BULLETIN DE LA S. M. F.

LAURENT DENIS

Géométrie et suites récurrentes

Bulletin de la S. M. F., tome 122, n° 1 (1994), p. 13-27

<http://www.numdam.org/item?id=BSMF_1994__122_1_13_0>

Bull. Soc. math. France,
122, 1994, p. 13–27.

GÉOMÉTRIE ET SUITES RÉCURRENTES

PAR

LAURENT DENIS (*)

RÉSUMÉ. — On s'intéresse au problème suivant : une variété algébrique peut-elle contenir énormément de termes d'une suite récurrente définie par un morphisme algébrique sans être stable sous une puissance de ce morphisme ? On répond à cette question quand le morphisme est un automorphisme de l'espace projectif ambiant. Sous certaines hypothèses de densité portant sur le nombre de points de l'intersection de la variété et de l'ensemble des termes de la suite récurrente, on aboutit au résultat pour un morphisme plat et surjectif.

ABSTRACT. — We ask the following question : can an algebraic variety contain many terms of a recurrence sequence defined by an algebraic morphism, without being stable under a power of that morphism ? We answer the question when the morphism is an automorphism of the projective ambiant space. Under some density assumption on the set of points which occurs in the intersection of the variety and the recurrence sequence we are also able to give the result for a surjective and flat morphism.

1. Motivations

Un cas particulier intéressant des récents théorèmes de G. FALTINGS (anciennement conjectures de Lang-Manin-Mumford) est le suivant : soit V une sous-variété algébrique d'une variété abélienne A, soit t_P la translation par un point P de A ; si P n'est pas de torsion et si

$$\{n \in \mathbb{N} ;\ (t_P)^n(0) = [n]P \in V\}$$

est infini, alors V contient le translaté d'une sous-variété abélienne de A. Quand A est remplacé par une variété algébrique X quelconque, on peut essayer d'imaginer un analogue à ce problème. Pour simplifier, on suppose $X = \mathbb{P}^N$ et on va regarder les morphismes de $\mathbb{P}^N$.

(*) Texte reçu le 4 mai 1992, révisé le 1 février 1993.
L. DENIS, Problèmes diophantiens, U.R.A 763 du CNRS, Université Pierre-et-Marie-Curie, tour 45–46, 5^e étage, 5 place Jussieu, 75252 Paris, France.

Classification AMS : 11G.

BULLETIN DE LA SOCIÉTÉ MATHÉMATIQUE DE FRANCE 0037–9484/1994/13/$ 5.00

On s'intéresse alors au problème suivant : une variété projective peut-elle rencontrer une infinité d'itérés d'un point sous l'action d'un morphisme de l'espace ambiant ? Énonçons cette question de manière plus précise.

Dans tout le texte, on entend par *variété* une sous-variété algébrique réduite de $\mathbb{P}^N$. Le morphisme α est un morphisme algébrique de $\mathbb{P}^N$ dans $\mathbb{P}^N$ et P est un point. On suppose que tous les $\alpha^i(P)$ (où $i \in \mathbb{N}$) sont distincts (ou, en d'autres termes, que P n'est pas un point périodique de α) et on désigne par

$$E_{V,P,\alpha} = \{i \in \mathbb{N};\ \alpha^i(P) \in V\}.$$

QUESTION 1. — A-t-on l'une des alternatives suivantes ?

a) $E_{V,P,\alpha}$ est fini.

b) Il existe des entiers $i_0 \geq 0$, $a > 0$ et une sous-variété W_P de V, de dimension ≥ 1, contenant $\alpha^{i_0}(P)$ telle que $\alpha^a(W_P) = W_P$.

RÉPONSE. — Non ! Tout au moins, peut-on construire des exemples où ceci est faux en caractéristique finie (voir paragraphe 3). Cependant, ce résultat est vrai pour un automorphisme en caractéristique nulle :

THÉORÈME 1. — *Soient V une variété, α un automorphisme de $\mathbb{P}^N$ et P un point de $\mathbb{P}^N$ définis sur un corps de caractéristique nulle. Si P n'est pas un point périodique de α, on a l'une des alternatives suivantes :*

a) *Le cardinal de $E_{V,P,\alpha}$ est fini.*

b) *Il existe des entiers $i_0 \geq 0$, $a > 0$ et une sous-variété W_P de V, de dimension ≥ 1, contenant $\alpha^{i_0}(P)$ telle que $\alpha^a(W_P) = W_P$.*

Pour le cas de caractéristique quelconque, on utilisera la notion suivante :

DÉFINITION 1. — Soit S une partie de l'ensemble des entiers naturels $\mathbb{N}$. On appelle $d(S)$, *densité banachique supérieure* de S, la limite supérieure des nombres $\operatorname{card}(I \cap S)/\operatorname{card}(I)$, où I décrit les intervalles de $\mathbb{N}$ et la longueur de I tend vers l'infini.

QUESTION 2. — A-t-on une des alternatives suivantes ?

a) La densité supérieure banachique de $E_{V,P,\alpha}$ est nulle.

b) Il existe des entiers $i_0 \geq 0$, $a > 0$ et une sous-variété W_P de V, de dimension ≥ 1, contenant $\alpha^{i_0}(P)$ telle que $\alpha^a(W_P) = W_P$.

