

On reducible trinomials, II

By ANDRZEJ SCHINZEL (Warszawa)

To Professor Kálmán Győry on his 60th birthday

Abstract. It is shown that if a trinomial has a binomial factor then under certain conditions the cofactor is irreducible.

1. Introduction

This paper is a sequel to [5]. In that paper we considered an arbitrary field K of characteristic π , the rational function field $K(\mathbf{y})$, where $\mathbf{y}$ is a variable vector, a finite algebraic extension L of $K(y_1)$ and a trinomial

$$(i) \quad T(x; A, B) = x^n + Ax^m + B, \quad \text{where } n > m > 0, \pi \nmid mn(n-m)$$

and either $A, B \in K(\mathbf{y})^*$, $A^{-n}B^{n-m} \notin K$ or $A, B \in L$, $A^{-n}B^{n-m} \notin \overline{K}$.

A necessary and sufficient condition was given for reducibility of $T(x; A, B)$ over $K(\mathbf{y})$ or L respectively, provided in the latter case that L is separable (This proviso was only made in the errata [6]). As a consequence a criterion was derived for reducibility of $T(x; a, b)$ over an algebraic number field containing a, b . In each case it was assumed that $n \geq 2m$, but this involved no loss of generality, since $x^n + Ax^m + B$ and $x^n + AB^{-1}x^{n-m} + B^{-1}$ are reducible simultaneously. Let

$$(ii) \quad n_1 = n/(n, m), \quad m_1 = m/(n, m).$$

Mathematics Subject Classification: 12E05, 12E10, 11R09.

Key words and phrases: reducibility, trinomials.

One case of reducibility of $T(x; A, B)$ over the field $\Omega = K(\mathbf{y})$ or L is that $x^n + Ax^{m_1} + B$ has in $\Omega[x]$ a linear factor. The aim of this paper is to prove that if n_1 is sufficiently large and $x^{n_1} + Ax^{m_1} + B$ has in $\Omega[x]$ a linear factor $F(x)$, but not a quadratic factor, then $T(x; A, B)F(x^{(m,n)})^{-1}$ is irreducible over Ω . More precisely, we shall prove using the notation introduced in (i) and (ii) the following three theorems.

Theorem 1. *Let $n_1 > 5$ and $A, B \in K(\mathbf{y})^*$, $A^{-n}B^{n-m} \notin K$. If $x^{n_1} + Ax^{m_1} + B$ has in $K(\mathbf{y})[x]$ a linear factor, $F(x)$, but not a quadratic factor, then $T(x; A, B)F(x^{(m,n)})^{-1}$ is irreducible over $K(\mathbf{y})$.*

Theorem 2. *Let $n_1 > 3$ and $A, B \in L^*$, where L is a finite separable extension of $K(y_1)$ with $\overline{KL}$ of genus g and $A^{-n}B^{n-m} \notin \overline{K}$. If $x^{n_1} + Ax^{m_1} + B$ has in $L[x]$ a linear factor $F(x)$, but not a quadratic factor, then*

$$(iii) \quad T(x; A, B)F(x^{(m,n)})^{-1} \quad \text{is reducible over } L$$

if and only if there exists an integer l such that

$$\left\langle \frac{n}{l}, \frac{m}{l} \right\rangle =: \langle \nu, \mu \rangle \in \mathbb{N}^2 : \nu < \max\{17, 8g\}$$

and $\frac{x^\nu + Ax^\mu + B}{F(x^{(\mu, \nu)})}$ is reducible over L . Moreover, if $g = 1$, then (iii) implies $n_1 \leq 6$.

Theorem 3. *Let $n_1 > 6$, K be an algebraic number field and $a, b \in K^*$. If the trinomial $x^{n_1} + ax^{m_1} + b$ has in $K[x]$ a monic linear factor $F(x)$, but not a quadratic factor, then $T(x; a, b)F(x^{(m,n)})^{-1}$ is reducible over K if and only if there exists an integer l such that $\langle n/l, m/l \rangle =: \langle \nu, \mu \rangle \in \mathbb{N}^2$ and $a = u^{\nu-\mu}a_0$, $b = u^\nu b_0$, $F = uF_0\left(\frac{x}{u}\right)$, where $u \in K^*$, $\langle a_0, b_0, F_0 \rangle \in F_{\nu, \mu}^1(K)$ and $F_{\nu, \mu}^1(K)$ is a certain finite set, possibly empty.*

There is no principal difficulty in determining in Theorems 1, 2 for $g = 1$, and 3 all cases of reducibility when $n_1 \leq 6$ in much the same way as it was done in [5] for $T(x; A, B)$ or $T(x; a, b)$, however this seems of secondary interest. On the other hand, it is natural to ask what happens when $x^{n_1} + Ax^{m_1} + B$ has a quadratic factor. We intend to return to this question in the next paper of this series.

In analogy with a conjecture proposed in [5] we formulate

Conjecture. For every algebraic number field one can choose sets $F_{\nu,\mu}^1(K)$ such that the set

$$\sum^1 = \bigcup_{\nu,\mu,F} \bigcup_{\langle a,b,F \rangle \in F_{\nu,\mu}^1} \{x^\nu + ax^\mu + b\} \text{ is finite.}$$

2. 16 lemmas to Theorems 1–2

Lemma 1. *If in a transitive permutation group G the length of a cycle $C \in G$ is at least equal to the length of a block of imprimitivity, then it is divisible by the latter.*

PROOF. Let $C = (a_1, \dots, a_\nu)$, $a_{\nu+i} := a_i$ ($i = 1, 2, \dots$) and let $B_1, B_2, \dots$ be conjugate blocks of imprimitivity. Let μ be the least positive integer such that for some i , a_i and $a_{i+\mu}$ belong to the same block B . If $\mu = 1$, then by induction $a_i \in B$ for all i , hence $\nu \leq |B|$ and, since $\nu \geq |B|$ by the assumption, we have $\nu = |B|$.

If $\mu > 1$ we may assume, changing if necessary the numeration of the a_i and of the blocks, that

$$a_i \in B_i \ (1 \leq i \leq \mu), \quad a_{\mu+1} \in B_1.$$

It follows by induction on i that

$$(1) \quad a_{k\mu+i} \in B_i \ (1 \leq i \leq \mu, \ k = 0, 1, \dots),$$

hence, in particular, $i \equiv j \pmod{\nu}$ implies $i \equiv j \pmod{\mu}$, thus $\mu \mid \nu$.

If $a \in B_1$ then $C(a) \in B_2$, hence $C(a) \neq a$ and there exists a_j such that $a = a_j$. By (1) we have

$$j \equiv 1 \pmod{\mu}.$$

Thus among a_j ($1 \leq j \leq \nu$, $j \equiv 1 \pmod{\mu}$) occur all elements of B_1 and only such elements. However a_j in question are distinct, hence

$$\frac{\nu}{\mu} = |B_1| \quad \text{and} \quad |B_1| \mid \nu. \quad \square$$

Lemma 2. *If $(m, n) = 1$ the polynomial $R_1(x, t) = \frac{x^n + tx^m - (1+t)}{x-1}$ is absolutely irreducible. The algebraic function $x(t)$ defined by the equation $R_1(x, t) = 0$ has just $n-2$ branch points $t_i \neq -1, \infty$ with one 2-cycle given by the Puiseux expansions*

$$x(t) = \xi_i \pm (t - t_i)^{1/2} P_{i1} \left(\pm (t - t_i)^{1/2} \right), \quad \xi_i \neq 0 \quad (1 \leq i \leq n-2)$$

and the remaining expansions

$$x(t) = P_{ij}(t - t_i) \quad (2 \leq j \leq n-2).$$

At the branch point -1 $x(t)$ has one m -cycle given by the Puiseux expansions

$$x(t) = \zeta_{2m}^{2i+1} (t+1)^{1/m} P_{n-1,1} \left(\zeta_{2m}^{2i+1} (t+1)^{1/m} \right) \quad (0 \leq i < m)$$

and the remaining expansions at this point are

$$x(t) = P_{n-1,j}(t+1) \quad (2 \leq j \leq n-m).$$

At the branch point ∞ $x(t)$ has one $(n-m)$ -cycle given by the Puiseux expansions

$$x(t) = \zeta_{2(n-m)}^{2i+1} t^{1/(n-m)} P_{n1} \left(\zeta_{2(n-m)}^{2i+1} t^{1/(n-m)} \right),$$

and the remaining expansions at this point are

$$x(t) = P_{nj}(t^{-1}) \quad (2 \leq j \leq m).$$

Here P_{ij} are ordinary formal power series with $P_{ij}(0) \neq 0$ and ζ_q is a primitive root of unity of order q . For a fixed i the values ξ_i and $P_{ij}(0)$ ($j > 1$) are distinct.

PROOF. The polynomial $R_1(x, t)$ is absolutely irreducible since it can be written as

$$\frac{x^n - 1}{x - 1} + t \frac{x^m - 1}{x - 1}$$

and, since $(m, n) = 1$, we have $\left(\frac{x^n - 1}{x - 1}, \frac{x^m - 1}{x - 1} \right) = 1$.

If τ is a finite branch point of the algebraic function $x(t)$ we have for some ξ

$$(2) \quad R_1(\xi, \tau) = R'_{1x}(\xi, \tau) = 0,$$

hence also $T(\xi; \tau, -\tau - 1) = T'_x(\xi; \tau, -\tau - 1) = 0$, which gives either $\xi = 0$, $\tau = -1$ or

$$\tau \neq 0, \quad \xi^{n-m} = -\frac{m}{n}\tau, \quad \xi^m = \frac{n}{n-m} \frac{\tau+1}{\tau}.$$

If $\tau = -\frac{n}{m}$, then $\xi^{n-m} = 1$, $\xi^m = 1$ and, since $(m, n) = 1$, $\xi = 1$. However $R'_{1x}(1, -\frac{n}{m}) = \frac{n(n-1)}{2} - \frac{n}{m} \cdot \frac{m(m-1)}{2} = \frac{n(n-m)}{2} \neq 0$ thus for $\tau \neq -1$ (2) implies $(-\frac{m}{n}\tau)^m = (\frac{n}{n-m} \frac{\tau+1}{\tau})^{n-m}$, $\tau \neq -\frac{n}{m}$, which gives

$$(-m)^m (n-m)^{n-m} \tau^n - n^n (\tau+1)^{n-m} = 0.$$

The only multiple root of this equation is $\tau = -\frac{n}{m}$ and it has multiplicity 2. Denoting the remaining roots by t_i ($1 \leq i \leq n-2$) we find $t_i \neq 0, -1$,

$$\left(-\frac{m}{n}t_i\right)^m = \left(\frac{n}{n-m} \frac{t_i+1}{t_i}\right)^{n-m},$$

hence for a uniquely determined $\xi_i \neq 0, 1$

$$\xi_i^{n-m} = -\frac{m}{n}t_i, \quad \xi_i^m = \frac{n}{n-m} \frac{t_i+1}{t_i}$$

and $R_1(\xi_i, t_i) = R'_{1x}(\xi_i, t_i) = 0$.

