Ann. Scuola Norm. Sup. Pisa Cl. Sci. (5)
Vol. VI (2007), 457-475

Equations in the Hadamard ring of rational functions

ANDREA FERRETTI AND UMBERTO ZANNIER

Abstract. Let K be a number field. It is well known that the set of recurrence-sequences with entries in K is closed under component-wise operations, and so it can be equipped with a ring structure. We try to understand the structure of this ring, in particular to understand which algebraic equations have a solution in the ring. For the case of cyclic equations a conjecture due to Pisot states the following: assume $\{a_n\}$ is a recurrence sequence and suppose that all the a_n have a d^{th} root in the field K; then (after possibly passing to a finite extension of K) one can choose a sequence of such d^{th} roots that satisfies a recurrence itself. This was proved true in a preceding paper of the second author. In this article we generalize this result to more general monic equations; the former case can be recovered for $g(X, Y) = X^d - Y = 0$. Combining this with the *Hadamard quotient theorem* by Pourchet and Van der Poorten, we are able to get rid of the monic restriction, and have a theorem that generalizes both results.

Mathematics Subject Classification (2000): 11B37 (primary); 12E25, 13F25 (secondary).

1. Introduction

Let K be a field of characteristic 0, and denote by $\overline{K}$ an algebraic closure. We define a *recurrence sequence* to be a sequence $a = \{a(n)\}_{n\in\mathbb{N}} \subset \overline{K}$ satisfying

$$a(n+m) + c_{m-1}a(n+m-1) + \cdots + c_0 a(n) = 0$$

for each $n \geq 0$, for some fixed $c_0, \ldots c_{m-1} \in K$, $c_0 \neq 0$. When m is minimal, the polynomial

$$q(T) = T^m + c_{m-1}T^{m-1} + \cdots + c_0$$

is said to be *associated* with the recurrence, and its roots α_i are by definition the *roots* of the recurrence.

On the other hand, whenever a rational function $r \in K(x)$ is defined at 0, Taylor coefficients may be taken, setting as usual $s_n = r^{(n)}(0)/n!$. It is well known that in the ring of formal power series the equality $r(x) = \sum s_n x^n$ holds, and it is

Received February 1, 2007; accepted in revised form August 30, 2007.

easy to show that a sequence $\{s_n\}$ represents a rational function if, and only if, it satisfies a linear recurrence except for a finite number of terms. In this case we call it a *rational power series*.

Now, it is well known (for all these facts see [14]) that recurrence sequences are characterized by an explicit closed form, given by *exponential polynomials*

$$a(n) = \sum_{i=1}^{l} a_i(n)\alpha_i^n$$

where $a_i \in \overline{K}[x]$ and $\alpha_i \in \overline{K}$ (the α_i, assuming that the $a_i \neq 0$ and the α_i are nonzero and distinct, are in fact the roots of the recurrence). Since the sum and products of exponential polynomials are sequences of the same kind, it follows that the set of recurrence sequences (or equivalently the set of rational power series) is closed under component-wise sum and product. This leads to the following

Definition 1.1. The *Hadamard ring* over the field K is the set of formal power series with coefficients in K which represent a rational function, equipped with component-wise operations. Equivalently it can be thought as the set of sequences from K eventually satisfying a linear recurrence. It is denoted by $\mathcal{H}(K)$. Whenever $a \in \mathcal{H}(K)$ we denote by $a(n)$ its n-th coefficient (or its n-th term, if you think of recurrence sequences).

Suppose now that we want to solve an algebraic equation in $\mathcal{H}(K)$: the first attempt is to solve it in the larger set $K[[x]]$, which we regard as a ring under component-wise sum and product of coefficients. This, in turn, amounts to solve infinitely many equations in the field K.

The case we are interested in is when K is a number field, and we shall assume this from now on. We shall also identify a formal power series with the sequence of its coefficients. With this terminology Zannier proves the following theorem, solving a conjecture of Pisot:

Theorem 1.2 ([16]). *Let K be a number field and let $\sum b(n)x^n \in \mathcal{H}(K)$. Suppose that for all n the equation $Y^d = b(n)$ has a solution in K. Then there exists a finite extension K'/K such that the same equation has a solution in $\mathcal{H}(K')$. In other words we may choose d-th roots for the $b(n)$ so that they satisfy themselves a linear recurrence.*

Another classical result for the problem of solving equations in this ring is the *Hadamard quotient theorem* (proved in [9] and [13], but see also [10] for a detailed account), which deals with linear equations.

Theorem 1.3 (Hadamard quotient). *Let F be a field of characteristic zero and let $\{b(n)\}, \{c(n)\} \in \mathcal{H}(F)$. Let $\{a_n\}$ be a sequence whose elements are in a subring R of F which is finitely generated over $\mathbb{Z}$, and suppose that $a_n = b(n)/c(n)$ whenever the quotient is defined. Then there exists an element $\{a(n)\} \in \mathcal{H}(F)$ such that $a(n) = a_n$ for every n such that $c(n) \neq 0$.*

In this paper we generalize these results, providing a solution to a more general conjecture of Van der Poorten ([15]).

Theorem 1.4. *Let K be a number field, $b_0, \dots, b_{d-1} \in \mathcal{H}(K)$, and consider the equation*

$$Y^d + b_{d-1}(n)Y^{d-1} + \cdots + b_0(n) = 0. \tag{1.1}$$

Suppose (1.1) *has a solution in K for all $n \in \mathbb{N}$; then there exists a finite extension K'/K such that the same equation has a solution in $\mathcal{H}(K')$.*

It will be convenient to restate Theorem 1.4 in terms of exponential polynomials; moreover we may assume that the b_j have roots contained in the same finite set $\{\beta_1, \dots, \beta_m\}$.

Theorem 1.4 (second form). *Let K be a number field and for $j = 0, \dots, d-1$ let*

$$b_j(n) = \sum_{i=1}^{m} b_{i,j}(n)\beta_i^n$$

be exponential polynomials, with $b_{i,j} \in K[x]$ and $\beta_i \in K$ for all i, j. Suppose that for every $n \in \mathbb{N}$ the equation

$$Y^d + b_{d-1}(n)Y^{d-1} + \cdots + b_0(n) = 0 \tag{1.1}$$

has a solution $a_n \in K$. Then there exists an exponential polynomial $\{a(n)\}$ with coefficients and roots in a finite extension of K that satisfies (1.1) *identically.*

Remark 1.5. Of course one can relax the hypothesis requiring that the equation has solutions in a fixed finite extension of K. Actually we will enlarge K in the course of the proof without further comment.

Remark 1.6. One can use the techniques of reduction of Rumely and Van der Poorten ([10,11]) to deduce from Theorem 1.4 an analogous statement for a field K finitely generated over $\mathbb{Q}$. We omit this verification, which is substantially straightforward after the quoted papers. See also the paper of Corvaja [1] for a somewhat different deduction.

Since our proof will involve an induction, it will be convenient to state and prove the following stronger form of Theorem 1.4.

