COMPOSITIO MATHEMATICA

JEAN-PAUL BÉZIVIN

Les suites q-récurrentes linéaires

Compositio Mathematica, tome 80, n° 3 (1991), p. 285-307

<http://www.numdam.org/item?id=CM_1991__80_3_285_0>

Compositio Mathematica **80**: 285–307, 1991.

Les suites q-récurrentes linéaires

JEAN-PAUL BÉZIVIN
Université de Caen, Mathématiques, Esplanade de la Paix, 14032 Caen Cedex, France

Received 12 June 1990; accepted 25 February 1991

1. Introduction

Soit K un corps commutatif, et q un élément non nul de K. On note dans la suite $R(K, q)$ l'ensemble des suites $u(n)$ d'éléments de K vérifiant une relation de récurrence de la forme:

$$\sum_{i=0}^{t} Q_i(q^n)u(n+i) = 0 \tag{1-1}$$

où les Q_i sont des polynômes de $K[x]$, avec Q_t non nul.

Ce type de relation de récurrence est analogue aux relations de récurrences vérifiées par les coefficients de taylor des fractions rationnelles régulières en zéro (les polynômes Q_i sont alors remplacés par des constantes, de sorte que toute suite récurrente linéaire à coefficients constants est un élément de $R(K, q)$ pour toute valeur de q), et aussi aux relations de récurrences vérifiées par les coefficients de taylor des séries formelles solutions d'une équation différentielle linéaire à coefficients polynômes (les facteurs $Q_i(q^n)$ doivent alors être remplacés par des polynômes en la variable n).

Si nous considérons l'ensemble $F(K, q)$ des séries formelles $\psi(x) = \Sigma u(n)x^n$ vérifiant une équation fonctionnelle de la forme:

$$\sum_{i=0}^{s} P_i(x)\psi(q^i x) = 0 \tag{1-2}$$

où les P_i sont des polynômes de $K[x]$ avec P_s non nul, il est facile de voir que les séries de $F(K, q)$ sont les séries génératrices des suites de $R(K, q)$.

La théorie analytique des équations fonctionnelles (1-2) a déjà été étudiée par Trjitzinsky, ([18]), dans le cas où les $P_i(x)$ sont des séries à coefficients dans $\mathbb{C}$ de rayon de convergence non nul, et $P_s(x)$ est égal à un.

Dans cet article, nous nous proposons d'étudier certains problèmes relatifs aux suites de $R(K, q)$ ou aux fonctions de $F(K, q)$, et plus ou moins bien résolus dans le cadre des suites récurrentes linéaires à coefficients constants, ou des

séries formelles vérifiant une équation différentielle linéaire à coefficients polynômes.

Plus précisément, dans la partie II nous démontrons quelques propriétés élémentaires qui nous serviront plus loin.

Dans la partie III, nous examinons ce que l'on peut dire de l'ensemble des indices n tels que $u(n) = 0$, avec u dans $R(K, q)$. Ce problème est bien résolu, dans le cadre des suites récurrentes linéaires à coefficients constants, par le théorème de Skolem-Mahler-Lech ([13]), et un peu moins bien dans le cadre des séries formelles vérifiant une équation différentielle linéaire à coefficients polynômes ([4], [11]).

Dans la partie IV, nous étudions le comportement des éléments $u(n)$ de $R(K, q)$ vis à vis de leur décomposition multiplicative. Ce problème est très bien résolu dans le cadre des suites récurrentes linéaires à coefficients constants ([2], [7], [14]) et bien résolu dans le cadre des séries formelles solutions d'une équation différentielle linéaire à coefficients polynômes ([3]).

Les parties V et VI présentent une analogue de la conjecture de Grothendieck pour les équations différentielles linéaires à coefficients polynômes. Nous avons fort peu de résultats complets sur cette conjecture.

La partie VII présente et démontre une version affaiblie de la conjecture précédente.

Nous supposerons toujours, sauf mention explicite du contraire, que q n'est pas une racine de l'unité quand nous nous trouverons en caractéristique nulle.

2. Propriétés élémentaires de $R(K, q)$

Nous avons tout d'abord quelques propriétés formelles simples:

Tout d'abord une remarque évidente, à savoir que $R(K, q)$ est égal à $R(K, 1/q)$ et que $R(K, q^e)$ est inclus dans $R(K, q)$ pour tout e dans $\mathbb{Z}$.

PROPOSITION 2.1. *On suppose que le corps commutatif K est de caractéristique nulle, et que q n'est pas une racine de l'unité. Alors:*

(a) *L'ensemble $F(K, q)$ est une q-algèbre de séries formelles.*
(b) *L'ensemble $R(K, q)$ est sous-K algèbre de l'algèbre de suites d'éléments de K.*
(c) *$F(K, q)$ est stable par dérivation.*
(d) *Soit $\psi(x)$ un élément de $F(K, q)$ et d un entier positif, r appartenant à $\{0, \ldots, d-1\}$. Alors la série $\eta(x)$ définie par $x^r\eta(x^d) = \Sigma\, \zeta^{-r}\psi(\zeta x)$, où la sommation a lieu sur les racines d'ièmes de l'unité, est un élément de $F(K, q)$.*

DÉMONSTRATION. Soit ψ un élément de $F(K, q)$. On considère le sous-espace vectoriel engendré sur $K(x)$ par les $\psi(q^i x)$, espace vectoriel que nous noterons $\langle\psi\rangle$. Dire que ψ appartient à $F(K, q)$ est équivalent à dire que $\langle\psi\rangle$ est de dimension finie sur $K(x)$.

Soient ψ_1 et ψ_2 dans $F(K, q)$; il est alors facile de voir que $\langle \psi_1 + \psi_2 \rangle$ est inclus dans $\langle \psi_1 \rangle + \langle \psi_2 \rangle$, et $\langle \psi_1 \psi_2 \rangle$ dans le sous-espace vectoriel engendré par $\langle \psi_1 \rangle \langle \psi_2 \rangle$. Par suite, $\langle \psi_1 + \psi_2 \rangle$ et $\langle \psi_1 \psi_2 \rangle$ sont de dimension finie, ce qui démontre (a).

(b) La démonstration de (b) est à peu près semblable à celle de (a), à ceci près que nous considérons au lieu des éléments de $R(K, q)$, les germes de ces suites à l'infini, comme espace vectoriel sur le corps $K(q^n)$ qui, puisque q n'est pas une racine de l'unité, est isomorphe à $K(x)$.

(c) Soit $\psi(x) = \Sigma u(n)x^n$ dans $F(K, q)$. On a $\psi'(x) = \Sigma (n + 1)u(n + 1)x^n$. Il est clair que la série $\Sigma u(n + 1)x^n$ est dans $F(K, q)$; d'après (b), le produit des deux suites $u(n + 1)$ et $n + 1$, qui sont dans $R(K, q)$, est encore dans $R(K, q)$, d'où le résultat.

(d) On a avec des notations déjà introduites $\eta(x) = \Sigma u(kd + r)x^k$. Soit $h_r(x) = \Sigma x^{kd+r} = \Sigma v_r(n)x^n = x^r/(1 - x^d)$, qui est un élément de $F(K, q)$.

Alors la suite égale à $u(n)$ si n est de la forme $kd + r$ et zéro sinon est égale à $u(n)v_r(n)$, et donc dans $R(K, q)$. Par suite $\eta(x^d)$ est dans $F(K, q)$. On écrit une relation fonctionnelle du type (1-2) vérifiée par $\eta(x^d)$:

$$\sum_{i=0}^{s} P_i(x)\eta(q^{id}x^d) = 0,$$

avec P_s non nul.

Soit m un entier tel que le coefficient de x^m dans P_s soit non nul; en ne conservant dans les polynômes P_i que les puissances de x dont les exposants sont congrus à m modulo d, on a une nouvelle relation avec des polynômes en x^d; remplaçant dans cette relation x^d par x, on voit que η appartient à $F(K, q)$.

Nous allons maintenant démontrer quelques propriétés analytiques des éléments de $F(K, q)$. Nous prendrons donc $K = \mathbb{C}$ ou $K = \mathbb{C}_p$, où p est un nombre premier, et $\mathbb{C}_p$ le complété d'une clôture algébrique du corps $\mathbb{Q}_p$ des nombres p-adiques.

