient le résultat suivant :

Corollaire - Soient $\mathcal{P}$ une fonction rationnelle sur C définie sur k et μ le nombre de pôles de $\mathcal{P}$ non conjugués sur k. Pour tout point M k-rationnel sur C, on a

$$\operatorname{Card} M_k(1/\mathcal{P}(M)) \geq \mu$$

dès que $h(\mathcal{P}(M))$ est assez grand (supérieur à une constante ne dépendant que de C et $\mathcal{P}$).

Enoncé sous des formes diverses, ce résultat se situe à la croisée de plusieurs travaux : [2] Th. p. 305, [10] § 2.4 Corollaire, [15] Prop. 4.4, [34]. Aux méthodes utilisées chez les trois premiers qui sont celles décrites dans cet exposé, R. Weissauer [34] en ajoute une troisième qui s'appuie sur des arguments non-standards.

On peut, comme Bombieri [2], voir le corollaire comme un résultat de finitude des points entiers (ou S-entiers) sur certaines courbes algébriques. En particulier, il donne l'exemple suivant :

Soit P un polynôme irréductible dans $\mathbb{Q}[X,Y]$. Supposons que la partie homogène de plus haut degré dans P ne soit pas la puissance d'un irréductible de $\mathbb{Q}[X,Y]$. Géométriquement, cela impose que sur C, un modèle projectif lisse du corps de fonctions $\mathrm{Fract}\,(\overline{\mathbb{Q}}[X,Y]/P)$, la fonction x ait au moins deux pôles non conjugués sur $\mathbb{Q}$ (soit, avec les notations du corollaire, $\mu \geq 2$ pour $P=x$). On déduit donc du corollaire qu'il n'y a qu'un nombre fini de points M $\mathbb{Q}$-rationnels sur C vérifiant $\mathrm{Card}(M_{\mathbb{Q}}(1/x(M))<2$. En particulier les points M, $\mathbb{Q}$-rationnels sur C pour lesquels $x(M)\in\mathbb{Z}$ sont en nombre fini; l'équation $P(x,y)=0$ n'admet donc qu'un nombre fini de solutions entières x,y. On retrouve ici un résultat de Runge [23].

Il est intéressant de noter que le théorème 2 et son corollaire restent valides si le corps k est plus généralement un corps muni d'un ensemble de valeurs absolues satisfaisant la formule du produit ([19] Ch. 2). En effet, on peut déduire directement du corollaire que le corps k est hilbertien. On obtient ainsi que tout corps avec une formule du produit est un corps hilbertien, un résultat dû à Weissauer.

Voici comment on procède pour déduire du corollaire l'hilbertianité de k. Les idées suivantes sont de M. Fried ([15] th. 4.2). Cependant, contrairement à lui, nous n'utiliserons pas ici l'existence d'un ultrafiltre maximal non trivial sur $\mathbb{N}$.

Via les réductions classiques rappelées en introduction, il s'agit de démontrer que si $P_1,\ldots,P_n\in k(X)[Y]$ sont n polynômes absolument irréductibles de degré ≥ 2, alors l'ensemble $V'_k(P_1,\ldots,P_n)$ est infini.

Remarquons tout d'abord que, quitte à changer X en $b+1/X$, pour b convenablement choisi dans k, on peut supposer que les corps de rupture sur $k(X)$ des polynômes P_i, $i= 1,2,\ldots,n$, ne sont pas ramifiés au-dessus de la place $x=\infty$.

Soit H une partie infinie de $k-\{0\}$ ayant la propriété suivante :

(1) Il existe un entier ℓ tel que pour tout x dans H, $\mathrm{Card}\, M_k(x) \leq \ell$.

Nous allons montrer que

(2) Il existe $a\in k$ tel que l'ensemble $a+1/H\cap V'_k(P_1,\ldots,P_n)$ soit infini, ce qui, en notant $P_i^{(a)}= P_i(a+1/X,Y)$ pour $i= 1,2,\ldots,n$ et $a\in k$, équivaut à

(2') Il existe $a \in k$ tel que l'ensemble $H \cap V'_k(P_1^{(a)},\dots,P_n^{(a)})$ soit infini.