Theorem 1.7. *Suppose that for each arithmetic progression $\mathfrak{A}$ there exists an $n \in \mathfrak{A}$ for which the equation* (1.1) *has a solution in K. Then there exists an exponential polynomial $\{a(n)\}$ with coefficients in a finite extension K' of K that satisfies*

$$a^d + b_{d-1}a^{d-1} + \cdots + b_0 = 0 \tag{1.2}$$

identically in $\mathcal{H}(K')$.

Remark 1.8. One could also try to prove something stronger than Theorem 1.7; namely that we have a solution to (1.1) in the Hadamard ring as soon as we have solution for infinitely many n. Anyway, our present techniques do not allow us to obtain this stronger statement. A statement of this kind for the Hadamard quotient theorem is proved, with different methods, in [2] or in [3] (the latter also deals in some cases with the root theorem). Some generalizations along the same lines are worked out in [6, 7].

The main theorem has a simple corollary, which deals with the case where the equation is not necessarily monic.

Corollary 1.9. *Let K be a number field, $b_0, \dots, b_d \in \mathcal{H}(K)$, and suppose that for every $n \in \mathbb{N}$ the equation*

$$b_d(n)Y^d + b_{d-1}(n)Y^{d-1} + \cdots + b_0(n) = 0 \tag{1.3}$$

has a solution $a_n \in K$. Then there exists a finite extension K'/K and two recurrence sequences $\{a_1(n)\}_{n\in\mathbb{N}}, \{a_2(n)\}_{n\in\mathbb{N}} \in \mathcal{H}(K')$ such that the sequence obtained as a component-wise quotient $a(n) = a_1(n)/a_2(n)$ (whenever defined) is a solution of (1.3).

To obtain the final form of our theorem we use for convenience a strengthening of the Hadamard quotient theorem, proved by Corvaja and Zannier in [2]. In Section 5 we give a precise statement of a corollary of their theorem that we need. Combining this with Corollary 1.9 we get our most general result:

Theorem 1.10. *In the hypothesis of Corollary* 1.9 *suppose moreover that the sequence of solutions $\{a_n\}_{n\in\mathbb{N}}$ to* (1.3) *can be taken inside a finitely generated ring. Then there exists a finite extension K'/K and a series $\sum a(n)x^n \in \mathcal{H}(K')$ such that $a(n)$ is a solution of* (1.3) *for all n such that $b_d(n) \neq 0$.*

Remark 1.11. A recent paper by Corvaja ([1]) gives another perspective on these theorems. Corvaja restates our results in the context of actions of algebraic groups over algebraic varieties. The theory appears there because the entries of a power A^n of a matrix are given by linear recurrences in n. In particular, Corvaja, using Theorem 1.4, proves the following

Theorem 1.12 (Corvaja). *Let K be a number field and G be a connected linear algebraic group, defined over K. Let V be a smooth affine algebraic variety and $\pi : V \mapsto G$ a finite map, both defined over K. Let $\Gamma \subset G(K)$ be a Zariski-dense semigroup. If Γ is contained in the set $\pi(V(K))$, then there exists a connected component V' of V such that the restriction $\pi\big|_{V'} : V' \mapsto G$ is an unramified cover. In particular V' has the structure of an algebraic group over K.*

As explained there, this can be seen as a geometric generalization of the Hilbert irreducibility theorem. Our result is used as a crucial starting point, giving the preceding assertion for the case where Γ is a cyclic subgroup of $\mathbb{G}_m^n$ (here and sequel $\mathbb{G}_m$ denotes the multiplicative group scheme).

As we will see in the proofs, a central point of our argument is to guarantee that, given an absolutely irreducible polynomial $t(X_1, \dots, X_r, Y)$ over the number field K (satisfying suitable conditons), we can find some suitable roots of unity $\{\zeta_i\}$ such that the specialized polynomial $t(\zeta_1, \dots, \zeta_r, Y)$ remains irreducible over $K(\zeta_i)$. In the Master thesis [5] this was achieved with a reduction modulo some prime and an application of the Lang-Weil theorem. Although this approach is more complicated, it should be useful in other contexts. This step is simplified in the present proof by using a strong form of Hilbert irreducibility theorem for cyclotomic fields, obtained by Dvornicich and Zannier in [4]; this work, in turn, is based on a result of Loxton ([8]), which bounds the number of addends necessary to write a cyclotomic integer α as a sum of roots of unity in terms of the maximum absolute value of the conjugates of α over $\mathbb{Q}$.

Before turning to the proofs we summarize here our notation.

$K, \tilde{K}$	number fields
K^*	the multiplicative group of the field K
$\mathcal{R}$	a ring of integers over a number field
$\mathcal{P}, \mathcal{Q}$	prime ideals in $\mathcal{R}$
$\mathcal{H}(K)$	the Hadamard ring over the field K
K^c	the maximal cyclotomic extension of a field K
$a(n), b(n)$	exponential polynomials, or the corresponding recurrence sequences
f, g, h	polynomials or Laurent polynomials
$\deg_Y f$	the degree of the polynomial f in the Y variable
$\mathbf{X}$	the vector of indeterminates $(X_1, \dots, X_r)$
$\mathbf{a}, \mathbf{b}$	multiindices
$\mathbf{X}^{\mathbf{a}}$	$X_1^{a_1} \cdots X_r^{a_r}$
$\mathfrak{A}, \mathfrak{A}'$	arithmetic progressions
$\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$	elements of Galois groups
$\mathbb{G}_m$	the multiplicative group variety GL_1
ζ	some root of unity
ω_n	a primitive n-th root of unity

Note that we use a different symbol to distinguish between some generic root of unity and one of a fixed order.

ACKNOWLEDGEMENT. We wish to thank Pietro Corvaja and Antonella Perucca for helpful comments. It is also a pleasure to thank the referee for his very detailed and useful report.

2. Some reductions

In the next sections we present the proof of Theorem 1.4; in the present section we make some easy reductions, while the following section collects some techniques about the specialization of polynomials at roots of unity, which will be central in our argument.

The proof will be divided in several steps. The first two steps will fix some notation and make some reductions, while the crux of the arguments will appear from Step 3 onwards. At the end of Step 2, when we have fixed our notation, we present a brief sketch of how the proof will go on.

Step 1. *Reduction to the case when the multiplicative subgroup generated by the β_i inside K^* is free.*

Namely we prove the following fact.