Il est clair qu'un élément de $F(\mathbb{C}, q)$ ou de $F(\mathbb{C}_p, q)$ peut avoir un rayon de convergence nul; c'est le cas pour la série $\Sigma q^{n(n+1)/2}x^n$, si q est un élément de module plus grand que un.

Le résultat suivant donne une condition suffisante pour qu'un opérateur fonctionnel L de la forme (1-2) soit tel que si ψ et η sont deux séries formelles liées par $L(\psi) = \eta$, et si η a un rayon de convergence non nul, alors il en est de même de ψ:

PROPOSITION 2-2. *Soit q un élément de module plus grand que un de $\mathbb{C}$ (resp $\mathbb{C}_p$). Soit L un opérateur fonctionnel de la forme* (1-2). *On suppose que $P_s(0)$ est non nul. Alors si ψ et η sont deux séries formelles telles que $L(\psi) = \eta$ et si η a un rayon de convergence non nul dans $\mathbb{C}$ (resp $\mathbb{C}_p$), il en est de même de ψ.*

Démonstration. Nous traduisons tout d'abord la relation $L(\psi) = \eta$ sur les coefficients de Taylor $u(n)$ de ψ et $v(n)$ de η.

Notons $P_i(x) = \Sigma a_{i,j}x^j$, les polynômes intervenant dans L.

Un calcul facile montre que l'on a avec t égal au maximum de degrés des polynômes P_i, et, pour $j = 0, \ldots, t$, $Q_j(x) = \Sigma a_{i,j}q^{-ij}x^i$, la relation suivante:

$$\sum_{j=0}^{t} Q_j(q^n)u(n-j) = v(n) \tag{2-1}$$

Les polynômes $Q_j(x)$ sont de degré au plus s; d'autre part, le polynôme Q_0 est de degré exactement s puisque $a_{s,0} = P_s(O)$ est non nul.

Puisque $|q|$ est plus grand que un, il existe une constante positive c_1 telle que $|Q_j(q^n)| \leqslant c_1|Q_0(q^n)|$ pourvu que n soit assez grand, et ceci pour tout j. D'autre part, il existe α et β positifs tels que $|v(n)| \leqslant \alpha\beta^n|Q_0(q^n)|$ pour tout n assez grand.

On en déduit:

$$|u(n)| \leqslant c_1(|u(n-1)| + \cdots + |u(n-t)|) + \alpha\beta^n \tag{2-2}$$

pour tout n assez grand.

Il est facile de déduire de (2-2) que la série ψ a un rayon de convergence non nul.

PROPOSITION 2-3. *On se place dans le cas où $K = \mathbb{C}$, et où q est un élément de $\mathbb{C}$ qui est de module un, mais n'est pas une racine de l'unité.*

On suppose de plus que la condition suivante est réalisée:

(∗) *Pour toute racine u de $Q_0(x)$ et pour $u = 1$, il existe des constantes c_2 et c_3 positives telles que l'on ait pour tout n assez grand l'inégalité:*

$$|q^n - u| \geqslant c_2c_3^n.$$

Soit ψ une série formelle telle que $L(\psi) = \eta$ ait un rayon de convergence non nul. Alors ψ a un rayon de convergence non nul dans $\mathbb{C}$.

On a le même résultat si $K = \mathbb{C}_p$, et q est un élément de module un de $\mathbb{C}_p$ qui n'est pas une racine de l'unité, vérifiant (∗).

Démonstration. Nous regardons d'abord le cas où $\eta(x)$ est la série nulle. Nous partons de la relation (2-1) avec $v(n) = 0$. Il existe une constante c_4 positive telle que l'on ait:

$$|u(n)||Q_0(q^n)| \leqslant c_4(|u(n-1)| + \cdots + |u(n-t)|) \tag{2-3}$$

pourvu que n soit assez grand.

Posons $w(n) = |u(n-1)| + \cdots + |u(n-t)|$.

On a alors

$$|u(n)||Q_0(q^n)| \leqslant c_4 w(n)$$

et par suite:

$$w(n+1)|Q_0(q^n)| \leqslant c_5 w(n) \tag{2-4}$$

où c_5 est une constante positive.

On en déduit que si N est assez grand et si $T(n)$ est, pour n plus grand que N, le produit des $|Q_0(q^k)|$ pour k compris entre N et n, on a:

$$w(n) \leqslant c_6/T(n)$$

où c_6 est une constante positive.

Pour prouver l'assertion, il suffit donc de démontrer qu'il existe deux constantes positives c_7 et c_8 telles que l'on ait pour tout n assez grand:

$$T(n) \geqslant c_7 c_8^n.$$

On décompose $Q_0(x)$ en facteurs linéaires du premier degré dans $\mathbb{C}$, de la forme $x - u$, et on voit que l'on est ramené à prouver l'assertion dans le cas où $Q_0(x) = x - u$.

Le cas $u = 0$ est trivial, nous supposons u non nul dans la suite.

Nous pouvons sans nuire à la généralité du raisonnement supposer $N = 1$, $q^k - u$ non nul pour $k \geqslant 1$. Soit $v(n)$ = le produit des $(q^k - u)^{-1}$ pour k compris entre 1 et n, et $\vartheta(x)$ la série $\vartheta(x) = 1 + \Sigma_{n \geqslant 1} v(n) x^n$.

On voit facilement que $\vartheta(x)$ vérifie l'équation fonctionnelle:

$$\vartheta(qx) - (x + u)\vartheta(x) = 1 - u \tag{2-4}$$

D'autre part, $\vartheta(x)$ est l'unique série formelle solution de (2-4) telle que $\vartheta(0)$ soit égal à un.

Soit $h(x)$ la série définie par

$$h(x) = \exp\left(\sum_{n \geqslant 0} (-1)^n x^{n+1}/((n+1)u^{n+1}(q^{n+1} - 1))\right).$$

D'après les hypothèses de la proposition, la série $h(x)$ a un rayon de convergence non nul dans $\mathbb{C}$, et $h(0)$ est égal à un.

Soit $g(x) = \Sigma c(n)x^n$ la solution de l'équation fonctionnelle:

$$g(qx) - ug(x) = u(1-u)/(h(x)(x+u)) = \sum b(n)x^n$$

telle que $g(0) = 1$.

On a $c(n)(q^n - u) = b(n)$ pour tout n; le fait que le rayon de convergence de $\Sigma b(n)x^n$ soit non nul et les hypothèses de la proposition impliquent alors que le rayon de convergence de $g(x)$ est non nul.

La série $h(x)$ vérifie l'égalité $h(qx) = (1 + x/u)h(x)$. On voit alors facilement que la série $g(x)h(x)$ vérifie l'équation (2-4) et est égale à 1 en $x = 0$; par suite elle est donc égale à $\vartheta(x)$, qui a donc un rayon de convergence non nul.

Dans le cas général, si on pose $\eta(x) = \Sigma a(n)x^n$, il vient l'inégalité:

$$|u(n)||Q_0(q^n)| \leqslant c_4(|u(n-1)| + \cdots + |u(n-t)|) + |a(n)|$$

Par suite, avec les mêmes notations que précédemment:

$$|Q_0(q^n)|w(n+1) \leqslant c_5 w(n) + |a(n)|.$$

Soit $T(n)$ la suite définie dans la partie qui précède. On a que $T(n)$ est non nul pour n assez grand et que $T(n)$ est minoré par une expression de la forme $c_7 c_8^n$, et aussi majoré par une expression de la même forme.

Posons $v(n) = w(n)(T(n-1))$.

La suite $v(n)$ vérifie l'inégalité:

$$v(n+1) \leqslant v(n) + c_6|a(n)|T(n-1)$$

On en déduit que le rayon de convergence de la série $\Sigma v(n)x^n$ est non nul, et par suite aussi celui de $\Sigma w(n)x^n$, donc celui de la série $\psi(x)$, ce qui termine la démonstration.

La démonstration dans le cas de $\mathbb{C}_p$ est évidemment la même.