Pour m un entier quelconque, on commence par construire par récurrence $a_1,\dots,a_m$ dans k de telle sorte que pour $j= 2,3,\dots,m$, les discriminants des polynômes $P_i^{(a_j)}$, $i= 1,2,\dots,n$ d'une part, et les discriminants des polynômes $P_i^{(a_\nu)}$, $i= 1,2,\dots,n$, $\nu= 1,\dots,j-1$, d'autre part, n'aient pas de racines en commun : cela est clairement réalisable vu la forme des polynômes $P_i^{(a)}$.

On raisonne ensuite par l'absurde. Notons $V_k(P_i^{(a)})$ l'ensemble des éléments x de k tels que le polynôme $P_i^{(a)}(x,Y)$ ait une racine dans k; si (2') est faux, l'ensemble $H \cap \bigcup_{j=1}^{m} V'_k(P_1^{(a_j)},\dots,P_n^{(a_j)})$ est fini. On en déduit que l'ensemble

$$H \cap \bigcup_{1\le i_1,\dots,i_m\le n} V_k(P_{i_1}^{(a_1)}) \cap \dots \cap V_k(P_{i_m}^{(a_m)})$$ est infini, et donc qu'il existe un m-uplet $(i_1,\dots,i_m)$ dans $\{1,\dots,n\}$ pour lequel

(3) l'ensemble $H \cap V_k(P_{i_1}^{(a_1)}) \cap \dots \cap V_k(P_{i_m}^{(a_m)})$ est infini.

Notons pour $j= 1,2,\dots,m$, y_j un zéro dans $\overline{k(X)}$ du polynôme $P_{i_j}^{(a_j)}$ et L le corps $L= k(X,y_1,\dots,y_m)$. A cause du choix des nombres $a_1,\dots,a_m$ pour $j=2,\dots,m$, l'intersection des clôtures normales sur $k(X)$ des extensions $k(X,y_j)$ et $k(X,y_1,\dots,y_{j-1})$ est ramifiée nulle part, donc vaut $k(X)$ (équivalent classique sur $k(X)$ du théorème de Hermite-Minkowsky). Ces extensions sont donc linéairement disjointes sur $k(X)$. En particulier, on a

(4) $$[L : k(X)]= \deg P_{i_1} \dots \deg P_{i_m}.$$

Considérons maintenant C (resp. C_j) un modèle projectif lisse du corps de fonctions $L\overline{k}$ (resp. $\overline{k}(X,y_j)$). (3) signifie qu'il existe une infinité de points M k-rationnels sur C vérifiant $x(M)\in H$. On déduit alors de la définition de H (1) et du corollaire (qu'on applique à $\mathcal{P}=1/x$), qui si μ désigne le nombre de zéros non conjugués sur k de la fonction x, alors

$\mu \leq \ell$.

Soit Q l'un de ces zéros. Il s'envoie par restriction (en le voyant comme une place du corps $L\overline{k}$ au dessus de $X=0$), sur un zéro Q_j de la fonction x sur la courbe C_j. Ce dernier, par la transformation $X \longrightarrow a_j+1/X$, correspond à un pôle de la fonction x sur la courbe "$P_{i_j}(x,y)=0$", c'est-à-dire l'une des courbes "$P_1(x,y)=0$",...,"$P_n(x,y)=0$". Conclusion : le corps de définition sur k du point Q qui est isomorphe au compositum des corps de définition sur k des points Q_j, $j=1,2,\ldots,m$ (à cause de la condition sur $a_1,\ldots,a_m$), a un degré sur k qui peut être majoré par un nombre r indépendant de m. Enfin à cause de la réduction faite en début de démonstration, on a $\mathrm{ord}_Q x=1$. Toutes ces remarques conduisent finalement à

$$\deg \mathcal{P} = \sum_{\substack{Q \\ x(Q)=0}} \mathrm{ord}_Q \mathcal{P} \leq l_r .$$