Lemma 2.1. *In proving Theorem* 1.7 *it is possible to assume as well that the multiplicative subgroup Γ of K^* generated by $\{\beta_i \mid i = 1, \dots, m\}$ is free.*

Proof. Let N be the order of the torsion part of Γ. Consider the exponential polynomials $b_{j,r}(n) = b_j(r + Nn)$, for some fixed r, $0 \le r \le N - 1$; their roots are the β_i^N, so they generate a torsion-free group. Suppose that the conclusion of the theorem holds under the additional hypothesis of this lemma: we then get some exponential polynomials $a_r(n)$ such that

$$a_r(n)^d + b_{d-1,r}(n)a_r(n)^{d-1} + \cdots + b_{0,r}(n) = 0.$$

We may choose exponential polynomials $c_r(n)$ such that $c_r(Nn) = a_r(n)$. We remark that the exponential polynomial

$$\theta(n) = \frac{1}{N}\sum_{i=1}^{N} \omega_N^n$$

takes the value 1 for $N|n$ and 0 otherwise. We define

$$a(n) = \sum_{r=0}^{N-1} \theta(n - r)c_r(n - r).$$

In this way if $n = s + Nm$, with $0 \le s \le N - 1$, we find $a(n) = a(s + Nm) = c_s(Nm) = a_s(m)$, and so equation (1.2) is satisfied. □

We shall henceforth work under the additional hypothesis that Γ is free. Having chosen a multiplicative basis $\gamma_1, \dots, \gamma_r$ we can write

$$b_j(n) = f_j(n, \gamma_1^n, \dots, \gamma_r^n),$$

where the f_j are rational function in $X_0, \ldots, X_r$ of the special form

$$f_j(X_0, \ldots, X_r) = \frac{\widetilde{f}_j(X_0, \ldots, X_r)}{X_1^{a_1} \cdots X_r^{a_r}},$$

$\widetilde{f}_j$ a polynomial. As usual we call such a rational function a *Laurent polynomial* (in the variables $X_1, \ldots, X_r$); in other words a Laurent polynomial is just an element of $K[X_0, X_1, X_1^{-1}, \ldots, X_r, X_r^{-1}]$. For all we need to do in this paper Laurent polynomials behave much like the classical ones. In particular the ring of Laurent polynomials is a localization of $\overline{K}[X_0, \ldots, X_r]$, hence a unique factorization domain.

Step 2. *Reduction to the problem of proving that some equations have solution in a ring of Laurent polynomials.*

Consider the equation

$$Y^d + f_{d-1}(X_0, X_1^D \ldots, X_r^D)Y^{d-1} + \cdots + f_0(X_0, X_1^D \ldots, X_r^D) = 0 \qquad (2.1)$$

where we look for a solution $Y = Y(X_0, \ldots, X_r)$ in the form of a Laurent polynomial in $X_0, \ldots, X_r$. If (2.1) has such a solution the conclusion of the theorem is proved: it is sufficient to put

$$a(n) = Y(n, \alpha_1^n, \ldots, \alpha_r^n),$$

where α_i is a D-th root of γ_i. By construction (1.2) holds.

Remark 2.2 (Geometric interpretation). As n varies in $\mathbb{N}$, the $(r+1)$-tuple $(n, \gamma_1^n, \ldots, \gamma_r^n)$ describes a cyclic subsemigroup C of $\mathbb{A}^1 \times \mathbb{G}_m^r$. The equation (2.1) defines a subvariety V of $\mathbb{A}^1 \times \mathbb{G}_m^r \times \mathbb{A}^1$; projection on the first $r+1$ coordinates gives a ramified covering of degree d

$$\pi : V \to \mathbb{A}^1 \times \mathbb{G}_m^r.$$

The hypothesis that equation (1.1) has a solution for all n can be rephrased saying that $C \subset \pi(V(K))$. The conclusion that we are trying to obtain is that for some D there is a Laurent polynomial $Y(X_0, \ldots, X_r)$ satisfying (2.1). Consider the unramified covering

$$\begin{aligned} \rho_D : \mathbb{A}^1 \times \mathbb{G}_m^r &\longrightarrow \mathbb{A}^1 \times \mathbb{G}_m^r. \\ (X_0, \ldots, X_r) &\longrightarrow (X_0, X_1^D, \ldots, X_r^D). \end{aligned}$$

This induces a cartesian diagram

$$\begin{array}{ccc} V' & \longrightarrow & V \\ \downarrow{\scriptstyle \pi'} & & \downarrow{\scriptstyle \pi} \\ \mathbb{A}^1 \times \mathbb{G}_m^r & \xrightarrow[\rho_D]{} & \mathbb{A}^1 \times \mathbb{G}_m^r, \end{array}$$

where V' is the fibered product of V and $\mathbb{A}^1 \times \mathbb{G}_m^r$. The Laurent polynomial $Y(X_0, \dots, X_r)$ gives rise to a section $\tau\colon \mathbb{A}^1 \times \mathbb{G}_m^r \to V'$ of π'; the existence of this section means that a component of V' is a trivial covering of $\mathbb{A}^1 \times \mathbb{G}_m^r$. This implies that some component of V doesn't ramify over $\mathbb{A}^1 \times \mathbb{G}_m^r$.

This is the point of view of [4] (see Theorem 1), of [17] (see the conjecure at page 62) and of [1], where this construction is generalized to ramified coverings of connected linear algebraic groups.

To prove Theorem 1.4 we can thus assume by contradiction that for each $D \geq 1$ the equation (2.1) does not have a solution in the ring $K[X_0, X_1, X_1^{-1}, \dots, X_r, X_r^{-1}]$. Gauss' lemma guarantees that the same equation has no solutions in the quotient field of $\overline{K}[X_0, \dots, X_r]$. Define the Laurent polynomials

$$s_D(X_0, \mathbf{X}, Y) = Y^d + f_{d-1}(X_0, X_1^D \dots, X_r^D)Y^{d-1} + \cdots + f_0(X_0, X_1^D \dots, X_r^D);$$

our hypothesis is that these polynomials have no linear factors in Y.

Sketch of strategy. The rest of the proof will be as follows. We consider a sequence $s_{D_1}, s_{D_2}, \dots$, where D_i divides D_{i+1}, and we look at the number of irreducible factors: this number stabilizes after finitely many steps since each of these Laurent polynomials is monic in Y. So for divisible enough values of D, the number of factors does not change; fix one such D. We factorize s_D and work with one of the factors, call it t. We will be able to show that, since $\deg_Y t \geq 2$,

there is some arithmetic progression $\mathfrak{A}$ such that for all $n \in \mathfrak{A}$ the specialization $t(n, \gamma_1^n, \dots, \gamma_r^n, Y)$ does not have roots in the base field.

This is the main arithmetical point (it is almost the thesis of Theorem 1.7); it will be achieved in two steps.

First we show that the same property holds for most specializations of t at roots of unity; namely if $(\zeta_0, \dots, \zeta_r)$ are generic roots of unity (that is, they lie outside a Zariski closed set), then the specialized polynomial $t(\zeta_0, \dots, \zeta_r, Y)$ does not have roots in K. Actually we obtain the stronger result that it does not have solutions $\bmod \mathcal{Q}$ for some suitable ideal $\mathcal{Q}$ in the ring of integers of K. Hence in the next section we study a criterion for the irreducibility of the specialization of polynomials at roots of unity. It is here that we use [4], see Section 3 below.

For the second step we use Chebotarev's theorem in order to choose roots of unity ζ_i that satisfy the congruences $\zeta_0 \equiv n$ and $\zeta_i \equiv \gamma_i^n \pmod{\mathcal{Q}}$ whenever n ranges in an arithmetic progression $\mathfrak{A}$. Combining these two steps we obtain the claim.

This takes already care of all the cases when s_D is irreducible (and so equals t), for example the cyclotomic case treated in [16].

If s_D is reducible, then we make a change of variables, in order to restrict our exponential polynomials to the progression $\mathfrak{A}$. Then we repeat the same procedure with another factor of s_D, and so on. If in the process we end up with a linear factor, we are done; otherwise we end up with an arithmetic progression $\mathfrak{A}'$ such that (1.1) does not have solution for $n \in \mathfrak{A}'$.

