THÉORIE DES NOMBRES. — *Parties hilbertiennes et progressions géométriques.* Note de **Pierre Dèbes**, présentée par Jean-Pierre Serre.

Nous montrons dans cette Note que si b est un entier distinct de 0,1, -1, toute partie hilbertienne de Q contient une progression géométrique de raison b.

NUMBER THEORY. Hilbert subsets and geometric progressions.

The main result of this paper asserts that every Hilbert subset of Q *contains a geometric progression* $(ab^m)_{m\geq 1}$, *for every integer* $b\neq 0,1,-1$.

Soient $P_1, \ldots, P_n$ n polynômes irréductibles dans $Q(X)[Y]$ et $H_{P_1,\ldots,P_n}$ l'ensemble des nombres rationnels ξ tels que les polynômes $P_1(\xi, Y), \ldots, P_n(\xi, Y)$ soient irréductibles dans $Q[Y]$. En 1892, D. Hilbert a démontré que tout ensemble du type $H_{P_1,\ldots,P_n}$, qu'on appelle depuis partie hilbertienne, est infini (théorème d'irréductibilité de Hilbert [7]).

Important en théorie des nombres (*voir* [11]), ce résultat a suscité depuis de multiples travaux : on sait ainsi depuis Siegel majorer en $O(\sqrt{N})$ le nombre des entiers ξ qui ne sont pas dans $H_{P_1,\ldots,P_n}$ et tels que $|\xi|\leqq N$; on sait aussi, grâce à A. Schinzel [9] et M. Fried [5], que toute partie hilbertienne contient une progression arithmétique. Plus récemment, V. G. Sprindzuk, à partir d'une méthode de Siegel, a obtenu de nouveaux résultats [13], lui permettant notamment de construire une partie hilbertienne universelle, c'est-à-dire une partie de Q contenue dans toute partie hilbertienne, à un nombre fini de ses éléments près ([12], *voir* aussi [6]).

L'objet de cette Note est le résultat suivant qui constitue une nouvelle version (effective) du théorème d'irréductibilité de Hilbert.

THÉORÈME 1. — *Soient* $P_1, \ldots, P_n$ n *polynômes irréductibles dans* $Q(X)[Y]$ *et* b *un entier distinct de* 0,1 *et* -1. *Alors il existe un entier* a *non nul vérifiant : pour tout entier* $m\geqq 1$, *les polynômes* $P_1(ab^m, Y), \ldots, P_n(ab^m, Y)$ *sont irréductibles dans* $Q[Y]$.

En d'autres termes, le théorème 1 signifie que si b est un entier distinct de 0,1 et -1, alors toute partie hilbertienne contient une progression géométrique de raison b. Il améliore le théorème 4 de [4] qui affirmait seulement l'existence de « beaucoup » de progressions géométriques dans toute partie hilbertienne.

La démonstration repose en grande partie sur les résultats récents de Sprindzuk [13], généralisés dans [4]. On emploie ici plutôt leur forme géométrique donnée par Bombieri dans [1] (*voir* aussi [3] et [4], § 2.4).

NOTATIONS. — Les valeurs absolues associées aux places v d'un corps de nombres F sont normalisées de telle façon que : si $v|p$ (c'est-à-dire si v est au-dessus du nombre premier p) :

$$|p|_v = p^{-1},$$

et si $v|\infty$ (c'est-à-dire si v est archimédienne) :

$$|\xi|_v = \xi \quad \text{pour tout nombre rationnel positif } \xi.$$

M_F désigne l'ensemble des places de F. Pour $v\in M_F$, nous notons d_v^F le degré local de la place v par rapport à Q. Enfin, si ξ est un nombre algébrique, $h(\xi)$ désigne la hauteur

0249-6291/86 03020087 $ 2.00

logarithmique de ξ ([8], chap. 3) définie par :

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

si F est un corps de nombres auquel ξ appartient.

De façon précise, le corollaire des résultats mentionnés plus haut, qu'on utilise ici est le lemme suivant; on le déduit du « Main Theorem » de [1] ou du théorème 3 de [4] de la même manière que la proposition 1 du paragraphe 3 de [4].

LEMME. — *Soient C une courbe projective irréductible lisse, définie sur un corps de nombres k, φ une fonction rationnelle sur C définie sur k, Q un pôle simple de φ, k(Q) son corps de définition sur k et ρ un élément non nul de k. On suppose qu'il existe une infinité de points M_m, $m \geqq 0$, k-rationnels sur C et une suite $(\mu_m)_{m \geq 0}$ d'entiers tels que $\varphi(M_m) = \rho^{\mu_m}$. Alors il existe une partie S de l'ensemble des places v du corps k(Q), où $|\rho|_v > 1$, telle que :*

$$\frac{1}{[k(Q) : \mathbf{Q}]} \sum_{v \in S} d_v^{k(Q)} \log |\rho|_v = \frac{1}{\deg \varphi} h(\rho).$$

ESQUISSE DE DÉMONSTRATION DU THÉORÈME 1. — Plusieurs arguments, classiques pour la plupart, permettent de se ramener à l'énoncé ci-dessous : principalement la proposition 1.1 du chapitre 9 de [8], le théorème de Puiseux, la proposition 3 du paragraphe 3 de [4] et le fait qu'une équation polynomiale $P(u, v) = 0$, où P est un polynôme irréductible sur un corps de nombres F, mais réductible dans $\bar{\mathbf{Q}}[X, Y]$, n'admet qu'un nombre fini de solutions (u, v) dans F^2.

