A CRITERION FOR POLYNOMIALS TO DIVIDE INFINITELY MANY k-NOMIALS

L. Hajdu and R. Tijdeman

To Wolfgang M. Schmidt on the occasion of his seventieth birthday

Abstract. In this paper we give necessary and sufficient conditions for polynomials in $\mathbb{Q}[x]$ having not too small Galois groups to divide infinitely many standard k-nomials over $\mathbb{Q}$.

1. Introduction

A polynomial $Q \in \mathbb{Q}[x]$ of the form

$$Q(x) = \sum_{i=1}^{k} a_i x^{m_i} \text{ with } m_1 > \ldots > m_{k-1} > m_k = 0 \text{ and } a_1 = 1$$

is called a standard k-nomial. It is worth to mention that the restriction to monic k-nomials is only for convenience. We may replace every standard k-nomial by any of its constant multiples, and the theorems would still be valid. We call $(m_1, \ldots, m_k)$ the exponent k-tuple of Q. Note that if Q is a standard k-nomial, but not a standard $(k-1)$-nomial, then its exponent k-tuple is uniquely determined. Let

$$\mathrm{PR}_k = \{P \in \mathbb{Q}[x] \ : \ \exists\, Q \in \mathbb{Q}[x] \text{ and } r \in \mathbb{Z} \text{ with } \deg(Q) < k$$
$$\text{and } r \geq 1 \text{ such that } P(x) \mid Q(x^r) \text{ over } \mathbb{Q}\}.$$

In 1965 Posner and Rumsey observed (see [5], pp. 339 and 348) that $P \in \mathrm{PR}_k$ implies that P divides infinitely many standard k-nomials over $\mathbb{Q}$. They conjectured that the converse is also true, that is, if a polynomial $P \in \mathbb{Q}[x]$ divides infinitely many standard k-nomials over $\mathbb{Q}$, then $P \in \mathrm{PR}_k$. For $k = 2$ the conjecture obviously holds.

In [2] Győry and Schinzel verified the conjecture in a quantitative form for $k = 3$. They proved that if P divides more than C_1 standard trinomials over $\mathbb{Q}$, then $P \in \mathrm{PR}_3$. Here C_1 is a number depending on the degree of P and some other

2000 Mathematics Subject Classification: 11C08 (11D57).

The research was supported in part by the Netherlands Organization for Scientific Research (NWO). The first author was further supported by the János Bolyai Research Fellowship of the Hungarian Academy of Sciences, by the grants F034981, T042985 and T048791 of the Hungarian National Foundation for Scientific Research and by the FKFP grant 3272-13/066/2001.

parameters, and it is explicitly given in [2]. Later, Schlickewei and Viola [6] provided a value for C_1 which depends only on the degree of P.

However, the authors of [2] disproved the conjecture for every $k \geq 4$. For every $k \geq 2$ they gave a polynomial $P \in \mathbb{Q}[x]$ that divides infinitely many standard quadrinomials over $\mathbb{Q}$ with $P \notin \mathrm{PR}_k$. In fact the quadrinomials have a zero constant term and have therefore only three non-zero terms. In case of polynomials with non-zero constant terms, the problem is more difficult. For every $k \geq 2$ Győry and Schinzel [2] provided a $P \notin \mathrm{PR}_k$ which divides infinitely many standard quintinomials over $\mathbb{Q}$ with non-zero constant terms. They proposed the following problem instead of the disproved conjecture of Posner and Rumsey.

Let k be an integer with $k \geq 4$. Is it true that a polynomial $P \in \mathbb{Q}[x]$ with $P(0) \neq 0$ divides infinitely many standard k-nomials with non-zero constant terms if and only if either $P \in \mathrm{PR}_k$, or P divides a standard $\left[\frac{k+1}{2}\right]$-nomial?

For $k \geq 6$ Hajdu [3] gave a negative answer to this question by providing other kinds of counterexamples. He proposed to modify the problem of Győry and Schinzel as follows.

Let k be an integer with $k \geq 4$. Is it true that a polynomial $P \in \mathbb{Q}[x]$ with $P(0) \neq 0$ divides infinitely many standard k-nomials with non-zero constant terms if and only if either $P \in \mathrm{PR}_k$ or P divides a standard $(k-2)$-nomial which divides infinitely many standard k-nomials over $\mathbb{Q}$?

Schlickewei and Viola [7] described a so-called 'proper' family $\mathcal{F}_k$ of standard k-nomials such that if a polynomial P having only simple zeros divides more than $C_2(k)$ elements of $\mathcal{F}_k$, then $P \in \mathrm{PR}_k$.

In [4] Hajdu and Tijdeman gave necessary and sufficient conditions for a polynomial $P \in \mathbb{Q}[x]$ having only simple zeros to divide infinitely many standard quadrinomials or standard quintinomials over $\mathbb{Q}$. Moreover, for $k = 5$ they presented a polynomial which yields negative answers to the problems stated by Győry and Schinzel, and by Hajdu.