Il suffit, pour obtenir la contradiction désirée, de choisir m assez grand, puisque, à cause de (4), on a aussi

$$\deg \mathcal{P} = [L : k(X)] \geq 2^m \qquad \square$$

La ramification est l'un des outils de base de la démonstration précédente. Elle joue également un rôle primordial dans un travail récent de R. Dvornicich et U. Zannier [12]. Soit P un polynôme irréductible dans $\mathbb{Q}[X,Y]$; pour $a \in \mathbb{Q}$, notons $\theta(X+a)$ une fonction algébrique solution de $P(X+a,\theta(X+a))=0$. En reprenant l'argument développé dans la démonstration précédente, on construit facilement $a_1,\ldots,a_m$ dans $\mathbb{Q}$ tels que l'extension $\mathbb{Q}(X,\theta(X+a_1),\ldots,\theta(X+a_m))$ soit de degré maximal sur $\mathbb{Q}(X)$, c'est-à-dire $(\deg_Y P)^m$.

Dvornicich et Zannier étudient l'analogue de ce problème, pour des valeurs de fonctions algébriques : si, pour $m \in \mathbb{N}$, on note θ_m une racine dans $\overline{\mathbb{Q}}$ du polynôme $P(m,Y)$, que peut-on dire du degré sur $\mathbb{Q}$ du corps $K(m)=\mathbb{Q}(\theta_1,\ldots,\theta_m)$.

Pour $m \in \mathbb{N}$, définissons l'entier $D(m)$ par

$$D(m)= \min_{\theta_1,\ldots,\theta_m} [\mathbb{Q}(\theta_1,\ldots,\theta_m):\mathbb{Q}]$$

où le "min" porte sur l'ensemble des m-uplets $(\theta_1,\ldots,\theta_m)$ vérifiant $P(i,\theta_i)=0$, $i=1,\ldots,m$. L'exemple du polynôme $P=Y^q-X$ pour lequel $K(m)=\mathbb{Q}(\sqrt[q]{p}$, p premier, $p \leq m)$ et donc $D(m) \leq q^{\pi(m)}$ avec $\pi(m) \sim m/\log m$, montre qu'on ne peut pas espérer une croissance

géométrique de $D(m)$. En fait, cet exemple est significatif puisque Dvornicich et Zannier démontrent que, pour P quelconque, il existe une constante $C>1$ vérifiant $D(m) \geq C^{m/\log m}$ pour m assez grand ([12] th. 2).

le résultat provient d'une étude de la ramification des corps $\mathbb{Q}(\theta_m)$, l'idée directrice étant de montrer que pour "beaucoup" d'entiers m, il existe un nombre premier p ramifié dans $\mathbb{Q}(\theta_m)$ et pas dans $\mathbb{Q}(\theta_j)$, $j= 1,2,\ldots,m-1$ de telle sorte qu'on puisse conclure que $K(m) \supsetneq K(m-1)$ pour "beaucoup" d'entiers m.

Le résultat-clé relie la ramification des corps $\mathbb{Q}(\theta_m)$ à celle du corps $\mathbb{Q}(X,\theta(X))$, de façon précise, Δ désignant le discriminant de l'extension $\mathbb{Q}(X,\theta(X))$ de $\mathbb{Q}(X)$, les nombres premiers p qui se ramifient dans $\mathbb{Q}(\theta_m)$ à ceux qui divisent $\Delta(m)$ (cf. [12] lemmes 3 et 4 pour des énoncés précis). On conclut grâce à des résultats classiques qui permettent d'estimer le nombre de premiers p pour lesquels l'équation $\Delta(m)=0$ a une solution dans $\mathbb{F}_p$.

Terminons cet exposé par une application spectaculaire des théorèmes 1 et 2. On appelle partie hilbertienne universelle (de $\mathbb{Q}$) toute suite $(x_m)_{m\geq 0}$ de nombres rationnels x_m ayant la propriété suivante : pour tout polynôme P irréductible dans $\mathbb{Q}(X)[Y]$, le polynôme $P(x_m,Y)$ est irréductible dans $\mathbb{Q}[Y]$ dès que $m \geq m(P)$ où $m(P)$ est une constante ne dépendant que de P. En d'autres termes, c'est une partie infinie de $\mathbb{Q}$ incluse dans toute partie hilbertienne de $\mathbb{Q}$, à un ensemble fini près. Commençons par quelques remarques :

(a) Pour e un entier quelconque supérieur à 2, il ne peut y avoir dans une partie hilbertienne universelle qu'un nombre fini de termes qui sont des puissances e-ièmes dans $\mathbb{Q}$ (considérer $P= Y^e-X$). En particulier, la suite des entiers positifs, la suite $(t^m)_{m\geq 0}$ où t est un rationnel fixé, ne sont pas des parties hilbertiennes universelles.

