A Hilbert irreducibility type result for polynomials over the ring of power sums

Clemens Fuchs

University of Salzburg, Department of Mathematics
Hellbrunnerstr. 34/I, 5020 Salzburg

BIRS Workshop "Specialisation and Effectiveness in Number Theory"

August 29, 2022

Generalities

Let K be a number field and let S a finite set of places (containing the archimedean ones). We denote the absolute logarithmic Weil height of an element $x \in K^*$ by

$$h(x) = \sum_{\nu} \max\left(0, \log |x|_{\nu}\right)$$

and the S-height by

$$h_S(x) = \sum_{\nu \notin S} \max\left(0, \log |x|_{\nu}\right),$$

where the sums are taken over all places of K.

We denote by $\mathcal{O}_S$ the ring of S-integers and by $\mathcal{O}_S^{\times} \cong \mu(K) \times \mathbb{Z}^{|S|-1}$ its group of units. Observe that $\mathcal{O}_S$ is integrally closed.

Polynomials

We look at $f \in K[X]$.

Firstly, we are interested in $x \in K$ with $f(x) = 0$.

- If f is monic, then $f \in \mathcal{O}_S[X]$ and $x \in \mathcal{O}_S$ for a suitable S,
- $h(x) = O(1)$ implies that all $\mathcal{O}_S$-solutions are effectively computable.

Secondly, we want to describe the K-factorizations of f.

- Letting L be the splitting field of f, we can describe the roots effectively,
- by combination of the roots and by using elementary symmetric polynomials, we get all K-factorizations of f.

Power sums

A power sum is a map $G : \mathbb{N} \to K$ such that

$$n \mapsto a_1\alpha_1^n + \cdots + a_t\alpha_t^n =: G_n,$$

where $a_i \in K, \alpha_i \in K$ for $i = 1, \ldots, t$. We denote by $\mathcal{E}$ the ring of K*-power sums*. Power sums are simple linear recurrence sequences. The α_i are called the (characteristic) *roots* and the a_i are called the *coefficients* of the recurrence G_n.

In applications we usually consider

$$\mathcal{E}_A = \{G_n \in \mathcal{E}; \alpha_i \in A \text{ for } i = 1, \ldots, t\}$$

for A a finitely generated subgroup of K^*. If the number of generators $= r$, then $\mathcal{E}_A \cong K[X_1^{\pm 1}, \ldots, X_r^{\pm 1}]$. This ring is factorial, noetherian and, in particular, integrally closed.

Polynomials and Power sums

Let $f \in \mathcal{E}[X]$.

Again, we are first interested in $x \in K$ with $f(x) = 0$. In the literature one can find:

- $X^2 - G_n = 0$
- $X^q - G_n = 0$
- $f(X) - G_n = 0$
- $X^d + G_n^{i_1} X^{d-1} + G_n^{i_2} X^{d-2} + \cdots + G_n^{i_d} = 0$
- $H_n X - G_n = 0$
- $G_n^{(0)} X^d + \cdots + G_n^{(d)} = 0$

In all cases, under suitable but restrictive conditions, the following is shown: *The equation has finitely many solutions* (n, x) *unless the equation has a solution in the ring* $\mathcal{E}$ *for* X.

Corvaja-Zannier

Let $f(\mathbf{X}) = \sum_{\mathbf{i}} a_{\mathbf{i}} \mathbf{X}^{\mathbf{i}}$ be a power series with algebraic coefficients in $\mathbb{C}_\nu$ converging in a neighborhood of the origin in $\mathbb{C}_\nu^r$. Let $\mathbf{x}_n = (x_{n1}, \ldots, x_{nr})$ $(n = 1, 2, \ldots)$ be a sequence in K^{*r}, tending to zero in K_ν^r and such that $f(\mathbf{x}_n)$ is defined and belongs to K. Suppose that:

1. For $i = 1, \ldots, r$ we have $h_S(x_{ni}) + h_S(x_{ni}^{-1}) = o(h(x_{ni}))$ as $n \to \infty$.
2. $\widehat{h}(\mathbf{x}_n) = O(-\log(\max_i |x_{ni}|_\nu))$.
3. $h_S(f(\mathbf{x}_n)) = o(h(\mathbf{x}_n))$.
4. $h(f(\mathbf{x}_n)) = O(h(\mathbf{x}_n))$.