The aim of this paper is to extend the results of [4] to polynomials dividing standard k-nomials for arbitrary $k \geq 4$. For this purpose, we impose a new type of assumption. More precisely, we assume that the polynomial P dividing infinitely many k-nomials is irreducible over $\mathbb{Q}$, and also that its Galois group is sufficiently large. We note that as "almost all" polynomials in $\mathbb{Q}[x]$ are irreducible and have the whole symmetric group as its Galois group, we exclude only a minor part of polynomials from our investigations. The new results indicate that the conditions (i) and (ii) of Theorem 1 of [4] (which are the same as in Theorem 1 below) are the "right ones" to characterize polynomials dividing infinitely many standard k-nomials over $\mathbb{Q}$. The proofs rely on the Subspace Theorem based on Schmidt's fundamental work.

2. The main results

Let $P \in \mathbb{Q}[x]$ be an irreducible polynomial of degree n, with Galois group $\mathcal{G}$ and with splitting field $\mathbb{K}$ over $\mathbb{Q}$. We keep this notation for the whole paper. For any $t \in \{1, \dots, n\}$ we say that the Galois group of P is t-times transitive, if for all ordered t-tuples $(\alpha_{i_1}, \dots, \alpha_{i_t})$ and $(\alpha_{j_1}, \dots, \alpha_{j_t})$ consisting of zeros of P there exists an automorphism σ of $\mathbb{K}$ such that $\sigma(\alpha_{i_l}) = \alpha_{j_l}$ for $l = 1, \dots, t$. It is well-known that the Galois group of any irreducible polynomial is transitive (with $t = 1$). Note that if P is t-times transitive then it is s-times transitive for any integer s with

$1 \le s \le t$.

Theorem 1. *Let k be an integer with $k \geq 4$. An irreducible polynomial $P \in \mathbb{Q}[x]$ with $[2k/3]$-times transitive Galois group $\mathcal{G}$ divides infinitely many standard k-nomials with non-zero constant terms over $\mathbb{Q}$ if and only if one of the following conditions holds:*

(i) $P \in PR_k$,

(ii) P divides over $\mathbb{Q}$ two different standard k-nomials with the same exponent k-tuple.

We note that for $k = 4$ the statement follows from Theorem 1 of [4]. We shall derive the following simple corollaries.

Corollary 1. *Let P be as in Theorem 1. Then P divides infinitely many standard k-nomials over $\mathbb{Q}$ if and only if either $P \in PR_k$, or P divides a standard $(k-1)$-nomial over $\mathbb{Q}$.*

Corollary 2. *Let P be as in Theorem 1, with the further assumption that $\deg(P) \geq k$. Then condition (i) can be replaced by*

(i') P divides a standard binomial over $\mathbb{Q}$.

The following statement shows that the conditions (i) and (ii) in Theorem 1 are independent.

Proposition. *For every $k \geq 5$ there exist polynomials $P_1, P_2 \in \mathbb{Q}[x]$ such that both divide infinitely many standard k-nomials over $\mathbb{Q}$, (i) holds for P_1 but not for P_2, and conversely, (ii) holds for P_2 but not for P_1.*

Remark 1. The Proposition, together with Theorem 1, strongly suggests that the conditions (i) and (ii) are necessary and sufficient to characterize polynomials dividing infinitely many standard k-nomials over $\mathbb{Q}$.

Remark 2. Following the proof of Theorem 1, one can easily see that there is an effectively computable constant $C_3(k)$ depending only on k, such that if P divides more than $C_3(k)$ standard k-nomials over $\mathbb{Q}$, then the conclusion of the theorem is still valid.

In case of $k = 5$ we need only double transitivity to have the same conclusion as in Theorem 1.

Theorem 2. *An irreducible polynomial $P \in \mathbb{Q}[x]$ with doubly transitive Galois group $\mathcal{G}$ divides infinitely many standard quintinomials with non-zero constant terms over $\mathbb{Q}$ if and only if condition (i) or (ii) in Theorem 1 with $k = 5$ holds.*

Remark 3. In Theorem 2 of [4] the authors proved that a polynomial $P \in \mathbb{Q}[x]$ with only simple zeros and with $P(0) \neq 0$ divides infinitely many standard quintinomials with non-zero constant terms over $\mathbb{Q}$ if and only if (i), (ii) or the next condition holds:

(iii) there exist integers M_1, M_2, M_3, M_4 such that P divides over $\mathbb{Q}$ infinitely many standard quintinomials Q_m of the form

$$Q_m(x) = x^{M_1+2m} + a_m x^{M_2+m} + b_m x^{M_3+m} + c_m x^{M_4+m} + d_m$$

with $m \in \mathbb{N}$ and $a_m, b_m, c_m, d_m \in \mathbb{Q}$.

The proof of Theorem 2 shows that if $k = 5$ and P has a doubly transitive Galois group, then condition (iii) implies (i) or (ii).

3. Basic lemmas

Two algebraic numbers β_1 and β_2 are called equivalent, if for some root of unity ε we have $\beta_1\varepsilon = \beta_2$. Hence we have a partition of the algebraic numbers into equivalence classes.

Lemma 1. *Let $k \in \mathbb{Z}$ with $k \geq 2$, and let $P \in \mathbb{Q}[x]$ be a polynomial having only simple zeros. Then $P \in PR_k$ if and only if the zeros of P belong to the union of at most $k-1$ equivalence-classes defined above.*

Proof. The statement is a reformulation of Proposition 2.1 of [7]. $\square$

Lemma 2. *Let $\alpha_1, \dots, \alpha_k$ be non-zero elements of a field of characteristic zero, such that α_i/α_j is not a root of unity ($1 \leq i < j \leq k$). Then the equation*

$$\begin{vmatrix} \alpha_1^{X_1} & \dots & \alpha_k^{X_1} \\ \vdots & \vdots & \vdots \\ \alpha_1^{X_k} & \dots & \alpha_k^{X_k} \end{vmatrix} = 0$$

has at most $exp((6k!)^{3k!})$ solutions in $(X_1, \dots, X_k) \in \mathbb{Z}^k$ with $X_k = 0$ for which the above determinant has no vanishing subdeterminant.