(b) La suite $(p_m)_{m\geq 0}$ des nombres premiers n'est certainement pas une partie hilbertienne universelle. En effet, on conjecture classiquement qu'il existe une infinité de nombres premiers p de la forme $p= y^2+1$ avec y entier, ce qui signifie que pour $P= Y^2+1-X$, le polynôme $P(p,Y)$ se décompose pour une infinité de nombres premiers p.

(c) L'image d'une suite $(x_m)_{m\geq 0}$, qui n'est pas une partie hilbertienne universelle, par une homographie rationnelle bijective $x \longrightarrow \frac{ax+b}{cx+d}$ n'est pas non plus une partie hilbertienne universelle.

L'existence de parties hilbertiennes universelles est une conséquence du théorème d'irréductibilité de Hilbert : on peut ordonner en une suite $(P_n)_{n\geq 0}$ l'ensemble des polynômes irréductibles dans $\mathbb{Q}(X)[Y]$; d'après le théorème de Hilbert, pour tout entier $m\geq 0$, l'ensemble $H_{\mathbb{Q}}(P_0,P_1,\ldots,P_m)$ est non vide; on choisit x_m dedans. Alors la suite $(x_m)_{m\geq 0}$ est une partie hilbertienne universelle.

Mais jusqu'en 1981, on ne disposait d'aucun exemple explicite de partie hilbertienne universelle. On peut désormais en construire grâce aux théorèmes 1 et 2. Le premier a été donné par Sprindzuk [31]. Il s'agit de la suite

$$x_m = [\exp(\sqrt{\log(\log m)})] + m!2^{m^2}, \qquad m\geq 3.$$

Nous allons donner ici un deuxième exemple. Sa construction repose sur le résultat suivant [11].

Théorème 3 - Soient $P\in\mathbb{Q}[X,Y]$ un polynôme de degré partiel en Y supérieur ou égal à 2 et $e\geq 1$ un entier tels que le polynôme $P(X^e,Y)$ soit absolument irréductible et possède une racine $\underset{\sim}{Y}$ dans $\overline{\mathbb{Q}}((X))$. Soit b un entier distinct de $0,1,-1$. Il existe un entier non nul $\alpha_0(P,b)$ tel que pour tout multiple non nul α de $\alpha_0(P,b)$, le polynôme $P(\alpha^e b^m,Y)$ n'ait pas de racine dans $\mathbb{Q}$ si m est un entier assez grand (précisément supérieur à une constante $m_0(P,b,\alpha)$ ne dépendant que de P,b,α).

Supposons pour simplifier $e=1$ (le cas général, un peu plus délicat, est traité dans [11]). On est alors sous les hypothèses du théorème 1. Rappelons que K désigne le corps engendré sur $\mathbb{Q}$ par les coefficients de $\underset{\sim}{Y}$. Pour démontrer le théorème 3, on distingue deux cas.

Premier cas : $[K:\mathbb{Q}] < \deg_Y P$ - On choisit $\alpha_0=1$. Soient α un entier non nul et Π un diviseur dans $\mathbb{Q}[Y]$ du polynôme $P(\alpha b^m,Y)$ de degré $\deg \Pi \geq 1$. Notre objectif est de montrer que $\deg \Pi \geq 2$.