3. Specialization of polynomials at roots of unity

Step 3. *A form of Hilbert irreducibility theorem for specializations at roots of unity.*

We will now prove the following result about the specialization of Laurent polynomials, as a corollary of work by Dvornicich and Zannier ([4]):

Proposition 3.1. *Let K be a number field and denote by K^c its maximal cyclotomic extension. Let f be a Laurent polynomial with coefficients in K^c and suppose that $f(X_1^{\mathbf{a}_1}, \ldots, X_r^{\mathbf{a}_r}, Y)$ is irreducible over K^c for every multiindex $\mathbf{a}$ with each $\mathbf{a}_i \leq \deg_Y f$. Then there exists a subvariety $W \subsetneq \mathbb{G}_m^{r+1}$ such that if the ζ_i are roots of unity and $(\zeta_1, \ldots, \zeta_r) \notin W$, the specialized polynomial $f(\zeta_1, \ldots, \zeta_r, Y)$ is irreducible in $K^c[Y]$.*

We shall make use of the following result from [12, Section 1.2, Lemma 2]

Proposition 3.2. *Let K be a field and $f \in K[\mathbf{X}, Y]$; there exist a polynomial $g \in K[\mathbf{X}, Y]$ and a non-zero polynomial $g_1 \in K[\mathbf{X}]$ with the following property. Suppose $x_1, \ldots, x_r$ lie in some extension L of K and $g_1(x_1, \ldots, x_r) \neq 0$; then $f(x_1, \ldots, x_r, Y)$ is reducible in $L[Y]$ if, and only if, $g(x_1, \ldots, x_r, Y)$ has a root in L.*

Actually the proposition is stated there for polynomials, but it is easy to derive the conclusion for Laurent polynomials as well. To prove Proposition 3.1 we will also need the following

Proposition 3.3. *Let $f(X_1, \ldots, X_r, Y)$ be a Laurent polynomial with coefficients in some field K, and suppose that $f(\mathbf{X}^{\mathbf{a}_1}, \ldots, \mathbf{X}^{\mathbf{a}_r}, Y)$ is reducible over K for some multiindices $\mathbf{a}_1, \ldots, \mathbf{a}_r \in \mathbb{Z}^r$. Suppose moreover that the $\mathbf{a}_i$ are linearly independent. Then there is a $m \leq \deg_Y f$ such that $f(X_1^m, \ldots, X_r^m, Y)$ is reducible over K.*

Proof. It is easy to see that any rank r lattice $\mathcal{L}$ inside $\mathbb{Z}^r$ contains a sublattice of the form

$$\langle (M, 0, \ldots, 0), (0, M, 0, \ldots, 0), \ldots, (0, \ldots, 0, M) \rangle ,$$

where M is the discriminant of $\mathcal{L}$. In fact if $B(\mathcal{L})$ is a matrix whose columns form a basis of $\mathcal{L}$ and $B'(\mathcal{L})$ is the cofactors matrix, then $B'(\mathcal{L}) \cdot B(\mathcal{L}) = M\mathrm{I}$, I being the identity matrix.

Moreover if the $\mathbf{b}_j$ form a sublattice of the lattice spanned by the $\mathbf{a}_j$, then by substitution we obtain that $f(\mathbf{X}^{\mathbf{b}_1}, \ldots, \mathbf{X}^{\mathbf{b}_r}, Y)$ is reducible too. Combining these facts we can assume that we have a factorization

$$f(X_1^M, \ldots, X_r^M, Y) = f_1(X_1, \ldots, X_r, Y) \cdots f_m(X_1, \ldots, X_r, Y)$$

for some $M \in \mathbb{N}$. We get an action of $(\mathbb{Z}/M\mathbb{Z})^r$ on the set $\{f_1, \ldots, f_m\}$ of factors by letting

$$(a_1, \ldots, a_r).f_i(X_1, \ldots, X_r, Y) = f_i(\omega_M^{a_1} X_1, \ldots, \omega_M^{a_r} X_r, Y).$$

The index of the stabilizer of the factor f_1 is $m' = \#\mathrm{Orb}(f_1) \leq m$, hence this stabilizer contains a subgroup of the form

$$k_1\mathbb{Z}/M\mathbb{Z} \times \cdots \times k_r\mathbb{Z}/M\mathbb{Z},$$

where k_i divides m'. This means that each monomial in f_1 involves the variable X_i at a power multiple of M/k_i, which in turn is a multiple of M/m'; hence we can write $f_1(X_1, \ldots, X_r, Y) = f_1'(X_1^{M/m'}, \ldots, X_r^{M/m'}, Y)$. The same holds for the complementary factor. But this implies that $f(X_1^{m'}, \ldots, X_r^{m'}, Y)$ is already reducible, and by construction $m' \leq \deg_Y f$ □

Proof of Proposition 3.1. By contradiction. Assume that there exists a set Z of roots of unity, Zariski dense in $\mathbb{G}_m$, such that $f(\zeta_1, \ldots, \zeta_r, Y)$ is reducible over K^c for each choice of $(\zeta_1, \ldots, \zeta_r) \in Z$. We apply Proposition 3.2 to f; let g and g_1 be as in the conclusion. It is not restrictive to suppose that for $(\zeta_1, \ldots, \zeta_r) \in Z$ we have $g_1(\zeta_1, \ldots, \zeta_r) \neq 0$; then Proposition 3.2 guarantees that $g(\zeta_1, \ldots, \zeta_r, Y)$ has a root in K^c. If g is reducible, there is at least one of his irreducible factors g_2 such that the subset of Z for which $g_2(\zeta_1, \ldots, \zeta_r, Y)$ has a root in K^c is still dense; we replace Z by this smaller subset.

We apply Theorem 1 of [4] with V the zero locus of g_2 inside $\mathbb{G}_m^{r+1}$ and $\pi : V \mapsto \mathbb{G}_m^r$ the projection on the X coordinates. The hypothesis of the theorem require that the subset J of V consisting of those elements mapping to roots of unity is dense in V. By construction we know that $\pi(J) \supset Z$, so it is dense in $\mathbb{G}_m^r$. It follows that $\dim \overline{J} \geq r$, so J is actually dense in V by irreducibility.

The theorem gives us a lot of information. First, it guarantees that the closure of $\pi(V)$ has the form ζT, where T is a subtorus of $\mathbb{G}_m^r$, and ζ is torsion. In our case T equals $\mathbb{G}_m^r$, since we already know that $\pi(V)$ is dense. Moreover it asserts the existence of an isogeny $\mu : T \mapsto T$ and a rational map $\rho : T \dashrightarrow V$, defined over K^c, such that $\pi \circ \rho = \zeta \cdot \mu$.