Proof. This is a reformulation of Theorem 1.1 in [8]. $\square$

Let $\mathbb{L}$ be an algebraic number field and $\alpha_{ij} \in \mathbb{L}^*$ for $1 \leq i \leq m$, $1 \leq j \leq n$, where m, n are positive integers. Moreover, let $a_i \in \mathbb{L}$ ($1 \leq i \leq m$). For $i = 1, \dots, m$ and $\underline{x} \in \mathbb{Z}^n$ with $\underline{x} = (x_1, \dots, x_n)$ write $\underline{\alpha_i}^{\underline{x}} = \alpha_{i1}^{x_1} \dots \alpha_{in}^{x_n}$ for brevity. Consider the equation

$$\sum_{i=1}^{m} a_i \underline{\alpha_i}^{\underline{x}} = 0 \quad \text{in} \quad \underline{x} \in \mathbb{Z}^n. \tag{1}$$

Let $\mathcal{P}$ be a partition of the set $\Lambda = \{1, \dots, m\}$, and consider the system of equations

$$\sum_{i \in \lambda} a_i \underline{\alpha_i}^{\underline{x}} = 0 \quad (\lambda \in \mathcal{P}) \qquad \text{in} \quad \underline{x} \in \mathbb{Z}^n, \tag{1.$\mathcal{P}$}$$

which is a refinement of (1). Let $\mathcal{S}(\mathcal{P})$ denote the set of those solutions of (1.$\mathcal{P}$) which are not solutions of any (1.$\mathcal{Q}$) where $\mathcal{Q}$ is a proper refinement of $\mathcal{P}$. Set $i_1 \overset{\mathcal{P}}{\sim} i_2$, if i_1 and i_2 are in the same class of $\mathcal{P}$, and put

$$G(\mathcal{P}) = \{\underline{z} \in \mathbb{Z}^n \ : \ \underline{\alpha_{i_1}}^{\underline{z}} = \underline{\alpha_{i_2}}^{\underline{z}} \ \text{ for any } \ i_1, i_2 \ \text{ with } \ i_1 \overset{\mathcal{P}}{\sim} i_2\}.$$

Denote the cardinality of the set A by $|A|$.

Lemma 3. *Using the above notation, there exists an explicitly computable constant $C(m,n)$ depending only on m and n such that if $\mathcal{P}$ is any partition of Λ with*

$$|\mathcal{S}(\mathcal{P})| \geq C(m,n)$$

then there are different solutions $\underline{z}'$ and $\underline{z}''$ of $(1.\mathcal{P})$ such that $\underline{z}' - \underline{z}'' \in G(\mathcal{P})$.

Proof. The statement follows from Theorem 1.1 of [1] by a simple induction argument. □

Lemma 4. *Let $P \in \mathbb{Q}[x]$ be an irreducible polynomial with doubly transitive Galois group $\mathcal{G}$. Then either all the zeros of P are equivalent or no pair of zeros of P is equivalent.*

Proof. Suppose $\alpha_1, \alpha_2, \alpha_i, \alpha_j$ are zeros of P such that $\alpha_1 \neq \alpha_2$, $\alpha_i \neq \alpha_j$ and α_1/α_2 is a root of unity. Choose a $\sigma \in \mathcal{G}$ such that $\sigma(\alpha_1) = \alpha_i$ and $\sigma(\alpha_2) = \alpha_j$. Then we obtain that α_i/α_j is also a root of unity. □

4. Proofs

As the proof of Theorem 2 is more concrete, we give it first. Thereafter we present the proofs of Theorem 1 and Corollaries 1 and 2. The verification of the Proposition is the final item of the section.

Proof of Theorem 2. As we mentioned in the Introduction, (i) is sufficient by a result of Posner and Rumsey (see [5], pp. 339 and 348). The sufficiency of (ii) follows by considering suitable linear combinations of the two polynomials. To prove necessity, in view of Remark 3, we may assume that there exist integers M_1, M_2, M_3, M_4 such that P divides over $\mathbb{Q}$ infinitely many standard quintinomials Q_m of the form

$$Q_m(x) = x^{M_1+2m} + a_m x^{M_2+m} + b_m x^{M_3+m} + c_m x^{M_4+m} + d_m$$

with $m \in \mathbb{N}$ and $a_m, b_m, c_m, d_m \in \mathbb{Q}$.