Further,

$$\begin{aligned} & R''_{1x}(\xi_i, t_i) \\ &= \frac{n(n-1)\xi_i^{n-1} - n(n-1)\xi_i^{n-2} + m(m-1)t_i\xi_i^{m-1} - m(m-1)t_i\xi_i^{m-2}}{(\xi_i-1)^2} \\ &= \frac{n(n-1)\xi_i^{n-2} + m(m-1)t_i\xi_i^{m-2}}{\xi_i-1} = \xi_i^{m-2} \frac{m(m-n)t_i}{\xi_i-1} \neq 0 \end{aligned}$$

and

$$R'_{1t}(\xi_i, t_i) = \frac{\xi_i^m - 1}{\xi_i - 1} = \frac{mt_i + n}{(\xi_i - 1)(n - m)} \neq 0.$$

It follows that the Taylor expansion of $R_1(x, t)$ at $\langle \xi, t_i \rangle$ has the lowest terms

$$\frac{1}{2}R''_{1x}(\xi_i, t_i)(x - \xi_i)^2 \quad \text{and} \quad R'_{1t}(\xi_i, t_i)(t - t_i),$$

which implies the existence at the point t_i of the two-cycle with the expansions given in the lemma. The remaining expansions are obtained using the fact that $R_1(x, t_i)$ has $n - 3$ distinct zeros, different from 0 and ξ_i . These zeros are $P_{ij}(0)$ ($2 \leq j \leq n - 2$). The assertions concerning branch points -1 and ∞ are proved in a standard way. $\square$

Lemma 3. *If $(m, n) = 1$, the discriminant $D_1(t)$ of $R_1(x, t)$ with respect to x equals*

$$c(t+1)^{m-n} \prod_{i=1}^{n-2} (t - t_i), \quad c \in K^*.$$

PROOF. Since R_1 is monic with respect to x we have

$$D_1(t) = \prod_{i < j} (x_i - x_j)^2,$$

where $R_1(x, t) = \prod_{j=1}^{n-1} (x - x_j)$. Using Lemma 2 we find that the only possible zeros of $D_1(t)$ are t_i ($1 \leq i \leq n-2$) and -1 . Taking for x_j the Puiseux expansion of $x(t)$ at these points we find the exponents with which $t - t_i$ and $t + 1$ divide $D_1(t)$. $\square$

Lemma 4. *If $(m, n) = 1$ the Galois group of the polynomial $R_1(x, t)$ over $\overline{K}(t)$ is the symmetric group S_{n-1} .*

PROOF. Since, by Lemma 2, $R_1(x, t)$ is absolutely irreducible, the group G in question is transitive. By Lemma 1(c) of [5] and Lemma 2 G contains a transposition (for $n > 2$), an m -cycle and an $(n - m)$ -cycle, where we may assume $m \leq n - m$. If G were imprimitive with blocks of imprimitivity of length b , $1 < b < n - 1$ we should have $2b \leq n - 1$, $b \leq n - m$ and by Lemma 1, $b \mid m$ and $b \mid (n, m)$, $b = 1$, a contradiction. Thus G is primitive and since it contains a transposition it must be symmetric by Theorem 14 in Chapter 1 of [7]. $\square$

Definition 1. Let $(m, n) = 1$, $R_1(x, t) = \prod_{i=1}^{n-1} (x - x_i(t))$. We set

$$L_1(k, m, n) = K(t, \tau_1(x_1, \dots, x_k), \dots, \tau_k(x_1, \dots, x_k))$$

$$L_1^*(k, m, n) = \overline{K}(t, \tau_1(x_1, \dots, x_k), \dots, \tau_k(x_1, \dots, x_k)),$$

where τ_j is the j -th fundamental symmetric function.

Remark. By Lemma 4 the fields $L_1(k, m, n)$ and $L_1^*(k, m, n)$ are determined by k, m, n up to an isomorphism fixing $K(t)$ and $\overline{K}(t)$, respectively.

Lemma 5. *The numerator of $t - t_i$ in $L_1^*(k, m, n)$ has $\binom{n-3}{k-1}$ prime divisors in the second power and none in the higher ones.*

PROOF. The proof is analogous to the proof of Lemma 5 in [5].

Lemma 6. *The numerator of $t + 1$ in $L_1^*(k, m, n)$ has*

$$\frac{1}{m} \sum_{l=0}^k \binom{n-m-1}{k-l} \sum_{d|(m,l)} \varphi(d) \binom{m/d}{l/d}$$

distinct prime divisors.

PROOF. By Lemma 1(a) of [5] the prime divisors of the numerator of $t + 1$ are in one-to-one correspondence with the cycles of the Puiseux expansions of a generating element of $L_1^*(k, m, n)$ at $t = -1$ provided the lengths of these cycles are not divisible by π . For the generating element we take $y(t) = \sum_{j=1}^k a^j \tau_j(x_1, \dots, x_k)$, where $a \in \overline{K}$ if K is finite and $a \in K$ otherwise, is chosen so that $\sum_{j=1}^k a^j \tau_j(x_{i_1}, \dots, x_{i_k}) = \sum_{j=1}^k a^j \tau_j(x_1, \dots, x_k)$ implies $\{i_1, \dots, i_k\} = \{1, \dots, k\}$. By Lemma 4 for each set $\{i_1, \dots, i_k\} \subset \{1, \dots, n-1\}$ there is an automorphism of the extension $\overline{K}(t, x_1(t), \dots, x_{n-1}(t)) / \overline{K}(t)$ taking $x_1(t), \dots, x_k(t)$ into $x_{i_1}(t), \dots, x_{i_k}(t)$, respectively. Thus at $t = -1$ we obtain the following Puiseux expansions for $y(t)$

$$\begin{aligned} Q(t, l, i_1, \dots, i_k) = & \sum_{j=1}^k a^j \tau_j \left(\zeta_{2m}^{2i_1+1} (t+1)^{1/m} P_{n-1,1} \left(\zeta_{2m}^{2i_1+1} (t+1)^{1/m} \right), \dots, \right. \\ & \zeta_{2m}^{2i_l+1} (t+1)^{1/m} P_{n-1,1} \left(\zeta_{2m}^{2i_l+1} (t+1)^{1/m} \right), \\ & \left. P_{n-1,i_{l+1}}(t+1), \dots, P_{n-1,i_k}(t+1) \right) \end{aligned}$$

where l runs from 0 to k , $\{i_1, \dots, i_l\}$ runs through all subsets of $\{0, 1, \dots, m-1\}$ of cardinality l and $\{i_{l+1}, \dots, i_k\}$ runs through all subsets of $\{2, 3, \dots, n-m\}$ of cardinality $k-l$.

To see this note that the fundamental symmetric functions of $Q(t, l, i_1, \dots, i_k)$ coincide with the fundamental symmetric functions of the conjugates of $y(t)$ over $\overline{K}(t)$.

If P is an ordinary formal power series, the conjugates of $P((t+1)^{1/m})$ over $\overline{K}((t+1)^{1/d})$, where $d \mid m$ are $P(\zeta_m^{de}(t+1)^{1/m})$, $(0 \leq e < m/d)$. Therefore

$$Q(t, l, i_1, \dots, i_k) \in \overline{K}\left((t+1)^{1/d}\right), \quad \text{where } d \mid m,$$

if and only if

$$Q(t, l, i_1, \dots, i_k) = Q(t, l, i_1 + ed, \dots, i_l + ed, i_{l+1}, \dots, i_k) \quad (0 \leq e < m/d),$$

hence by the choice of a if and only if

$$\{i_1, \dots, i_l\} + d \equiv \{i_1, \dots, i_l\} \pmod{m}.$$

It follows by Lemma 7 of [5] that $y(t)$ has at $t = -1$ exactly

$$\sum_{l=0}^k f(m, l, d) \binom{n-m-1}{k-l}$$

expansions belonging to $\overline{K}((t+1)^{1/d}) \setminus \bigcup_{\delta < d} \overline{K}((t+1)^{1/\delta})$, where $d \mid m$ and

$$f(m, l, d) = \begin{cases} \sum_{\delta \mid (d, dl/m)} \mu(\delta) \left(\frac{d/\delta}{m} \right) & \text{if } m \mid dl, \\ 0 & \text{otherwise.} \end{cases}$$

These expansions split into cycles of d conjugate expansions each, where $m \mid dl$, i.e.

$$d = e \frac{m}{(m, l)}, \quad e \mid (m, l).$$

Hence the number of distinct prime divisors of the numerator of $t+1$ is

$$\sum_{l=0}^k \frac{m}{(m, l)} \sum_{e \mid (m, l)} \frac{1}{e} f\left(m, l, \frac{em}{(m, l)}\right) \binom{n-m-1}{k-l}$$

which, by the formula (1) of [5], equals

$$\frac{1}{m} \sum_{l=0}^k \binom{n-m-1}{k-l} \sum_{d|(m,l)} \varphi(d) \binom{m/d}{l/d}. \quad \square$$

Lemma 7. *The denominator of t in $L_1^*(k, m, n)$ has*

$$\frac{1}{n-m} \sum_{l=0}^k \binom{m-1}{k-l} \sum_{d|(n-m,l)} \varphi(d) \binom{(n-m)/d}{l/d}$$

distinct prime divisors.