In our situation we can assume that $\zeta = 1$, since T is the whole $\mathbb{G}_m^r$. Moreover it is well known that any isogeny $\mu : \mathbb{G}_m^r \mapsto \mathbb{G}_m^r$ is of the form

$$(x_1, \ldots, x_r) \mapsto (\mathbf{x}^{\mathbf{a}_1}, \ldots, \mathbf{x}^{\mathbf{a}_r})$$

for suitable linearly independent multiindices $\mathbf{a}_i$. The rational map ρ can be written as $\big(R_1(X_1, \ldots, X_r), \ldots, R_{r+1}(X_1, \ldots, X_r)\big)$, where the $R_i \in K^c(X_1, \ldots, X_r)$. The fact that ρ takes values in V can be translated saying that

$$g_2\big(R_1(X_1, \ldots, X_r), \ldots, R_{r+1}(X_1, \ldots, X_r)\big) = 0.$$

The fact that it is, up to isogeny, a section of π means that $R_i(X_1, \ldots, X_r) = \mathbf{X}^{\mathbf{a}_i}$ for $i = 1, \ldots, r$. So *a fortiori*

$$g\big(\mathbf{X}^{\mathbf{a}_1}, \ldots, \mathbf{X}^{\mathbf{a}_r}, R_{r+1}(X_1, \ldots, X_r)\big) = 0.$$

This means that $g(\mathbf{X}^{\mathbf{a}_1}, \ldots, \mathbf{X}^{\mathbf{a}_r}, Y)$ has a root in $K^c(X_1, \ldots, X_r)$; by Proposition 3.2 again we obtain that $f(\mathbf{X}^{\mathbf{a}_1}, \ldots, \mathbf{X}^{\mathbf{a}_r}, Y)$ is reducible over K^c. Proposition 3.3 now allows us to conclude. □

Step 4. *The irreducibility properties of our polynomials.*

We do not know much about the irreducibility of our Laurent polynomials s_D, but let us vary D, making it more and more divisible. The number of factors will stabilize to a number less than $\deg_Y g$, since g is monic in the Y variable. So there is a D_0 such that if s_{D_0} factors as

$$s_{D_0}(X_0, \mathbf{X}, Y) = t_1(X_0, \mathbf{X}, Y) \cdots t_l(X_0, \mathbf{X}, Y),$$

then for every $M \in \mathbb{N}$

$$s_{MD_0}(X_0, \mathbf{X}, Y) = t_1(X_0, X_1^M, \ldots, X_r^M, Y) \cdots t_l(X_0, X_1^M, \ldots, X_r^M, Y)$$

will also be a decomposition into prime factors. Our hypothesis in Step 2 amounts to saying that $\deg_Y t_i \geq 2$ for each $i = 1, \ldots, l$.

It is not restrictive to assume that $D_0 = 1$, as we shall do from now on. In fact multiplying by D_0 the terms of an arithmetic progression yields another arithmetic progression (see also Step 4). We now want to specialize the first variable X_0 in such a way to preserve irreducibility. By the Hilbert irreducibility theorem ([12, Section 4.4]) we can find some $\theta \in K$ such that each factor $t_j(\theta, X_1^m, \ldots, X_r^m, Y)$ remains irreducible for $m \leq \deg_Y t_j$. Proposition 3.3 guarantees that $t_j(\theta, \mathbf{X}^{\mathbf{a_r}}, \ldots, \ldots \mathbf{X}^{\mathbf{a_r}}, Y)$ will be irreducible for each choice of linearly independent multi-indices $\mathbf{a}_j$.

4. Proof of the main theorem

Step 5. *Some irreducible factor t of s_D admits an irreducible specialization at roots of unity.*

We choose a rational prime β multiplicatively independent from the γ_i's, and put $\delta_i = \gamma_i \beta^{k_i}$, for some integers k_i which we shall choose later. The following lemma is proved in [16] (it is here that we make use of the fact that the multiplicative group Γ is free).

Lemma 4.1 ([16]). *There exists a number L such that, whenever we take $M \geq 1$ and a prime $\ell > L$, then β^M doesn't belong to the multiplicative group generated by the δ_i and by $((K^c)^*)^{\ell M}$. The number L depends on K, β and γ_i, but it doesn't depend on the k_i.*

We fix once and for all a natural number L greater than $\deg_Y g$ and big enough for the preceding lemma to hold. Consequently we choose D divisible by each prime factor less than L and big enough, so that the inclusion $\mathbb{Q}^c \cap K \subset \mathbb{Q}(\omega_D)$ holds. The latter choice will guarantee that for each $c \geq 1$, $\mathbb{Q}(\omega_{cD})/\mathbb{Q}(\omega_D)$ and $K(\omega_D)/\mathbb{Q}(\omega_D)$ are linearly disjoint extensions.

Now we fix some factor t, say t_1, of s; we will work with this polynomial until the last step. Let us put

$$\widetilde{t}(X_1, \ldots, X_r, Y) = t(\theta, X_1^D, \ldots, X_r^D, Y),$$

where θ is defined at the end of the previous section.

Lemma 4.2. *Let $W \subsetneq \mathbb{G}_m^r$ be an algebraic subvariety of a torus, defined over K, and fix a natural number M. Then there exist roots of unity $\zeta_1, \dots, \zeta_r$ such that*:

i) $(\zeta_1, \dots, \zeta_r) \notin W(K^c)$
ii) *the order of each ζ_j is not multiple of a prime less than M.*

Proof. Let S be the set of roots of unity whose order is not multiple of a prime less than M. Since S is infinite, it is dense in $\mathbb{G}_m$. It follows that S^r is dense in $\mathbb{G}_m^r$. □

The preceding lemma, together with Proposition 3.1, allows us to fix roots of unity $\zeta_1, \dots, \zeta_r$ such that the multiplicative order of ζ_j is not multiple of a prime smaller than L, and at the same time

$$h(Y) = \widetilde{t}(\zeta_1, \dots, \zeta_r, Y) \tag{4.1}$$

remains irreducible over K.

Step 6. *We prove that the specialized polynomial h has no roots, even modulo some suitable primes.*

We start with a lemma.

Lemma 4.3. *There exist infinitely many primes of the form $p = 1 + Dm$ such that*

i) *every prime factor of m is greater than L*
ii) *we can write $\zeta_i = \omega_{p-1}^{k_i}$ for suitable integers k_i.*

Proof. This is an easy consequence of Dirichlet's theorem on the existence of primes in arithmetic progressions. Let c be the lowest common multiple of the orders of $\zeta_0, \dots, \zeta_r$. We need a prime p satisfying the following congruences:

$$\begin{cases} p \equiv 1 \pmod{Dc} \\ p \not\equiv 1 \pmod{D\ell} \text{ for each prime } \ell \le L. \end{cases} \tag{4.2}$$

Indeed the first congruence guarantees that p can be written in the form $1 + Dm$ for some m, and that $p - 1$ is multiple of the order of every root of unity ζ_i, while the second condition implies that m doesn't have any prime factor smaller than L. Thanks to the chinese remainder theorem and Dirichlet's theorem we find a prime solution to (4.2). □

The preceding lemma allows to fix the numbers k_i mentioned at the beginning of the section. We define

$$\begin{aligned} \tilde{K} &= K(\omega_{p-1}) \\ E &= K(\omega_{p-1}, \beta^{1/m}, \delta_1^{1/m}, \dots, \delta_r^{1/m}). \end{aligned} \tag{4.3}$$