Let A be an infinite set of such quintinomials. We may suppose that $n = \deg(P) \geq 5$, otherwise (i) holds by Lemma 1. Let $\alpha_1, \ldots, \alpha_n$ be the zeros of P. If any two of these zeros are equivalent, then by Lemmas 4 and 1 we are done. So we may assume that α_i/α_j is not a root of unity whenever $i \neq j$. Observe that the equation

$$\begin{vmatrix} \alpha_{i_1}^{M_1+2m} & \alpha_{i_2}^{M_1+2m} & \alpha_{i_3}^{M_1+2m} & \alpha_{i_4}^{M_1+2m} & \alpha_{i_5}^{M_1+2m} \\ \alpha_{i_1}^{M_2+m} & \alpha_{i_2}^{M_2+m} & \alpha_{i_3}^{M_2+m} & \alpha_{i_4}^{M_2+m} & \alpha_{i_5}^{M_2+m} \\ \alpha_{i_1}^{M_3+m} & \alpha_{i_2}^{M_3+m} & \alpha_{i_3}^{M_3+m} & \alpha_{i_4}^{M_3+m} & \alpha_{i_5}^{M_3+m} \\ \alpha_{i_1}^{M_4+m} & \alpha_{i_2}^{M_4+m} & \alpha_{i_3}^{M_4+m} & \alpha_{i_4}^{M_4+m} & \alpha_{i_5}^{M_4+m} \\ 1 & 1 & 1 & 1 & 1 \end{vmatrix} = 0 \tag{2}$$

has infinitely many solutions in m for any $i_1, \ldots, i_5$ with $1 \leq i_1 < \ldots < i_5 \leq n$. Thus by Lemma 2 the determinant in (2) must have a vanishing subdeterminant for infinitely many m. If there is a vanishing subdeterminant of type 2×2, then the corresponding zeros are equivalent, which is a contradiction. Thus we may assume that

$$D_{u_1u_2u_3} := \begin{vmatrix} \alpha_{u_1}^{M_2} & \alpha_{u_2}^{M_2} & \alpha_{u_3}^{M_2} \\ \alpha_{u_1}^{M_3} & \alpha_{u_2}^{M_3} & \alpha_{u_3}^{M_3} \\ \alpha_{u_1}^{M_4} & \alpha_{u_2}^{M_4} & \alpha_{u_3}^{M_4} \end{vmatrix} = 0$$

for some u_1, u_2, u_3 with $1 \leq u_1 < u_2 < u_3 \leq n$, otherwise by Lemma 2 we get a contradiction. Note that $D_{u_1u_2u_3}$ does not have a 2×2 vanishing subdeterminant, otherwise we obtain two equivalent zeros, which is a contradiction again.

Suppose first that $D_{u_1u_2u_3} = 0$ for each choice of u_1, u_2, u_3. Then there are $r_3, r_4 \in \mathbb{K}$ such that P divides $x^{M_2} + r_3x^{M_3} + r_4x^{M_4}$ over $\mathbb{K}$. Therefore, for an appropriate choice of m, P divides both Q_m and the polynomial

$$x^{M_1+2m} + (a_m + 1)x^{M_2+m} + (b_m + s_3)x^{M_3+m} + (c_m + s_4)x^{M_4+m} + d_m$$

over $\mathbb{Q}$, where $s_i = \mathrm{trace}(r_i)$ $(i = 3, 4)$. Thus we have (ii), and the theorem follows in this case.

So we may assume that $D_{123} = 0$ and $D_{124} \neq 0$. Then, by the double transitivity of $\mathcal{G}$, there is an automorphism σ of $\mathbb{K}$ such that $\sigma(\alpha_1) = \alpha_1$ and $\sigma(\alpha_2) = \alpha_4$. Observe that by $D_{124} \neq 0$, $\sigma(\alpha_3) \neq \alpha_2$. Moreover, $\sigma(\alpha_3) = \alpha_3$ is impossible, since $D_{123} = 0$ and $D_{134} = 0$ yield $D_{124} = 0$. Hence without loss of generality we may assume that $\sigma(\alpha_3) = \alpha_5$, whence $D_{123} = D_{145} = 0$ and $D_{124} \neq 0$. It is easy to check that $D_{j_1j_2j_3} = 0$ with $1 \leq j_1 < j_2 < j_3 \leq 5$ only if $(j_1, j_2, j_3) = (1, 2, 3)$ or $(1, 4, 5)$.

Consider now (2), with $(i_1, i_2, i_3, i_4, i_5) = (1, 2, 3, 4, 5)$. Expanding the determinant by its middle three rows, after dividing by $(\alpha_1\alpha_2\alpha_3\alpha_4\alpha_5)^m$, we obtain

$$\sum_{\substack{\{i_1,i_2,i_3,i_4,i_5\}=\{1,2,3,4,5\} \\ i_3<i_4<i_5}} (-1)^{i_1+i_2+1} \cdot \mathrm{sgn}(i_2 - i_1) \cdot D_{i_3i_4i_5} \cdot \alpha_{i_1}^{M_1}(\alpha_{i_1}/\alpha_{i_2})^m = 0. \tag{3}$$

Observe that, by $D_{123} = 0$ and $D_{145} = 0$, (3) is an exponential equation in $\mathbb{K}$ with exactly 16 nonzero terms. Choose a system $\mathcal{P}$ of subsums of the left hand side of (3) such that each subsum in $\mathcal{P}$ vanishes simultaneously for the exponent quintuples corresponding to polynomials in an infinite subset A_1 of A, but all the proper subsums of each of these subsums do not vanish. Without loss of generality we may assume that $A = A_1$. Applying Lemma 3 to the partition $\mathcal{P}$, we obtain $G(\mathcal{P}) \neq \{0\}$. Note that each class of $\mathcal{P}$ contains at least two elements. There exists a $z \in \mathbb{Z}$ with $z \neq 0$ such that for all $(i_1, i_2), (j_1, j_2)$ we have that if $(\alpha_{i_1}/\alpha_{i_2})^m$ and $(\alpha_{j_1}/\alpha_{j_2})^m$ occur in the same class of $\mathcal{P}$, then