PROPOSITION 2-4. *On se place dans $K = \mathbb{C}$ et on suppose $|q| > 1$ (resp $K = \mathbb{C}_p$ et $|q|_p > 1$). Soit ψ une solution de l'équation fonctionnelle* (1-2), *que l'on suppose de rayon de convergence non nul. Alors ψ est méromorphe dans $\mathbb{C}$ tout entier (resp $\mathbb{C}_p$ tout entier); de plus les pôles de ψ sont de la forme $q^k\alpha$ où k est dans $\mathbb{N}$ et α un zéro non nul du polynôme $P_s(x)$ figurant dans* (1-2).

Démonstration. Nous reprenons l'équation (1-2), que nous écrivons sous la forme:

$$\sum_{i=0}^{s} P_i(q^{-s}x)\psi(q^{i-s}x) = 0 \qquad (2\text{-}5)$$

Soit R le rayon de méromorphie de ψ, qui est non nul par hypothèse. On déduit facilement de (2-5) que si R est fini, alors $R \geqslant |q|R$, ce qui est absurde puisque $|q|$ est plus grand que 1.

Donc ψ est méromorphe dans tout $\mathbb{C}$.

Soit maintenant un pôle λ de ψ et supposons que λ ne soit pas de la forme $q^k\alpha$, où k est dans $\mathbb{N}$ et α un zéro de $P_s(x)$.

On déduit alors de (2-5) qu'il existe i, $i \leqslant s-1$ tel que $\lambda_1 = q^{i-s}\lambda$ soit un pôle de ψ. On a $|\lambda_1| \leqslant |\lambda|/|q|$, et il est clair que λ_1 vérifie les mêmes propriétés que λ.

Par suite, en réitérant le procédé, on construit une suite λ_n de pôles de ψ de limite zéro, ce qui est absurde et termine la démonstration.

Nous examinons maintenant la croissance d'une fonction méromorphe satisfaisant à une équation fonctionnelle du type (1-2).

PROPOSITION 2-5. *Soit $\psi(x)$ une solution de l'équation* (1-2), *où le corps de base est $\mathbb{C}$ et où q est de module plus grand que un.*

On suppose que le rayon de convergence de ψ est non nul, de sorte que ψ est méromorphe dans $\mathbb{C}$ tout entier. Pour r réel positif tel que ψ n'ait aucun pôle sur le cercle de centre zéro et rayon r, on pose $|\psi|(r)$ égal à la borne supérieure des $|\psi(z)|$ pour z de module r dans $\mathbb{C}$. D'autre part, on pose $m_i =$ degré de P_i et $L = \mathrm{Max}\{m_i, 0 \leqslant i < s\} - m_s$.

Soit ε un réel positif. Il existe alors un ensemble fini $I_1, \ldots, I_h$, d'intervalles de $]0, +\infty[$, dont la réunion a une mesure inférieure à ε, et tels que si A est la réunion des $|q|^k I_j$ pour k dans $\mathbb{N}$ et j dans $\{1, \ldots, h\}$, on ait la propriété suivante:

Si r n'appartient pas à A, alors ψ n'a pas de pôles sur le cercle de centre zéro, rayon r, et $|\psi|(r) \leqslant \exp(L(\mathrm{Log}\, r)^2/2\, \mathrm{Log}|q| + O(\mathrm{Log}\, r))$.

Démonstration. D'après la proposition 2-4, ψ n'a de pôles que sur les cercles de rayons $|q|^k|\alpha|$, où k est dans $\mathbb{N}$ et α un zéro non nul de P_s. Soit S l'ensemble de ces rayons, qui forme une suite qui tend vers l'infini, et B le complémentaire de S dans $]0, +\infty[$.

Pour r appartenant à B, $|\psi|(r)$ est défini et on a:

$$|\psi|(r) \leqslant c_9 \left(\sum_{i=0}^{s-1} r^{m_i - m_s} |\psi|(r|q|^{i-s}) \right)$$

où c_9 est une constante positive.

Posons

$$H(r) = \mathrm{Max}\{|\psi|(r|q|^{i-s}), \qquad i = 0, \ldots, s-1\}$$

On a alors:

$$|\psi|(r) \leqslant c_{10} r^L H(r)$$

Donc

$$H(|q|r) \leqslant c_{10} r^L H(r) \tag{2-6}$$

Par une récurrence facile, on déduit de (2-6) que, si k est un entier naturel:

$$H(r) \leqslant c_{10}^k r^{kL} |q|^{-L(k-1)k/2} H(|q|^{-k} r) \tag{2-7}$$

Soit $R > 0$ fixé. On isole les éléments de S se trouvant dans $]0, R[$ dans des intervalles ouverts $I_1, \ldots, I_h$, de longueur totale inférieure à ε. Soit C le complémentaire de la réunion de ces intervalles dans $]0, R[$. Sur l'ensemble C, la fonction $H(r)$ est continue et donc bornée, disons par c_{11}.

Soit maintenant r dans l'ensemble A correspondant et k un entier naturel tel que $r|q|^{-k} < R$ et $r|q|^{-k+1} \geqslant R$. Il résulte de (2-7) que:

$$H(r) \leqslant c_{10}^k r^{kL} |q|^{-L(k-1)k/2} c_{11}.$$

En tenant compte de $k = \operatorname{Log} r / \operatorname{Log}|q| + O(1)$, il vient:

$$H(r) \leqslant \exp(L(\operatorname{Log} r)^2/(2 \operatorname{Log}|q|) + O(\operatorname{Log} r))$$

On en déduit facilement l'assertion.

3. Le q-analogue du théorème de Skolem-Mahler-Lech

Dans cette partie, nous allons démontrer le résultat suivant:

THÉORÈME 3-1. *Soit ψ appartenant à $F(\mathbb{C}, q)$, on suppose que $|q| > 1$, et que le rayon de convergence de ψ est non nul. On suppose de plus que ψ vérifie une équation fonctionnelle de la forme* (1-2) *avec m_i = degré de P_i tels que m_s soit supérieur ou égal à tous les m_i. Alors il existe un entier d positif tel que, en posant $\psi(x) = \Sigma u(n) x^n$, on ait pour tout h appartenant à $\{0, \ldots, d-1\}$ l'alternative suivante:*

(a) $u(kd + h) = 0$ *pour tout k assez grand.*
(b) *Si $A_h = \{k | u(kd + h) = 0\}$, alors A_h a une densité arithmétique nulle.*

Nous utiliserons le résultat suivant (Szemeredi, [17]):

THÉORÈME SZ. *Soit E une partie de $\mathbb{N}$; on suppose que la densité arithmétique supérieure de E est non nulle. Alors, pour tout entier s, il existe une infinité de progressions arithmétiques de même raison m, et de longueur s, inclus dans E.*

Démonstration du théorème. Elle suit d'assez près celle de [4], dans un contexte différent.

On sait d'après la proposition 2-4 que ψ est méromorphe dans tout $\mathbb{C}$, et que ses pôles sont de la forme $q^k\alpha$ où k est dans $\mathbb{N}$ et α un zéro de $P_s(x)$.

Soit $B = \{\zeta$, racine de l'unité de la forme ω_1/ω_2, où ω_1 et ω_2 sont des pôles de $\psi\}$. Alors B est fini.

En effet, une telle racine de l'unité est d'après ce qui précède de la forme $q^k\alpha_1/\alpha_2$, où α_1 et α_2 sont des zéros de $P_s(x)$ et k est un élément de $\mathbb{Z}$.

En exprimant que le module de cette racine de l'unité est un, on montre que les valeurs possibles pour k sont en nombre fini, d'où l'assertion.

Soit d un entier positif égal à un si B est vide, et au plus petit commun multiple des ordres des éléments de B si B est non vide.

On pose, pour h dans $\{0, \ldots, d-1\}$:

$$\varphi_h(x) = \sum u(kd + h)x^k$$

On a la relation:

$$\mathrm{d}x^h\varphi_h(x^d) = \sum \lambda^{-h}\psi(\lambda x)$$

où λ parcourt les racines d-ièmes de l'unité.

Nous distinguons deux cas:

Premier cas. La fonction $\varphi_h(x)$ n'a aucun pôle dans $\mathbb{C}$. Alors φ_h est une fonction entière. D'autre part il résulte des hypothèses et de la proposition 2-5 qu'il existe une suite r_n de réels positifs de limite l'infini, et des constantes positives c_{12} et c_{13} telles que:

$$|\psi|(r_n) \leqslant c_{13}r_n^{c_{12}}$$

Il en est donc de même pour la fonction φ_h; mais celle-ci est entière, et donc c'est un polynôme, et ceci termine la démonstration dans ce cas.