PROOF. The proof is analogous to the proof of Lemma 6. $\square$

Lemma 8. *If $n \geq 6$, $(m, n) = 1$, $n-1 \geq 2k \geq 4$, the genus $g_1^*(k, m, n)$ of $L_1^*(k, m, n)$ satisfies $g_1^*(k, m, n) \geq \frac{n}{6}$.*

PROOF. By Lemma 2 the only branch points of $y(t)$ may be t_i ($1 \leq i \leq n-2$), -1 and ∞ . It follows now from Lemma 2(a) of [5], 5, 6 and 7 that

$$\begin{aligned} g_1^*(k, m, n) &= \frac{1}{2} \binom{n-3}{k-1} (n-2) - \frac{1}{2m} \sum_{l=0}^k \binom{n-m-1}{k-l} \sum_{d|(m,l)} \varphi(d) \binom{m/d}{l/d} \\ &\quad - \frac{1}{2(n-m)} \sum_{l=0}^k \binom{m-1}{k-l} \sum_{d|(n-m,l)} \varphi(d) \binom{(n-m)/d}{l/d} + 1. \end{aligned}$$

Using this formula we verify the lemma by direct calculation for $n = 6, 7, 8$. To proceed further we first establish the inequality

$$(3) \quad g_1^*(k, m, n) \geq 1 + \frac{1}{2(n-1)} \binom{n-1}{k} p_1(k, m, n),$$

where

$$p_1(k, m, n) = k(n-k-1) - \begin{cases} \frac{n^2 - n + 3.5}{n-1} & \text{if } m = 1, n-1, \\ \frac{(n-1)(n^2 - 3n + 5.5)}{(n-2)^2} & \text{if } m = 2, n-2, \\ n \left(1 + \frac{3.5}{m(n-m)} \right) & \text{if } 2 < m < n-2. \end{cases}$$

Indeed, by Lemma 13 of [5] we have for $l > 0$

$$\sum_{d|(m,l)} \varphi(d) \binom{m/d}{l/d} \leq \left(1 + \frac{3.5}{m}\right) \binom{m}{l}$$

and trivially for $l \geq 0$

$$\sum_{d|(m,l)} \varphi(d) \binom{m/d}{l/d} \leq m \binom{m}{l}.$$

Similar inequalities hold with m replaced by $n - m$. Hence, for $m = 1$

$$\begin{aligned} g_1^*(k, m, n) &= \frac{1}{2} \binom{n-3}{k-1} (n-2) - \frac{1}{2} \sum_{l=0}^1 \binom{n-2}{k-l} \\ &\quad - \frac{1}{2(n-1)} \sum_{d|(n-1,k)} \varphi(d) \binom{(n-1)/d}{k/d} + 1 \\ &\geq 1 + \frac{k(n-k-1)}{2(n-1)} \binom{n-1}{k} - \frac{1}{2} \binom{n-1}{k} \\ &\quad - \frac{1}{2(n-1)} \left(1 + \frac{3.5}{n-1}\right) \binom{n-1}{k}, \end{aligned}$$

for $m = 2$

$$\begin{aligned} g_1^*(k, m, n) &\geq \frac{1}{2} \binom{n-3}{k-1} (n-2) - \frac{1}{2} \sum_{l=0}^2 \binom{n-3}{k-l} \binom{2}{l} \\ &\quad - \frac{1}{2(n-1)} \sum_{l=k-1}^k \left(1 + \frac{3.5}{n-2}\right) \binom{n-2}{l} + 1 \\ &= 1 + \frac{k(n-k-1)}{2(n-1)} \binom{n-1}{k} - \frac{1}{2} \binom{n-1}{k} \\ &\quad - \frac{1}{2(n-2)} \left(1 + \frac{3.5}{n-2}\right) \binom{n-1}{k}, \end{aligned}$$

for m between 2 and $n - 2$

$$\begin{aligned}
& m - 1 - \frac{3.5}{m} > 0, \quad n - m - 1 - \frac{3.5}{n - m} > 0, \\
& \binom{n - m - 1}{k} \leq \frac{n - m - 1}{n - 1} \binom{n - 1}{k}, \quad \binom{m - 1}{k} \leq \frac{m - 1}{n - 1} \binom{n - 1}{k}; \\
& g_1^*(k, m, n) \geq \frac{1}{2} \binom{n - 3}{k - 1} (n - 2) - \frac{1}{2m} \binom{n - m - 1}{k} m \\
& \quad - \frac{1}{2m} \sum_{l=1}^k \binom{n - m - 1}{k - l} \left(1 + \frac{3.5}{m}\right) \binom{m}{l} - \frac{1}{2(n - m)} \binom{m - 1}{k} (n - m) \\
& \quad - \frac{1}{2(n - m)} \sum_{l=1}^k \binom{m - 1}{k - l} \left(1 + \frac{3.5}{n - m}\right) \binom{n - m}{l} + 1 \\
& = \frac{1}{2} \binom{n - 3}{k - 1} (n - 2) - \frac{1}{2m} \binom{n - m - 1}{k} \left(m - 1 - \frac{3.5}{m}\right) \\
& \quad - \frac{1}{2m} \left(1 + \frac{3.5}{m}\right) \sum_{l=0}^k \binom{n - m - 1}{k - l} \binom{m}{l} \\
& \quad - \frac{1}{2(n - m)} \binom{m - 1}{k} \left(n - m - 1 - \frac{3.5}{n - m}\right) \\
& \quad - \frac{1}{2(n - m)} \left(1 + \frac{3.5}{n - m}\right) \sum_{l=0}^k \binom{m - 1}{k - l} \binom{n - m}{l} + 1 \\
& \geq 1 + \frac{k(n - k - 1)}{2(n - 1)} \binom{n - 1}{k} \\
& \quad - \frac{n - m - 1}{2m(n - 1)} \binom{n - 1}{k} \left(m - 1 - \frac{3.5}{m}\right) - \frac{1}{2m} \left(1 + \frac{3.5}{m}\right) \binom{n - 1}{k} \\
& \quad - \frac{m - 1}{2(n - m)(n - 1)} \binom{n - 1}{k} \left(n - m - 1 - \frac{3.5}{n - m}\right) \\
& \quad - \frac{1}{2(n - m)} \left(1 + \frac{3.5}{n - m}\right) \binom{n - 1}{k}.
\end{aligned}$$

In each case the right hand side of the obtained inequality coincides with

the right hand side of (3). Now for $n \geq 9$, $p_1(k, m, n) \geq p_1(2, \min\{m, 3\}, n) \geq \min_{m \leq 3} p_1(2, m, 9) = 1.25$, hence by (3)

$$g_1^*(k, m, n) \geq 1 + \frac{1.25}{2(n-1)} \binom{n-1}{2} > \frac{n}{4}. \quad \square$$

Lemma 9. *Let $n \geq 3$, $(m, n) = 1$, $R_1(x, t) = \prod_{i=1}^{n-1} (x - x_i(t))$. In the field $\overline{K}(t, x_1(t), x_2(t))$ we have the factorizations*

$$\begin{aligned} t+1 &\cong \frac{\prod_{i=1}^{m-1} \mathfrak{p}_i^m \prod_{j=1}^{n-m-1} \mathfrak{q}_j^m \prod_{j=1}^{n-m-1} \mathfrak{r}_j^m \prod_{k=1}^{(n-m-1)(n-m-2)} \mathfrak{s}_k}{\prod_{j=1}^{n-m-1} \mathfrak{t}_j^{n-m} \prod_{i=1}^{m-1} \mathfrak{u}_i^{n-m} \prod_{i=1}^{m-1} \mathfrak{v}_i^{n-m} \prod_{l=1}^{(m-1)(m-2)} \mathfrak{w}_l}, \\ x_1(t) &\cong \frac{\prod_{i=1}^{m-1} \mathfrak{p}_i \prod_{j=1}^{n-m-1} \mathfrak{q}_j}{\prod_{j=1}^{n-m-1} \mathfrak{t}_j \prod_{i=1}^{m-1} \mathfrak{u}_i}, \\ x_2(t) &\cong \frac{\prod_{i=1}^{m-1} \mathfrak{p}_i \prod_{j=1}^{n-m-1} \mathfrak{r}_j}{\prod_{j=1}^{n-m-1} \mathfrak{t}_j \prod_{i=1}^{m-1} \mathfrak{v}_i} \end{aligned}$$

where $\mathfrak{p}_i, \mathfrak{q}_j, \mathfrak{r}_j, \mathfrak{s}_k, \mathfrak{t}_j, \mathfrak{u}_i, \mathfrak{v}_i, \mathfrak{w}_l$ are distinct prime divisors. For t_i defined in Lemma 2 the numerators of $t - t_i$ has $(n-3)(n-4)$ factors in the first power only, the remaining factors are double.

PROOF. By Lemma 1(a)(b) of [5] the prime divisors of the numerator or the denominator of $t - c$ are in one-to-one correspondence with the cycles of the Puiseux expansions of a generating element of $\overline{K}(t, x_1(t), x_2(t))/\overline{K}(t)$ at $t = c$ or $t = \infty$, respectively, provided the lengths of the cycles are not divisible by π . For the generating element we take $y(t) = ax_1(t) + bx_2(t)$, where $a, b \in \overline{K}$ are chosen so that for all $i < n$, $j < n$, $i \neq j$ we have either $ax_i(t) + bx_j(t) \neq ax_1(t) + bx_2(t)$ or $\langle i, j \rangle = \langle 1, 2 \rangle$. By Lemma 4 for each pair $\langle i, j \rangle$ with $i < n$, $j < n$ there is an automorphism of the extension $\overline{K}(t, x_1(t), \dots, x_n(t))/\overline{K}(t)$ taking $x_1(t), x_2(t)$ into $x_i(t), x_j(t)$, respectively. At $t = -1$ we obtain for $y(t)$ the expansions

$$\begin{aligned} &a\zeta_{2m}^{2i+1}(1+t)^{1/m}P_{n-1}\left(\zeta_{2m}^{2i+1}(1+t)^{1/m}\right) \\ &+ b\zeta_{2m}^{2j+1}(1+t)^{1/m}P_{n-1}\left(\zeta_{2m}^{2j+1}(1+t)^{1/m}\right) \\ &\quad (0 \leq i < m, 0 \leq j < m, i \neq j), \end{aligned}$$

$$a\zeta_{2m}^{2i+1}(1+t)^{1/m}P_{n-1}\left(\zeta_{2m}^{2i+1}(1+t)^{1/m}\right) + bP_{n-1}(1+t)$$

$$(0 \leq i < m, 2 \leq j \leq n-m),$$

$$aP_{n-1}(1+t) + b\zeta_{2m}^{2i+1}(1+t)^{1/m}P_{n-1}\left(\zeta_{2m}^{2i+1}(1+t)^{1/m}\right)$$

$$(0 \leq i < m, 2 \leq j \leq n-m),$$

$$aP_{n-1}(1+t) + bP_{n-1}(1+t) \quad (2 \leq i \leq n-m, 2 \leq j \leq n-m, i \neq j).$$

The $m(m-1)$ expansions of the first set form $m-1$ m -cycles corresponding to the divisors $\mathfrak{p}_1, \dots, \mathfrak{p}_{m-1}$, that divide the numerators of $x_1(t), x_2(t)$ in exactly first power. (Note that $\text{ord}_{\mathfrak{p}_\mu} x_1 = m \text{ord}_{t+1}(1+t)^{1/m} P_{n-1}(\zeta_{2m}^{2i+1}(1+t)^{1/m})$ for $\mu < m$ and similarly for x_2). The $m(n-m-1)$ expansions of the second set form $n-m-1$ m -cycles corresponding to the divisors $\mathfrak{q}_1, \dots, \mathfrak{q}_{n-m-1}$, that divide the numerator of $x_1(t)$ in exactly first power and do not divide the numerator of $x_2(t)$.