THÉORÈME 2. — *Soient $P \in \mathbf{Q}[X, Y]$ un polynôme de degré partiel en Y supérieur ou égal à 2 et $e \geqq 1$ un entier tels que le polynôme $\Pi(Y) = P(X^e, Y)$ soit absolument irréductible et possède une racine dans $\bar{\mathbf{Q}}((X))$. Soit b un entier distinct de 0, 1 et -1. Il existe un entier non nul α_0 tel que pour tout multiple non nul α de α_0, le polynôme $P(\alpha^e b^m, Y)$ n'ait pas de racine dans Q si m est un entier suffisamment grand.*

On remarque tout d'abord qu'on peut supposer que b est un entier positif non puissance stricte d'un autre entier; sa décomposition en facteurs premiers est donc de la forme :

$$b = q_1^{\alpha_1} \dots q_g^{\alpha_g},$$

où les q_i sont des nombres premiers distincts et les α_i des entiers non nuls premiers entre eux dans leur ensemble. L'introduction du polynôme Π, qui est essentielle pour la suite, oblige cependant à travailler, non plus sur l'entier b, mais sur une racine e-ième β de b. On note k le corps $\mathbf{Q}(\beta)$.

Pour se placer sous les hypothèses du lemme, on procède de la façon suivante. On note R le corps de fonctions :

$$R = k(X)[Y]/\Pi,$$

C un modèle projectif lisse du corps de fonctions $R\bar{\mathbf{Q}} = \bar{\mathbf{Q}}(X)[Y]/\Pi$ et x, y les classes modulo Π de X et de Y. La définition de l'entier e impose que la fonction x possède au moins un zéro simple sur C. On note Q un zéro simple de x pour lequel le nombre $[k(Q) : k]$ soit minimal. On distingue alors deux cas suivant que $[k(Q) : k] = \deg_Y P$ ou non (on a toujours $[k(Q) : k] \leqq \deg_Y P$).

Premier cas : $[k(Q) : k] \neq \deg_Y P$. — Le lemme va permettre de conclure pour $\alpha_0 = 1$. Soit α un entier non nul. On raisonne par l'absurde : on suppose qu'il existe une infinité d'entiers m pour lesquels le polynôme $P(\alpha^e b^m, Y)$ ait une racine dans Q. En remarquant

que $P(\alpha^r b^m, Y) = \Pi(\alpha\beta^m, Y)$, on en déduit qu'il existe une infinité de points M_m, $m \geqq 0$, k-rationnels sur C, et une suite $(\mu_m)_{m\geq 0}$ d'entiers tels que $x(M_m) = \alpha\beta^{\mu_m}$. D'après le lemme, qu'on applique sur la courbe C à la fonction $\varphi = \alpha/x$ et au nombre $\rho = 1/\beta$, il existe donc une partie S de l'ensemble des places v du corps $k(Q)$ où $|\beta|_v < 1$, vérifiant la relation :

$$\frac{1}{[k(Q) : \mathbf{Q}]} \sum_{v\in S} d_v^{k(Q)} \log|\beta|_v + \frac{1}{\deg_Y P} h(\beta) = 0,$$

qui multipliée par e, donne :

$$\sum_{\substack{w\in M_{\mathbf{Q}} \\ |b|_w<1}} \left[\frac{1}{[k(Q) : \mathbf{Q}]} \sum_{\substack{v\in S \\ v|w}} d_v^{k(Q)} - \frac{1}{\deg_Y P} \right] \log|b|_w = 0.$$

Mais les nombres $\operatorname{Log}|b|_w$, où $w \in M_{\mathbf{Q}}$ et $|b|_w < 1$, sont linéairement indépendants sur $\mathbf{Q}$. On obtient donc :

$$(R) \qquad \deg_y P. \sum_{\substack{v\in S \\ v|q_j}} d_v^{k(Q)} = [k(Q) : \mathbf{Q}] \qquad \text{pour } j = 1, \ldots, g.$$

Quelques considérations arithmétiques montrent alors que :

$$e/\operatorname{pgcd}(e, \alpha_j) \text{ divise } \sum_{\substack{v\in S \\ v|q_j}} d_v^{k(Q)} \qquad \text{pour } j = 1, \ldots, g.$$

Ensuite, à cause de l'hypothèse $\operatorname{pgcd}(\alpha_1, \ldots, \alpha_g) = 1$, on a

$$\operatorname{ppcm}((e/\operatorname{pgcd}(e, \alpha_j))_{1\leq j\leq g}) = e.$$

Enfin, le théorème de Capelli ([10], I. 13, th. 21) montre que $[k : \mathbf{Q}] = e$. Tous ces résultats, reportés dans (R), conduisent à :

$$\deg_Y P \text{ divise } [k(Q) : k],$$

ce qui contredit l'hypothèse du premier cas.