On se propose de montrer au paragraphe 2 que — pour les automorphismes — la réponse est oui.

THÉORÈME 2. — *Soient V une variété, α un automorphisme de $\mathbb{P}^N$ et P un point de $\mathbb{P}^N$. Si P n'est pas un point périodique de α, on a l'une des alternatives suivantes :*

a) *La densité supérieure banachique de $E_{V,P,\alpha}$ est nulle.*

b) *Il existe des entiers $i_0 \geq 0$, $a > 0$ et une sous-variété W_P de V, de dimension ≥ 1, contenant $\alpha^{i_0}(P)$ telle que $\alpha^a(W_P) = W_P$.*

La méthode utilise un théorème de SZÉMÉREDI (cf. [S]) qui affirme l'existence d'une progression arithmétique dans un ensemble de densité banachique non nulle. Pour un morphisme quelconque, on utilisera une hypothèse de même nature, mais plus restrictive.

DÉFINITION 2. — Soient S une partie de l'ensemble des entiers naturels $\mathbb{N}$ et k un entier ≥ 1. On dira que S est *très dense à l'ordre k* si, pour tout entier ℓ, il existe des entiers $r, b > 0$ avec

$$r \leq \max\bigl(\mathrm{Log}^{(k)}(\ell), 1\bigr)$$

tels que $ar + b \in S$ pour $0 \leq a \leq \ell$, la notation $\mathrm{Log}^{(u)}$ désignant la u-ième itération du logarithme.

Une méthode inspirée de celle du lemme de zéro avec isogénies de [Hi] nous permet d'aboutir au paragraphe 3 au résultat suivant :

THÉORÈME 3. — *Soit V une variété. On suppose que α est un morphisme plat et surjectif et que $E_{V,P,\alpha}$ est très dense à l'ordre $2\dim V - 1$. Alors il existe un entier $a > 0$ et une sous-variété W_P de V de dimension ≥ 1, contenant un $\alpha^{i_0}(P)$, telle que $\alpha^a(W_P) = W_P$*

REMARQUE. — La preuve de SZÉMÉREDI (cf. [S]) n'est pas effective; il serait intéressant de voir si une hypothèse du type $d(E) \geq 1 - \varepsilon$ entraîne que l'ensemble E est très dense à l'ordre 1.

Nous verrons au paragraphe 2 que les THÉORÈMES 1 et 2 se déduisent de résultats concernant l'étude des zéros des suites récurrentes linéaires. Au paragraphe 3, on donne une seconde preuve du THÉORÈME 2 par une méthode géométrique. Cette méthode est adaptée au paragraphe 4 pour prouver le THÉORÈME 3.

L'auteur remercie le referee pour d'utiles suggestions lui ayant permis d'améliorer la rédaction et de corriger une faute dans une version préliminaire de ce texte.

2. Suites récurrentes

On montre dans la partie A, que le THÉORÈME 2 (resp. 1) implique le résultat de Bézivin sur les suites récurrentes en caractéristique finie (resp. le théorème de Skolem-Mahler-Lech en caractéristique nulle (voir [Le] et [Ma])). Puis dans la partie B, on prouve les THÉORÈMES 1 et 2 à partir des résultats correspondants sur les suites récurrentes.

A. Traduction des théorèmes 1 et 2.

Dans [B], BÉZIVIN prouve le théorème suivant :

THÉORÈME (cf. [B, p. 230 et rem., p. 233]). — *Soient K un corps commutatif de caractéristique quelconque, $u(n)$ une suite récurrente linéaire d'éléments de K. Il existe un entier $d \geq 1$, tel que, en notant*

$$A_r = \{k\,;\ u(kd+r) = 0\}, \qquad 0 \leq r \leq d-1,$$

on ait l'alternative suivante :

a) *A_r est de densité banachique nulle,*

b) $A_r = \mathbb{N}$.

Montrons rapidement comment on peut retrouver ce théorème, comme cas particulier du THÉORÈME 2. On se donne donc une suite récurrente $(u_n)_{n\in\mathbb{N}}$ déterminée par $(u_0, \ldots, u_{h-1})$ et une relation

$$u_{n+h} = a_{h-1}u_{n+h-1} + \cdots + a_0 u_n$$

où les a_i sont dans un corps K et $a_0 \neq 0$. On choisit alors pour α l'automorphisme de $(\boldsymbol{G_a})^h$ donné par la matrice compagnon :

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ \vdots & & \ddots & 0 \\ 0 & \cdots & \cdots & 1 \\ a_0 & a_1 & \cdots & a_{h-1} \end{pmatrix}.$$

On prolonge alors α à $\mathbb{P}^h$ en y plongeant naturellement $(\boldsymbol{G_a})^h$ et en posant :

$$\widetilde{\alpha}(X_0, \ldots, X_h) = \big(X_0, \alpha(X_1, \ldots, X_h)\big).$$

Soit V l'ensemble des zéros du polynôme X_1. Soient P_0 le point de coordonnées $(1, u_0, \ldots, u_{h-1})$ et $P_n = \alpha^n(P_0)$. Le point P_n est dans V si et seulement si u_n est nul.