Second cas. La fonction φ_h a au moins un pôle dans $\mathbb{C}$. On voit facilement que les pôles de φ_h sont parmi les puissances d-ièmes de pôles de ψ, de sorte que d'après le choix de d, aucun quotient de pôles de φ_h n'est une racine de l'unité différente de un.

Nous raisonnons par l'absurde, en supposant que la densité supérieure de l'ensemble A_h est non nulle.

Posons $b(k) = u(kd + h)$. La suite $b(k)$ vérifie d'après la proposition 2-1, (d) une relation de récurrence de la forme (1-1), de longueur t.

D'après le théorème SZ, il existe un entier m tel que A_h contienne une infinité de progressions arithmétiques de t termes, de raison m. Par suite, il existe une

infinité de valeurs x dans $\mathbb{N}$, et une valeur y dans $\{0, \ldots, m-1\}$ telles que l'on ait $b((x+j)m+y) = 0$ pour $j = 0, \ldots, t-1$.

Soit $c(n) = b(nm+y)$. Cette suite vérifie une relation de la forme (1-1); on voit facilement qu'il en existe une de longueur inférieure ou égale à t, donc de la forme:

$$\sum_{k=0}^{r} H_k(q^n)c(n+k) = 0 \tag{3-1}$$

avec H_r non nul et r inférieur ou égal à t.

Soit x un entier assez grand, tel que $H_r(q^n)$ soit non nul pour tout n plus grand que x, et que $c(n)$ soit nul pour n égal à $x, x+1, \ldots, x+t-1$.

Il résulte de (3-1), par une récurrence facile, que $c(n)$ est alors nul pour tout n plus grand que x.

On a donc montré que:

$$\Sigma\, \lambda^{-y}\varphi_h(\lambda x) \tag{3-2}$$

où la sommation est faite sur les racines m-ièmes de l'unité, est un polynôme.

Soit alors ω un pôle de φ_h. Ce qui précède permet d'affirmer qu'il existe un autre pôle de φ_h dont le quotient avec ω est une racine de l'unité, et cette contradiction termine la démonstration.

4. Propriétés arithmétiques des éléments de R(K, q)

Dans un cas élémentaire, le problème que nous examinons maintenant est du type suivant:

Soit $\psi(x) = \Sigma\, u(n)x^n$ appartenant à $F(\mathbb{Q}, q)$, où q appartient à $\mathbb{Z}$. On suppose que $u(n)$ appartient à $\mathbb{Z}$ pour toute valeur de n. Que peut-on dire de $\psi(x)$ si l'on suppose que l'ensemble des $\{u(n), n$ dans $\mathbb{N}$ tels que $u(n)$ est non nul$\}$ a un nombre fini de diviseurs premiers?

Nous allons démontrer le résultat suivant:

THÉORÈME 4-1. *Soit $\psi(x)$ appartenant à $F(\mathbb{C}, q)$, avec $|q| > 1$. On suppose que ψ vérifie les conditions du théorème* 3-1. *D'autre part, on fait l'hypothèse qu'il existe un sous-groupe G du groupe multiplicatif de $\mathbb{C}$-$\{0\}$, de type fini, tel que $u(n)$ appartienne à G ou soit nul pour toute valeur de n.*

Alors $\psi(x)$ est une fraction rationnelle, et il existe d entier positif, et pour tout h dans $\{0, \ldots, d-1\}$ des éléments a_h et b_h dans $\mathbb{C}$ tels que, pour tout h dans $\{0, \ldots, d-1\}$ et tout k assez grand, on ait:

$$u(kd+h) = a_h(b_h)^k.$$

La démonstration utilise le résultat suivant dû à Evertse et Schlickewei-Van der Poorten ([7], [16]):

THÉORÈME E-S-VDP. *Soit K un corps commutatif de caractéristique nulle, et T un sous-groupe de type fini du groupe multiplicatif de K. Soit s un entier positif. Alors il existe seulement un nombre fini de points $(x_0, \ldots, x_s)$ dans $\mathbb{P}_s(K)$ tels que les trois propriétés suivantes soient vérifiées:*

(a) *pour tout $i = 0, \ldots, s$, x_i appartient à T.*
(b) $x_0 + \cdots + x_s = 0$.
(c) *Pour toute partie A de $\{0, \ldots, s\}$, non vide et propre, on a: Σx_i non nul, où la somme est étendue aux indices i dans A.*

On déduit de ce théorème le corollaire suivant:

COROLLAIRE 4-2. *Sous les hypothèses du théorème* E-S-VDP, *il existe un ensemble fini W dans K-$\{0\}$ tel que, pour tout élément $(x_0, \ldots, x_s)$ vérifiant* (a) *et* (b), *et pour tout i dans $\{0, \ldots, s\}$, il existe j différent de i et w dans W tel que l'on ait: $x_i = wx_j$.*

Nous passons maintenant à la démonstration du théorème 4-1.

Nous pouvons pour cela supposer que les éventuels pôles de ψ (qui est méromorphe dans $\mathbb{C}$ d'après les hypothèses du théorème 4-1), sont tels que les quotients de deux quelconques d'entre eux n'est pas une racine de l'unité, par un procédé analogue à celui utilisé dans la démonstration du théorème 3-1.

Nous écrivons alors une relation de récurrence pour $u(n)$:

$$\sum_{i=0}^{t} Q_i(q^n)u(n+i) = 0 \tag{4-1}$$

On pose de plus $Q_i(x) = \Sigma b_{i,k}x^k$.

On a donc:

$$\sum b_{i,k}q^{kn}u(n+i) = 0$$

Soit $L = \{(i, k) \mid b_{i,k} \text{ est non nul}\}$.

On pose, spour $h = (i, k)$ dans L: $y_h(n) = b_{i,k}q^{kn}u(n+i)$.

Soit H le sous-groupe engendré par G, q et les $b_{i,k}$ pour (i, k) dans L.

Le groupe H, comme G, est de type fini.

On a pour tout h dans L et tout n, $y_h(n) = 0$ ou $y_h(n)$ appartient à H.

D'autre part:

$$\sum y_h(n) = 0 \text{ pour tout } n,$$

où la sommation est faite sur les éléments de L.

Soit $E = \{n \mid \text{il existe } h \text{ dans } L \text{ tel que } y_h(n) = 0\}$.

L'entier n appartient à E, si, et seulement si il existe j, $0 \leqslant j \leqslant t$, tel que $u(n+j) = 0$.

Nous supposons d'abord que la densité arithmétique supérieure de l'ensemble E est positive.

On en déduit facilement que la densité supérieure de l'ensemble $\{n \mid u(n) = 0\}$ est positive.

D'après le raisonnement fait dans la démonstration du théorème 3-1, on en déduit que ψ ne peut avoir de pôles dans $\mathbb{C}$; en effet sinon, il y aurait deux pôles distincts de ψ dont le quotient serait une racine de l'unité, ce qui n'est pas le cas.

Si ψ n'a aucun pôle, c'est une fonction entière; on en déduit comme dans la démonstration du théorème 3-1 que ψ est un polynôme, et ceci termine la démonstration.

Nous supposons donc dans la suite que l'ensemble E est de densité arithmétique nulle.

D'après le corollaire 4-2, il existe un ensemble fini W d'éléments non nuls de $\mathbb{C}$ tels que, pour tout n dans $\mathbb{N}$, n n'appartenant pas à E, on ait pour une constante M indépendante de n la propriété suivante:

Il existe j dans $\{1, \ldots, s\}$, w dans W, k dans $\mathbb{Z}$ tel que $|k| \leqslant M$, avec:

$$u(n+j) = wq^{kn}u(n).$$

A chaque triplet $T = (w, j, k)$ avec j dans $\{1, \ldots, s\}$, w dans W, et k dans $\mathbb{Z}$, $|k| \leqslant M$, on associe $A(T) = \{n \mid u(n+j) = wq^{kn}u(n)\}$.

D'après ce qui précède, $\mathbb{N}$ est la réunion de E et des $A(T)$. Comme E est de densité nulle, il existe un $T = T_0 = (w_0, j_0, k_0)$ tel que $A(T_0)$ soit de densité arithmétique supérieure positive.

