POLSKA AKADEMIA NAUK, INSTYTUT MATEMATYCZNY

DISSERTATIONES MATHEMATICAE

(ROZPRAWY MATEMATYCZNE)

CCCXXIX

ANDRZEJ SCHINZEL

On reducible trinomials

WARSZAWA 1993

Andrzej Schinzel
Institute of Mathematics
Polish Academy of Sciences
P.O. Box 137
Śniadeckich 8
00-950 Warszawa, Poland
E-mail: schinzel@impan.impan.gov.pl

Published by the Institute of Mathematics, Polish Academy of Sciences
Typeset in TEX at the Institute
Printed and bound by
drukarnia
herman & herman

PRINTED IN POLAND

ISSN 0012-3862

CONTENTS

1991 *Mathematics Subject Classification*: 12E05, 12E10.
Received 9.4.1993; revised version 2.6.1993.

Introduction and the statement of results

The problem of reducibility of binomials over $\mathbb{Q}$ was settled nearly a hundred years ago by Vahlen [32]. His criterion was soon generalized to all fields of characteristic 0 by Capelli [3] and much later to all fields of positive characteristic by Rédei [18]. It is the aim of the present paper to prove similar results for trinomials at least over algebraic number fields or function fields in one variable. In the latter case, when the field in question is rational, one variable can be replaced by any number of variables, and the results are definitive.

In the sequel n, m denote positive integers, $n > m$,

$$n_1 = \frac{n}{(n,m)}\,, \qquad m_1 = \frac{m}{(n,m)}\,;$$

K is a field of characteristic $\pi \geq 0$ with $\pi \nmid nm(n-m)$, $\overline{K}$ is the algebraic closure of K, $\mathbf{y}$ is a variable vector, and ζ_n is a primitive root of unity of order n in K.

THEOREM 1. *Let $n \geq 2m$ and $A, B \in K(\mathbf{y})^*$, $A^{-n}B^{n-m} \notin K$. The trinomial $x^n + Ax^m + B$ is reducible over $K(\mathbf{y})$ if and only if either*

(i) *$x^{n_1} + Ax^{m_1} + B$ has a proper linear or quadratic factor over $K(\mathbf{y})$*

or

(ii) *there exists an integer l such that*

$$\left\langle \frac{n}{l}, \frac{m}{l} \right\rangle := \langle \nu, \mu \rangle \in S_0 := \bigcup_{p \text{ prime}} \langle 2p, p \rangle \cup \{\langle 6,1\rangle, \langle 6,2\rangle, \langle 7,1\rangle, \langle 8,2\rangle, \langle 8,4\rangle, \langle 9,3\rangle, \langle 10,2\rangle, \langle 10,4\rangle, \langle 12,2\rangle, \langle 12,3\rangle, \langle 12,4\rangle, \langle 15,5\rangle\}$$

and $A = u^{\nu-\mu}A_{\nu,\mu}(v)$, $B = u^{\nu}B_{\nu,\mu}(v)$, where $u, v \in K(\mathbf{y})$ and the polynomials $A_{\nu,\mu}$, $B_{\nu,\mu}$ are given in Table 1.

THEOREM 2. *Let $n \geq 2m$ and $A, B \in L^*$, where L is a finite extension of $K(y_1)$ with $\overline{K}L$ of genus $g > 0$ and $A^{-n}B^{n-m} \notin \overline{K}$.*

For $g = 1$ the trinomial $x^n + Ax^m + B$ is reducible over L if and only if at least one of the following three conditions is satisfied:

(iii) *$x^{n_1} + Ax^{m_1} + B$ has a proper linear or quadratic factor over L;*

(iv) *there exists an integer l such that*

Table 1

ν, μ	$A_{\nu,\mu}$	$B_{\nu,\mu}$
$2p$, p	$-\left(\frac{1+\sqrt{1-4v}}{2}\right)^p - \left(\frac{1-\sqrt{1-4v}}{2}\right)^p$	v^p
6, 1	$8v(v^2+1)$	$(v^2+4v-1)(v^2-4v-1)$
6, 2	$4(v+1)$	$-v^2$
7, 1	$-(2v+1)^4(4v^2-3v+1)$ $\times (v^3-2v^2-v+1)$	$v(2v-1)(2v+1)^5(3v-2)$ $\times (v^2-v-1)$
8, 2	$-v^2+8v-8$	$(2v-2)^2$
8, 4	$2v^2-8v+4$	v^4
9, 3	$v^3-81v+243$	$27(v-3)^3$
10, 2	$4v^3-8v+4$	$-(v^2-4v+2)^2$
10, 4	$v^5(-v^3+8v-8)$	$-4v^8(v-1)^4$
12, 2	$1024(v-4)^8(2v-3)(v^2-6v+6)$ $\times (v^2-2v+2)$	$1024(v-4)^{10}(v^3-8v+8)^2$
12, 3	$-729v(v-1)^7(2v-1)(3v^2-6v+2)$ $\times (3v^2-3v+1)$	$729(v-1)^9(3v^3-3v+1)^3$
12, 4	$512(2v-1)(2v^2+2v-1)(2v^2-2v+1)$	$1024(2v^2-4v+1)^4$
15, 5	$5(5v-5)^7(5v^4-5v^3-5v^2+5v-1)$ $\times (5v^4-10v^3+100v^2-5v+1)$	$(5v-5)^{10}(5v^2-5v+1)^5$

$$\left\langle \frac{n}{l}, \frac{m}{l} \right\rangle := \langle \nu, \mu \rangle \in S_0 \qquad \textit{and} \qquad A = u^{\nu-\mu} A_{\nu,\mu}(v)\,,\ B = u^{\nu-\mu} B_{\nu,\mu}(v)\,,$$

where $u, v \in L$ and $A_{\nu,\mu}$, $B_{\nu,\mu}$ are given in Table 1;

(v) *there exists an integer l such that*

$$\left\langle \frac{n}{l}, \frac{m}{l} \right\rangle := \langle \nu, \mu \rangle \in S_1 := \{\langle 7,2\rangle, \langle 7,3\rangle, \langle 8,1\rangle, \langle 9,1\rangle, \langle 14,2\rangle, \langle 21,7\rangle\}$$

and $A = u^{\nu-\mu} A_{\nu,\mu}(v,w)$, $B = u^{\nu-\mu} B_{\nu,\mu}(v,w)$, where $u \in L$, $\langle v, w\rangle \in E_{\nu,\mu}(L)$, and the elliptic curve $E_{\nu,\mu}$ and the polynomials $A_{\nu,\mu}$, $B_{\nu,\mu}$ are given in Table 2. *For $\langle \nu, \mu\rangle = \langle 8,1\rangle$ there is a double choice.*

For $g > 1$ the trinomial $x^n + Ax^m + B$ is reducible over L if and only if either (iii) *or* (iv) *holds or there exists an integer l such that*

$$\left\langle \frac{n}{l}, \frac{m}{l} \right\rangle := \langle \nu, \mu \rangle \in \mathbb{Z}^2, \qquad \nu < 24g$$

and $x^\nu + Ax^\mu + B$ is reducible over L.

THEOREM 3. *Let L be a finite separable extension of $K(\mathbf{y})$, $L \cap \overline{K} = K_0$, and $A, B \in L^*$, $A^{-n}B^{n-m} \in \overline{K}$. The trinomial $x^n + Ax^m + B$ is reducible over L if and only if there exists a $q \,|\, (m, n)$, $q = 1, 4$ or a prime, and a $C \in L$ such that*

$$A = aC^{(n_1 - m_1)q}, \qquad B = bC^{n_1 q}, \qquad a, b \in K_0,$$

and

$$x^{n_1 q} + ax^{m_1 q} + b \text{ is reducible over } K_0.$$

Theorem 1 has the following consequences.

THEOREM 4. *Let $a \in K^*$ and $B \in K(\mathbf{y}) \setminus K$. The trinomial $x^n + ax^m + B$ is reducible over $K(\mathbf{y})$ if and only if for a certain $t \in K(\mathbf{y})$ either $B = -t^{n_1} - at^{m_1}$ or $n_1 \geq 4$, $m_1 = n_1 - 1$,*

$$B = (-a)^{n_1} t^{n_1 - 1} \frac{f_{n_1 - 1}(t)^{n_1 - 1}}{f_{n_1}(t)^{n_1}}, \qquad f_l(t) = \frac{(1 + \sqrt{1 - 4t})^l - (1 - \sqrt{1 - 4t})^l}{2^l \sqrt{1 - 4t}}$$

or there exists an integer l such that

$$\left\langle \frac{n}{l}, \frac{m}{l} \right\rangle := \langle \nu, \mu \rangle \in \{\langle 4, 1\rangle, \langle 4, 2\rangle, \langle 6, 2\rangle, \langle 6, 3\rangle, \langle 6, 4\rangle, \langle 6, 5\rangle, \langle 7, 6\rangle, \langle 8, 6\rangle\}$$

and $B = B^*_{\nu,\mu}(t)$, where the rational functions $B^*_{\nu,\mu}$ are given in Table 3. If $\langle \nu, \mu \rangle = \langle 8, 6 \rangle$ we must have $a = \alpha^2 - 2\beta^2$, where $\alpha, \beta \in K$.