Notons S_m l'ensemble $S_m = S(\alpha b^m,\Pi) \cap M_K(b)$. Le théorème 1 donne

$$\frac{1}{[K:\mathbb{Q}]} \sum_{v\in S_m} d_v^K \log|b|_v + \frac{\deg \Pi}{\deg_Y P} h(b) = O\left(\sqrt{\frac{h(b)}{m}}\right).$$

Notons x_m le terme de gauche. Comme $1 \leq \deg \Pi \leq \deg_Y P$ et que $S_m \subset M_K(b)$, la suite $(x_m)_{m\geq 1}$ ne prend qu'un nombre fini de valeurs. Comme, d'après la relation précédente, elle tend vers 0, elle est nulle à partir d'un certain rang.

b est un nombre rationnel; la relation $\chi_m=0$ s'écrit donc :

$$\sum_{w\in M_{\mathbb{Q}}(b)} \left[\frac{1}{[K:\mathbb{Q}]} \sum_{\substack{v\in S_m \\ v/w}} d_v^K - \frac{\deg \Pi}{\deg_Y P}\right] \log |b|_w = 0.$$

Mais les nombres $\log |b|_w$, où w décrit l'ensemble $M_{\mathbb{Q}}(b)$ sont linéairement indépendants sur $\mathbb{Q}$. On obtient donc, que pour tout entier m assez grand, on a

$$[K : \mathbb{Q}] \deg \Pi = \deg_Y P \sum_{\substack{v\in S_m \\ v/w}} d_v^K \quad \text{pour tout } w\in M_{\mathbb{Q}}(b)$$

ce qui donne en particulier

$$\deg \Pi \geq \frac{\deg_Y P}{[K:\mathbb{Q}]} > 1.$$

Deuxième cas : $[K : \mathbb{Q}]= \deg_Y P$ - Moyennant un petit changement sur P, cette hypothèse signifie que le polynôme $P(0,Y)$ est irréductible dans $\mathbb{Q}[Y]$. D'après un résultat classique de Hasse, il existe un nombre premier p tel que l'équation $P(0,y)=0$ n'ait pas de solutions y dans $\mathbb{F}_p$. Prenons $\alpha_0=p$. Si α est un multiple de α_0, le polynôme $P(\alpha b^m,Y)$ ne peut avoir de racine rationnelle y puisqu'en passant aux classes modulo p, on aurait alors $P(0,y)\equiv 0$ modulo p □

Appliqué à plusieurs polynômes à la fois, le théorème 3 conduit à une nouvelle version du théorème d'irréductibilité de Hilbert [11] : si b est un entier distinct de 0,1 et -1, toute partie hilbertienne de $\mathbb{Q}$ contient une progression géométrique $(ab^m)_{m\geq 1}$ de raison b. Mais le théorème 3 permet d'aller plus loin encore.

Notons, pour tout nombre réel x, $p(x)$ et $\theta(x)$ les entiers définis par

$$\begin{cases} p(x)= \text{Max } \{p/p \text{ premier}, \ p\leq x\} & \text{si } x\geq 2 \\ p(x)= 1 & \text{si } x<2 \end{cases}$$

$$\theta(x)= \prod_{\substack{p \text{ premier} \\ p\leq x}} p.$$

Théorème 4 - Soit b un entier distinct de 0,1 et -1. Pour $m\geq 2$, soit

$$x_m= p(\log \log m)\, \theta(\log m)^{[\log \log m]!}\, b^m.$$

La suite $(x_m)_{m\geq 2}$ est une partie hilbertienne universelle. Autrement dit, si P est un polynôme irréductible dans $\mathbb{Q}(X)[Y]$, alors dès que m est suffisamment grand, le polynôme $P(x_m,Y)$ est irréductible dans $\mathbb{Q}[Y]$.

Le gros du travail restant à faire consiste à préciser le théorème 3. En utilisant un résultat effectif de J.C. Lagarias, H.L. Montgomery et A.M. Odlyzko sur le théorème de Chebotarev [18], dont le lemme de Hasse est un corollaire, on montre qu'on peut choisir pour $a_0(P,b)$ un nombre premier vérifiant

$$a_0(P,b) \leq \nu(P,b)$$

où $\nu(P,b)$ est une constante qu'on peut calculer effectivement, ne dépendant que de P,b. Le calcul des constantes intervenant dans le théorème 1, qui est fait dans [10], fournit d'autre part une majoration explicite de $m_0(P,b,\alpha)$ en fonction de P, b et de α.