Then there exists a finite number of cosets $\mathbf{u}_1 H_1, \ldots, \mathbf{u}_t H_t \subseteq \mathbb{G}_{\mathrm{m}}^r$ such that $\{\mathbf{x}_n\}_{n \in \mathbb{N}} \subseteq \bigcup_{i=1}^t \mathbf{u}_i H_i$ and such that, for $i = 1, \ldots, t$, the restriction of $f(\mathbf{X})$ to $\mathbf{u}_i H_i$ coincides with a polynomial in $K[\mathbf{X}]$.

We consider

$$G_n^{(0)} Z^d + \cdots + G_n^{(d-1)} Z + G_n^{(d)} = 0,$$

where $G_n^{(i)}$ are K-power sums. We are, in a first step, interested in solutions $(n, z) \in \mathbb{N} \times \mathcal{O}_S$.

It follows that we can choose a common numbering $\beta_1, \ldots, \beta_r$ of all occurring characteristic roots and rewrite the equation as

$$a_0(\beta_1^n, \ldots, \beta_r^n) Z^d + \cdots + a_d(\beta_1^n, \ldots, \beta_r^n) = 0 \qquad (\bigstar)$$

with linear polynomials $a_0(X_1, \ldots, X_r), \ldots, a_d(X_1, \ldots, X_r)$. Therefore the problem translates into an equation given by a (rather special lacunary) polynomial for which we seek integral solutions in $\mathbb{G}_{\mathrm{m}}^r \times \mathbb{A}^1$.

Preliminaries

Conversely, every hypersurface in $\mathbb{G}_{\mathrm{m}}^r \times \mathbb{A}^1$ can be written in the form

$$a_0(X_1, \ldots, X_r)Z^d + \cdots + a_d(X_1, \ldots, X_r) = 0$$

for (not necessarily linear) polynomials $a_j(X_1, \ldots, X_r)$. The integral points on such a hypersurface are the elements of $(\mathcal{O}_S^\times)^r \times \mathcal{O}_S$ which satisfy the given equation. If the equation is monic in Z or the leading coefficient is a constant times a monomial in $X_1, \ldots, X_r$, then it describes a finite cover $W \to \mathbb{G}_{\mathrm{m}}^r$ given by projection on the first r components. We remark that all regular maps $\mathbb{G}_{\mathrm{m}} \to W$, i.e. function field integral points, of the finite cover $W \to \mathbb{G}_{\mathrm{m}}^r$ can be described.

Here, we specialize to a 1-parameter subgroup of $\mathbb{G}_{\mathrm{m}}^r$ for which ($\bigstar$) is the typical description.

Preliminaries

Let an equation of the form (★) be given.

Define

$$g(X_1, \ldots, X_r, Z) = a_0(X_1, \ldots, X_r)Z^d + \cdots + a_d(X_1, \ldots, X_r).$$

Furthermore, let $\widetilde{g} \in K[X_1, \ldots, X_r, \widetilde{Z}]$ be the polynomial given by the equation

$$\widetilde{g}(X_1, \ldots, X_r, a_0(X_1, \ldots, X_r)Z) = a_0(X_1, \ldots, X_r)^{d-1} g(X_1, \ldots, X_r, Z).$$

We assume that

- either $a_0(0, \ldots, 0) \neq 0$ and $g(0, \ldots, 0, Z)$ has no multiple zero as a polynomial in Z,
- or $a_0(0, \ldots, 0) = 0$ and $\widetilde{g}(0, \ldots, 0, \widetilde{Z})$ has no multiple zero as a polynomial in $\widetilde{Z}$.

Preliminaries

Let $\gamma_1, \ldots, \gamma_r \in K^*$ such that $|\gamma_i| < 1$ for all $1 \leq i \leq r$ and such that no ratio γ_i/γ_j for $i \neq j$ is a root of unity.

Assume that S is a finite set of places of K, containing all archimedean ones, and such that $\gamma_1, \ldots, \gamma_r$ and all non-zero coefficients of $a_i(X_1, \ldots, X_r)$ for $i = 0, \ldots, d$ are S-units.