THEOREM 5. *Let $n \geq 2m$, $A \in K(\mathbf{y}) \setminus K$ and $b \in K^*$. The trinomial $x^n + Ax^m + b$ is reducible over $K(\mathbf{y})$ if and only if for a certain $t \in K(\mathbf{y})^*$ either $A = -t^{n_1 - m_1} - bt^{-m_1}$ or there exists an integer l such that*

$$\left\langle \frac{n}{l}, \frac{m}{l} \right\rangle := \langle \nu, \mu \rangle \in \bigcup_{p \text{ prime}} \{\langle 2p, p\rangle\} \cup \{\langle 6, 2\rangle, \langle 8, 2\rangle, \langle 8, 4\rangle, \langle 9, 3\rangle\},$$

$A = A^*_{\nu,\mu}(t, b_1)$ and b, $b_1 \in K$ satisfy a suitable equation, which together with the rational function $A^*_{\nu,\mu}$ is given in Table 4.

Let us note that Theorems 4 and 5 contain as very special cases Lemmas 2 and 3 of [11], which are crucial for the determination obtained in that paper of all quadrinomials in two variables reducible over K (l.c. Theorem 1). Combining the tools developed for the proof of Theorems 1 and 3 with the Faltings theorem one obtains

THEOREM 6. *Let $n \geq 2m$, K be an algebraic number field, and $a, b \in K^*$. The trinomial $x^n + ax^m + b$ is reducible over K if and only if at least one of the following four conditions is satisfied*:

Table 2

ν, μ	$E_{\nu,\mu}$	$A_{\nu,\mu}$	$B_{\nu,\mu}$
7, 2	$w^2 = v^3 + 16v^2 + 64v + 80$	$2v^2 - 8v - 48 + w(2v - 4)$	$-(4v + 12 + w)$ $\times (v^2 + 12v + 32 + 4w)$
7, 3	$w^2 = v^3 - 675v + 13662$	$(-v^3 + 27v^2 + 3753v$ $- 34803 + w(6v - 666))$ $\times (v - 39)$	$6(v - 39)^2$ $\times (-v^2 - 12v + 693 + 6w)$ $\times (9v^2 + 162v - 4455$ $- w(v + 33))$
8, 1	$w^2 = v^3 - 10v + 12$	$-8v^3 + 20v^2 + 8v - 32$ $+w(3v^2 - 12v - 10)$	$(w - 3v + 5)(-3v^2 + 15v$ $- 17 + w(2v - 5))$
	$w^2 = v^3 - 20v - 16$	$128(w - 2v - 8)^4$ $\times (v + 2)(v^2 + 12v + 4)$ $\times (2w - v^2 + 4v + 4)$ $\times (4w - v^2 - 12)$	$64(w - 2v - 8)^4(9v^4 + 8v^3$ $- 8v^2 + 288v + 272$ $- w(v^3 + 18v^2 + 76v + 24))$ $\times (v^4 + 24v^3 + 152v^2$ $+ 96v + 16$ $+ w(v^3 - 22v^2 - 52v - 72))$
9, 1	$w^2 = v^3 + 18v - 36$	$81(w - 2v - 9)^4$ $\times ((v^7 + 27v^6$ $+ 351v^5 + 639v^4$ $- 675v^3 - 5589v^2$ $+ 6318v - 7290)w$ $+ (-9v^8 - 66v^7 - 936v^6$ $+ 1890v^5 + 4995v^4$ $- 5670v^3 + 14580v^2$ $- 72900v + 37179))$	$27(w - 2v - 9)^5((5v^7 - 603v^6$ $- 765v^5 + 5661v^4$ $+ 3213v^3 + 29889v^2$ $- 28674v + 10206)w$ $+ (-v^9 + 63v^8 + 1719v^7$ $- 4959v^6 - 10611v^5 + 1917v^4$ $+ 111456v^3 - 145800v^2$ $+ 207036v - 61236))$

(vi) *$x^{n_1} + ax^{m_1} + b$ has a proper linear or quadratic factor over K*;

(vii) *there exists an integer l such that $\langle n/l, m/l\rangle := \langle \nu, \mu\rangle \in S_0$ and $a = u^{\nu-\mu}A_{\nu,\mu}(v)$, $b = u^{\nu}B_{\nu,\mu}(v)$, where $u, v \in K$*;