On procède alors de la façon suivante. Il s'agit de montrer que si $P\in\mathbb{Q}[X,Y]$ est un polynôme absolument irréductible de degré partiel en Y supérieur ou égal à 2, le polynôme $P(x_m,Y)$ n'a pas de racine dans $\mathbb{Q}$ si m est un entier assez grand.

Soit $e\geq 1$ un entier tel que le polynôme $P(X^e,Y)$ admette une racine dans $\overline{\mathbb{Q}}((X))$; l'existence de e est assurée par le théorème de Puiseux. On introduit ensuite le polynôme $P_m = P(p(\log\log m)X,Y)$, défini pour $m\geq 2$. Enfin, notons α_m le nombre

$\alpha_m = 9(\log m)^{[\log\log m]!/e}$; c'est un entier dès que m est assez grand. Deux cas se présentent.

Premier cas : $P(X^e,Y)$ n'est pas absolument irréductible - Le polynôme $P_m(X^e,Y)$ est alors lui aussi non absolument irréductible. Par contre, d'après la proposition 3 du paragraphe 4 de [10], dès que m est assez grand, il est irréductible dans $\mathbb{Q}(\beta)[X,Y]$, où β désigne une racine e-ième de b. Sous ces conditions, le polynôme $P_m((\alpha_m\beta^m)^e,Y) = P(x_m,Y)$ ne peut avoir de racine dans $\mathbb{Q}(\beta)$ (en particulier dans $\mathbb{Q}$) que si elle est multiple. Cela ne peut se produire que pour un nombre fini d'entiers m.

Deuxième cas : $P(X^e,Y)$ est absolument irréductible - Le polynôme P_m vérifie alors les hypothèses du théorème 3. Quelques calculs basés sur les estimations préliminaires des constantes $a_0(P,b)$ et $m_0(P,b,\alpha)$ montrent que, dès que m est assez grand

$\log m \geq \nu(P_m,b)$ de telle sorte que $\alpha_0(P_m,b)$ divise α_m et $m \geq m_0(P_m,b,\alpha_m)$.

Pour m assez grand, le polynôme $P_m(\alpha_m^{e_1}b^m,Y) = P(x_m,Y)$ n'a donc pas de racine dans $\mathbb{Q}$. □

BIBLIOGRAPHY

[1] E. Bombieri.- On G-functions, Recent progress in analytic number theory, H. Halberstam and C. Hooley ed., Acad. Press (1981), vol. 2, 1-67.

[2] E. Bombieri.- On Weil's "Théorème de Décomposition", Amer. J. Math., 105 (1983), 295-308.

[3] P. Bundschuh.- Une nouvelle application de la méthode de Gel'fond. Sem. Delange-Pisot-Poitou, Théorie des Nombres, 19ème année (1977-78), N° 42.

[4] D.V. and G.V. Chudnovsky.- Applications of Padé approximations to diophantine inequalities in values of G-functions, Number Theory, Sem. N.Y., 1983-84, Lect. Notes Math. 1135, (1985), 9-51.

[5] S.D. Cohen.- The distribution of the Galois groups of integral polynomials, Illinois J. Math. (1979), Vol. 23, N°1, 135-152.

[6] P. Dèbes.- Une version effective du théorème d'irréductibilité de Hilbert, Sém. Anal; Ultramétrique, Amice-Christol-Robba, 10ème année (1982-83), N° 10.

[7] P. Dèbes.- Spécialisations de polynômes, Math. rep. Acad. Sc., Royal Soc. Canada, Vol. V, n° 6, (Dec. 1983).

[8] P. Dèbes.- Valeurs algébriques de fonctions algébriques et théorème d'irréductibilité de Hilbert, Thèse 3ème cycle, Univ. P. et M. Curie (Paris VI), (1984).

[9] P. Dèbes.- Quelques remarques sur un article de Bombieri concernant le théorème de décomposition de Weil, Amer. J. Math. 107 (1985), 39-44.