a) On sait (voir [R] et [B, th. 8]) qu'on peut écrire u_n sous la forme

$$u_n = \sum_{1 \leq i \leq t} b_i (a_i)^n$$

où les b_i sont dans une extension finie de K et les a_i sont distincts. On peut alors choisir m tel que pour toutes les sous-suites u_{km+r} aucun quotient a_i/a_j ne soit une racine de l'unité. Pour retrouver le théorème de Bézivin, on est donc ramené au cas où la suite u_n vérifie cette hypothèse. Si la densité banachique de l'ensemble des indices où la suite s'annule est > 0, celle de l'ensemble des indices où les itérés de P_0 rencontrent V l'est également. La conclusion du THÉORÈME 2 dit qu'il existe une sous-variété W de V stable sous une puissance de α, ceci veut bien dire qu'on a une progression arithmétique $kd+r$ telle que $u_{kd+r} = 0$ pour tout k assez grand. Si on avait $d \geq 2$, on en déduirait que le quotient de deux des a_i est une racine de l'unité (comme dans [B, p. 233]) contrairement à ce qu'on a supposé. Donc $d = 1$ et on a bien retrouvé le théorème de Bézivin.

b) On sait qu'on peut écrire u_n sous la forme

$$u_n = \sum_{1 \leq i \leq t} P_i(n)(a_i)^n$$

où les P_i sont des polynômes et les a_i sont distincts. On peut alors choisir m tel que pour toutes les sous-suites u_{km+r} aucun quotient a_i/a_j ne soit une racine de l'unité. Pour retrouver le théorème de Skolem-Mahler-Lech, on est donc ramené au cas où la suite u_n vérifie cette hypothèse.

Si il y a une infinité d'indices où la suite u_n s'annule et si on est en caractéristique nulle, la conclusion du THÉORÈME 1 fournit une progression arithmétique $kd + r$ telle que $u_{kd+r} = 0$ pour tout k assez grand. Si on avait $d \geq 2$, on en déduirait que le quotient de deux des a_i est une racine de l'unité contrairement à ce qu'on a supposé. Donc $d = 1$ et on a bien retrouvé le théorème de Skolem-Mahler-Lech.

REMARQUE. — L'exemple de LECH donné dans [B, p. 230]

$$u_n = (1+z)^n - 1 - z^n,$$

donne alors la réponse négative de la question 1 (puisqu'il donne la même réponse pour les suites récurrentes). En effet en caractéristique $p > 0$, si z est bien choisi, cette suite ne s'annule que lorsque n est une puissance de p. Remarquons cependant que dans cet exemple les itérés du point P_0 ne sont pas distincts modulo l'action du Frobenius.

B. Réciproque et preuve des théorèmes 1 et 2.

Prouvons les THÉORÈMES 1 et 2 à partir de Skolem-Mahler-Lech et de [B]. Soit V sous-variété algébrique de $\mathbb{P}^N$, soient α un automorphisme de $\mathbb{P}^N$ et P un point. On note K un corps de définition de tous ces objets.

Soit donc un point P tel que tous les $\alpha^i(P)$ (où $i \in \mathbb{N}$) sont distincts. On suppose d'abord (THÉORÈME 1) que $E_{V,P,\alpha} = \{i \in \mathbb{N}\,;\ \alpha^i(P) \in V\}$ est infini et que la caractéristique de K est nulle. Il existe un ouvert affine U de la forme $U = \{(X_0, \ldots, X_N)\,;\ X_i \neq 0\}$ tel que si on remplace V par $V_1 = V \cap U$, alors $E_{V_1,P,\alpha}$ est encore infini. Comme les automorphismes de $\mathbb{P}^N$ forment $\mathrm{PGL}_N(K)$, α est représenté sur l'ouvert affine U par une matrice $M \in \mathrm{GL}_N(K)$. La décomposition en sous-espaces cycliques montre qu'il existe une matrice de passage P telle que $P^{-1}MP$ soit une matrice formée de blocs de matrices compagnons (du type apparaissant dans la partie A). Quitte à changer V_1 en PV_1P^{-1}, on peut supposer que M est de cette forme. Les itérés de M définissent alors des suites récurrentes $u_1(n), \ldots, u_k(n)$ (où k est le nombre de blocs dans la matrice). La variété affine V_1 est définie par un nombre fini de polynômes $P_1, \ldots, P_s$. Il y a donc une infinité d'entiers n tels que :

$$P_1(u_1(n), \ldots, u_k(n)) = 0, \ldots, P_s(u_1(n), \ldots, u_k(n)) = 0.$$

Comme tout polynôme en des suites récurrentes est encore une suite récurrente, on a ainsi s suites récurrentes $v_1(n), \ldots, v_s(n)$ s'annulant simultanément en une infinité d'entiers. Observons alors que toutes les valeurs prises par ces suites récurrentes sont contenues dans une extension de type fini de $\mathbb{Q}$. Il existe alors un polynôme Q homogène en s variables n'ayant que le zéro trivial sur cette extension (voir remarque 2 ci-dessous). Mais $Q(v_1(n), \ldots, v_s(n))$ est encore une suite récurrente ; le théorème de Skolem-Mahler-Lech nous dit qu'il existe une progression arithmétique où elle s'annule. Comme Q n'a que le zéro trivial chacune des suites $v_i(n)$ (avec $1 \leq i \leq s$) s'annule également sur cette progression arithmétique. On a donc tout une progression arithmétique dans $E_{V,P,\alpha}$. Autrement dit, il existe des entiers naturels $r > 0$ et $b \geq 0$ tels que $\alpha^{ar+b}(P) \in V$ pour tout a dans $\mathbb{N}$.