$$(\alpha_{i_1}/\alpha_{i_2})^z = (\alpha_{j_1}/\alpha_{j_2})^z$$

holds. Thus we obtain many multiplicative relations among the α_i's. If $(\alpha_1/\alpha_2)^z = (\alpha_2/\alpha_1)^z$, $(\alpha_1/\alpha_i)^z$ or $(\alpha_i/\alpha_2)^z$ for some i with $3 \leq i \leq 5$, then we obtain that two zeros of P are equivalent, which is a contradiction. If $(\alpha_1/\alpha_2)^z$ equals $(\alpha_i/\alpha_1)^z$ or $(\alpha_2/\alpha_i)^z$ for some i with $3 \leq i \leq 5$ then we get

$$\alpha_{j_1}^z \alpha_{j_2}^z \alpha_{j_3}^{-2z} = 1 \tag{4}$$

for some distinct j_1, j_2, j_3 with $1 \leq j_1, j_2, j_3 \leq 5$. Suppose that $(\alpha_1/\alpha_2)^z = (\alpha_3/\alpha_4)^z$. Checking the possible elements of the class of $(\alpha_1/\alpha_5)^z$, we find that in each case two zeros of P are equivalent or some relation (4) holds. Thus, since the former case is excluded, it remains to prove that (4) is impossible. Assume that (4) holds for some distinct j_1, j_2, j_3 with $1 \leq j_1, j_2, j_3 \leq 5$. Write $\beta_i = \alpha_{j_i}$ for $i = 1, 2, 3$. By the double transitivity of $\mathcal{G}$, there exists an automorphism σ_1

of $\mathbb{K}$, such that $\sigma_1(\beta_1) = \beta_2$, $\sigma_1(\beta_2) = \beta_3$. Write $\beta_4 = \sigma_1(\beta_3)$. We observe that if $\beta_1 = \beta_4$ then from (4) we get $\beta_1^{3z} = \beta_3^{3z}$, which is a contradiction. So assume that $\beta_1 \neq \beta_4$, and choose inductively automorphisms σ_i of $\mathbb{K}$ such that $\sigma_i(\beta_i) = \beta_{i+1}$, $\sigma_i(\beta_{i+1}) = \beta_{i+2}$, and write $\beta_{i+3} = \sigma_i(\beta_{i+2})$. As P has n zeros, after j steps with $j \leq n-3$, we get that $\beta_{j+3} = \beta_l$ with some $l \leq j$. Without loss of generality we may assume that j is minimal with this property and that $l = 1$. Define the numbers λ_i for $i = 1, \ldots, j+1$ in the following way. Put $\lambda_1 = 1$, $\lambda_2 = -1$, and let $\lambda_{i+2} = 2\lambda_i - \lambda_{i+1}$ $(i = 1, \ldots, j-1)$. A simple calculation yields $\lambda_i = (1-(-2)^i)/3$ $(i = 1, \ldots, j+1)$. Observe that by (4) and the definition of the β_i and λ_i we have

$$(\beta_{j+1}^z \beta_{j+2}^z \beta_1^{-2z})^{\lambda_{j+1}} \prod_{i=1}^{j} (\beta_i^z \beta_{i+1}^z \beta_{i+2}^{-2z})^{\lambda_i} = \beta_1^{z(\lambda_1 - 2\lambda_{j+1})} \beta_{j+2}^{z(-2\lambda_j + \lambda_{j+1})} = 1.$$

By induction it is easy to see that $-2\lambda_j + \lambda_{j+1} = -\lambda_1 + 2\lambda_{j+1}$. As clearly $\lambda_1 \neq 2\lambda_{j+1}$, we find that β_1 and β_{j+2} are equivalent. However, by the minimality of j we have $\beta_1 \neq \beta_{j+2}$. This is a contradiction, and the theorem follows. $\square$

Proof of Theorem 1. The sufficiency of (i) and (ii) just follows as in the proof of Theorem 2. To prove necessity, suppose that $P \in \mathbb{Q}[x]$ of degree n divides infinitely many standard k-nomials, and that P is irreducible with $[2k/3]$-times transitive Galois group $\mathcal{G}$. If $n < k$ then (i) holds by Lemma 1 and we are done. Moreover, if two zeros of P are equivalent then the theorem follows from Lemmas 4 and 1. Thus without loss of generality we may assume that $n \geq k$ and that the zeros of P are pairwise non-equivalent. Let A be an infinite set of k-nomials divisible by P. Observe that $P \in \mathrm{PR}_{k-1}$ implies that $P \in \mathrm{PR}_k$. Moreover, if P divides two standard $(k-1)$-nomials with the same exponent $(k-1)$-tuple, then either these polynomials are also standard k-nomials, or P divides a polynomial of degree less than k. Hence, as the statement is true for $k = 4$ (cf. Theorem 1 of [4]), by induction we may assume that A does not contain any $(k-1)$-nomial. Let $\alpha_1, \ldots, \alpha_n$ be the zeros of P. If P divides a standard k-nomial $x^{m_1} + a_2 x^{m_2} + \ldots + a_k$ over $\mathbb{Q}$, then for any $i_1, \ldots, i_k$ with $1 \leq i_1 < \ldots < i_k \leq n$ we have