Results & remarks

Theorem 1 (F.-Heintze)

Let $K, g, \widetilde{g}, \gamma_1, \ldots, \gamma_r$ and S be as above. Then there are finitely many cosets $\mathbf{u}_1 H_1, \ldots, \mathbf{u}_t H_t \subseteq \mathbb{G}_{\mathrm{m}}^r$ and for each coset $\mathbf{u}_i H_i$ a polynomial P_i in r unknowns such that the following holds: For each solution $(n, z) \in \mathbb{N} \times \mathcal{O}_S$ of $g(\gamma_1^n, \ldots, \gamma_r^n, z) = 0$ with $z \neq 0$ and n large enough, there exists an index i such that $(\gamma_1^n, \ldots, \gamma_r^n) \in \mathbf{u}_i H_i$ and $z' = P_i(\gamma_1^n, \ldots, \gamma_r^n)$, where $z' = z$ in the case $a_0(0, \ldots, 0) \neq 0$ and $z' = a_0(\gamma_1^n, \ldots, \gamma_r^n)z$ if $a_0(0, \ldots, 0) = 0$, respectively.

Results & remarks

- Let us emphasize that this result goes in the same direction as Corvaja and Zannier's result on $f(G_n, Z) = 0$ from 2002 and uses similar assumptions, though the results are not quite equal (in the sense that our result does not directly follow from theirs and vice-versa). Moreover, we completely build on the methods developed by them.
- In contrast to earlier results we have now a much more powerful tool in our hands; instead of applying the Subspace theorem we can apply Corvaja-Zannier, which leads to a much quicker proof.
- The main and most restrictive technical condition is the existence of "dominant roots". Without this condition one can currently expect only weaker results.

Results & remarks

Corollary (F.-Heintze)

Let $K, g, \widetilde{g}, \gamma_1, \ldots, \gamma_r$ *and* S *be as in Theorem 1. Then there are finitely many linear recurrences* $R_1(n), \ldots, R_s(n)$ *with algebraic roots and algebraic coefficients, arithmetic progressions* $\mathcal{P}_1, \ldots, \mathcal{P}_s$*, as well as finite sets* M *and* N *such that the set of solutions* $(n, z) \in \mathbb{N} \times \mathcal{O}_S$ *of the equation* $g(\gamma_1^n, \ldots, \gamma_r^n, z) = 0$ *is equal to*

$$\bigcup_{j=1}^{s} \{(n, R_j(n)) : n \in \mathcal{P}_j, R_j(n) \in \mathcal{O}_S\} \cup \{(n, z) : n \in N, z \in \mathcal{O}_S\} \cup M.$$

Results & remarks

Theorem 2 (F.-Heintze)

Let $K, g, \gamma_1, \dots, \gamma_r$ and S be as above. Moreover, assume that g is monic as a polynomial in Z, i.e. $a_0(X_1, \dots, X_r) = 1$. Then $g(\gamma_1^n, \dots, \gamma_r^n, Z)$ is reducible in $K[Z]$ for infinitely many $n \in \mathbb{N}$ if and only if there exist monic polynomials $h_1(n, Z)$, $h_2(n, Z)$, whose coefficients are linear recurrences with algebraic characteristic roots and algebraic coefficients, and an arithmetic progression $\mathcal{P}$ such that $g(\gamma_1^n, \dots, \gamma_r^n, Z) = h_1(n, Z)h_2(n, Z)$ is a factorization in $K[Z]$ for all $n \in \mathcal{P}$.

Results & remarks

- In the case that the polynomial g is not monic in Z, one can use the transformation to $\widetilde{g}$ written down in Theorem 1. Then $\widetilde{g}$ is monic in $\widetilde{Z}$ and the above theorem can be applied to it. Going back to g then yields the result that $g(\gamma_1^n, \ldots, \gamma_r^n, Z)$ is reducible in $K[Z]$ for infinitely many $n \in \mathbb{N}$ if and only if there exist polynomials $h_1(n, Z), h_2(n, Z)$, whose coefficients are linear recurrences with algebraic characteristic roots and algebraic coefficients, and an arithmetic progression $\mathcal{P}$ such that

$$a_0(\gamma_1^n, \ldots, \gamma_r^n)^{d-1} g(\gamma_1^n, \ldots, \gamma_r^n, Z) = h_1(n, Z) h_2(n, Z)$$

  is a factorization in $K[Z]$ for all $n \in \mathcal{P}$.
- We remark that generic decompositions, as they occur in the statement of the above theorem, can be computed.