Or d'une manière générale (pour un morphisme algébrique β quelconque) si V contient tous les itérés d'un point P, alors il existe W, stable sous β contenue dans V et passant par un itéré de P : il suffit de prendre pour W l'adhérence de Zariski de l'orbite du point P sous β.

Ici, on prend donc le morphisme $\beta = \alpha^a$ et le point $\alpha^b(P)$. On obtient alors une variété W_P telle que $\beta(W_P) \subset W_P$. Comme β est un isomorphisme on vérifie bien qu'on a la conclusion du THÉORÈME 1.

Passons au THÉORÈME 2. En caractéristique $p > 0$, la même preuve convient en remplacant le nombre infini de termes nuls d'une suite récurrente par un ensemble de densité banachique > 0. La sous-additivité de la densité banachique permet encore de se ramener au cas affine. Enfin, le théorème de Skolem-Mahler-Lech est remplacé par celui de Bézivin cité au début de la partie A.

REMARQUE 1. — Pour montrer qu'il existe un polynôme Q homogène en s variables n'ayant que le zéro trivial sur un corps de type fini, on pourra faire appel aux notions de dimension diophantienne. L'exemple suivant m'a été fourni par Y. ANDRÉ :

• Si la caractéristique de K est différente de 2, il est facile de voir qu'il existe α dans K qui n'est pas un carré, on prend alors :

$$Q(X_1, \ldots, X_s) = \left(\left((X_1)^2 - \alpha(X_2)^2\right)^2 - \cdots\right)^2 - \alpha(X_s)^2.$$

• Si la caractéristique de K est égale à 2, le même argument marche avec des cubes à la place des carrés.

3. Cas des automorphismes

Dans ce paragraphe on redémontre le THÉORÈME 2 sans utiliser les résultats de Bézivin. Rappelons d'abord quelques définitions. Pour tout polynôme $Q \neq 0$, on note $Z(Q)$ le diviseur de ses zéros et on désigne par $\deg V$ le degré d'une variété V de $\mathbb{P}^N$ (non nécessairement irréductible).

On désigne par α un automorphisme linéaire de $\mathbb{P}^N$. Voici d'abord quelques lemmes préliminaires :

LEMME 1. — *Pour toute variété V de $\mathbb{P}^N$ on a* $\deg V = \deg \alpha(V)$.

Preuve. — Clair.

LEMME 2. — *Soient E un ensemble, β une application de E dans E et u, v deux entiers. On suppose que E contient $\{\beta^i(P)\,;\ 0 \leq i \leq v\}$ et que tous les $\beta^i(P)$ sont distincts. Dans ces conditions, il existe u applications $\gamma_1, \ldots, \gamma_u$, puissances distinctes de β telles que pour $1 \leq j \leq u$,*

$$\left\{\gamma_j^i(P)\,;\ 0 \leq i \leq v/u\right\}$$

est encore dans E.

Preuve. — On prend $\gamma_j = \beta^j$.

Remarquons d'abord que sous les hypothèses du THÉORÈME 2, on a forcément $\dim V \geq 1$ (rappelons que les $\alpha^i(P)$ sont distincts). Comme $d(E_{V,P,\alpha}) > 0$, d'après les résultats de Szémeredi [S], il existe des progressions arithmétiques arbitrairement grandes dans $E_{V,P,\alpha}$. Pour tout entier $\ell > 0$, il existe des entiers naturels $r > 0$ et $b \geq 0$ tels que l'on ait $\alpha^{ar+b}(P) \in V$ pour $0 \leq a \leq \ell$. Autrement dit :

$$(*) \quad \begin{cases} \textit{Pour tout entier } \ell > 0, \textit{ il existe } \beta \textit{ (égal à } \alpha^r) \textit{ morphisme} \\ \textit{de degré 1 et un point } Q \textit{ (égal à } \alpha^b(P)) \textit{ de } \mathbb{P}^N \textit{ tels que l'on} \\ \textit{ait } \beta^a(Q) \in V \textit{ pour } 0 \leq a \leq \ell. \end{cases}$$

Explicitons d'abord le cas plus simple d'une courbe. Soit C une courbe non nécessairement irréductible. Considérons

$$C' = C_1 \cup \cdots \cup C_t$$

la réunion des composantes de C contenant au moins un itéré de P sous l'action de α. A tout entier ℓ est associé un β de la forme α^r (voir (*)). Pour $\ell \geq (\deg C)^2 + 1$, considérons alors la variété $C' \cap \beta(C')$. Si pour un β cette variété est de dimension 0, Bézout et le LEMME 1 donnent :

$$\ell + 1 - 1 \leq (\deg C)^2.$$

On a une contradiction, donc C' et $\beta(C')$ ont une composante commune. La construction précédente donne pour chaque β un couple (i_β, j_β) tel que $C_{i_\beta} = \beta(C_{j_\beta})$. Si pour un β on a $i_\beta = j_\beta$ la composante $C_{i_\beta} = W$ est stable et satisfait la conclusion du théorème. Sinon