The $m(n-m-1)$ expansions of the third set form $n-m-1$ m -cycles corresponding to the divisors $\mathfrak{r}_1, \dots, \mathfrak{r}_{n-m-1}$ that divide the numerator of $x_2(t)$ in exactly first power and do not divide the numerator of $x_1(t)$. The $(n-m-1)(n-m-2)$ expansions of the fourth set form as many 1-cycles corresponding to the divisors that divide the numerator of $1+t$ in exactly first power and divide the numerator of neither $x_1(t)$ nor $x_2(t)$.

Since $x_1(t) = 0$ implies $t = -1$ we have found all factors of the numerator of $x_1(t)$ and similarly of $x_2(t)$.

At $t = \infty$ we obtain for $y(t)$ again four sets of expansions that correspond to the four sets of divisors: $\mathfrak{t}_j$ ($1 \leq j \leq n-m-1$), $\mathfrak{u}_i, \mathfrak{v}_i$ ($1 \leq i \leq m-1$) and $\mathfrak{w}_l$ ($1 \leq l \leq (m-1)(m-2)$) occurring in the denominator of $1+t, x_1(t)$ and $x_2(t)$.

Since $x_1(t) = \infty$ implies $t = \infty$ no other divisor occurs in the denominator of $x_1(t)$, or of $x_2(t)$.

At $t = t_i$ we obtain for $y(t)$ among others the expansions

$$aP_i + bP_i \quad (1 \leq i \leq n-2, 2 \leq j \leq n-2, 2 \leq k \leq n-2, j \neq k)$$

which form $(n-3)(n-4)$ 1-cycles corresponding to $(n-3)(n-4)$ simple factors of the numerator of $t - t_i$. All the remaining expansions contain $(t - t_i)^{1/2}$. $\square$

Lemma 10. *If $(m, n) = 1$, for all primes p*

$$\sqrt[n]{t+1} \notin \overline{K}(t, x_1(t), \dots, x_{n-1}(t)) =: \Omega.$$

PROOF. The argument used in the proof of Lemma 9 applied to the field Ω gives that the multiplicity of every prime divisor of the numerator and the denominator of $t+1$ divides m and $n-m$, respectively. Since $(m, n) = 1$ we cannot have $1+t = \gamma^p$, $\gamma \in \Omega$. $\square$

Lemma 11. *Let $(m, n) = 1$, $n \geq 3$. For every positive integer $q \not\equiv 0 \pmod{\pi}$ and for every choice of q th roots we have*

$$\left[\overline{K} \left(\sqrt[q]{x_1(t)}, \dots, \sqrt[q]{x_{n-1}(t)} \right) : \overline{K}(t, x_1(t), \dots, x_{n-1}(t)) \right] = q^{n-1}.$$

PROOF. By Theorem 1 of [4] it is enough to prove that for every prime $p \mid q$

$$(4) \quad \prod_{j=1}^{n-1} x_j^{\alpha_j} = \gamma^p, \quad \gamma \in \Omega = \overline{K}(t, x_1(t), \dots, x_{n-1}(t))$$

implies $\alpha_j \equiv 0 \pmod{p}$ for all $j < n$. Assume that (4) holds, but say $\alpha_1 \not\equiv 0 \pmod{p}$.

If for all j we have $\alpha_j \equiv \alpha_1 \pmod{p}$ it follows from (4) that

$$\left(\prod_{j=1}^{n-1} x_j \right)^{\alpha_1} = \gamma'^p, \quad \gamma' \in \Omega,$$

and since

$$\prod_{j=1}^{n-1} x_j = (-1)^{n-1}(t+1)$$

we obtain $\sqrt[n]{t+1} \in \Omega$, contrary to Lemma 10. Therefore, there exists an $i \leq n-1$ such that $\alpha_i \not\equiv \alpha_1 \pmod{p}$, and in particular $n \geq 3$. Changing, if necessary, the numeration of x_i we may assume that $i = 2$. By Lemma 4 there exists an automorphism τ of $\Omega/\overline{K}(t)$ such that $\tau(x_1) = x_2$, $\tau(x_2) = x_1$, $\tau(x_i) = x_i$ ($i \neq 1, 2$). Applying τ to (4) we obtain

$$x_1^{\alpha_2} x_2^{\alpha_1} \prod_{j=1}^{n-1} x_j^{\alpha_j} = (\gamma^\tau)^p,$$

hence on division

$$\left(\frac{x_1}{x_2}\right)^{\alpha_1 - \alpha_2} = \left(\frac{\gamma}{\gamma^\tau}\right)^p.$$

Since $\alpha_1 - \alpha_2 \not\equiv 0 \pmod{p}$ it follows that

$$(5) \quad \frac{x_1}{x_2} = \delta^p, \quad \delta \in \Omega.$$

The extension $\overline{K}(t, x_1, x_2, \delta)/\overline{K}(t, x_1, x_2)$ is a normal subextension of $\Omega/\overline{K}(t, x_1, x_2)$ of degree 1 or p and, since by Lemma 4 the latter has the symmetric Galois group, we have either $\delta \in \overline{K}(t, x_1, x_2)$, or $p = 2$,

$$\delta \in \overline{K}\left(t, x_1, x_2 \prod_{\substack{\mu, \nu=3 \\ \nu > \mu}}^{n-1} (x_\nu - x_\mu)\right) \setminus \overline{K}(t, x_1, x_2).$$

In the former case we compare the divisors on both sides of (5) and obtain

$$\delta^p \cong \frac{\prod_{j=1}^{n-m-1} \mathfrak{q}_j \prod_{i=1}^{m-1} \mathfrak{v}_i}{\prod_{j=1}^{n-m-1} \mathfrak{r}_j \prod_{j=1}^{m-1} \mathfrak{u}_i},$$

a contradiction.

In the latter case, since the conjugates of δ with respect to $\overline{K}(t, x_1, x_2)$ are $\pm\delta$ we have

$$\delta = \varepsilon \prod_{\substack{\mu, \nu=3 \\ \nu > \mu}}^{n-1} (x_\nu - x_\mu), \quad \varepsilon \in \overline{K}(t, x_1, x_2),$$

hence

$$\begin{aligned} \delta &= \varepsilon \prod_{\substack{\mu, \nu=3 \\ \nu > \mu}}^{n-1} (x_\nu - x_\mu) \cdot \frac{x_1 - x_2}{\prod_{\nu > 1} (x_\nu - x_1) \cdot \prod_{\nu \neq 2} (x_\nu - x_2)} \\ &= \eta \prod_{\substack{\mu, \nu=1 \\ \nu > \mu}}^{n-1} (x_\nu - x_\mu), \quad \eta \in K(t, x_1, x_2). \end{aligned}$$

It follows by (5) and Lemma 3 that

$$\frac{x_1}{x_2} = \eta^2 \operatorname{disc}_x R_1(x, t) = \operatorname{const} \eta^2 (t+1)^{m-1} \prod_{i=1}^{n-2} (t-t_i).$$

For $n \geq 5$, by Lemma 9, $t-t_1$ has at least one simple factor, which occurs with a non-zero exponent on the right-hand side, but not on the left, a contradiction. On the other hand for $n = 3$ or 4 the divisor of the right hand side is a square, of the left hand side is not. $\square$

Lemma 12. *Let $n \geq 3$, $(n, m) = 1$, $q \not\equiv 0 \pmod{\pi}$, $q \geq 2$ and $y_{iq}^q = x_i(t)$ ($1 \leq i < n$). Then*

$$\left[\overline{K} \left(t, \left(\sum_{i=1}^{n-1} y_{iq} \right)^q \right) : \overline{K}(t) \right] = q^{n-2}.$$

PROOF. By Lemmas 4 and 11 all embeddings of $\overline{K}(t, y_{1q}, \dots, y_{n-1,q}) / \overline{K}(t)$ into $\overline{K}(t) / \overline{K}(t)$ are given by

$$(6) \quad y_{iq} \rightarrow \zeta_q^{\alpha_i} y_{\sigma(i)q} \quad (1 \leq i < n),$$

where σ is a permutation of $\{1, 2, \dots, n-1\}$ and

$$(7) \quad \langle \alpha_1, \dots, \alpha_{n-1} \rangle \in (\mathbb{Z}/q\mathbb{Z})^{n-1}.$$

We shall show that there are exactly q^{n-2} distinct images of $(\sum_{i=1}^{n-1} y_{iq})^q$ under transformations (6). Indeed, if we apply (7) with $\sigma(i) = i$ to $(\sum_{i=1}^{n-1} y_{iq})^q$ we obtain

$$\left(\sum_{i=1}^{n-1} \zeta_q^{\alpha_i} y_{iq} \right)^q.$$

If this were equal to $(\sum_{i=1}^{n-1} \zeta_q^{\beta_i} y_{iq})^q$ for a vector $\langle \beta_1, \dots, \beta_{n-1} \rangle \in (\mathbb{Z}/q\mathbb{Z})^{n-1}$ with $\beta_j - \beta_1 \neq \alpha_j - \alpha_1$ for a certain j we should obtain

$$y_{1q} \in \overline{K}(y_{2q}, \dots, y_{n-1,q}), \text{ or } y_{jq} \in \overline{K}(y_{1q}, \dots, y_{j-1,q}, y_{j+1,q}, \dots, y_{n-1,q}),$$

contrary to Lemma 11. Thus the number of distinct images is at least equal to the number of vectors satisfying (7) with $\alpha_1 = 0$, thus to q^{n-2} . On the other hand, $(\sum_{i=1}^{n-1} y_{iq})^q$ is invariant under transformations (6) with $\alpha_1 = \alpha_2 = \dots = \alpha_{n-1}$, which form a group, hence the number in question does not exceed q^{n-2} . $\square$

Definition 2. Let $(m, n) = 1$, $q \not\equiv 0 \pmod{\pi}$ and $y_{iq}^q = x_i(t)$, where $x_i(t)$ are defined in Definition 1. We set

$$M_1(m, n, q) = K \left(t, \left(\sum_{i=1}^{n-1} y_{iq} \right)^q \right), \quad M_{1*}(m, n, q) = \overline{K} \left(t, \left(\sum_{i=1}^{n-1} y_{iq} \right)^q \right).$$

Remark. By Lemma 12, for $n \geq 3$, $M_1(m, n, q)$ and $M_{1*}(m, n, q)$ are determined by m, n, q up to an isomorphism which fixes $K(t)$ and $\overline{K}(t)$, respectively.

Lemma 13. For $n > 3$ the numerator of $t - t_i$ has in $M_{1*}(m, n, q) \times (q^{n-2} - q^{n-3})/2$ factors in the second power.