$$\begin{vmatrix} \alpha_{i_1}^{m_1} & \ldots & \alpha_{i_k}^{m_1} \\ \vdots & \vdots & \vdots \\ \alpha_{i_1}^{m_k} & \ldots & \alpha_{i_k}^{m_k} \end{vmatrix} = 0 \tag{5}$$

with $m_k = 0$. We may assume that the set of such k-tuples $(m_1, \ldots, m_k)$ is infinite, otherwise (ii) holds. Thus, by Lemma 2 we get that for any $i_1, \ldots, i_k$ the determinant in (5) must have a proper subdeterminant which vanishes for infinitely many k-tuples $(m_1, \ldots, m_k)$. Choose such a subdeterminant of size $t \times t$ with some $1 \leq u_1 < \ldots < u_t \leq n$ and $0 \leq m_{j_t} < \ldots < m_{j_1} \leq m_1$ such that

$$\begin{vmatrix} \alpha_{u_1}^{m_{j_1}} & \ldots & \alpha_{u_t}^{m_{j_1}} \\ \vdots & \vdots & \vdots \\ \alpha_{u_t}^{m_{j_t}} & \ldots & \alpha_{u_t}^{m_{j_t}} \end{vmatrix} = 0 \tag{6}$$

for infinitely many $(m_1, \ldots, m_k)$, and t is minimal with this property. Observe that $3 \leq t \leq k-1$, since in case of $t = 2$, P has two equivalent zeros, which is a contradiction.

Suppose first that $t \leq 2k/3$. Take any standard k-nomial Q_1 from A with exponent k-tuple $(m_1, \ldots, m_k)$ for which (6) is valid. Observe that as $\mathcal{G}$ is $[2k/3]$-times transitive (6) holds for any system of t zeros of P. Hence there are numbers $r_{j_1}, \ldots, r_{j_t}$ from $\mathbb{K}$, one of them being 1, such that P divides $r_{j_1}x^{m_{j_1}} + \ldots + r_{j_t}x^{m_{j_t}}$ over $\mathbb{K}$. Therefore, P divides the non-zero polynomial $Q_2(x) = s_{j_1}x^{m_{j_1}} + \ldots + s_{j_t}x^{m_{j_t}}$ over $\mathbb{Q}$, where $s_{j_l} = \mathrm{trace}(r_{j_l})$ $(l = 1, \ldots, t)$. Then P divides the standard k-nomial $Q_1 + Q_2$ (or rather $(1/2)Q_1 + (1/2s_{j_1})Q_2$ if $\deg(Q_1) = m_{j_1}$ and $s_{j_1} \neq 0$) over $\mathbb{Q}$. This implies (ii), and the theorem follows in this case.

Assume now that $t > 2k/3$. Without loss of generality we may assume that there is no k-nomial in A for which there is a vanishing subdeterminant in (5) with some $i_1, \ldots, i_k$ of size smaller than $t \times t$, and by the minimality of t that the set A is infinite. As in (6) there are no vanishing subdeterminants, we obtain from Lemma 2 that there exist integers $M_{j_1} > \ldots > M_{j_t} \geq 0$ such that for infinitely many k-nomials from A we have $m_{j_1} - m_{j_l} = M_{j_1} - M_{j_l}$ $(l = 2, \ldots, t)$. Again, we may assume that all the k-nomials in A have this property.

Now by a simple process we are going to separate the exponents (more precisely, the indices of the exponents) of the polynomials in A into certain sets. Let $I_1 \supset \{j_1, \ldots, j_t\}$ be a maximal subset of $\{1, \ldots, k\}$ such that there exists an infinite subset A_1 of A with the following property: for each $i \in I_1$ there exists an integer C_i such that for each polynomial $Q \in A_1$ the exponent tuple satisfies

$$m_{j_1} - m_i = C_i \quad (i \in I_1).$$

Suppose that I_γ and A_γ with some integer $\gamma \geq 1$ have already been defined. If $\{1, \ldots, k\} \setminus (I_1 \cup \ldots \cup I_\gamma)$ is nonempty, let $I_{\gamma+1}$ be a maximal subset of $\{1, \ldots, k\} \setminus (I_1 \cup \ldots \cup I_\gamma)$ such that there exists an infinite subset $A_{\gamma+1}$ of A_γ with the following property: for each pair (j, k) with $j, k \in A_{\gamma+1}$ there is an integer C_{jk} such that each polynomial $Q \in A_{\gamma+1}$ has an exponent tuple satisfying