$$\operatorname{card}\{(i,j)\,;\ i \neq j \text{ et } 1 \leq i,j \leq t\} = t^2 - t$$

et dès qu'on prend strictement plus de $(t^2 - t)$ automorphismes de type β, un couple de composantes va être joint par deux β différents : il existe β_1 et β_2 tels que

$$C_{i_{\beta_1}} = \beta_1(C_{j_{\beta_1}}), \quad C_{i_{\beta_2}} = \beta_2(C_{j_{\beta_2}})$$

avec $(i_{\beta_1}, j_{\beta_1}) = (i_{\beta_2}, j_{\beta_2})$. On en déduit $(\beta_2)^{-1} \circ \beta_1(C_{j_{\beta_1}}) = (C_{j_{\beta_1}})$. En résumé, ce qui précède est réalisé dès qu'il existe plus de $(t^2 - t)$ morphismes β associé à un $\ell \geq (\deg C)^2 + 1$. On remarque que $t \leq \deg C$ et on applique alors le LEMME 2 avec

$$E = V, \quad u = \deg(C)^2 - \deg C + 1 \quad \text{et} \quad v = u\big((\deg C)^2 + 1\big).$$

REMARQUE. — On peut aussi conclure de la façon suivante : comme il y a au plus $\deg C$ composantes de dimension 1 dans $C' \cap \beta(C')$, dès qu'on dispose de plus de $(\deg C)^2$ morphismes β tels que cette variété soit de dimension 1, alors une de ces composantes est stable. Si il existe β, puissance de α, et Q de la forme $\alpha^b(P)$ tels que l'ensemble

$$\{\beta^i(Q)\,;\ 0 \leq i \leq (\deg C)^4\}$$

soit dans C, cette condition est réalisée.

On peut obtenir des résultats avec une effectivité comparable pour des intersections complètes.

Passons au cas général (sans souci d'effectivité). Donnons maintenant la preuve du THÉORÈME 2. D'après (*), V contient les ℓ_β premiers itérés d'un point sous l'action d'un automorphisme β. On va supposer que ℓ_β est assez grand en fonction de $\deg V$ et montrer qu'une sous variété de V est stable sous une puissance de β.

Le théorème de van der Waerden affirme qu'il existe une fonction $f(k,r)$ telle que si S est un sous-ensemble de $\mathbb{N}$ qui contient plus de $f(k,r)$ éléments consécutifs, toutes ses partitions en r parties comportent un élément qui contient plus de k entiers en progression arithmétique (cf. [G.R]).

On applique d'abord ce théorème en prenant $r = r_0 =$ le nombre de composantes de V. On obtient alors X_0, composante irréductible de V contenant plus de k_0 éléments consécutifs de la suite des itérés de P sous une puissance β_0 de β.

Soit alors $X_1 = X_0 \cap \beta_0^{-1}(X_0)$. Si X_1 et X_0 sont de la même dimension $d_0 \geq 1$, elles sont égales, X_0 est stable sous β_0 donc sous un itéré de α et passe par un itéré de P. Sinon X_1 est de dimension strictement inférieure et est composé de moins de $(\deg X_0)^2$ composantes par le théorème de Bézout raffiné [F, exercice 12-3-1] (Remarquons au passage que comme on travaille ici avec des isomorphismes on pourrait en fait montrer que si V est incomplétement définie par des équations de degré $\leq D, X_1$ l'est aussi et appliquer la proposition 3.3 de [P].) Si V ne contient aucune sous-variété stable passant par un itéré de P, on définit par récurrence la suite $(X_i)_{i\in\mathbb{N}}$ et les automorphismes β_i :

$$X_{2(i-1)} \text{ est irréductible,} \quad X_{2i-1} = X_{2(i-1)} \cap (\beta_{i-1})^{-1}\big(X_{2(i-1)}\big).$$

L'hypothèse faite sur V entraîne $\dim X_{2i-1} < \dim X_{2(i-1)}$; on applique le théorème de van der Waerden avec $r = r_{i-1} =$ nombre de composantes irréductibles de $X_{2i-1} \leq (\deg X_{(i-1)})^2$ et on définit X_{2i} comme étant

une composante irréductible de $X_{2(i-1)}$ contenant plus de k_{i-1} éléments consécutifs de la suite des itérés de P sous une puissance β_i de β_{i-1}.

La suite $(\dim(X_i))_{i\in\mathbb{N}}$ est strictement décroissante; on aboutit alors à une contradiction : V contient une sous-variété stable passant par un itéré de P.

Le point essentiel de cette preuve est qu'à chaque étape le nombre de composantes est majorable indépendemment de β. Ce ne sera plus le cas au paragraphe suivant pour les morphismes de degré > 1.

4. Morphismes de degré supérieur à 1

Rappelons les hypothèses du THÉORÈME 3.

On suppose dans ce paragraphe que α est un morphisme plat et surjectif (voir [H]) *et que $E_{V,P,\alpha}$ est très dense à l'ordre* $2\dim V - 1$.