PROOF. Let us put for each $i \leq n - 2$

$$y_{i1q} = \xi_i^{1/q} \sum_{k=0}^{\infty} \binom{1/q}{k} \xi^{-k/q} (t - t_i)^{k/2} P_{i1} \left((t - t_i)^{1/2} \right)^k,$$

$$y_{i2q} = \xi_i^{1/q} \sum_{k=0}^{\infty} (-1)^k \binom{1/q}{k} \xi^{-k/q} (t - t_i)^{k/2} P_{i1} \left(-(t - t_i)^{1/2} \right)^k,$$

so that for $j = 1, 2$

$$y_{ijq}^q = \xi_i + (-1)^{j-1} (t - t_i)^{1/2} P_{i1} \left((-1)^{j-1} (t - t_i)^{1/2} \right),$$

$$(8) \quad y_{i1q} + y_{i2q} \in \overline{K}((t - t_i)),$$

$$(9) \quad (y_{i1q} - y_{i2q})(t - t_i)^{1/2} \in \overline{K}((t - t_i))$$

and choose in an arbitrary way

$$(10) \quad y_{ijq} = (P_{i,j-1}(t - t_i))^{1/q} \in \overline{K}((t - t_i)) \quad (2 < j < n).$$

It follows from Lemma 2 that over the field $\overline{K}((t - t_i))$

$$\prod_{j=1}^{n-1} \prod_{\alpha=0}^{q-1} (x - \zeta_q^\alpha y_{jq}) = R_1(x^q, t) = \prod_{j=1}^{n-1} \prod_{\alpha=0}^{q-1} (x - \zeta_q^\alpha y_{ijq}),$$

thus the corresponding fundamental symmetric functions of $\zeta_q^\alpha y_{jq}$ ($1 \leq j < n$, $0 \leq \alpha < q$) and of $\zeta_q^\alpha y_{ijq}$ coincide. Hence

$$\begin{aligned} & \prod_{\alpha_2=0}^{q-1} \cdots \prod_{\alpha_{n-1}=0}^{q-1} \left(x - \left(y_{1q} + \sum_{j=2}^{n-1} \zeta_q^{\alpha_j} y_{jq} \right)^q \right) \\ &= \prod_{\alpha_2=0}^{q-1} \cdots \prod_{\alpha_{n-1}=0}^{q-1} \left(x - \left(y_{i1q} + \sum_{j=2}^{n-1} \zeta_q^{\alpha_j} y_{ijq} \right)^q \right), \end{aligned}$$

which means that $(\sum_{i=1}^{n-1} y_{jq})^q$ has the following Puiseux expansions at $t = t_i$

$$\left(y_{i1q} + \zeta_q^{\alpha_2} y_{i2q} + \sum_{j=3}^{n-1} \zeta_q^{\alpha_j} y_{ijq} \right)^q, \quad \langle \alpha_2, \dots, \alpha_{n-1} \rangle \in (\mathbb{Z}/q\mathbb{Z})^{n-2}.$$

If such an expansion belongs to $\overline{K}((t - t_i))$, then either

$$y_{i1q} + \zeta_q^{\alpha_2} y_{i2q} + \sum_{j=3}^{n-1} \zeta_q^{\alpha_j} y_{ijq} \in \overline{K}((t - t_i))$$

or $2 \mid q$ and

$$\left(y_{i1q} + \zeta_q^{\alpha_2} y_{i2q} + \sum_{j=3}^{n-1} \zeta_q^{\alpha_j} y_{ijq} \right) (t - t_i)^{\frac{1}{2}} \in \overline{K}((t - t_i)).$$

In the former case, by (8) and (10)

$$\left(1 - \zeta_q^{\alpha_2} \right) y_{i1q} \in \overline{K}((t - t_i))$$

and since $P_{i1}(0) \neq 0$, $\alpha_2 = 0$.

In the latter case, by (9), on multiplying it by $(\zeta_q^{\alpha_i} - 1)/2$ and adding

$$\left(\frac{1 + \zeta_q^{\alpha_2}}{2} (y_{i1q} + y_{i2q}) + \sum_{j=3}^{n-1} \zeta_q^{\alpha_j} y_{ijq} \right) (t - t_i)^{1/2} \in \overline{K}((t - t_i))$$

and, since

$$\frac{1 + \zeta_q^{\alpha_2}}{2} (y_{i1q} + y_{i2q}) + \sum_{j=3}^{n-1} \zeta_q^{\alpha_j} y_{ijq} \in \overline{K}((t - t_i))$$

by (8) and (10), we obtain

$$(11) \quad \frac{1 + \zeta_q^{\alpha_2}}{2} (y_{i1q} + y_{i2q}) + \sum_{j=3}^{n-1} \zeta_q^{\alpha_j} y_{ijq} = 0.$$

However the left hand side is an expansion at $t = t_i$ of

$$\frac{1 + \zeta_q^{\alpha_2}}{2} (y_{iq} + y_{2q}) + \sum_{j=3}^{n-1} \zeta_q^{\alpha_j} y_{jq},$$

hence (11) contradicts for $n > 3$ the linear independence of y_{jq} ($1 \leq j < n$) over $\overline{K}$ resulting from Lemma 11.

Therefore for $n > 3$ we obtain $q^{n-2} - q^{n-3}$ expansions for $(\sum_{j=3}^{n-1} y_{jq})^q$ belonging to $\overline{K}((t - t_i)^{1/2}) \setminus \overline{K}((t - t_i))$, which correspond to $(q^{n-2} - q^{n-3})/2$ distinct prime divisors of the numerator of $t - t_i$ in $M_{1*}(m, n, q)$. $\square$

Lemma 14. *The numerator of $t + 1$ in $M_{1*}(m, n, q)$ has at most*

$$\frac{q^{\max\{n-3, m-1\}}}{m} \left(1 + \frac{m-1}{q^{\varphi(mq)/\varphi(q)}} \right)$$

distinct prime divisors.

PROOF. By Lemma 1(a) in [5] the prime divisors of the numerator of $t + 1$ correspond to the cycles of the Puiseux expansions of $(\sum_{i=1}^{n-1} y_{iq})^q$ at $t = -1$ provided the lengths of these cycles are not divisible by π . By Lemma 2 and the argument about symmetric functions used in the proof of Lemma 13 we obtain the expansions

$$(12) \quad \left(\sum_{j=1}^m \zeta_q^{\alpha_j} \zeta_{2mq}^{2j-1} (t+1)^{1/qm} P_{n-1,1} \left(\zeta_{2m}^{2j-1} (t+1)^{1/q} \right)^{1/q} \right. \\ \left. + \sum_{j=m+1}^{n-1} \zeta_q^{\alpha_j} P_{n-1,j-m+1} (t+1)^{1/q} \right)^q,$$

where $\langle \alpha_1, \dots, \alpha_{n-1} \rangle \in (\mathbb{Z}/q\mathbb{Z})^{n-1}$, $\alpha_1 = 0$. Note that $qm \not\equiv 0 \pmod{\pi}$. Let S be the set of vectors $\langle \alpha_2, \dots, \alpha_m \rangle \in (\mathbb{Z}/q\mathbb{Z})^{m-1}$ such that

$$1 + \sum_{j=2}^m \zeta_q^{\alpha_j} \zeta_{qm}^{j-1} = 0.$$

By Lemma 21 of [5]

$$(13) \quad \text{card } S \leq q^{m-\varphi(qm)/\varphi(q)-1}.$$

If $n \geq m+2$ and $\langle \alpha_2, \dots, \alpha_m \rangle \notin S$ the least power of $t+1$ occurring in the first or the second sum in (12) is $(t+1)^{1/qm}$ and $(t+1)^{\nu_0}$, respectively, where ν_0 is a nonnegative integer. Hence the expansion (12) contains with a non-zero coefficient

$$(14) \quad (t+1)^{1/m} \text{ and } (t+1)^{(q-1)/qm+\nu_0}.$$

Indeed, if we had for some nonnegative integers a_μ ($\mu = 0, 1, \dots$)

$$\sum_{\mu=0}^{\infty} a_\mu = q \text{ and } \sum_{\mu=0}^{\infty} a_\mu \left(\frac{1}{qm} + \frac{\mu}{m} \right) = \frac{q-1}{qm} + \nu_0$$

it would follow from the second formula that $\sum_{\mu=0}^{\infty} a_\mu \equiv q-1 \pmod{q}$, contrary to the first formula.

The least common denominator of the two exponents in (14) is

$$\left[m, \frac{qm}{(qm, q-1)} \right] = \frac{q^2 m}{(q^2 m, (q-1)m, qm)} = qm,$$

hence we obtain at most

$$\frac{(q^{m-1} - \text{card } S)q^{n-m-1}}{qm}$$

qm -cycles.

If $n \geq m+2$ and $\langle \alpha_2, \dots, \alpha_m \rangle \in S$ the least power of $t+1$ occurring in the first or the second sum in (12) is $(t+1)^{\frac{1}{qm} + \frac{\mu_0}{m}}$ and $(t+1)^{\nu_0}$, respectively, where $\mu_0 \in \mathbb{N}$ and $\nu_0 \in \mathbb{N}$. Hence the expansion (12) contains with a non-zero coefficient

$$(t+1)^{\frac{q-1}{qm} + \frac{(q-1)\mu_0}{m} + \nu_0} \quad \text{if } \frac{1}{qm} + \frac{\mu_0}{m} < \nu_0$$

and

$$(t+1)^{\frac{1}{qm} + \frac{\mu_0}{m} + (q-1)\nu_0}, \quad \text{otherwise.}$$

Since both exponents in the reduced form have q in the denominator we obtain at most

$$\frac{\text{card } S \cdot q^{n-m-1}}{q}$$

q -cycles.

If $n = m + 1$ and $\langle \alpha_2, \dots, \alpha_m \rangle \notin S$ the least power of $t + 1$ occurring in the parentheses in (12) is $(t + 1)^{1/q^m}$, thus the expression (12) contains with a non-zero exponent $(t + 1)^{1/m}$ and we obtain at most $\frac{q^{m-1} - \text{card } S}{m}$ m -cycles.

Finally if $n = m + 1$ and $\langle \alpha_2, \dots, \alpha_m \rangle$ runs through S we bound the number of cycles by $\text{card } S$. Therefore by (13), if $n \geq m + 2$ the total number of cycles does not exceed

$$\begin{aligned} & \frac{(q^{m-1} - \text{card } S)q^{n-m-1}}{qm} + \frac{\text{card } S \cdot q^{n-m-1}}{q} \\ &= \frac{q^{n-3}}{m} \left(1 + \frac{(m-1) \text{card } S}{q^{m-1}} \right) \leq \frac{q^{n-3}}{m} \left(1 + \frac{m-1}{q^{\varphi(qm)/\varphi(q)}} \right), \end{aligned}$$

if $n = m + 1$ the total number of cycles does not exceed

$$\begin{aligned} & \frac{(q^{m-1} - \text{card } S)}{m} + \text{card } S = \frac{q^{m-1}}{m} \left(1 + \frac{(m-1) \text{card } S}{q^{m-1}} \right) \\ &= \frac{q^{m-1}}{m} \left(1 + \frac{m-1}{q^{\varphi(qm)/\varphi(q)}} \right). \quad \square \end{aligned}$$

Lemma 15. *The denominator of t has in $M_{1*}(m, n, q)$ at most*

$$\frac{q^{\max\{n-3, n-m-1\}}}{n-m} \left(1 + \frac{n-m-1}{q^{\varphi(q(n-m))/\varphi(q)}} \right)$$

distinct prime divisors.