Lemma 4.4. *The polynomial h defined in* (4.1) *remains irreducible in E.*

Proof. Assume this is not the case, and factor h as $h = h_1 h_2$ where $0 < d_i = \deg h_i < \deg h$. Let E' be obtained by adding a root of h_1 to E. By Kummer theory we know that $[E : \tilde{K}]$ divides a power of m, so $[E' : \tilde{K}]$ divides d_1 times a power of m. On the other hand, by construction h admits a root in E', so $\deg h$ divides $[E' : \tilde{K}]$; this is impossible since each prime factor of m is $> L \geq d$. □

Lemma 4.5.

$$[E : K(\omega_{p-1}, \delta_1^{1/m}, \ldots, \delta_r^{1/m})] = m. \tag{4.4}$$

Proof. If the degree were lower, it would be a proper divisor of m, again by Kummer theory. Take a prime ℓ such that this degree divides m/ℓ. We can apply Kummer theory to the field $\tilde{K}$: the two groups

$$\Delta = \langle (\tilde{K}^*)^m, \beta, \delta_1, \ldots, \delta_r \rangle$$
$$\Delta' = \langle (\tilde{K}^*)^m, \beta^\ell, \delta_1, \ldots, \delta_r \rangle$$

define the same extension $E/\tilde{K}$, so they coincide. In particular we can express

$$\beta = \alpha^m \beta^{\ell a_0} \delta_1^{a_1} \cdots \delta_r^{a_r}$$

for some $\alpha \in \tilde{K}$. But this contradicts Lemma 4.1 with $M = 1$ (note that $\ell > L$). □

Since the extension $E/k(\omega_{p-1}, \delta_1^{1/m}, \ldots, \delta_r^{1/m})$ is cyclic we can take a generator $\mathfrak{a}$ of its Galois group.

Lemma 4.6. *Call E' the splitting field of $h(Y)$ over E. There exists $\mathfrak{b} \in Gal(E', \tilde{K})$ such that*:

i) $\mathfrak{b}\big|_E = \mathfrak{a}$,

ii) *if y is a root of h, then $\mathfrak{b}(y) \neq y$.*

Proof. We first show the existence of some $\mathfrak{c} \in G = \mathrm{Gal}(E', \tilde{K})$ satisfying ii). This amounts to proving that the union of the stabilizers of the roots of h is not all of G. By the irreducibility of h these stabilizers are conjugate subgroups. Let H be one of them; then there are at most $|G|/|H|$ stabilizers, each one of order $|H|$, so the union cannot be all of G (they all contain the identity).

Let $\tilde{\mathfrak{c}} = \mathfrak{c}\big|_E \in \mathrm{Gal}(E, \tilde{K})$, and $\mathfrak{d} = \tilde{\mathfrak{c}}^{-1}\mathfrak{a}$. We only need to extend $\mathfrak{d}$ to E' in such a way that $\mathfrak{d}(y) = y$ for every root y of h. If we call F the splitting field of h over $\tilde{K}$, so that $E' = EF$, we reduce to the problem of verifying that E and F are linearly disjoint over $\tilde{K}$. This follows by comparison of the degrees: $[F : \tilde{K}]$ divides $d!$, while $[E : \tilde{K}]$ divides some power of m, and each prime factor of m is $> L \geq d$. □

Let $\mathcal{R}$ be the ring of integers of $\tilde{K}$. By the Chebotarev theorem we get a set of primes $\mathcal{Q}$ of $\mathcal{R}$, of positive density, whose Frobenius verifies $\phi(\mathcal{Q}'|\mathcal{Q}) = \mathfrak{b}$ in E', for some prime $\mathcal{Q}'$ over $\mathcal{Q}$. We do not affect the density if we further ask that $\mathcal{Q}$ is unramified over the rationals. Subject to these conditions, we take a big prime $\mathcal{Q}$ at which the reductions of β, γ_j and f_j are defined, and call $\mathcal{Q}'$ a prime over it such that $\phi(\mathcal{Q}'|\mathcal{Q}) = \mathfrak{b}$.

Lemma 4.7. *If $\mathcal{Q}$ has big enough norm, then the congruence $h(Y) \equiv 0 \pmod{\mathcal{Q}}$ has no solutions.*

Proof. First we remark that if $\mathcal{Q}$ is big enough, h has distinct roots mod $\mathcal{Q}$. Let y be one of such roots: by Lemma 4.6 we know that $\mathfrak{b}(y) \neq y$. If $\mathcal{Q}$ has big enough norm and $\mathcal{Q}'$ is above $\mathcal{Q}$, then $\mathcal{Q}'$ is not a prime factor of the number $\mathfrak{b}(y) - y$ for any root y of h. Hence for every root y we have $\mathfrak{b}(y) \not\equiv y \pmod{\mathcal{Q}'}$.

This means that the Frobenius of $\mathbb{F}_q = \mathcal{R}/\mathcal{Q}$ does not fix the class $\overline{y}$ in the algebraic closure $\overline{\mathbb{F}_q}$ of $\mathbb{F}_q$; that is, h has no roots mod $\mathcal{Q}$. □

Step 7. *Here we prove that when n is chosen in a suitable arithmetic progression, the polynomial $t(n, \gamma_1^n, \dots, \gamma_r^n, Y)$ has no roots in the base field.*

Lemma 4.8. *There exists an arithmetic progression $\mathfrak{A}$ such that if $n \in \mathfrak{A}$, then for each $j = 1, \dots, r$*

$$\begin{cases} n \equiv \theta & \pmod{\mathcal{Q}} \\ \gamma_j^n \equiv \omega_m^{k_j} & \pmod{\mathcal{Q}}. \end{cases}$$

Proof. Denote $q = N_{\mathbb{Q}}^{\tilde{K}}(\mathcal{Q})$ the norm of $\mathcal{Q}$. By our choices we know that q splits completely in $\mathbb{Q}(\omega_{p-1})$, so we deduce that $q \equiv 1 \pmod{p-1}$, and in particular $m | q - 1$. Moreover $\mathfrak{b}$ fixes each $\delta_j^{1/m}$, so δ_j is a m-th power mod $\mathcal{Q}$, hence

$$\delta_j^{\frac{q-1}{m}} \equiv 1 \pmod{\mathcal{Q}}.$$

Similarly $\mathfrak{b}(\beta) = \omega_m^a \beta$ for some a, which is coprime with m by (4.4), so

$$\beta^{\frac{q-1}{m}} \equiv \omega_m^a \pmod{\mathcal{Q}}.$$

Putting the two relations together we deduce

$$\gamma_j^{\frac{q-1}{m}} \equiv \omega_m^{ak_j} \pmod{\mathcal{Q}}.$$

Calling b the inverse of $a \bmod m$ we find that

$$\gamma_j^{b\frac{q-1}{m}} \equiv \omega_m^{k_j} \pmod{\mathcal{Q}}.$$

Moreover, we can take $c \in \mathbb{N}$ satisfying $c \equiv \theta \pmod{\mathcal{Q}}$. If $n \in \mathbb{N}$ is a solution of the congruences

$$n \equiv c \pmod{q}, \qquad n \equiv b\frac{q-1}{m} \pmod{q-1},$$

then we have the relations

$$\begin{cases} n \equiv \theta & (\text{mod } \mathcal{Q}) \\ \gamma_j^n \equiv \omega_m^{k_j} & (\text{mod } \mathcal{Q}) \quad j = 1, \ldots, r. \end{cases} \tag{4.5}$$

□

We fix an arithmetic progression

$$\mathfrak{A} = \{an + b,\ n \in \mathbb{N}\} \tag{4.6}$$

satisfying the conclusion of Lemma 4.8.