Results & remarks

- It follows, under the conditions we work in, that if $g(\gamma_1^n, \ldots, \gamma_r^n, Z)$ is irreducible as a polynomial in Z over the ring of K-power sums (or, more general, the Hadamard ring of linear recurrences in K), then it cannot be reducible in $K[Z]$ for infinitely many $n \in \mathbb{N}$.
- As usual one may deduce that all decompositions can be described in "finite terms" coming from finitely many generic decompositions of $g(\gamma_1^n, \ldots, \gamma_r^n, Z)$ over the ring whose coefficients are linear recurrences in K with finitely many exceptions.

Theorem 1 (F.-Heintze)

Let $K, g, \widetilde{g}, \gamma_1, \ldots, \gamma_r$ and S be as above. Then there are finitely many cosets $\mathbf{u}_1 H_1, \ldots, \mathbf{u}_t H_t \subseteq \mathbb{G}_{\mathrm{m}}^r$ and for each coset $\mathbf{u}_i H_i$ a polynomial P_i in r unknowns such that the following holds: For each solution $(n, z) \in \mathbb{N} \times \mathcal{O}_S$ of $g(\gamma_1^n, \ldots, \gamma_r^n, z) = 0$ with $z \neq 0$ and n large enough, there exists an index i such that $(\gamma_1^n, \ldots, \gamma_r^n) \in \mathbf{u}_i H_i$ and $z' = P_i(\gamma_1^n, \ldots, \gamma_r^n)$, where $z' = z$ in the case $a_0(0, \ldots, 0) \neq 0$ and $z' = a_0(\gamma_1^n, \ldots, \gamma_r^n) z$ if $a_0(0, \ldots, 0) = 0$, respectively.

- We assume that $a_0(0,\dots,0) \neq 0$ and that $g(0,\dots,0,Z)$ has only simple zeros. The other case uses $\widetilde{g}$ instead of g and goes similarly.
- Consider now an infinite sequence $((n,z_n))_{n\in W}$ of solutions of the equation
$$g(\gamma_1^n,\dots,\gamma_r^n,z)=0$$
in $(n,z)\in\mathbb{N}\times\mathcal{O}_S$ with $z\neq 0$, where W is an infinite subset of $\mathbb{N}$.
- We first show that the z-component must be bounded.
- It follows that $g(0,\dots,0,z_n)\to 0$ as $n\to\infty$. Thus the z_n lie in the union of arbitrary small neighborhoods of the solutions of $g(0,\dots,0,z)=0$ for n large enough. Thus we can split the sequence into finitely many subsequences and consider in what follows only an infinite sequence (z_n) which converges to a solution z_* of $g(0,\dots,0,z)=0$.

- Afterwards we calculate a bound on the height of the z-component.
- Then we can apply the Implicit Function theorem which gives a power series $f(X_1, \ldots, X_r)$ with algebraic coefficients such that for n large enough we have $z_n = f(\gamma_1^n, \ldots, \gamma_r^n)$.
- Then we apply Corvaja-Zannier which gives finitely many cosets $\mathbf{u}_1 H_1, \ldots, \mathbf{u}_t H_t \subseteq \mathbb{G}_{\mathrm{m}}^r$ such that $\{(\gamma_1^{w_n}, \ldots, \gamma_r^{w_n})\}_{n\in\mathbb{N}} \subseteq \bigcup_{i=1}^t \mathbf{u}_i H_i$ and such that, for $i = 1, \ldots, t$, the restriction of f to $\mathbf{u}_i H_i$ coincides with a polynomial P_i in $K[X_1, \ldots, X_r]$.
- Hence for all $n \in W$ there exists an index i such that $(\gamma_1^n, \ldots, \gamma_r^n) \in \mathbf{u}_i H_i$ and $z_n = P_i(\gamma_1^n, \ldots, \gamma_r^n)$.