$$m_j - m_k = C_{jk}$$

(where C_{jk} is independent of Q). We continue this process as far as we can. By this method in finitely many, say Γ steps we get an infinite set A_Γ and a partition of $\{1, \ldots, k\}$ into disjoint subsets I_γ $(\gamma = 1, \ldots, \Gamma)$. Note that the sets I_γ $(\gamma = 1, \ldots, \Gamma)$ are connected in the sense that if $s_1, s_2 \in I_\gamma$ and s is an integer with $s_1 < s < s_2$, then s also belongs to I_γ. Moreover, without loss of generality we may assume that $A = A_\Gamma$. Then for any $Q, Q' \in A$ with exponent k-tuples $(m_1, \ldots, m_k)$ and $(m'_1, \ldots, m'_k)$, respectively, we have $m_{s_1} - m_{s_2} = m'_{s_1} - m'_{s_2}$ if and only if s_1 and s_2 belong to the same I_γ for some $\gamma \in \{1, \ldots, \Gamma\}$. Hence there exist integers M_i $(i = 1, \ldots, k)$ such that if $(m_1, \ldots, m_k)$ is the exponent k-tuple of a standard k-nomial from A, then $i \in I_\gamma$ implies $m_i = M_i + m^{(\gamma)}$ with some positive integers $m^{(\gamma)}$ $(\gamma = 1, \ldots, \Gamma)$ where $m^{(\gamma)}$ depends only on γ and not further on i. For each $\gamma \in \{1, \ldots, \Gamma\}$ put $l_\gamma = |I_\gamma|$, and for any $u_1, \ldots, u_{l_\gamma}$ with $1 \leq u_1 < \ldots < u_{l_\gamma} \leq n$ write

$$D^{(\gamma)}_{u_1 \ldots u_{l_\gamma}} = |\alpha_{u_r}^{M_i}|_{\substack{i \in I_\gamma \\ r = 1, \ldots, l_\gamma}}.$$

Note that $l_1 \geq t > 2k/3$, and consequently $l_\gamma < k/3$ for each $\gamma \in \{2, \ldots, \Gamma\}$. Thus by the minimality of t and our assumptions on A, we obtain that $D^{(\gamma)}_{u_1 \ldots u_{l_\gamma}} \neq 0$ for all $\gamma \geq 2$ and $u_1, \ldots, u_{l_\gamma}$ with $1 \leq u_1 < \ldots < u_{l_\gamma} \leq n$. Further, if $D^{(1)}_{u_1 \ldots u_{l_1}} = 0$ for all $u_1, \ldots, u_{l_1}$ with $1 \leq u_1 < \ldots < u_{l_1} \leq n$, then by a similar argument as in case of $t \leq 2k/3$, we obtain (ii), and we are done. So, without loss of generality we may assume that $i_1 = 1, \ldots, i_k = k$ in (5), and that $D^{(1)}_{q_1 \ldots q_{l_1}} \neq 0$ for some $q_1, \ldots, q_{l_1}$ with $1 \leq q_1 < \ldots < q_{l_1} \leq k$. Expanding the determinant in equation (5) by the rows corresponding to the elements of I_1, and then dividing by $(\alpha_1 \ldots \alpha_k)^{m^{(1)}}$, we obtain an exponential equation in $\mathbb{K}$ of the form

$$\sum (-1)^{\varepsilon} \left(\prod_{\gamma=1}^{\Gamma} D^{(\gamma)}_{v_{\gamma 1} \ldots v_{\gamma l_\gamma}} \right) \prod_{\gamma=2}^{\Gamma} \left(\alpha_{v_{\gamma 1}} \ldots \alpha_{v_{\gamma l_\gamma}} \right)^{m^{(\gamma)} - m^{(1)}} = 0. \tag{7}$$

Here the summation is taken over all partitions $H_\gamma = \{v_{\gamma 1}, \ldots, v_{\gamma l_\gamma}\}$ of $\{1, \ldots, k\}$ such that $\bigcup_{\gamma=1}^{\Gamma} H_\gamma = \{1, \ldots, k\}$, and $v_{\gamma 1} < \ldots < v_{\gamma l_\gamma}$ for each γ. The exponent ε of (-1) depends only on the choice of the partition H_γ $(\gamma = 1, \ldots, \Gamma)$. Further, in view of the previous considerations, the coefficients $\prod_{\gamma=1}^{\Gamma} D^{(\gamma)}_{v_{\gamma 1} \ldots v_{\gamma l_\gamma}}$ are not all zero. Recall that if ${m'}^{(\gamma)}$ and ${m''}^{(\gamma)}$ $(\gamma = 1, \ldots, \Gamma)$ correspond to the exponent k-tuples of the standard k-nomials Q' and Q'' in A, respectively, then by the definition of I_γ we have

$${m'}^{(\gamma)} - {m'}^{(1)} \neq {m''}^{(\gamma)} - {m''}^{(1)} \quad (\gamma = 2, \ldots, \Gamma).$$

Hence equation (7) is satisfied by infinitely many distinct exponent tuples $(m^{(2)} - m^{(1)}, \ldots, m^{(\Gamma)} - m^{(1)})$. Thus, by Lemma 3 there exist integers $z_2, \ldots, z_\Gamma$ such that

$$\prod_{\gamma=2}^{\Gamma} \left(\alpha_{v'_{\gamma 1}} \ldots \alpha_{v'_{\gamma l_\gamma}} \right)^{z_\gamma} = \prod_{\gamma=2}^{\Gamma} \left(\alpha_{v''_{\gamma 1}} \ldots \alpha_{v''_{\gamma l_\gamma}} \right)^{z_\gamma} \tag{8}$$

for some different partitions $\{H'_\gamma\}_{\gamma=1}^{\Gamma}$ and $\{H''_\gamma\}_{\gamma=1}^{\Gamma}$ of the set $\{1, \ldots, k\}$ with $H'_\gamma = \{v'_{\gamma 1}, \ldots, v'_{\gamma l_\gamma}\}$ and $H''_\gamma = \{v''_{\gamma 1}, \ldots, v''_{\gamma l_\gamma}\}$ $(\gamma = 1, \ldots, \Gamma)$, where