Nous posons

$$v(n) = u(n+j_0) - w_0 q^{k_0 n} u(n), \qquad \text{et } \tau(x) = \sum v(n)x^n.$$

Soit $\eta(x) = x^{j_0}\tau(x) = \psi(x) - w_0 x^{j_0}\psi(q^{k_0}x) + S(x)$, où $S(x)$ est un polynôme.

La série $\eta(x)$ appartient à $F(\mathbb{C}, q)$.

Par suite, comme la densité arithmétique supérieure de l'ensemble des n tels que $v(n)$ soit nul est positive, il existe un entier positif m et un entier h dans $\{0, \ldots, m-1\}$ tels que $\Sigma \lambda^{-h}\eta(\lambda x)$, où la sommation a lieu sur les racines m-ièmes de un, est un polynôme.

Ceci veut dire que

$$\sum \lambda^{-h}(\psi(\lambda x) - \lambda^{j_0} w_0 x^{j_0}\psi(\lambda q^{k_0}x)) \tag{3-4}$$

est un polynôme.

La fonction ψ a au moins une singularité dans $\mathbb{C}$, sinon c'est un polynôme et il n'y a rien à démontrer.

Considérons l'une d'entre elles, soit ω, qui soit la plus proche de l'origine; alors pour tout λ racine de l'unité, $\lambda\omega$ n'est pas un pôle de ψ.

D'après ce qui précède, il en résulte que ω est pôle d'une des fonctions

$$\psi(\lambda q^{k_0} x).$$

Si k_0 est négatif, on a un pôle plus proche de l'origine que ω, contradiction; de même si k_0 est positif on trouve une contradiction en raisonnant de manière analogue.

Par suite on a nécessairement $k_0 = 0$.

Soit alors $g(x) = (1 - w_0 x^{j_0})\psi(x)$. En reprenant la relation (3-4), on voit que $g(x)$ ne peut avoir de pôles dans $\mathbb{C}$, car sinon elle en aurait deux dont le quotient serait une racine de l'unité.

Par suite $g(x)$ est une fonction entière. On a encore une relation de la forme $|g|(r_n) \leqslant c_{13} r_n^{c_{12}}$ pour une suite de réels tendant vers l'infini, et par suite $g(x)$ est un polynôme.

On a donc $\psi(x) = P(x)/(1 - w_0 x^{j_0}) = A(x)/B(x)$, où A et B sont deux polynômes premiers entre eux. Si le degré de B est supérieur à un, alors ψ a deux pôles distincts solutions de $1 - w_0 x^{j_0} = 0$, donc dont le quotient est une racine de l'unité, ce qui est contraire à l'hypothèse faite. Par suite le degré de B est un, et $u(n) = ab^n$ pour n assez grand, ce qui termine la démonstration du théorème 4-1.

5. La *q*-analogue de la conjecture de Grothendieck

La conjecture de Grothendieck est la suivante:

Soit E une équation différentielle à coefficients polynômes de $\mathbb{K}[x]$, *où* $\mathbb{K}$ *est un corps de nombres.*

$$(E) \quad \sum_{i=0}^{s} P_i(x) y^{(i)}(x) = 0 \quad \text{(avec } P_s \text{ non nul).}$$

On suppose que, pour presque tout idéal premier P de $\mathbb{K}$, *il existe un système de s solutions de E dans* $\bar{\mathbb{F}}_p[\![x]\!]$ *(où p est le nombre premier rationnel au dessous de P et* $\bar{\mathbb{F}}_p$ *une clôture algébrique de* $\mathbb{F}_p$*), linéairement indépendantes sur* $\bar{\mathbb{F}}_p((x^p))$.

Alors toutes les solutions de E sont des fonctions algébriques.

Pour tout ce qui concerne cette conjecture, voir [5], [8], [9], [10].

Nous allons dans cette partie énoncer et étudier la q-analogue de cette conjecture:

Soit E_q une équation fonctionnelle de la forme:

$$\sum_{i=0}^{s} P_i(x)\psi(q^i x) = 0$$

où les P_i sont des polynômes de $\mathbb{K}[x]$, $\mathbb{K}$ corps de nombres, avec P_s non nul.

On suppose que l'élément q de $\mathbb{K}$ n'est pas une racine de l'unité.

On suppose de plus que pour presque tout idéal premier $\mathscr{P}$ de $\mathbb{K}$, E_q a un système de s solutions dans $\bar{\mathbb{F}}_p[\![x]\!]$ linéairement indépendantes sur $\bar{\mathbb{F}}_p((x^m))$, où $m = m_p$ est l'ordre de l'image de q dans le groupe multiplicatif de $\bar{\mathbb{F}}_p$ (on a donc supposé que q était $\mathscr{P}$-entier).

Alors toutes les solutions de E_q sont des fractions rationnelles.

Nous supposerons toujours dans la suite que q est $\mathscr{P}$-entier, et m sera son ordre dans le groupe multiplicatif de $\bar{\mathbb{F}}_p$.

Nous appellerons désormais cet énoncé la q-conjecture.

Avant d'étudier les propriétés que l'on peut déduire de l'énoncé précédent, nous justifions certaines des hypothèses.

Tout d'abord le fait que $\bar{\mathbb{F}}_p((x^p))$ est remplacé par $\bar{\mathbb{F}}_p((x^m))$. Le corps des constantes de la dérivation opérant sur un espace de séries formelles en caractéristique p est le corps $\bar{\mathbb{F}}_p((x^p))$. On sait que la q-analogue de la dérivation est l'opérateur qui à $\psi(x)$ associe $(\psi(qx) - \psi(x))/(x(q-1))$. Il est facile de voir que les séries d'image nulle par cet opérateur sont les séries en x^m.

Il existe d'autre part des fonctions algébriques solutions d'équations de la forme E_q, mais nous verrons à la fin de la partie VII que ce sont uniquement des séries de la forme $F(x^{1/d})$, où d est un entier positif, et que, sous les hypothèses de la q-conjecture, toute solution de cette forme de E_q est une fraction rationnelle.

La q-conjecture a beaucoup de points communs avec la conjecture de Grothendieck.

Cependant, on peut dire que les aspects globaux sont plus simples, puisque dès qu'une série formelle solution d'une équation du type (1-2) a un rayon de convergence non nul dans $\mathbb{C}$ (ou $\mathbb{C}_p$) et que $|q|$ est plus grand que un, elle est méromorphe dans $\mathbb{C}$ (ou $\mathbb{C}_p$) tout entier.

Ceci permet d'utiliser les critères de rationalité; dans le cas de la conjecture de Grothendieck, il faut démontrer des énoncés d'algébricité, ce qui est plus difficile.

Evidemment, on paie ceci par le fait que l'arithmétique modulo p est plus compliquée dans le cas de la q-conjecture que dans le cas de la conjecture de Grothendieck: on a des congruences exponentielles là où on avait des congruences polynomiales.

Cependant ceci nous permettra de démontrer dans la partie 7, un résultat dont la contrepartie, qui est l'énoncé suivant (se reporter à la partie 7 pour les notations), n'a semble-t-il pas été démontré:

Soit E une équation différentielle à coefficients dans $\mathbb{K}[x]$ *où* $\mathbb{K}$ *est un corps de nombres. On suppose que E possède un système complet de solutions dans* $\tilde{\mathbb{K}}[\![x]\!]$, *linéairement indépendantes sur* $\mathbb{K}$. *Alors toutes les solutions de E sont algébriques.*

Nous avons suivi d'assez près la présentation de Honda ([8]) de la conjecture de Grothendieck, beaucoup de résultats se transposant sans grande modification.

PROPOSITION 5-1. *Soit s un entier positif, et* $\psi_1, \ldots, \psi_s$ *dans* $\bar{\mathbb{F}}_p[\![x]\!]$. *On pose* $W(x)$ *égal au déterminant de la matrice* $\psi_i(q^j x)$, *avec* $i = 1, \ldots, s$ *et* $j = 0, \ldots, s-1$ (*Que nous appellerons wronskien de* $\psi_1, \ldots, \psi_s$).

Alors $W(x)$ *est non nul si et seulement si* $\psi_1, \ldots, \psi_s$ *sont linéairement indépendants sur* $\bar{\mathbb{F}}_p((x^m))$.