On sait qu'un morphisme Ψ de $\mathbb{P}^N$ dans $\mathbb{P}^N$, non constant s'écrit

$$\Psi = \sigma_d \circ p \circ i$$

où σ_d le plongement d-uple de $\mathbb{P}^N$ dans $\mathbb{P}^M$, avec $M = \binom{N+d}{d} - 1$, p est une projection linéaire sur $\mathbb{P}^m$ et i est un isomorphisme de $\mathbb{P}^m$ (cf. [H, exercice 7.3]).

Les hypothèses sur α reviennent à supposer $m = N$ et α plat.

Montrons tout de suite que, pour tout entier t, il existe des ensembles très denses à l'ordre t et de densité nulle (banachique et naturelle). Ceci permet en particulier de voir qu'on a pas forcément une progression arithmétique dans un ensemble très dense.

EXEMPLE. — Soit $S = \bigcup_{N=f(k)} \{aN\}_{1\le a\le\phi(N)}$ où les fonctions f et ϕ sont construites par récurrence vérifiant :

(i) $f(k+1) > \max\big(f(k)\phi(k),\, k^2\phi(k)\big)$ pour $k \ge 1$,

(ii) $f(k)$, $\phi(k) \in \mathbb{N}$ sont croissantes et vérifient $\phi(k) \ge e^{e^{\cdot^{\cdot^{e^k}}}}$, où on a pris t itérations de l'exponentielle.

Alors S est de densité banachique nulle et contient des progressions arithmétiques de longueur ℓ arbitrairement grande et de raison

$$r \le \mathrm{Log}^{(t)}\, \ell.$$

Preuve. — Par construction, la propriété annoncée sur les suites arithmétiques est vraie. Prenons un intervalle quelconque de longueur u,

il est de la forme $[e, e+u]$. On dispose de l'inclusion :

$$[e, e+u] \cap S \subset \bigcup_{k \in F} [f(k), f(k)\phi(k)] \cap S$$

où $F = \{k\,;\ [f(k), f(k)\phi(k)] \cap [e, e+u] \neq \emptyset\}$. Si F est non vide, on désigne par k_1 (resp. k_2) le plus petit (resp. le plus grand) élément de F. Il vient :

$$\begin{aligned}
&\operatorname{card}\{[e, e+u] \cap S\} \\
&\quad \leq \operatorname{card}\{[e, e+u] \cap [f(k_1), f(k_1)\phi(k_1)] \cap S\} \\
&\qquad + \sum_{k_1 < k < k_2} \phi(k) + \operatorname{card}\{[e, e+u] \cap [f(k_2), f(k_2)\phi(k_2)] \cap S\}; \\
&f(k_1) \leq e \leq f(k_1)\phi(k_1), \quad f(k_2) \leq e+u \leq f(k_2)\phi(k_2).
\end{aligned}$$

D'où l'on tire :

$$\frac{\operatorname{card}\{[e, e+u] \cap S\}}{\operatorname{card}\{[e, e+u] \cap \mathbb{N}\}} \leq (k_2 - k_1)\frac{\phi(k_2 - 1)}{f(k_2) - f(k_1)\phi(k_1)} + \frac{1}{u}\left[\frac{[e+u]}{f(k_2)}\right].$$

On en déduit :

$$\begin{aligned}
\frac{\operatorname{card}\{[e, e+u] \cap S\}}{\operatorname{card}\{[e, e+u] \cap \mathbb{N}\}} \leq (k_2 - k_1)&\frac{\phi(k_2 - 1)}{f(k_2) - f(k_1)\phi(k_1)} \\
&+ \frac{1}{f(k_2) - f(k_1)\phi(k_1)}\phi(k_2).
\end{aligned}$$

Quand u tend vers l'infini, k_2 tend également vers l'infini et le quotient précédent tend vers 0.

Pour la preuve du THÉORÈME 3, on utilisera l'analogue affaibli suivant du LEMME 1 :

LEMME 3. — *Il existe un entier $q \geq 1$ tel que pour tout entier $i \geq 0$:*

$$\deg \alpha^{-i}(V) = q^{i(N - \dim V)} \deg V.$$

Preuve. — Soit H un hyperplan de $\mathbb{P}^N$. Comme α est représenté par des polynômes de degré q (où $q = d$ avec les notations du début du paragraphe 4) sans zéro commun, $\alpha^*(H)$ est linéairement équivalent à qH et $\beta^*(H)$ est linéairement équivalent à $q^i H$, d'où l'on tire :

$$\text{(e)} \qquad \beta^*\big(V \cdot (H)^{\dim V}\big) = \beta^*(V) \cdot (q^i H)^{\dim V}.$$

Comme pour tout zéro-cycle Z, le degré de $\beta^*(Z)$ est $q^{iN}\deg Z$; on en déduit $\deg\beta^*(V) = q^{i(N-\dim V)}\deg V$. Enfin, on conclut en remarquant que comme α est plat, le degré de $\beta^*(V)$ est celui de $\beta^{-1}(V)$ [F, lemme 1.7.1].

Preuve du théorème 2. — D'après l'hypothèse de densité, V contient les ℓ_β premiers itérés d'un point sous l'action d'un morphisme β. On va supposer que ℓ_β est assez grand en fonction de $\deg V$ et montrer qu'une sous-variété de V est stable sous une puissance de β.