[10] P. Dèbes.- G-fonctions et théorème d'irréductibilité de Hilbert, Acta Arithmetica, Vol. 47, N° 4, (à paraître).

[11] P. Dèbes.- Parties hilbertiennes et progressions géométriques, C.R. Acad. Sc. Paris, t. 302, Série I, n° 3, (1986).

[12] R. Dvornicich and U. Zannier.- Fields containing values of algebraic functions, Publ. Univ. Pisa (Novembre 1983).

[13] M. Fried.- On Hilbert's irreducibility theorem, J. Number Theory, 6 (1974), 211-231.

[14] M. Fried.- Constructions arising from Neron's high rank curves, Trans. Amer. Math. Soc. Vol. 281, N°2, 1984.

[15] M. Fried.- On the Sprindzuk-Weissauer approach to universal Hilbert subsets, Israel. J. Math. vol. 51, N° 4, 1985.

[16] A.L. Galochkin.- Lower bounds of polynomials in the values of a certain class of analytic functions, Math. Sb. 95 (1974), 396-417.

[17] D. Hilbert.- Uber die Irreduzibilität ganzer rationaler Funktionen mit ganzahligen Koeffizienten, Gesammelte Afhandlungen, Springer-Verlag (1983) [réimpression Chelsea (1965)] Vol. 2, N° 18, 264-286. Ou J. für die reine und angew. Math. 110 (1982), 104-129.

[18] J.C. Lagarias, H.L. Montgomery and A.M. Odlyzko.- The bound for the least prime ideal in the Chebotarev density theorem, Invent. Math. 54 (1979), 271-296.

[19] S. Lang.- Fundamentals of Diophantine Geometry, Springer-Verlag (1983).

[20] J.F. Mestre.- C.R. Acad. Sci. Paris 295 (1982), 643-644.

[21] A. Néron.- Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps, Bull. Soc. Math. France, 80 (1952), 101-166.

[22] A. Néron.- Quasi-fonctions et hauteurs sur les variétés abéliennes, Ann. of Math. 82 (1965) n° 2, 249-331.

[23] C. Runge.- Veber ganzzahlige Lösungen von Gleichungen zwischen zwei Veränderlichen, J. für die reine und angew. Math. 100 (1887), 425-435.

[24] A. Schinzel.- On Hilbert's irreducibility theorem, Acta Arithmetica 16 (1965), 334-340.

[25] T. Schneider.- Rationale Punkte Uber ciner algebraischen Kurve, Sem. Delange-Pisot-Poitou, Théorie des Nombres, 15ème année (1973/74), N° 20.

[26] T. Schneider.- Eine bemerkung zu einem Satz von C.L. Seigel, Comm. pure and applied Math. 29 (1976), 775-782.

[27] J.-P. Serre.- Autour du théorème de Mordell-Weil, II, Cours au Collège de France, (1980/81), Notes rédigées par M. Waldschmidt.

[28] C.L. Siegel.- Uber Einige Anwandungen diophantischer Approximationen, Gesammelte Afhandlungen, Springer-Verlag (1966), vol. 1, N° 16, 209-266. Ou Abh. Preus. Akad. Wiss. Phys. Math. Kl. 1 (1929), 14-67.

[29] V.G. Sprindzuk.- Hilbert's irreducibility theorem and rational points on algebraic curves, Doklady Acad. Nauk. SSSR 247 (1979), 285-289.

[30] V.G. Sprindzuk.- Reducibility of polynomials and rational points on algebraic curves Doklady Acad. Nauk. SSSR 250 (1980), 1327-1330.

[31] V.G. Sprindzuk.- Diophantine equations involving unknown primes, Trudy M.I.A.N. SSSR 158 (1981), 180-186.

[32] V.G. Sprindzuk.- Arithmetic specializations in polynomials, J. Reine und Angew. Math. 340 (1983), 26-52.

[33] A. Weil.- Arithmetic on algebraic varieties, Annals of Math. 53 (1951), 412-444.

[34] R. Weissauer.- Hilbertsche Körper, Thesis, Heidelberg (1980).

Pierre DEBES
Department of Mathematics
University of Florida
Gainesville FLA 32611
U.S.A.