Lemma 4.9. *Assume that $n \in \mathfrak{A}$. Then the polynomial $t(n, \gamma_1^n, \ldots, \gamma_r^n, Y)$ has no roots in K.*

Proof. The conditions (4.5) imply that

$$t(n, \gamma_1^n, \ldots, \gamma_r^n, Y) \equiv t(\theta, \omega_{p-1}^{k_1}, \ldots, \omega_{p-1}^{k_r}, Y) \equiv h(Y) \pmod{\mathcal{Q}}.$$

If $t(n, \gamma_1^n, \ldots, \gamma_r^n, Y)$ had a root in K, then h would have a root mod $\mathcal{Q}$, which is excluded by Lemma 4.7 □

Step 8. *Conclusion of the proof of Theorem* 1.7.

Now if t_1 is the only factor of s, we are done. Otherwise we proceed in the following way. Let $a, b \in \mathbb{N}$ be given by (4.6). We operate the substitution

$$t_i'(X_0, X_1, \ldots, X_r, Y) = t_i(aX_0 + b, \gamma_1^b X_1^a, \ldots, \gamma_r^b X_r^a, Y).$$

This amounts to restricting the corresponding recurrence sequences to $\mathfrak{A}$. In this way we do not have to care about the factor t_1, and we proceed with the next factor. The t_i' may not be irreducible anymore, but after further factorization and relabeling we assume that t_2' is irreducible. If t_2' has degree greater than one, we call it t and repeat the whole procedure on and on. Since the t_i are monic polynomials in Y, the process must stop in at most $(\deg_Y s)/2$ steps. Eventually one of the following cases will happen:

i) We get an arithmetic progression $\mathfrak{A}' = \{a'n + b',\ n \in \mathbb{N}\}$ and a degree one (in the last variable) factor of $s(a'X_0 + b', \gamma_1^{b'} X_1^{a'}, \dots, \gamma_r^{b'} X_r^{a'}, Y)$, say $Y - Y(X_0, \dots, X_r)$. In this case let us take α_i such that $\alpha_i^{a'} = \gamma_i$. Put $a(n) = Y(n/a', \alpha_1^n \dots, \alpha_r^n)$; then $a(n)$ is an exponential polynomial, and the relation

$$S(a'X_0 + b', \gamma_1^{b'} X_1^{a'}, \dots, \gamma_r^{b'} X_r^{a'}, Y(X_0, \dots, X_r)) = 0$$

gives, for $X_0 = n/a'$ and $X_i = \alpha_i^n$,

$$S(n + b', \gamma_1^{n+b'}, \dots, \gamma_r^{n+b'}, a(n)) = 0,$$

that is

$$a(n)^d + b_{d-1}(n + b)a(n)^{d-1} + \cdots + b_0(n + b) = 0,$$

so we have a solution of the original equation in the Hadamard ring.

ii) We never get a degree one factor. In this case, after at most $d/2$ steps we end with an arithmetic progression $\mathfrak{A}' = \{a'n + b',\ n \in \mathbb{N}\}$ such that (1.1) has no solution in K for $n \in \mathfrak{A}'$, which is the thesis. □

5. Proof of the remaining assertions

The aim of the present section is to prove Corollary 1.9 and Theorem 1.10, which deal with not necessarily monic equations.

Proof of Corollary 1.9. Multiplying (1.3) by $b_d(n)^{d-1}$ and putting $Z = b_d(n)Y$ we obtain the equation

$$Z^d + b_{d-1}(n)Z^{d-1} \cdots + b_0(n)b_d(n)^{d-1} = 0;$$

this has a solution $a_2(n) \in \mathcal{H}(k')$ for some finite extension K'/K, thanks to Theorem 1.4. Putting $a_1(n) = b_d(n)$ we get the thesis. □

Preliminary to the proof of Theorem 1.10 we cite a stronger form of the Hadamard quotient theorem, due to Corvaja and Zannier ([2, Corollary 2])

Theorem 5.1. *Let K be a number field and $R \subset K$ a finitely generated ring. Let $\sum b(n)x^n, \sum c(n)x^n \in \mathcal{H}(K)$ and assume that their roots generate a torsion-free group. Then either $b(n)/c(n)$ is a recurrence sequence or the set of natural numbers n for which $b(n)/c(n) \in R$ has zero density.*

We will also need the Skolem-Mahler-Lech theorem (see [14]).

Theorem 5.2 (Skolem, Mahler, Lech). *Let K be a field of characteristic* 0 *and let $\{a(n)\}$ be a linear recurrence over K. Then the zero set of a*

$$\{n \in \mathbb{N} \mid a(n) = 0\}$$

is the union of a finite set with a finite number of arithmetic progressions.

Proof of Theorem 1.10. By Corollary 1.9 we know that we can find two recurrence sequences $\{a_1(n)\}$ and $\{a_2(n)\}$ such that $a_2(n)/a_1(n)$ satisfies equation (1.3) for every n such that the quotient is defined. We can argue as in Lemma 2.1 to restrict ourselves to the case where the roots of $\{a_1(n)\}$ and $\{a_2(n)\}$ generate a torsion-free group, call it G. Let us call A the ring of the recurrence sequences with roots in G. A is isomorphic to a localization of a polynomial ring over K: if $g_1, \ldots, g_r$ are free generators of G, then an isomorphism

$$\varphi\colon K[H, X_1, X_1^{-1} \ldots, X_r, X_r^{-1}] \mapsto A \tag{5.1}$$

is defined by sending $f(H, X_1, \ldots, X_r)$ to $\{f(n, g_1^n, \ldots, g_r^n)\}$. In particular A is a unique factorization domain. We can divide both a_1 and a_2 by their greatest common divisor in A, so we shall assume that a_1 and a_2 are relatively prime.

At first suppose that b_d never vanishes; then the same holds true for a_1, which divides b_d. In particular the quotient $a_2(n)/a_1(n)$ is always defined. The polynomial

$$b_d(n)Y^d + b_{d-1}(n)Y^{d-1} + \cdots + b_0(n)$$

is divisible by $a_1(n)Y - a_2(n)$ in $\tilde{K}[Y]$, where $\tilde{K}$ is the field of fractions of A; by Gauss' lemma the same is true in $A[Y]$. So we have a factorization of the original equation as

$$(a_1(n)Y - a_2(n))\left(c_{d-1}(n)Y^{d-1} + c_{d-2}(n)Y^{d-2} + \cdots + c_0(n)\right) = 0,$$

for suitable recurrence sequences $c_i(n)$. By induction on the degree, we know that either the equation

$$c_{d-1}(n)Y^{d-1} + c_{d-2}(n)Y^{d-2} + \cdots + c_0(n) = 0 \tag{5.2}$$

has a solution in some Hadamard ring (in which case we are done), or it is not solvable in the field K for all n in some arithmetic progression $\mathfrak{A}$. But then we must have $a_n = a_2(n)/a_1(n)$ for $n \in \mathfrak{A}$; by the theorem of Corvaja and Zannier the quotient of $a_2(n)$ by $a_1(n)$ is then a recurrence sequence itself.