(viii) *there exists an integer l such that $\langle n/l, m/l\rangle := \langle \nu, \mu\rangle \in S_1$ and $a = u^{\nu-\mu}A_{\nu,\mu}(v, w)$, $b = u^{\nu}B_{\nu,\mu}(v, w)$, where $u \in K$, $\langle v, w\rangle \in E_{\nu,\mu}(K)$*;

(ix) *there exists an integer l such that $\langle n/l, m/l\rangle := \langle \nu, \mu\rangle \in \mathbb{Z}^2$ and $a = u^{\nu-\mu}a_0$, $b = u^{\nu}b_0$, where $\langle a_0, b_0\rangle \in F_{\nu,\mu}(K)$ and $F_{\nu,\mu}(K)$ is a certain finite set, possibly empty.*

Table 2 (cont.)

$\nu,\ \mu$	$E_{\nu,\mu}$	$A_{\nu,\mu}$	$B_{\nu,\mu}$
14, 2	$w^2 = v^3 - 6v + 5$	$4(v-2)^7(4v^4 - v^3 - 34v^2 + 51v - 18 + w(v^3 + 6v^2 - 18v + 8))$	$-(v-2)^8(v^3 - 12v + 14 + w(2v-6))^2$
21, 7	$w^2 = v^3 - 1715v + 33614$	*)	$14^7(w - 7v - 343)^{14} \times (21v^2 - 686v - 7203 - (v+49)w)^7$

*) $A_{\nu,\mu} = 3764768(w - 7v - 343)^7((-70v^{13} - 52822v^{12} + 19467098v^{11} + 3451790790v^{10} - 68568103744v^9 - 7533659832748v^8 + 155066962439572v^7 + 6992189738638860v^6 + 111845300294417242v^5 - 2615541950886590670v^4 - 18520719744403646964 6v^3 - 21674061456637587473 14v^2 - 17859482834686233287988v - 18838244084537504480336)w + v^{15} + 2625v^{14} + 91584v^{13} - 411648706v^{12} - 8059651761v^{11} + 1191725696763v^{10} + 27401291878562v^9 - 2107086579531888v^8 - 82212564592345537v^7 + 256086487817460003 9v^6 + 64436612556278953228v^5 - 6530447317005690352 82v^4 - 20619925798094466268271v^3 - 39964825892126689494688 3v^2 - 17492015250159665074110 86v - 96422978975763738021865 12).$

For $\langle \nu, \mu \rangle \in S_0 \cup S_1 \setminus \{\langle 9, 1\rangle\}$ *we can take*

$$F_{\nu,\mu}(K) = \begin{cases} \left\{ \left\langle 2 \cdot 7^{13},\ 7^{14}\left(\frac{7+\sqrt{21}}{2}\right)^7 \right\rangle, \right. \\ \qquad \left. \left\langle 2 \cdot 7^{13},\ 7^{14}\left(\frac{7-\sqrt{21}}{2}\right)^7 \right\rangle \right\} & \text{if } \langle \nu, \mu \rangle = \langle 21, 7\rangle,\ \sqrt{21} \in K, \\ \emptyset & \text{otherwise.} \end{cases}$$

Note that for any $p \in K[x] \setminus K$ there are only finitely many trinomials $x^n + ax^m + b \in K[x]$, $ab \neq 0$, divisible by p and satisfying neither (vi) nor (vii) (see [12]).

Note also that for $\langle \nu, \mu \rangle \in S_1 \setminus \{\langle 7, 2\rangle, \langle 21, 7\rangle\}$ the set $E_{\nu,\mu}(\mathbb{Q})$ is infinite, but $E_{7,2}(\mathbb{Q}) = \{\langle -4, 4\rangle, \langle -4, -4\rangle\}$, $E_{21,7}(\mathbb{Q}) = \{\langle -49, 0\rangle\}$. Since $B_{7,2}(-4, 4) = 0$ and $x^7 + A_{7,2}(-4, -4)x^2 + B_{7,2}(-4, -4)$ is divisible by $x + 2$ and $A_{21,7}(-49, 0) = B_{21,7}(-49, 0) = 0$, for $K = \mathbb{Q}$ the cases $\langle \nu, \mu \rangle = \langle 7, 2\rangle, \langle 21, 7\rangle$ can be disregarded.

The sets $F_{\nu,\mu}(K)$ are not uniquely determined. We propose the following conjecture.