Deuxième cas : $[k(Q) : k] = \deg_Y P$. — Dans ce cas, on commence par construire une fonction $y^* \in R$, entière sur l'anneau $k[x]$ et dont la valeur $y^*(Q)$ en Q engendre le corps $k(Q)$ sur k. Si $\Pi^* \in k[X, Y]$ désigne le polynôme minimal de y^* sur $k(x)(\simeq k(X))$, le polynôme $\Pi^*(0, Y)$ est, sous l'hypothèse $[k(Q) : k] = \deg_Y P$, nécessairement irréductible dans $k[Y]$.

A cause d'un lemme de Hasse ([2], chap. VIII, th. 9), il existe un idéal premier $\mathfrak{p}$ de k vérifiant :

(a) L'équation $\Pi^*(0, y) = 0$ n'a pas de solution y dans le corps résiduel de $\mathfrak{p}$.

(b) Les coefficients du polynôme Π^* sont dans l'anneau de valuation de $\mathfrak{p}$.

On note p le nombre premier au-dessous de l'idéal $\mathfrak{p}$ et on choisit $\alpha_0 = p$.

Soit α un multiple non nul de p. Comme dans le premier cas, on suppose qu'il existe une infinité de points M_m, $m \geqq 0$, k-rationnels sur C et une suite $(\mu_m)_{m\geq 0}$ d'entiers tels que $x(M_m) = \alpha\beta^{\mu_m}$.

En appliquant aux points M_m la relation $\Pi^*(x, y^*) = 0$, on obtient que l'équation $\Pi^*(\alpha\beta^m, y) = 0$ a une solution y_m dans k pour une infinité d'entiers m. La condition (b) autorise à réduire cette équation modulo $\mathfrak{p}$, ce qui conduit à :

$$\Pi^*(0, y_m) = 0 \text{ modulo } \mathfrak{p} \text{ pour une infinité d'entiers } m$$

et contredit donc la condition (a).

Remise le 18 novembre 1985.

RÉFÉRENCES BIBLIOGRAPHIQUES

[1] E. BOMBIERI, On Weil's « théorème de décomposition », *Amer. J. Math.*, 105, 1983, p. 295-308.

[2] J. W. S. CASSELS et A. FRÖHLICH, *Algebraic number theory*, Acad. Press, 1967.

[3] P. DÈBES, Quelques remarques sur un article de Bombieri concernant le théorème de décomposition de Weil, *Amer. J. Math.*, 107, 1985, p. 39-44.

[4] P. DÈBES, G-fonctions et théorème d'irréductibilité de Hilbert, *Acta Arithmetica*, 47, n° 4 (à paraître).

[5] M. FRIED, On Hilbert's irreducibility theorem, *J. Number Theory*, 6, 1974, p. 211-231.

[6] M. FRIED, On the Sprindzuk-Weissauer approach to universal Hilbert subsets, *Israel J.*, 51, n° 4, 1985.

[7] D. HILBERT, Uber die Irreduzibilität ganzer rationaler Funktionen mit ganzahligen Koeffizienten, *Gesammelte Abhandlungen*, Springer-Verlag, 1983, reimp., Chelsea, 2, n° 18, 1965, p. 264-286.

[8] S. LANG, *Fundamentals of diophantine geometry*, Springer-Verlag, 1983.

[9] A. SCHINZEL, On Hilbert's irreducibility theorem, *Acta Arithmetica*, 16, 1965, p. 334-340.

[10] A. SCHINZEL, *Selected topics on polynomials*, Ann. Arbor, the Univ. of Michigan press, 1982.

[11] J.-P. SERRE, Autour du théorème de Mordell-Weil, II, *Cours au Collège de France*, 1980/1981, Notes rédigées par M. Waldschmidt.

[12] V. G. SPRINDZUK, Diophantine equations involving unknown primes, *Trudy M.I.A.N., S.S.S.R.*, 158, 1981, p. 180-186.

[13] V. G. SPRINDZUK, Arithmetic specializations in polynomials, *J. reine und angew. Math.*, 340, 1983, p. 26-52.

E.R.A. n° 979 du C.N.R.S., Institut Henri-Poincaré,
11, *rue Pierre-et-Marie-Curie*, 75231 *Paris Cedex* 05.