PROOF. Proof is analogous to the proof of Lemma 14. $\square$

Lemma 16. *For all positive integers m, n and q where $n > 3$, $n > m$, $(n, m) = 1$, $qnm(n-m) \not\equiv 0 \pmod{\pi}$ and $q \geq 2$ the genus $g_{1*}(m, n, q)$ of $M_{1*}(m, n, q)$ is greater than $\frac{nq}{8}$ unless $nq \leq 16$. Moreover $g_{1*}(m, n, q) > 1$ unless $n < 6$.*

PROOF. By Lemma 2(a) of [5] and by Lemmas 13–15 we have

$$g_{1*}(m, n, q) \geq 1 + \frac{q^{n-3}}{2} \left(\frac{q-1}{2}(n-2) - \frac{q^{\max\{0, m-n+2\}}}{m} \left(1 + \frac{m-1}{q^{\varphi(qm)/\varphi(q)}} \right) - \frac{q^{\max\{0, 2-m\}}}{n-m} \left(1 + \frac{n-m-1}{q^{\varphi(q(n-m))/\varphi(q)}} \right) \right).$$

Hence, by Lemma 24 of [5]

$$g_{1*}(m, n, q) \geq 1 + \frac{q^{n-3}}{2} \gamma_1(q, n, m),$$

where

$$\gamma_1(q, n, m) = \begin{cases} \frac{q-1}{2}(n-2) - 1 - \frac{q+1}{n-1} & \text{if } m = 1 \text{ or } m = n-1, \\ \frac{q-1}{2}(n-2) - \left(\frac{1}{m} + \frac{1}{n-m} \right) \left(1 + \frac{1}{q} \right) & \text{otherwise.} \end{cases}$$

For $n \geq 6$ we have $q^{n-3} \geq \frac{2}{3}nq$, $\gamma_1(q, n, m) \geq \frac{2}{5}$, hence $g_{1*}(m, n, q) > \frac{2nq}{15} > \frac{nq}{8} > 1$; for $6 > n > 3$ $g_{1*}(m, n, q) \leq \frac{nq}{8}$ implies $nq \leq 16$. $\square$

3. Proof of Theorem 1

Let $F(x) = x - C$, where $C \in K(\mathbf{y})$. Since $F(x) \mid x^{n_1} + Ax^{m_1} + B$ we obtain $B = -C^{n_1} - AC^{m_1}$, $C \neq 0$. From $A^{-n}B^{n-m} \notin K$ we infer that $t := AC^{m_1-n_1} \notin K$. We have the identity

$$(15) \quad \begin{aligned} Q(x) &:= \frac{x^{n_1} + Ax^{m_1} + B}{F(x)} \\ &= C^{n_1-1} \frac{(C^{-1}x)^{n_1} + t(C^{-1}x)^{m_1} - (t+1)}{C^{-1}x - 1}. \end{aligned}$$

If $T(x; A, B)F(x^{(m,n)})^{-1}$ is reducible over $K(\mathbf{y})$, then by Capelli's Lemma (see e.g. [1], p. 662) either

$$(16) \quad Q(x) \text{ is reducible over } K(\mathbf{y}),$$

or

$$(17) \quad x^{(m,n)} - \xi \text{ is reducible over } K(\mathbf{y}, \xi), \text{ where } \xi \text{ is a zero of } Q(x).$$

In the former case $Q(x)$ has in $K(\mathbf{y})[x]$ a factor $x^k + \sum_{i=1}^k a_i x^{k-i}$, where, by the assumption, $2 \leq k \leq \frac{n_1-1}{2}$. The identity (15) implies that the field $L_1^*(k, m_1, n_1)$ defined in Definition 1 is a rational function field parametrized as follows:

$$t = AC^{m_1-n_1}, \quad \tau_i(x_1, \dots, x_k) = (-1)^i a_i C^{-i} \quad (1 \leq i \leq k).$$

By Lemma 2(b) of [5] $g_1^*(k, m_1, n_1) = 0$.

Assume now that we have (17) but not (16). It follows by Capelli's theorem that either

$$(18) \quad \xi = \eta^p, \text{ where } p \text{ is a prime, } p \mid (m, n), \quad \eta \in K(\mathbf{y}, \xi),$$

or

$$(19) \quad \xi = -4\eta^4, \text{ where } 4 \mid (m, n), \quad \eta \in K(\mathbf{y}, \xi),$$

Let

$$\frac{x^{n_1} + tx^{m_1} - (t+1)}{x-1} = \prod_{j=1}^{n_1-1} (x - x_j), \quad y_{jq}^q = x_j.$$

It follows from (15) that if $t = AC^{m_1-n_1}$ one can take

$$q = p, \quad y_{jq} = C^{-1/p} \eta_j \quad \text{if (18) holds,}$$

$$q = 4, \quad y_{jq} = (1 + \zeta_4) C^{-1/4} \eta_j \quad \text{if (19) holds,}$$

where η_j are conjugates of η over $K(\mathbf{y})$. Hence the field

$$M_{1*}(m_1, n_1, q) = \overline{K}(t, (y_{1q} + \dots + y_{n_1-1,q})^q)$$

is parametrized by rational functions as follows

$$t = AC^{m_1-n_1},$$

$$(y_{1q} + \dots + y_{n_1-1,q})^q = \begin{cases} C^{-1}(\eta_1 + \dots + \eta_{n_1-1})^p & \text{if (18) holds,} \\ -4C^{-1}(\eta_1 + \dots + \eta_{n_1-1})^4 & \text{if (19) holds} \end{cases}$$

and, by Lemma 2(b) of [5], $g_{1*}(m_1, n_1, q) = 0$, contrary to Lemma 16.

PROOF of Theorem 2. The sufficiency of the condition is obvious. The proof of the necessity is similar to that of Theorem 1.

Let $F(x) = x - C$, where $C \in L$,

$$Q(x; A, B) = \frac{x^{n_1} + Ax^{m_1} + B}{F(x)}.$$

Since $F(x) \mid x^{n_1} + Ax^{m_1} + B$ and $B \neq 0$ we have $C \neq 0$, $B = -C^{n_1} - AC^{m_1}$. Since $A^{-n}B^{n-m} \notin \overline{K}$, we have $t := AC^{m_1-n_1} \notin \overline{K}$.

If $T(x; A, B)F(x^{(m,n)})^{-1} = Q(x^{(m,n)}; A, B)$ is reducible over L then either

$$(20) \quad Q(x) := Q(x; A, B) \text{ is reducible over } L$$

or

$$(21) \quad x^{(m,n)} - \xi \text{ is reducible over } L(\xi) \text{ where } \xi \text{ is a zero of } Q.$$

In the former case Q has in $L[x]$ a factor of degree k , where by the assumption $2 \leq k \leq \frac{n_1-1}{2}$ and it follows from the identity (15) that the field $L_1^*(k, m_1, n_1)$ is isomorphic to a subfield of $\overline{K}L$. Hence, by Lemma 2(c) of [5], $g_1^*(k, m_1, n_1) \leq g$ and, by Lemma 8, $n_1 \leq 6 \max\{1, g\}$. In particular, for $g = 1$ we have $n_1 \leq 6$. The condition given in the theorem holds with $l = (m, n)$, $\langle \nu, \mu \rangle = \langle n_1, m_1 \rangle$.

Assume now that we have (21), but not (20). Then in the same way as in the proof of Theorem 1 we infer that for a certain $q \mid (m, n)$, $q = 4$ or a prime

$$(22) \quad x^q - \xi \text{ is reducible over } L(\xi)$$

and the field $M_{1*}(m_1, n_1, q)$ is isomorphic to a subfield of $\overline{K}L$. Hence, by Lemma 2(c) of [5], we have $g_{1*}(m_1, n_1, q) \leq g$, thus by Lemma 16 for $n_1 > 3$ we have $n_1 q < \max\{17, 8g\}$ and $g > 1$ for $n_1 \geq 6$. On the other hand, by (22), $Q(x^q)$ is reducible over L . Hence the condition given in the theorem holds with $l = \frac{(m, n)}{q}$, $\langle \nu, \mu \rangle = \langle n_1 q, m_1 q \rangle$. $\square$

4. 2 lemmas to Theorem 3

Lemma 17. *Let L be a finite extension of a field K , q a prime different from $\text{char } K$. There exists a finite subset $F = F(q, L/K)$ of K^* of cardinality at most $q^{\text{ord}_q[L:K]}$ such that if*

$$(23) \quad c \in K^*, \gamma \in L, \quad c = \gamma^q,$$

then there exist $f \in F$ and $e \in K^*$ such that

$$(24) \quad c = fe^q.$$

PROOF. Let

$$(25) \quad A = \{a \in K^* : a = \alpha^q, \alpha \in L\}$$

and let B be a finite subset of A with the property that for all functions $x : B \rightarrow \mathbb{Z}$

$$(26) \quad \prod_{a \in B} a^{x(a)} = b^q, \quad b \in K \text{ implies } x(a) \equiv 0 \pmod{q} \text{ for all } a \in B.$$

It follows from Theorem 1 of [4] that for every choice of q -th roots

$$[K(\sqrt[q]{a} : a \in B) : K] = q^{\text{card } B},$$

hence by (25), in view of $B \subset A$,

$$q^{\text{card } B} \mid [L : K]$$

and $\text{card } B \leq \text{ord}_q[L : K]$. Among all subsets B of A with the property (26) let us choose one of maximal cardinality and denote it by A_0 . We assert that the set

$$F = \left\{ \prod_{a \in A_0} a^{x(a)} : x(A_0) \subset \{0, 1, \dots, q-1\} \right\}$$

has the property asserted in the lemma. Indeed

$$\text{card } F = q^{\text{card } A_0} \leq q^{\text{ord}_q[L:K]}.$$

On the other hand, if $c \in A_0$, (24) holds with $d = c$, $e = 1$. If $c \notin A_0$ the set $B = A_0 \cup \{c\}$ has more elements than A_0 . By definition of A_0 it has not the property (26). Hence there exist integers $x(a)$ ($a \in A_0$) and $x(c)$ such that $c^{x(c)} \prod_{a \in A_0} a^{x(a)} = b^q$, $b \in K$ and either

$$(27) \quad x(c) \equiv 0 \pmod{q} \text{ and for at least one } a \in A_0 : x(a) \not\equiv 0 \pmod{q}$$

or

$$(28) \quad x(c) \not\equiv 0 \pmod{q}.$$

The case (27) is impossible, since it implies

$$\prod_{a \in A_0} a^{x(a)} = \left(bc^{-\frac{x(c)}{q}} \right)^q,$$

contrary to the choice of A_0 .