D'après le théorème de van der Waerden, on peut supposer V irréductible (cette étape n'est pas absolument nécessaire mais comme le degré de β n'intervient pas ici, cette réduction du problème est naturelle).

On considère les suites de variétés $(X_i)_{i\in\mathbb{N}}$ et $(X'_i)_{i\in\mathbb{N}}$ définies par les relations de récurrence :

- $X_0 = V$, $X'_0 = X_0 \cap \beta^{-1}(X_0)$;
- pour $i \geq 1$, X_i est l'union des composantes de X'_{i-1} qui passent par au moins un itéré de P et $X'_i = X_i \cap \beta^{-1}(X_i)$.

Soit N_i, le nombre total de composantes de X_i.

LEMME 4.

a) $(X_i)_{i\in\mathbb{N}}$ *est une suite décroissante.*

b) $\beta(X_{j+1}) \subset X_j$ *pour tout* $j \geq 0$,

c) $N_i \leq (N_{i-1})^2(\deg(X_{i-1}))^2 q^{rN}$,

d) $\deg(X_{i-1}) \leq (N_{i-2})^2(\deg(X_{i-2}))^2 q^{rN}$,

e) $N_i \leq (\deg V)^{4^{i+1}} q^{4^i rN}$.

Preuve. — Les propriétés a) et b) sont claires.

Pour prouver c), on écrit $X_{i-1} = Y_1 \cup \cdots \cup Y_{N_{i-1}}$ où les Y_i sont irréductibles. Comme β est plat, $\beta^{-1}(Y_i)$ est équidimensionnelle pour $1 \leq i \leq N_{i-1}$ (théorème de Cohen-Seidenberg, cf. [H, 9.5 et 9.6]).

Or $X'_{i-1} = \bigcup_{i,j}(Y_i \cap \beta^{-1}(Y_j))$ et comme $Y_i \cap \beta^{-1}(Y_j)$ est une intersection de deux variétés équidimensionnelles, le nombre de composantes de cette intersection est plus petit que $\deg Y_i \deg\beta^{-1}(Y_j)$ (cf. [F, exercice 12.3.1]).

Le LEMME 3 montre que ce dernier degré est $\leq (\deg(X_{i-1}))^2 q^{rN}$. D'où l'on déduit que le nombre de composantes de X_i est plus petit que $(N_{i-1})^2(\deg(X_{i-1}))^2 q^{rN}$.

Le d) est traité de la même manière.

On déduit le e) de c) et d).

Supposons que V ne contienne aucune sous-variété stable passant par un itéré de P et montrons que la suite $(X_i)_{i\in\mathbb{N}}$ n'a qu'un nombre fini (majorable par une fonction ne dépendant que du degré de V) de termes consécutifs de même dimension.

Supposons que pour des indices j et k on ait

$$X_j \supset X_{j+1} \supset \cdots \supset X_{j+k}$$

avec chaque variété de cette suite de dimension n. Sous l'hypothèse précédente, on veut majorer k en fonction de $\deg V$ et de j.

Comme $\beta(X_{j+1}) \subset X_j$, on a $\beta^v(X_{j+k}) \subset X_j$ pour tout $1 \leq v \leq k$. Soit Y une composante de X_{j+k} de dimension n ; on a encore $\beta^v(Y) \subset X_j$. Les $\beta^v(Y)$ sont des composantes de X_j, le e) du LEMME 4 nous dit alors que si $k > (\deg V)^{4^{j+1}} q^{4^j rN}$, il existe $v_1 > v_2$ tels que $\beta^{v_1}(Y) = \beta^{v_2}(Y)$. La variété $\beta^{v_2}(Y)$ est donc stable par $\beta^{v_1-v_2}$ et c'est une sous-variété de V qui passe par un itéré de P.

Pour faire chuter la dimension de $V = X_0$ de 1, il suffit de prendre $k_1 = (\deg V)^4 q^{rN} + 1$. Pour arriver en dimension $\dim V - i$, il suffit d'après l'inégalité précédente de prendre :

$$k_i = (\deg V)^{4^{(k_1+\cdots+k_{i-1})+1}} q^{4^{(k_1+\cdots+k_{i-1})} rN} + 1.$$

A chaque étape à partir de la dimension $\dim V - 1$, on utilise donc deux exponentielles d'écart entre la raison et la longueur de la progression arithmétique. Pour arriver en dimension zéro, il en a donc fallu $2\dim V - 1$. On a alors une contradiction avec l'hypothèse de densité en comptant le nombre de points de la variété de dimension zéro obtenue.

5. Exemples liés au théorème 3

a) Hypersurfaces.

La version effective que l'on montre du THÉORÈME 3 permet d'avoir le type d'énoncé suivant : soit P un polynôme absolument irréductible, on suppose qu'il existe un point $(x_0, \ldots, x_N)$ tel que

$$P\big((x_0)^{2^k}, \ldots, (x_N)^{2^k}\big) = 0$$

pour tout k dans un ensemble très dense à l'ordre $2N - 3$; alors cette propriété est vraie pour tout k dans une progression arithmétique (le morphisme défini par $(x_0, \ldots, x_N) \mapsto ((x_0)^2, \ldots, (x_N)^2)$ est plat car lisse si l'on suppose la caractéristique de K différente de 2).