Démonstration. Il est immédiat que si $\psi_1, \ldots, \psi_s$ sont linéairement dépendants sur $\bar{\mathbb{F}}_p((x^m))$, alors $W(x)$ est nul.

Pour la réciproque, nous commençons par le cas $s = 2$.

On a alors $W(x) = \psi_1(x)\psi_2(qx) - \psi_2(x)\psi_1(qx)$.

Si $W(x) = 0$, alors il vient, en supposant que $\lambda(x) = \psi_1(x)/\psi_2(x)$ est dans $\bar{\mathbb{F}}_p[[x]]$, que $\lambda(qx) = \lambda(x)$, d'où on déduit facilement le résultat.

Nous procédons ensuite par récurrence sur s. On développe $W(x)$ suivant la dernière colonne, d'où:

$$W(x) = \sum_{j=1}^{s} \Delta_j(x)\psi_j(q^{s-1}x) \tag{5-1}$$

où $\Delta_j(x)$ est le mineur associé. Par suite $\Delta_s(x)$ est le wronskien de $\psi_1, \ldots, \psi_{s-1}$, de sorte que si Δ_s est nul, l'hypothèse de récurrence s'applique. Nous supposons donc Δ_s non nul dans ce qui suit.

On a:

$$\sum_{j=1}^{s} \Delta_j(x)\psi_j(q^r x) = 0 \qquad \text{pour } r = 0, \ldots, s-1 \tag{5-2}$$

ceci par hypothèse pour $r = s-1$, et parce que c'est le développement d'un déterminant ayant deux colonnes égales sinon.

On a donc pour $r = 0, \ldots, s-2$:

$$\sum_{j=1}^{s} (\Delta_j(qx) - \Delta_j(x))\psi_j(q^{r+1}x) = 0 \tag{5-3}$$

On réécrit les $s-1$ équations (5-3) en faisant passer les termes $(\Delta_s(qx) - \Delta_s(x))\psi_s(q^{r+1}x)$ dans le second membre, et on résout par les formules de Cramer. Il vient:

$$\Delta_j(qx) - \Delta_j(x) = (\Delta_s(qx) - \Delta_s(x))\Delta_j(qx)/\Delta_s(qx)$$

Par suite:

$$\Delta_j(qx)/\Delta_s(qx) = \Delta_j(x)/\Delta_s(x)$$

et on en déduit facilement le résultat.

PROPOSITION 5-3. *Soient $\psi_1, \ldots, \psi_s$ dans $K[\![x]\!]$, où K est un corps de caractéristique nulle, et q un élément non nul de K et non racine de l'unité Alors $\psi_1, \ldots, \psi_s$ sont linéairement indépendants sur K, si et seulement si $W(x)$ est non nul.*

Démonstration. C'est essentiellement la même que pour la proposition précédente.

PROPOSITION 5-3. *Soient P et Q deux polynômes non nuls de $\mathbb{K}[x]$, premiers entre eux. On suppose que l'équation fonctionnelle:*

$$\psi(qx)Q(x) - \psi(x)P(x) = 0$$

vérifie les conditions de la q-conjecture.

Alors $P(0)$ et $Q(0)$ sont non nuls, les degrés de P et Q sont égaux, et pour tout idéal premier $\mathscr{P}$ de $\mathbb{K}$ tel que les hypothèses de la q-conjecture soient réalisés pour $\mathscr{P}$, il existe une numérotation des racines de P et Q dans $\bar{\mathbb{F}}_p$ telle que, pour toute racine α_i de P, il existe une racine β_i de Q et un entier k_i tel que $\alpha_i = q^{k_i}\beta_i$ pour tout i. En particulier, si a et b sont les termes constants de P et Q, alors il existe k dans $\mathbb{Z}$ tel que $a = bq^k$.

Démonstration. Soit $\psi(x)$ une série formelle de $\bar{\mathbb{F}}_p[\![x]\!]$, non nulle, et solution de l'équation fonctionnelle de la proposition. En posant $\psi(x) = cx^k + \cdots$ avec c non nul, et en reportant dans l'équation fonctionnelle, il est immédiat que $P(0)Q(O)$ est non nul (On a pris p assez grand de façon que q soit $\mathscr{P}$-entier).

Le fait que ψ soit solution de l'équation fonctionnelle implique:

$$P(x)P(qx)\cdots P(q^{m-1}x) = Q(x)Q(qx)\cdots Q(q^{m-1}x) \quad \text{dans } \bar{\mathbb{F}}_p[x] \tag{5-4}$$

(m est l'ordre de l'image de q dans $\bar{\mathbb{F}}_p$).

On déduit facilement de (5-4) que P et Q ont même degré, et les dernières assertions de la proposition.

PROPOSITION 5-4. *Soit E_q une équation fonctionnelle de la forme* (1-2) *vérifiant les hypothèses de la q-conjecture. Soit $\mathscr{P}$ un idéal premier de $\mathbb{K}$ tel que q soit une $\mathscr{P}$-unité et que les hypothèses de la q-conjecture soient vérifiées pour $\mathscr{P}$. Alors E_q a s solutions polynomiales linéairement indépendantes sur $\bar{\mathbb{F}}_p((x^m))$.*

Démonstration. Soit $y(x)$ dans $\bar{\mathbb{F}}_p[\![x]\!]$ solution de E_q, $y(x) = \Sigma c(k)x^k$. Ceci est équivalent à dire que:

$$\sum_{i=0}^{t} Q_i(q^n)c(n+i) = 0 \tag{5-4}$$

Il en résulte que si pour un k on a $c(k+1) = c(k+2) = \cdots = c(k+t) = 0$, le polynôme $c(0) + c(1)x + \cdots + c(k)x^k$ est solution de E_q.

Soit s un entier tel que $sm \geqslant t$.

On pose $v(n) = c(nsm) + c(nsm+1)x + \cdots + c((n+1)sm-1)x^{sm-1}$.

Soit $v(i_1), \ldots, v(i_r)$, où $i_1 < \cdots < i_r$, une base du $\bar{\mathbb{F}}_p$-espace vectoriel engendré par les $v(n)$ et λ dans $\mathbb{N}$ tel que $ms(\lambda - i_r) > N$ où N est un entier fixé.

On pose $v(\lambda) = b_1 v(i_1) + \cdots + b_r v(i_r)$ (5-5)

Alors:

$$y_1(x) = y(x)(1 - b_1 x^{ms(\lambda - i_1)} - \cdots - b_r x^{ms(\lambda - i_r)})$$

est aussi une solution de E_q; on voit facilement que les coefficients de $x^{ms\lambda + h}$ dans $y_1(x)$ sont nuls pour $h = 0, \ldots, ms-1$.

Par suite, en prenant les $ms\lambda$ premiers termes de $y_1(x)$, on a trouvé une solution polynomiale ψ de E_q telle que $\psi(x)$ est congrue à $y(x)$ modulo x^N.

Si l'on a maintenant s solutions séries formelles linéairement indépendantes sur $\bar{\mathbb{F}}_p((x^m))$, alors leur wronskien est non nul; en choisissant s solutions polynomiales congrues aux précédentes modulo x^N où N est choisi assez grand, on voit que le wronskien de ces solutions polynômes sera aussi non nul, d'où le résultat.

PROPOSITION 5-5. *Soit E_q une équation fonctionnelle de la forme* (1-2) *vérifiant les hypothèses de la q-conjecture pour l'idéal premier $\mathscr{P}$ de $\mathbb{K}$. On suppose que les P_i sont premiers entre eux. Alors*:

(a) *$P_s(0)$ et $P_0(O)$ sont non nuls et P_s et P_0 sont de même degré.*

(b) *Le polynôme $H(x) = \Sigma_{i=0}^{s} P_i(0)x^i$ a toutes ses racines dans $\bar{\mathbb{F}}_p$ de la forme q^k où k est dans $\mathbb{Z}$.*

Démonstration. Nous allons raisonner par récurrence sur l'ordre s de l'équation fonctionnelle (1-2). Pour $s = 1$, la proposition (5-3) permet d'affirmer que le résultat est correct.

Soit $W(x)$ le wronskien des s solutions linéairement indépendantes sur $\bar{\mathbb{F}}_p((x^m))$ données par les hypothèses.