$$z_\gamma = ({m'}^{(\gamma)} - {m'}^{(1)}) - ({m''}^{(\gamma)} - {m''}^{(1)})$$

for certain ${m'}^{(\gamma)}, {m'}^{(1)}, {m''}^{(\gamma)}, {m''}^{(1)}$ corresponding to two distinct k-nomials in A. In particular, by the definition of I_γ we have $z_{\gamma_1} \neq z_{\gamma_2}$ whenever $\gamma_1 \neq \gamma_2$ $(\gamma_1, \gamma_2 \in \{2, \ldots, \Gamma\})$. Equation (8) leads to an equation of the form

$$\alpha_{w_1}^{\lambda_1} \ldots \alpha_{w_h}^{\lambda_h} = 1 \tag{9}$$

with $2 \leq h \leq 2(k - |I_1|)$, $1 \leq w_1 < \ldots < w_h \leq k$ and non-zero integers $\lambda_1, \ldots, \lambda_h$. As $|I_1| > 2k/3$, we have $2 \leq h \leq 2k/3$. Since $\mathcal{G}$ is $[2k/3]$-times transitive, there exists an automorphism σ of $\mathbb{K}$ such that $\sigma(\alpha_{w_1}) = \alpha_{w_2}$, $\sigma(\alpha_{w_2}) = \alpha_{w_1}$, and $\sigma(\alpha_{w_p}) = \alpha_{w_p}$ for $p = 3, \ldots, h$. Together with (9) this yields that α_{w_1} and α_{w_2} are equivalent. It contradicts an earlier assumption. □

Proof of Corollary 1. Suppose that (ii) holds, and P divides the standard k-nomials

$$Q(x) = \sum_{i=1}^{k} a_i x^{m_i} \quad \text{and} \quad Q'(x) = \sum_{i=1}^{k} b_i x^{m_i}$$

where $m_1 > \ldots > m_{k-1} > m_k = 0$, $a_1 = b_1 = 1$ and $a_i \neq b_i$ for some i with $2 \leq i \leq k-1$. Then P divides the standard $(k-1)$-nomial $(b_i Q - a_i Q')/(b_i - a_i)$.

On the other hand, if P divides a standard $(k-1)$-nomial Q, then P divides the standard k-nomials $x^l Q$ for any non-negative integer l. Hence the statement follows. $\square$

Proof of Corollary 2. As a binomial can be considered as a linear polynomial in some x^r, (i') implies $P \in \mathrm{PR}_2$, whence (i) follows. On the other hand, if (i) holds then as $\deg(P) \geq k$, by Lemmas 1 and 4 we get that any two zeros of P are equivalent, which yields (i'). $\square$

Proof of the Proposition. Fix any k with $k \geq 5$. Then by Lemma 3 of [3] there exists a polynomial $P_1 \in \mathbb{Q}[x]$ of degree $k-1$ such that P_1 does not divide any standard $(k-1)$-nomial over $\mathbb{Q}$. Then by definition (i) is valid for P_1, and P_1 divides infinitely many standard k-nomials. Moreover, (ii) cannot hold for P_1, as in that case P_1 would divide a standard $(k-1)$-nomial over $\mathbb{Q}$.

On the other hand, the Proposition in [4] in case of $k = 5$ and the Theorem together with Lemma 1 and its proof in [3] when $k \geq 6$ guarantees the existence of a polynomial $P_2 \in \mathbb{Q}[x]$ such that (ii) is valid for P_2 but (i) is not. $\square$

5. Acknowledgment

The authors are grateful to J.-H. Evertse and K. Győry for their useful remarks and to the referee for his valuable and helpful suggestions.

References

[1] J.-H. Evertse, H. P. Schlickewei and W. M. Schmidt, *Linear equations in variables which lie in a multiplicative group*, Ann. Math. **155** (2002), 1–30.

[2] K. Győry and A. Schinzel, *On a conjecture of Posner and Rumsey*, J. Number Theory **47** (1994), 63–78.

[3] L. Hajdu, *On a problem of Győry and Schinzel concerning polynomials*, Acta Arith. **78** (1997), 287–295.

[4] L. Hajdu and R. Tijdeman, *Polynomials dividing infinitely many quadrinomials or quintinomials*, Acta Arith. **107** (2003), 381–404.

[5] E. C. Posner and H. Rumsey, Jr., *Polynomials that divide infinitely many trinomials*, Michigan Math. J. **12** (1965), 339–348.

[6] H. P. Schlickewei and C. Viola, *Polynomials that divide many trinomials*, Acta Arith. **78** (1997), 267–273.

[7] H. P. Schlickewei and C. Viola, *Polynomials that divide many k-nomials*, Number Theory, Proc. Number Theory '97 (ed. by K. Győry and H. Iwaniec), Walter de Gruyter, Berlin–New York, 1999, pp. 445–451.

[8] H. P. Schlickewei and C. Viola, *Generalized Vandermonde determinants*, Acta Arith. **95** (2000), 123–137.

Lajos Hajdu

Number Theory Research Group
of the Hungarian Academy of Sciences, and
University of Debrecen

Institute of Mathematics
P.O. Box 12
4010 Debrecen
Hungary

Robert Tijdeman

Leiden University
Mathematical Institute
P.O. Box 9512
2300 RA Leiden
The Netherlands

E-mail address:
hajdul@math.klte.hu
tijdeman@math.leidenuniv.nl