Now consider the general case. By the theorem of Skolem-Mahler-Lech we know that the zero set of b_d is a union of a finite number of elements and a finite number of arithmetic progressions. Since we are working in $\mathcal{H}(K)$ we can disregard the finite number of terms; so we can assume that there is an $m \in \mathbb{N}$ and some numbers $n_1, \ldots, n_r \in \{0, \ldots, m-1\}$ such that $b_d(n) = 0$ if, and only if, $n \equiv n_i \pmod{m}$ for some i.

Fix a number $c \in \{0, \ldots, m-1\}$ different from all the n_i, and consider the equation

$$b_d(c + nm)Y^d + b_{d-1}(c + nm)Y^{d-1} + \cdots + b_0(c + nm) = 0.$$

The coefficients $b_i(c + nm)$ are linear recurrences in n (up to a finite number of terms), and by construction $b_d(c+nm)$ never vanishes. By the first part of the proof

we can find a series $\sum a_c(n)x^n \in \mathcal{H}(K')$ such that $a_c(n)$ satisfies the equation for all n. For $c = n_i$ we can choose any linear recurrence a_c, for example put $a_c(n) = 0$ for all n.

As we have seen in the proof of Lemma 2.1, the exponential polynomial

$$\theta(n) = \frac{1}{m}\sum_{i=1}^{m} \omega_m^n$$

takes the value 1 for $m|n$ and 0 otherwise. Choose exponential polynomials $a'_c(n)$ such that $a'_c(mn) = a_c(n)$. We define

$$a(n) = \sum_{r=0}^{m-1} \theta(n-r)a'_r(n-r).$$

By construction $a(c + nm) = a_c(n)$ for all $c = 0, \dots, m-1$, so $a(n)$ satisfies equation (1.3) whenever $b_d(n) \neq 0$. □

Remark 5.3. With a bit more work we can do without the result of Corvaja and Zannier. Keep the notation of the proof and assume that (5.2) does not have a solution in a Hadamard ring. Then there is an arithmetic progression $\mathfrak{A}$ such that $a_n = a_2(n)/a_1(n)$ for $n \in \mathfrak{A}$.

Consider the restriction of $\{a_1(n)\}$ and $\{a_2(n)\}$ for $n \in \mathfrak{A}$. These are recurrence sequences, and for such n the quotients $a_2(n)/a_1(n) = a_n$ lie in R. By the Hadamard quotient theorem there exists a recurrence sequence $\{b(n)\}_{n\in\mathfrak{A}}$ such that $a_2(n)/a_1(n) = b(n)$ for all $n \in \mathfrak{A}$. We can extend b to a recurrence sequence $\{b(n)\}_{n\in\mathbb{N}}$ defined for all $n \in \mathbb{N}$, and we can do this in such a way that the roots of b lie in G. We claim that then the equality $a_2(n)/a_1(n) = b(n)$ holds for all $n \in \mathbb{N}$. This is easily seen using the isomorphism φ in (5.1).

In fact, call $f_1 = \varphi^{-1}(a_1)$, $f_2 = \varphi^{-1}(a_2)$ and $g = \varphi^{-1}(b)$. Moreover write $\mathfrak{A} = \{sn+t \mid n \in \mathbb{N}\}$; it is not restrictive, up to shifting the recurrence sequences, to assume that $t = 0$. Then the conclusion of the Hadamard quotient theorem amounts to saying that

$$f_2(sH, X_1^s, \dots, X_r^s) = f_1(sH, X_1^s, \dots, X_r^s)g(sH, X_1^s, \dots, X_r^s).$$

From this it is clear that $f_2 = f_1 g$, since the indeterminates $X_1^s, \dots, X_r^s$ are still algebraically independent.

References

[1] P. CORVAJA, *Rational fixed points for linear group actions*, 2007, Preprint, available at `http://www.arxiv.org/abs/math/0610661` to appear in Ann. Scuola Norm. Sup. Pisa Cl. Sci. (5).

[2] P. CORVAJA and U. ZANNIER, *Finiteness of integral values for the ratio of two linear recurrences*, Invent. Math. **149** (2002), 431–451.

[3] P. CORVAJA and U. ZANNIER, *Some new applications of the Subspace Theorem*, Compositio Math. **131** no. 3 (2002), 319–340.
[4] R. DVORNICICH and U. ZANNIER, *Cyclotomic diophantine problems (Hilbert irreducibility and invariant sets for polynomial maps)*, Duke Math. J. **139** (2007).
[5] A. FERRETTI, *Equazioni nell'anello di Hadamard*, Master thesis, available at http://etd.adm.unipi.it/theses/available/etd-08272004-153939/, 2004.
[6] C. FUCHS and A. SCREMIN, *Diophantine inequalities involving several power sums*, Manuscripta Math. **115** (2004), 163–178.
[7] C. FUCHS and A. SCREMIN, *Polynomial-exponential equations involving several linear recurrences*, Publ. Math. Debrecen **65** (2004), 149–172.
[8] J. H. LOXTON, *On the maximum modulus of cyclotomic integers*, Acta Arith. **22** (1972), 69–85.
[9] Y. POURCHET, *Solution du problème arithmétique du quotient de Hadamard de deux fractions rationnelles*, C. R. Acad. Sci. Paris **288** (1979), 1055–1057.
[10] R. RUMELY, *Notes on van der Poorten's proof of the Hadamard quotient theorem*, In: "Seminaire de Théorie des Nombres" Catherine Goldstein (ed.), Progress in Mathematics, no. 75, Birkhäuser, Boston – Basel, 1986-87, 349–409.
[11] R. RUMELY and A. J. VAN DER POORTEN, *A note on the Hadamard k^{th} root of a rational function*, J. Aust. Math. Soc. **43** (1987), 314–327.
[12] A. SCHINZEL, "Polynomials with Special Regard to Reducibility", Encyclopedia of mathematics and its applications, Vol. 77, Cambridge University Press, 2000.
[13] A. J. VAN DER POORTEN, *Solution de la conjecture de Pisot sur le quotient de Hadamard de deux fractions rationnelles*, C. R. Acad. Sci. Paris **306** (1988), 97–102.
[14] A. J. VAN DER POORTEN, *Some facts that should be better known, especially about rational functions*, In: "Number Theory and Applications", Richard A. Mollin (ed.), Kluwer Academic Publishers, Dordrecht, 1989, 497–528.
[15] A. J. VAN DER POORTEN, *A note on Hadamard roots of rational functions*, Rocky Mountain J. Math. **26** (1996), 1183–1197.
[16] U. ZANNIER, *A proof of Pisot's d^{th} root conjecture*, Ann. of Math. **151** (2000), 375–383.
[17] U. ZANNIER, "Some Applications of Diophantine Approximation to Diophantine Equations", Forum Editrice, Udine, 2002.

Dipartimento di Matematica
Sapienza Università di Roma
Piazzale Aldo Moro 2
00185 Roma, Italy
ferretti@mat.uniroma1.it

Scuola Normale Superiore
Piazza dei Cavalieri 7
56126 Pisa, Italy
u.zannier@sns.it