Du système:

$$\sum_{i=0}^{s-1} P_i(x)\psi_j(q^i x) = -P_s(x)\psi_j(q^s x), \qquad j = 1, \ldots, s$$

On tire par les formules de cramer:

$$P_0(x) = -P_s(x)W(qx)/W(x).$$

La proposition 5-3 permet alors d'affirmer que P_s et P_0 ont même degré et même valuation x-adique.

Soit $\psi_0(x)$ une solution polynomiale non nulle de E_q, qui existe d'après la proposition (5-4). On pose dans E_q, $\psi(x) = \varphi(x)\psi_0(x)$. On a donc l'équation:

$$\sum_{i=0}^{s} P_i(x)\varphi(q^i x)\psi_0(q^i x) = 0 \tag{5-6}$$

D'autre part:

$$\sum_{i=0}^{s} P_i(x)\psi_0(q^i x) = 0 \tag{5-7}$$

En multipliant (5-7) par $\varphi(x)$, et en soustrayant à (5.6) il vient:

$$\sum_{i=0}^{s} P_i(x)(\varphi(q^i x) - \varphi(x))\psi_0(q^i x) = 0 \tag{5-8}$$

Posons $\eta(x) = \varphi(qx) - \varphi(x)$, on a alors:

$$\sum_{i=1}^{s} P_i(x)(\eta(x) + \cdots + \eta(q^{i-1}x))\psi_0(q^i x) = 0 \tag{5-9}$$

L'équation d'ordre $s - 1$ (5-9) admet $s - 1$ solutions linéairement indépendantes sur $\bar{\mathbb{F}}_p((x^m))$. Par hypothèse de récurrence, en tenant compte du fait que ses coefficients ne sont pas forcément premiers entre eux, il vient que la valuation x-adique de $\psi_0(q^s x)P_s(x)$ est inférieure ou égale à la valuation x-adique de $P_s(x)\psi_0(q^s x) + \cdots + P_j(x)\psi_0(q^j x)$, pour $j = s, \ldots, 1$.

On en déduit que la valuation x-adique de P_s est inférieure ou égale à celle de P_j pour tout $j = s, \ldots, 1$.

Comme les P_j sont premiers entre eux, il en résulte que la valuation x-adique de P_s et de P_0 est nulle, d'où le résultat (a).

Pour (b) on voit que si le polynôme $\psi_0(x)$ commence par un terme de la forme cx^h avec c non nul, alors nécessairement on a $H(q^h)$ égal à zéro, en calculant le terme constant dans l'expression (5-7) après simplification par x^h.

D'autre part, le polynôme $H_1(x)$ associé à l'équation (5-9), toujours après simplification par x^h, est alors lié à H par l'égalité:

$$(x - 1)H_1(x) = H(q^h x).$$

Par hypothèse de récurrence, le polynôme $H_1(x)$ a toutes ses racines qui sont des puissances de q, et par suite il en est de même de $H(x)$, et ceci termine la démonstration.

6. La q-conjecture dans le cas de l'équation d'ordre un

Dans cette partie, nous traitons les quelques cas de l'équation du premier ordre où nous savons démontrer la q-conjecture.

Il s'agit du résultat suivant:

THÉORÈME 6-1. *La q-conjecture est vraie dans le cas de l'équation du premier ordre:*

$$Q(x)\psi(qx) - P(x)\psi(x) = 0$$

où Q est un polynôme de degré au plus trois.

Pour la démonstration, nous aurons besoin du résultat suivant, dû à Schinzel ([15]):

THÉORÈME SC. *Soit $\mathbb{K}$ un corps de nombres, et $\alpha_1, \ldots, \alpha_t$ des éléments non nuls de $\mathbb{K}$, f un polynôme à une variable à coefficients dans $\mathbb{K}$, de degré g. On suppose que la congruence:*

$$f(\alpha_1^{x_1} \cdots \alpha_t^{x_t}) \equiv 0[\mathscr{P}]$$

a une solution dans $\mathbb{Z}^t$ pour presque tout idéal premier $\mathscr{P}$ de $\mathbb{K}$. Alors l'équation $f(\alpha_1^{x_1} \cdots \alpha_t^{x_t}) = 0$ dans $\mathbb{K}$ a une solution dans $\mathbb{Q}^t$, avec un dénominateur commun inférieur ou égal à $\max(1, g-1)$.

Démonstration du théorème 6-1. Nous commençons par le cas où le degré de Q (et donc de P) est un. On a de plus $P(o)$ et $Q(o)$ non nuls. On suppose pour commencer que $P(0) = Q(0) = 1$.

L'équation s'écrit alors $\psi(qx)/\psi(x) = (1 - \alpha x)/(1 - \beta x)$.

D'après la proposition 5-3, il existe pour presque tout idéal premier $\mathscr{P}$ de $\mathbb{K}$ un entier k tel que $\alpha/\beta = q^k$ dans $\bar{\mathbb{F}}_p$. Le théorème SC permet alors d'affirmer que α/β est une puissance de q. On en déduit alors facilement une solution polynomiale de l'équation, de la forme

$$\psi(x) = (1 - \beta x)(1 - q\beta x) \cdots (1 - q^{k-1}\beta x)$$

si $\alpha/\beta = q^k$ avec k dans $\mathbb{N}$. Si k est négatif, on obtient l'inverse d'un polynôme.

Passons maintenant au cas général. Comme on l'a vu dans la démonstration de la proposition 5-3, pour presque tout idéal premier $\mathscr{P}$ de $\mathbb{K}$, il existe k dans $\mathbb{Z}$

tel que l'on ait $P(O)q^k - Q(0) = 0$ dans $\bar{\mathbb{F}}_p$. Le théorème SC prouve alors qu'une telle égalité est vraie dans $\mathbb{K}$. En regardant alors l'équation vérifiée par $x^k\psi(x)$, on voit que l'on s'est ramené au cas précédent, d'où le résultat.

Le cas $s = 2$ se démontre encore de cette façon, sans grandes modifications.

Si $s = 3$, on montre, après s'être ramené comme précédemment au cas où $P(O) = Q(O) = 1$, en utilisant la proposition 5-3 et le théorème SC, que si la conjecture n'est pas vraie, alors il existe un rangement des racines de P et de Q tel que l'on ait dans $\mathbb{K}$ pour $i = 1, 2, 3$:

$$\alpha_i = \delta_i \omega q^{k_i} \beta_i \tag{6-1}$$

où δ_i est égal à 1 ou -1, $\omega^2 = q$ et k_i est dans $\mathbb{Z}$.

D'autre part, la proposition 5-3 montre que pour presque tout idéal premier $\mathscr{P}$ de $\mathbb{K}$ convenable, il existe n dans $\mathbb{Z}$ tel que $\alpha_1\alpha_2\alpha_3 = q^n\beta_1\beta_2\beta_3$ dans $\bar{\mathbb{F}}_p$.

Utilisant encore le théorème SC, on voit qu'il en est de même dans $\mathbb{K}$.

En multipliant entre elles les égalités (6-1), utilisant ce dernier renseignement et en élevant au carré, il vient:

$$q^{2M+1} = 1$$

avec $M = k_1 + k_2 + k_3 + 1 - n$ appartenant *à* $\mathbb{Z}$, ce qui est absurde puisque q n'est pas une racine de l'unité, ce qui termine la démonstration.

REMARQUE. On démontre facilement que la véracité de la q-conjecture pour les cas où le degré de Q est égal à un, est en fait équivalente au cas particulier du théorème SC où le degré du polynôme f est égal à un.

7. Une version faible de la q-conjecture

Nous allons dans cette partie démontrer une version faible de la q-conjecture. Soit $\mathbb{K}$ un corps de nombres. Nous notons dans ce qui suit par $\tilde{\mathbb{K}}[\![x]\!]$ la partie de $\mathbb{K}[\![x]\!]$ formée des séries formelles $f(x)$ telles que f ait ses coefficients de taylor $\mathscr{P}$-entiers pour tout idéal premier $\mathscr{P}$ de $\mathbb{K}$ sauf un nombre fini (dépendant de f).