In the case (28) there exist integers y and z such that

$$-x(c)y = 1 + qz$$

and we obtain (24) with

$$f = \prod_{a \in A_0} a^{q\{\frac{x(a)y}{q}\}}, \quad e = b^{-y}c^{-z} \prod_{a \in A_0} a^{\left[\frac{x(a)y}{q}\right]},$$

where $\{\cdot\}$ and $[\cdot]$ denote the fractional and the integral part, respectively. $\square$

Lemma 18. *Let q be a prime or $q = 4$. For every finite extension $K(\xi)$ of a field K there exists a finite subset $S(q, K, \xi)$ of K such that if $c \in K^*$ and*

$$(29) \quad \begin{aligned} c\xi &= \eta^q, & \eta &\in K(\xi)^* & \text{if } q \text{ is a prime,} \\ c\xi &= -4\eta^4, & \eta &\in K(\xi)^* & \text{if } q = 4, \end{aligned}$$

then

$$(30) \quad c = de^q, \quad \text{where } d \in S(q, K, \xi), \quad e \in K^*.$$

PROOF. Assume first that q is a prime. If there is no $c \in K^*$ such that (29) holds we put $S(q, K, \xi) = \emptyset$. Otherwise we have

$$(31) \quad c_0\xi = \eta_0^q, \quad \eta_0 \in K(\xi)^*, \quad c_0 \in K^*$$

and the equations (29) and (31) give

$$c/c_0 = (\eta/\eta_0)^q.$$

Hence, by Lemma 17

$$c/c_0 = fe^q, \quad \text{where } f \in F(q, K(\xi)/K), \quad e \in K^*$$

and in order to satisfy (30) it is enough to put

$$S(q, K, \xi) = \{c_0 f : f \in F(q, K(\xi)/K)\}.$$

Assume now that $q = 4$. Again if there is no c such that (29) holds we put $S(q, K, \xi) = \emptyset$. Otherwise, we have

$$(32) \quad c_0 \xi = -4\eta_0^4, \quad \eta_0 \in K(\xi)^*, \quad c_0 \in K^*$$

and the equations (29) and (32) give

$$(33) \quad c/c_0 = (\eta/\eta_0)^4.$$

By Lemma 17 applied with $q = 2$

$$(34) \quad c/c_0 = fe^2, \quad f \in F(2, K(\xi)/K), \quad e \in K^*.$$

If for a given $f \in F(2, K(\xi)/K)$ there exists $e_f \in K^*$ such that

$$(35) \quad fe_f^2 = \vartheta^4, \quad \vartheta \in K(\xi)$$

the equations (33)–(35) give

$$(e/e_f)^2 = (\eta/\eta_0\vartheta)^4, \quad \text{hence } e/e_f = \pm (\eta/\eta_0\vartheta)^2$$

and another application of Lemma 17 gives

$$e/e_f = \pm f_1 e_1^2, \quad f_1 \in F(2, K(\xi)/K), \quad e_1 \in K^*.$$

Hence, by (34)

$$c/c_0 = fe_f^2 f_1^2 e_1^4$$

and in order to satisfy (30) it is enough to put

$$S(q, K, \xi) = \bigcup_{\substack{f \in F(2, K(\xi)/K) \\ e_f \text{ exists}}} \{c_0 f e_f^2 f_1^2 : f_1 \in F(2, K(\xi)/K)\}. \quad \square$$

5. Proof of Theorem 3

We begin by defining the sets $F_{\nu,\mu}^1(K)$. This is done in three steps. First we put $q = (\mu, \nu)$, $\nu_1 = \nu/q$, $\mu_1 = \mu/q$ and introduce the fields $L_1(k, \mu_1, \nu_1)$ and $M_1(\mu_1, \nu_1, q)$ as defined in Definitions 1, 2. Since K is infinite we have $L_1(k, \mu_1, \nu_1) = K(t, y(t))$, where $y(t)$ is defined up to a conjugacy over $K(t)$ in the proof of Lemma 6. Let Φ_k^1 be the minimal polynomial of $y(t)$ over $K(t)$. It follows from the definition of $y(t)$ that $\Phi_k^1 \in K[t, z]$. By Lemma 12 the function $(y_{1q} + \cdots + y_{\nu_1-1,q})^q$ generating $M_1(\mu_1, \nu_1, q)$ over $K(t)$ is determined up to a conjugacy. Let Ψ_q^1 be its minimal polynomial over $K(t)$. Since y_{iq} are integral over $K[t]$ we have $\Psi_q^1 \in K[t, z]$. If $\nu_1 > 6$ we put

$$S_{\nu,\mu}^1(K) = \begin{cases} \bigcup_{2 < 2k < \nu_1} \{t_0 \in K : \Phi_k^1(t_0, z) \text{ has a zero in } K\} & \text{if } q = 1, \\ \{t_0 \in K : \Psi_q^1(t_0, z) \text{ has a zero in } K\} & \text{if } q > 1. \end{cases}$$

Since for $\nu_1 > 6$ and $k > 1$ or $q > 1$ we have $g_1^*(k, \mu_1, \nu_1) > 1$ or $g_{1*}(\mu_1, \nu_1, q) > 1$, respectively, it follows by the Faltings theorem that the sets $S_{\nu,\mu}^1(K)$ are finite. Now we put

$$T_{\nu,\mu}^1(K) = \begin{cases} \bigcup_{t_0 \in S_{\nu,\mu}^1(K)} \{ \langle t_0, -t_0 - 1, 1 \rangle \} & \text{if } q = 1, \\ \bigcup_{t_0 \in S_{\nu,\mu}^1(K)} \{ \langle t_0 d^{\nu_1 - \mu_1}, -(t_0 + 1)d^{\nu_1}, d \rangle : \exists_{\xi_0} d \in S(q, K, \xi_0), \\ \quad \xi_0^{\nu_1} + t_0 \xi_0^{\mu_1} - (t_0 + 1) = 0 \} & \text{if } q \text{ is a prime or } q = 4, \\ \emptyset & \text{otherwise} \end{cases}$$

($S(q, K, \xi)$ is defined in Lemma 18);

$$F_{\nu,\mu}^1(K) = \{ \langle a, b, x - d \rangle : \langle a, b, d \rangle \in T_{\nu,\mu}^1(K) \text{ and } \frac{x^\nu + ax^\mu + b}{x^q - d} \text{ is a polynomial reducible over } K \}.$$

Since the sets $S_{\nu,\mu}^1(K)$ and the sets $S(q, K, \xi_0)$ are finite, so are the sets $F_{\nu,\mu}^1(K)$. We proceed to prove that they have all the other properties asserted in the theorem.

By the assumption $n_1 > 6$ and $x^{n_1} + ax^{m_1} + b$ has in $K[x]$ a linear factor $F(x)$ but not a quadratic factor. Let $F(x) = x - c$, where $c \in K^*$, so that $b = -c^{n_1} - ac^{m_1}$. Put

$$(36) \quad t_0 = ac^{m_1-n_1}, \quad Q(x; a, b) = \frac{x^{n_1} + ax^{m_1} + b}{F(x)}.$$

Assume that

$$\frac{x^n + ax^m + b}{F(x^{(m,n)})} = Q\left(x^{(m,n)}; a, b\right) \text{ is reducible over } K.$$

By Capelli's lemma either

$$(37) \quad Q(x; a, b) \text{ is reducible over } K$$

or

$$(38) \quad x^{(n,m)} - \xi \text{ is reducible over } K, \text{ where } Q(\xi; a, b) = 0$$

In the case (37) $Q(x; a, b)$ has a factor in $K[x]$ of degree k such that $1 < k \leq \frac{n_1-1}{2}$, say $\prod_{i=1}^k (x - \xi_i)$. It follows from the identity

$$(39) \quad \frac{x^{n_1} + t_0 x^{m_1} - (t_0 + 1)}{x - 1} = c^{1-n_1} Q(cx; a, b)$$

that the left hand side has the factor $\prod_{i=1}^k (x - c^{-1}\xi_i)$, thus $\tau_i(c^{-1}\xi_1, \dots, c^{-1}\xi_k) \in K$ ($1 \leq i \leq k$) and at least one value of the algebraic function $y(t)$ at $t = t_0$ lies in K , hence $t_0 \in S_{n_1, m_1}^1(K)$. It follows that $\langle t_0, -t_0 - 1, 1 \rangle \in T_{n_1, m_1}^1(K)$, $\langle t_0, -t_0 - 1, x - 1 \rangle \in F_{n_1, m_1}^1(K)$ and the condition given in the theorem holds with $l = (m, n)$, $\nu = n_1$, $\mu = m_1$, $a_0 = t_0$, $b_0 = -t_0 - 1$, $F_0 = x - 1$, $u = c$.

In the case (38) note that

$$(40) \quad Q(\xi; a, b) = 0, \quad \text{implies} \quad \xi \neq 0.$$

Further, by Capelli's theorem, there exists a $q \mid (m, n)$ such that

$$(41) \quad \begin{aligned} &\text{either } q \text{ is a prime and } \xi = \eta^q, \eta \in K(\xi)^* \text{ or } q = 4 \\ &\text{and } \xi = -4\eta^4, \eta \in K(\xi)^*. \end{aligned}$$

If $\eta_1, \dots, \eta_{n_1-1}$ are all the conjugates of η over K we have

$$Q(x; a, b) = \begin{cases} \prod_{i=1}^{n_1-1} (x - \eta_i^q) & \text{if } q \text{ is a prime,} \\ \prod_{i=1}^{n_1-1} (x + 4\eta_i^4) & \text{if } q = 4, \end{cases}$$

hence

$$(42) \quad Q(x^q; a, b) \text{ is reducible over } K.$$

By the identity (39) it follows that

$$\frac{x^{n_1} + t_0 x^{m_1} - (t_0 + 1)}{x - 1} = \begin{cases} \prod_{i=1}^{n_1-1} (x - c^{-1} \eta_i^q) & \text{if } q \text{ is a prime,} \\ \prod_{i=1}^{n_1-1} (x + 4c^{-1} \eta_i^4) & \text{if } q = 4. \end{cases}$$

Hence $\Psi_q^1(t_0, u_0) = 0$, where

$$u_0 = \begin{cases} c^{-1}(\eta_1 + \dots + \eta_{n_1-1})^q & \text{if } q \text{ is a prime,} \\ -4c^{-1}(\eta_1 + \dots + \eta_{n_1-1})^4 & \text{if } q = 4. \end{cases}$$

and, since $\eta_1 + \dots + \eta_{n_1-1} \in K$, we have $u_0 \in K$, $t_0 \in S_{n_1, m_1}(K)$.