Remarquons ici que l'on peut alors caractériser les polynômes P qui interviennent ici (cf. [M]).

b) Exemples liés aux t-modules.

On a proposé dans [D] des analogues sur les t-modules aux conjectures de Lang-Manin-Munford. On rappelle ici le cas particulier analogue à notre exemple de l'introduction sur les théorèmes de Faltings.

On rappelle qu'un t-module E, de rang d et de dimension n est la donnée d'un triplet $((\boldsymbol{G_a})^n, \phi, \theta)$ où :

- $(\boldsymbol{G_a})^n$ est le groupe additif de dimension n;
- ϕ est un homomorphisme d'anneau injectif de $\mathbf{F}_q[t]$ dans $\mathrm{End}_{\mathbf{F}_q}((\boldsymbol{G_a})^n)$ déterminé par

$$\phi(t) = a_0 F^0 + \cdots + a_d F^d \quad (\text{où } F \text{ est le Frobenius}),$$

avec $a_0, \ldots, a_d \in M_{n\times n}(C)$, où a_0 a pour seule valeur propre un élément θ transcendant sur $\mathbf{F}_q$, où a_d est inversible et où C est le complété d'une clôture algébrique de $\mathbf{F}_q((1/T))$.

On plonge alors naturellement $(\boldsymbol{G_a})^n$ dans $\mathbb{P}^n$ et on prolonge de même ϕ à $\mathbb{P}^n$. La condition a_d inversible assure le fait que ϕ est un morphisme surjectif représenté par des polynômes de degré q^d. La condition sur a_0 donne la platitude. L'analogue à l'exemple de l'introduction est la :

CONJECTURE. — *Soit P un point de E, si V est une sous-variété de E, on a : si $\{a \in \mathbf{F}_q[T]\,;\ \phi(a)P \in V\}$ est infini, alors il existe un élément $b \in \mathbf{F}_q[T]$ tel que V contienne un b-module.*

Le théorème 3 joint à une extension immédiate du lemme 4 de [D] (ici on obtient seulement un a^k-module dans la conclusion) fournit alors le corollaire suivant :

COROLLAIRE 1. — *Soient P un point de E et $a \in (\mathbf{F}_q[T])^*$ et V une sous-variété de E; on a : si $\{n \in \mathbb{N}\,;\ \phi(a^n)P \in V\}$ est très dense à l'ordre $2\dim V - 1$, alors il existe un entier k tel que V contienne un a^k-module.*

REMARQUE. — Dans le cas où le T-module est produit de modules de Drinfeld, on a vu dans [D] qu'un b-module est nécessairement un T-module.

BIBLIOGRAPHIE

[B] BÉZIVIN (J.P.). — *Suites récurrentes linéaires en caractéristique non nulle*, Bull. S.M.F., t. **115**, 1987, p. 227–239.

[D] DENIS (L.). — Géométrie diophantienne sur les modules de Drinfeld, *The arithmetic of functions fields*, Proceedings of the Workshop at the Ohio State University, 1992, p. 285–302.

[F] FALTINGS (G.). — *Diophantine approximation on abelian varieties*, Annals of Math, t. **133**, 1991, p. 549–576.

[F] FULTON (W.). — *Intersection theory*. — Springer Verlag, 1984.

[G.R.] GRAHAM (R.L.) and ROTHSCHILD (B.L.). — *A short proof of van der Waerden's theorem on arithmetic progression*, Proc. Amer. Math. Soc., t. **42**, 1974, p. 385–386.

[H] HARTSHORNE (R.). — *Algebraic geometry*. — Springer Verlag, 1977.

[Hi] HINDRY (M.). — *Géométrie et hauteurs dans les groupes algébriques*, Thèse de l'université Paris 6, 1987.

[L] LAURENT (M.). — *Équations exponentielles polynômes et suites récurrentes linéaires*, Astérisque, t. **147-148**, 1987, p. 121–139.

[Le] LECH (C.). — *A note on recurring series*, Ark. Mat.1, t. **2**, p. 417–421.

[M] MASSER (D.W.). — *A vanishing theorem for power series*, Invent. Math., t. **67**, 1982, p. 275–296.

[Ma] MAHLER (K.). — *On the Taylor coefficients of rational functions*, Proc. Cambridge Phil. soc, t. **52**, 1956, p. 39–48.

[ML] BROWN (M.L.). — *Density of rational and integral points on algebraic varieties*, Ann. Sci. École Norm. Sup., t. **25**, 1992, p. 135–178.

[P] PHILIPPON (P.). — *Lemmes de zéros sur les groupes algébriques commutatifs*, Bull. S.M.F., t. **114**, 1987. Voir aussi *Errata et addenda*, Bull. S.M.F., t. **115**, p. 397–398, 1987, p. 355–383.

[R] REUTENAUER (C.). — *Sur les éléments inversibles de l'algèbre de Hadamard des séries rationnelles*, Bull. S.M.F., t. **110**, 1982, p. 225–232.

[S] SZÉMÉREDI (E.). — *On sets of integers containing no k elements in arithmetic progression*, Acta Arithmetica, t. **27**, 1975, p. 199–245.