//

Corollary (F.-Heintze)

Let $K, g, \widetilde{g}, \gamma_1, \ldots, \gamma_r$ and S be as in Theorem 1. Then there are finitely many linear recurrences $R_1(n), \ldots, R_s(n)$ with algebraic roots and algebraic coefficients, arithmetic progressions $\mathcal{P}_1, \ldots, \mathcal{P}_s$, as well as finite sets M and N such that the set of solutions $(n, z) \in \mathbb{N} \times \mathcal{O}_S$ of the equation $g(\gamma_1^n, \ldots, \gamma_r^n, z) = 0$ is equal to

$$\bigcup_{j=1}^{s} \{(n, R_j(n)) : n \in \mathcal{P}_j, R_j(n) \in \mathcal{O}_S\} \cup \{(n, z) : n \in N, z \in \mathcal{O}_S\} \cup M.$$

- Clearly, it suffices to classify the solutions of the form $(n, z) \in \mathbb{N} \times \mathcal{O}_S$ with $z \neq 0$ and n large.
- We apply Theorem 1 and get finitely many cosets $\mathbf{u}_1 H_1, \ldots, \mathbf{u}_t H_t \subseteq \mathbb{G}_\mathrm{m}^r$ as well as for each coset $\mathbf{u}_i H_i$ a polynomial P_i such that for all remaining solutions (n, z) there is an index $i \in \{1, \ldots, t\}$ with the property that either

$$z = P_i(\gamma_1^n, \ldots, \gamma_r^n) \qquad \text{or} \qquad z = \frac{P_i(\gamma_1^n, \ldots, \gamma_r^n)}{a_0(\gamma_1^n, \ldots, \gamma_r^n)}.$$

- For each i we distinguish four cases.
- If there are only finitely many solutions satisfying the first or second equations they are contained in M.
- If the first equation has infinitely many solutions we put z into the original equation and use the Skolem-Mahler-Lech theorem.

- If the second equation has infinitely many solutions we first apply the Hadamard Quotient theorem and then proceed as in case three.
- This concludes the proof.

//

Theorem 2 (F.-Heintze)

Let $K, g, \gamma_1, \dots, \gamma_r$ and S be as above. Moreover, assume that g is monic as a polynomial in Z, i.e. $a_0(X_1, \dots, X_r) = 1$. Then $g(\gamma_1^n, \dots, \gamma_r^n, Z)$ is reducible in $K[Z]$ for infinitely many $n \in \mathbb{N}$ if and only if there exist monic polynomials $h_1(n, Z)$, $h_2(n, Z)$, whose coefficients are linear recurrences with algebraic characteristic roots and algebraic coefficients, and an arithmetic progression $\mathcal{P}$ such that $g(\gamma_1^n, \dots, \gamma_r^n, Z) = h_1(n, Z)h_2(n, Z)$ is a factorization in $K[Z]$ for all $n \in \mathcal{P}$.

- We first prove, as in Theorem 1, that all zeros z of $g(\gamma_1^n, \ldots, \gamma_r^n, z)$ can be described by finitely many power series $f(\gamma_1^n, \ldots, \gamma_r^n)$. Thus we have

$$g(\gamma_1^n, \ldots, \gamma_r^n, Z) = (Z - f_1(\gamma_1^n, \ldots, \gamma_r^n)) \cdots (Z - f_d(\gamma_1^n, \ldots, \gamma_r^n)).$$

- We get that for infinitely many n we have

$$g(\gamma_1^n, \ldots, \gamma_r^n, Z) = h_1(n, Z) h_2(n, Z)$$

with fixed monic polynomials $h_1(n, Z)$, $h_2(n, Z)$ in Z having power series of the form $f(\gamma_1^n, \ldots, \gamma_r^n)$ as coefficients.

- Applying Corvaja-Zannier to the coefficients of $h_1(n, Z)$, $h_2(n, Z)$, we get that these coefficients coincide with polynomials of the form $P(\gamma_1^n, \ldots, \gamma_r^n)$.

- Thus for infinitely many n we get the factorization

$$g(\gamma_1^n, \ldots, \gamma_r^n, Z) = h_1(n, Z)h_2(n, Z)$$

  with fixed monic polynomials $h_1(n, Z), h_2(n, Z)$ in Z having polynomials of the form $P(\gamma_1^n, \ldots, \gamma_r^n)$ as coefficients; hence the coefficients are linear recurrence sequences.
- The statement about the arithmetic progressions follows by using Skolem-Mahler-Lech.

//

Thank you for your attention!