Further, it follows from (39) and (40) that $\xi_0 = c^{-1}\xi$ is a zero of $\frac{x^{n_1} + t_0 x^{m_1} - (t_0 + 1)}{x - 1}$ and, by (41), $c\xi_0 = \eta^q$ or $-4\eta^4$, where $\eta \in K(\xi_0)^*$ and q is a prime or $q = 4$, respectively.

By Lemma 18 $c = de^q$, where $d \in S(q, K, \xi_0)$, $e \in K$, hence

$$\langle t_0 d^{n_1 - m_1}, -(t_0 + 1)d^{n_1}, d \rangle \in T_{n_1 q, m_1 q}^1(K).$$

By (39)

$$\frac{x^{n_1 q} + t_0 d^{n_1 - m_1} x^{m_1 q} - (t_0 + 1)d^{n_1}}{x^q - d} = (cd^{-1})^{1-n_1} Q((ex)^q; a, b),$$

hence, by (42)

$$\frac{x^{n_1 q} + t_0 d^{n_1 - m_1} x^{m_1 q} - (t_0 + 1)d^{n_1}}{x^q - d} \text{ is reducible over } K$$

and $\langle t_0 d^{n_1 - m_1}, -(t_0 + 1)d^{n_1}, x - d \rangle \in F_{n_1 q, m_1 q}^1(K)$. Thus the condition given in the theorem holds with $l = (m, n)/q$, $\nu = n_1 q$, $\mu = m_1 q$, $a_0 = t_0 d^{n_1 - m_1}$, $b_0 = -(t_0 + 1)d^{n_1}$, $F_0 = x - d$, $u = e$.

Assume now that for an integer $l : n/l = \nu$, $m/l = \mu$ and $a = u^{\nu-\mu}a_0$, $b = u^\nu b_0$, $F(x) = uF_0\left(\frac{x}{u}\right)$, where $u \in K^*$, $\langle a, b, F_0 \rangle \in F_{\nu,\mu}^1(K)$. Then by the definition of $F_{\nu,\mu}^1(K)$

$$\frac{x^\nu + ax^\mu + b}{F_0(x^{(\mu,\nu)})} \text{ is a polynomial reducible over } K,$$

and by the substitution $x \mapsto \frac{x^l}{u}$ we obtain reducibility of $T(x; a, b)F(x^{(n,m)})^{-1}$ over K .

The proof of Theorem 3 is complete.

6. Addenda and corrigenda to the paper [5]

The paper [5] has been corrected in [6]. Regretfully further corrections are needed.

- Page 6, Table 1: $A_{6,1}$ should read $4v(v^2 + 3)$, $B_{6,1}$ should read $-(v^2 + 4v - 1)(v^2 - 4v - 1)$.
in $B_{7,2}$ for $v^2 - v - 1$ read $v^2 - v + 1$
(This correction is due to G. Turnwald).
in $A_{15,5}$ for $100v^2$ read $10v^2$
(This correction is due to J. Browkin).
- Page 27, lines –13
to –1: for $\overline{K}(x_1, \dots)$ read $\overline{K}(t, x_1, \dots)$ nine times.
- Page 28, line –10: for $\sum_{i=1}^n y_{iq}$ read $(\sum_{i=1}^n y_{iq})^q$.
- Page 31, line –13: for $\frac{1}{n} +$ read $1 +$.
- Page 37, formula (24): for n read (m, n) .
line –13: for η_4 read η_{n_1} .
- Page 40, line –3: for $(p-1)n$ read $(p-1)d$, not pd as indicated in [6].
- Page 41, line –14: after 2 insert 7.
line –7: for $v^2 - v - 1$ read $v^2 - v + 1$ (This and the previous correction are due to G. Turnwald).
- Page 55, line –2: As pointed out in [6] (with a misprint)
the following inclusion has been used

$$(*) \quad K_0(\mathbf{y})^{\text{sep}} \cap K_1(\mathbf{y}) \subset (K_0^{\text{sep}} \cap K_1)(\mathbf{y}),$$

where K_0 is a subfield of K_1 , $\mathbf{y} = \langle y_1, \dots, y_r \rangle$ is a variable vector, K_0^{sep} and $K_0(\mathbf{y})^{\text{sep}}$ is the separable closure of K_0 and $K_0(\mathbf{y})$, respectively.

Here is a proof of (*) by induction on r . For $r = 0$ (*) is obvious. Assume (*) is true for $\mathbf{y}$ of $r - 1$ coordinates and let

$$t \in K_0(\mathbf{y})^{\text{sep}} \cap K_1(\mathbf{y}).$$

We have $F(\mathbf{y}, t) = 0$, where $F \in K_0[\mathbf{y}, T]$ and the discriminant $D(y)$ of $F(y, T)$ with respect to T is not zero. Let $a \in K_0[\mathbf{y}]$ be the leading coefficient of F with respect to T , so that

$$(**) \quad G(\mathbf{y}, at) = 0,$$

where $G(\mathbf{y}, T) := a^{\deg_T F - 1} F(\mathbf{y}, T/a)$ is monic with respect to T . We have $at \in K_1[\mathbf{y}]$, hence

$$(*)_{**} \quad at = \sum_{\nu=0}^n a_\nu y_r^{n-\nu}, \quad a_\nu \in K_1[y_1, \dots, y_{r-1}] \quad (0 \leq \nu \leq n).$$

Choose $n + 1$ distinct elements $\eta_0, \dots, \eta_n$ of K_0^{sep} such that

$$(**)_{**} \quad a(y_1, \dots, y_{r-1}, \eta_i) D(y_1, \dots, y_{r-1}, \eta_i) \neq 0 \quad (0 \leq i \leq n).$$

Since by (**) and $(*)_{**}$

$$G\left(y_1, \dots, y_{r-1}, \eta_i, \sum_{\nu=0}^n a_\nu \eta_i^{n-\nu}\right) = 0$$

and, by $(**)$, the discriminant of $G(y_1, \dots, y_{r-1}, \eta_i, T)$ with respect to T is not zero, we have

$$\sum_{\nu=0}^n a_\nu \eta_i^{n-\nu} \in K_0(y_1, \dots, y_{r-1})^{\text{sep}}.$$

Since $\det(\eta_i^{n-\nu}) \neq 0$ we have $a_\nu \in K_0(y_1, \dots, y_{r-1})^{\text{sep}} (0 \leq \nu \leq n)$. By the inductive assumption $a_\nu \in (K_0^{\text{sep}} \cap K_1)(y_1, \dots, y_{r-1}) (0 \leq \nu \leq n)$ and by (**) $(**)$

$$t \in (K_0^{\text{sep}} \cap K_1)(\mathbf{y}).$$

Page 61, line -9: for ν read ν_1 .

Page 62, lines 10 and 11: The formulae make sense only for $u_0 \neq 0$. If $u_0 = 0$ one should write instead, both for q prime and $q = 4$, $\langle t_0^\rho d^{\nu-\mu}/q, t_0^\sigma d^{\nu/q} \rangle$, where $d \in S(q, K, \xi_0)$ and $\xi_0^{\nu/q} + t_0^\rho \xi_0^{\mu/q} + t_0^\sigma = 0$. $S(q, K, \xi)$ is the set defined in Lemma 18 above.

If $x^n + ax^m + b$ is reducible over K and $x^{n_1} + ax^{m_1} + b$ is irreducible over K , then retaining the notation of [5] and putting $\xi_0 = a^{-s}b^r\xi$ we argue as follows.

Since $a^sb^{-r}\xi_0 = \xi = \eta^q$ or $-4\eta^4$, where $\eta \in K(\xi)^*$ and q is a prime or $q = 4$, respectively, we have by Lemma 18 above

$$a^sb^{-r} = de^q, \quad d \in S(q, K, \xi_0), \quad e \in K.$$

Since, by (74) $t_0 = a^{-n_1}b^{n_1-m_1}$ we obtain

$$\begin{aligned} a &= a^{s(n_1-m_1)-rn_1} = t_0^r(de^q)^{n_1-m_1} = t_0^r d^{n_1-m_1} e^{n_1q-m_1q}, \\ b &= b^{s(n_1-m_1)-rn_1} = t_0^s(de^q)^{n_1} = t_0^s d^{n_1} e^{qn_1}. \end{aligned}$$

By (75) $x^{n_1q} + t_0^r d^{n_1-m_1} x^{m_1q} + t_0^s d^{n_1}$ is reducible over K , hence $\langle t_0^r d^{n_1-m_1}, t_0^s d^{n_1} \rangle \in F_{n_1q, m_1q}$ and (ix) holds with $l = \frac{(m, n)}{q}$, $\nu = n_1q$, $\mu = m_1q$, $u = e$.

Page 80, Table 5: Insert three new examples

<i>Number</i>	<i>Trinomial</i>	<i>Factor</i>	<i>Discoverer</i>
11a	$x^{10} + 3^6 \cdot 11x + 2 \cdot 3^8$	$x^3 + 3x^2 + 9x + 18$	Cisłowska [2]
12a	$x^{10} + 2^6 \cdot 5 \cdot 7^6 \cdot 11 \cdot 631x$ $+ 2^7 \cdot 7^7 \cdot 17 \cdot 19 \cdot 73$	$x^3 + 14x^2 + 392x + 3332$	Cisłowska [2]
36a	$x^{15} - 3^6x^6 + 3^9$	$x^5 + 3x^4 + 9x^3 + 18x^2$ $+ 27x + 27$	Chaladus [1]

References

- [1] S. CHALADUS, Letter to the author of July 7, 1994.
- [2] R. CISŁOWSKA, Master dissertation, *Siedlce University*, 1995.
- [3] L. RÉDEI, Algebra, *Erster Teil*, Leipzig, 1959.
- [4] A. SCHINZEL, On linear dependence of roots, *Acta Arith.* **28** (1975), 161–175.
- [5] A. SCHINZEL, On reducible trinomials, *Dissert. Math.* **329** (1993).

- [6] A. SCHINZEL, Errata to [5], *Acta Arith.* **73** (1995), 399–400.
- [7] N. TSCHEBOTARÖW, Grundzüge der Galoisschen Theorie, übersetzt und bearbeitet von H. Schwerdtfeger, *Groningen-Djakarta*, 1950.

ANDRZEJ SCHINZEL
MATHEMATICS INSTITUTE PAN
P.O. BOX 137, 00-950 WARSZAWA
POLAND

E-mail: schinzel@plearn.edu.pl

(Received July 26, 1999; revised January 10, 2000)