Nous allons démontrer le résultat suivant:

THÉORÈME 7-1. *Soit $\mathbb{K}$ un corps de nombres, q un élément non nul de $\mathbb{K}$ qui ne soit pas une racine de l'unité, et E_q une équation fonctionnelle de la forme* (1-2):

$$(E_q) \quad \sum_{i=0}^{s} P_i(x)\psi(q^i x) = 0$$

où les $P_i(x)$ sont des polynômes de $\mathbb{K}[x]$, P_s est non nul et les P_i sont premiers entre eux.

On suppose que (E_q) *admet un système de s solutions dans* $\tilde{\mathbb{K}}[\![x]\!]$, *linéairement indépendantes sur* $\mathbb{K}$.

Alors toutes les solutions de (E_q) *sont des fractions rationnelles.*

Nous utiliserons dans la démonstration le résultat suivant (critère de Borel-Dwork, voir [6] et [1] page 170):

CRITÈRE B-D. *Soit* $\mathbb{K}$ *un corps de nombres, et* $f(x) = \Sigma\, a(n)x^n$ *une série formelle de* $\mathbb{K}[\![x]\!]$. *S'il existe une partie finie* $P_1(\mathbb{K})$ *de l'ensemble* $P(\mathbb{K})$ *des places finies de* $\mathbb{K}$ *telle que*:

(i) *Pour tout* $\mathcal{P}$ *n'appartenant pas à* $P_1(\mathbb{K})$, $a(n)$ *est* $\mathcal{P}$*-entier pour tout n.*

(ii) *Pour chacune des t places infinies de* $\mathbb{K}$, f *définit dans* $\mathbb{C}$ *une fonction méromorphe dans un disque de centre* 0, *rayon* R_i, $i = 1, \ldots, t$.

(iii) *Pour* $\mathcal{P}$ *appartenant à* $P_1(\mathbb{K})$, f *définit dans* $\mathbb{C}_p$, *(où p est le nombre premier rationnel correspondant à* $\mathcal{P}$*), une fonction méromorphe dans le disque de centre zéro, rayon* $R(\mathcal{P})$.

(iv) *Le produit* $R = R_1 \cdots R_t \Pi R(\mathcal{P})$, *où le deuxième produit est étendu aux* $\mathcal{P}$ *dans* $P_1(\mathbb{K})$, *est plus grand que un.*

Alors f est une fraction rationnelle.

Démonstration du théorème 7-1. Nous remarquerons tout d'abord que les hypothèses de la q-conjecture sont impliqués par les hypothèses du théorème 7-1.

Par suite, d'après la proposition 5-5, $P_s(0)$ et $P_0(0)$ sont non nuls.

Nous examinons maintenant le rayon de convergence d'une série formelle solution de (E_q), pour les différentes places de $\mathbb{K}$.

S'il s'agit d'une place v, finie ou infinie, telle que $|q|_v > 1$, alors la proposition 2-2 permet d'affirmer que le rayon de convergence est non nul.

S'il s'agit d'une place v telle que $|q|_v < 1$, on pose $q_1 = 1/q$, et on constate que c'est le fait que $P_0(0)$ est non nul qui permet d'affirmer que le rayon de convergence est aussi non nul.

Supposons maintenant que $|q|_v = 1$. Soit u un nombre algébrique qui soit aussi de module un. Les minorations de formes linéaires en logarithmes permettent alors d'affirmer que, tant dans le cas d'une place finie que d'une place infinie, il existe des constantes c_{14} et c_{15} positives telles que:

$$|q^n - u|_v \geqslant c_{14} n^{-c_{15}} \quad \text{pour } n \text{ assez grand} \tag{7-1}$$

Si $|u|_v$ est différent de un, l'inégalité (7-1) est trivialement vérifiée.

On peut alors appliquer la proposition 2-3, ce qui permet de conclure que le rayon de convergence est non nul dans ce cas.

Finalement, le rayon de convergence d'un série formelle de $\mathbb{K}[\![x]\!]$ solution de (E_q) est non nul, pour toute place de $\mathbb{K}$.

Il existe au moins une place v de $\mathbb{K}$ telle que $|q|_v > 1$. En effet, sinon le nombre q serait une racine de l'unité, d'après un théorème bien connu de Kronecker.

On peut alors appliquer le critère B-D: les s séries formelles linéairement indépendantes de (E_q) données par les hypothèses du théorème 7-1 sont toutes des fractions rationnelles, ceci montre que toute solution de (E_q) est une fraction rationnelle et termine la démonstration.

REMARQUE. Soit $\psi(x)$ une fonction algébrique solution d'une équation (E_q) vérifiant les hypothèses de la q-conjecture. Il existe alors un entier d positif tel que $\psi(x) = A(x^{1/d})$, où $A(x)$ est une série de Laurent n'ayant qu'un nombre fini de termes à exposant négatif.

Nous allons montrer que ψ est une fraction rationnelle. On voit facilement que l'on peut supposer que A n'a pas de termes d'exposants négatifs. On considère alors le premier indice k tel que le coefficient de taylor de x^k soit non nul dans $A(x)$ et tel que d ne divise pas k.

En considérant l'équation (E_q), on montre alors que $H(q^{k/d})$ est nul, où $H(x)$ est le polynôme introduit dans la proposition 5-5. D'autre part, on sait que ce polynôme admet pour presque tout idéal premier $\mathcal{P}$ de $\mathbb{K}$, toutes ses solutions dans $\overline{\mathbb{F}}_p$ comme des puissances entières de q; d'après le théorème SC, il en est de même dans $\mathbb{K}$. Donc $q^{k/d}$ est une puissance entière de q, et par suite d divise k. Cette contradiction montre que $\psi(x)$ est une série formelle algébrique à coefficients dans $\mathbb{K}$. La démonstration du théorème 7-1 montre alors que ψ est une fraction rationnelle, d'où l'assertion.

Bibliographie

1. Y. Amice, *Les nombres p-adiques.* Collection sup, no. 14, Les presses universitaires de France, Paris 1975.
2. B. Benzaghou, Algèbres de Hadamard, *Bull. Soc. Math. France* 28, (1970) 209–252.
3. J-P. Bézivin, Sur un théorème de G. Polya, *J. reine und ang. Math.* 364 (1986) 60–68.
4. J-P. Bézivin, Une généralisation du théorème de Skolem-Mahler-Lech, *Quarterly J. of Math.* 40 (1989) 133–138.
5. D. V. Chudnovsky and G. V. Chudnovsky, Applications of Padé approximants to the Grothendieck conjecture on linear differential equations, *Lecture Notes in Math.* 1135, Springer-Verlag, New York, 85–167.
6. B. Dwork, On the rationality of the dzeta function of an algebraic variety, *Amer. J. of Math.* 82 (1960) 631–648.
7. J. H. Evertse, On sums of S-units and linear recurrence, *Compositio Math.* 53 (1984) 225–244.
8. T. Honda, Algebraic differential equations, *Symposia Math.* no. 24 (1979) 169–204.
9. N. Katz, Nilpotent connections and the monodromy theorem: Application of a result of Turrittin, *Publ. Math.* IHES. no. 39 (1970) 355–412.
10. N. Katz, Algebraic solutions of differential equations (p-curvature and the Hodge filtration), *Invent. Math.* 18 (1972) 1–118.
11. V. Laohakosol, Some extensions of the Skolem-Mahler-Lech theorem. *Expositiones Math.* 7 (1989) 137–189.
12. C. Lech, A note on recurring series, *Ark. Mat.* 2 (1953) 417–421.

13. K. Mahler, On the taylor coefficients of rational functions, *Proc. Cambridge. Phil. Soc.* 52 (1956) 39–48.
14. G. Polya, Arithmetische Eigenschaften der Reihenentwicklungen rationaler Funktionen, *J. reine und ang. Math.* 151 (1921) 1–31.
15. A. Schinzel, Abelian binomials, power residues and exponential congruences, *Acta Arithm.* 27 (1975) 397–420.
16. H-P. Schlickewei and A. J. van der Poorten, The growth condition for recurrent sequences, *Macquarie Math. Reports* 82-0041, Northride, Australia 1982.
17. E. Szemeredi, On sets of integers containing no k elements in arithmetic progression, *Acta Arithm.* 27 (1975) 199–245.
18. W. J. Trjiztinsky, Analytic theory of q-linear difference equations, *Acta Math.* 61 (1933) 1–38.