Table 3

ν, μ	$B^*_{\nu,\mu}$
4, 1	$\dfrac{1-a^2t^6}{4t^4}$
4, 2	$\left(\dfrac{t^2+a}{2}\right)^2$
6, 2	$-\left(\dfrac{4t^4+a}{4t}\right)^2$
6, 3	$\left(\dfrac{t^3+a}{3t}\right)^2$
6, 4	$-\left(\dfrac{a^2t^4+8at^2+16}{16t^3}\right)^2$
6, 5	$a^6\dfrac{B_{6,1}(t)^5}{A_{6,1}(t)^6}$
7, 6	$a^7\dfrac{B_{7,1}(t)^6}{A_{7,1}(t)^7}$
8, 6	$((2\alpha-2\beta)t^2+(2\alpha-4\beta)t+(\alpha-\beta))^6$ $\times\dfrac{((2\alpha+2\beta)t^2-(2\alpha+4\beta)t+(\alpha+\beta))^2}{4(2t^2-1)^8}$, where $\alpha^2-2\beta^2=a$

CONJECTURE. *For every algebraic number field K one can choose sets $F_{\nu,\mu}(K)$ such that*

$$\Sigma=\bigcup_{\langle\nu,\mu\rangle}\ \bigcup_{\langle a,b\rangle\in F_{\nu,\mu}(K)}\{x^\nu+ax^\mu+b\}\quad \textit{is finite}\,.$$

Even in the case $K=\mathbb{Q}$ one cannot choose $F_{\nu,\mu}(K)$ so that Σ is empty, as Table 5 at the end of the paper shows.

The above conjecture has the following simple consequences.

CONSEQUENCE 1. *For every algebraic number field K there exists a constant $C_1(K)$ such that if $n_1>C_1(K)$ and $a,b\in K^*$ then x^n+ax^m+b is reducible over K if and only if* (i) *holds.*

CONSEQUENCE 2. *For every algebraic number field K there exists a constant $C_2(K)$ such that if $a,b\in K$ then x^n+ax^m+b has in $K[x]$ an irreducible factor with at most $C_2(K)$ non-zero coefficients.*

Table 4

ν, μ	Condition on b	$A^*_{\nu,\mu}$
$2p$, p	$b = b_1^p$	$-\left(\frac{t+\sqrt{t^2-4b_1}}{2}\right)^p - \left(\frac{t-\sqrt{t^2-4b_1}}{2}\right)^p$
6, 2	$b = -b_1^2$	$4t(t^3+b_1)$
8, 2	$b = b_1^2$	$\frac{-4t^8+12b_1t^4-b_1^2}{4t^2}$
8, 4	$b = b_1^4$	$4t^4-8b_1t^2+2b_1^2$
9, 3	$b = b_1^3$	$\frac{t^9-18b_1t^6+27b_1^2t^3+27b_1^3}{27t^3}$

Consequence 3. *There are only finitely many integers b such that for some $n \neq 2m$, $x^n + bx^m + 1$ is reducible over $\mathbb{Q}$.*

From this point to the end of the introduction reducibility is meant over $\mathbb{Q}$. It is clear from Table 5 that if $C_1(\mathbb{Q})$ exists we have $C_1(\mathbb{Q}) \geq 52$.

The problem of existence of $C_2(\mathbb{Q})$ was formulated in [21]. Bremner [1] has shown that if $C_2(\mathbb{Q})$ exists we have $C_2(\mathbb{Q}) \geq 8$ (see also [6]).

Using Theorem 5 of [22] one can determine an explicit value $c(a,b)$ such that if $a, b \in \mathbb{Q}^*$, $n_1 > c(a,b)$ and $x^n + ax^m + b$ is reducible then $x^{n_1} + ax^{m_1} + b$ has a *cyclotomic* linear or quadratic factor.

The problem of existence of integers b with $|b| > 2$ such that for some $n \neq 2m$ the trinomial $x^n + bx^m + 1$ is reducible was formulated in [23]. First Coray (unpublished) and then Bremner [2] have found an affirmative answer which is clear from Table 5, positions 28, 31, 48.

Here are some arithmetical applications of Theorems 4 and 5.

Theorem 7. *For all $a, b \in \mathbb{Z} \setminus \{0\}$ and all n there exist only finitely many reducible trinomials $ax^n + bx^m + c$ where $c \in \mathbb{Z} \setminus \{0\}$ without a factor $x^{(m,n)} - d$ apart from the following*

$$T_1(x^l;t) = ax^{4l} + bx^{2l} + a\left(\frac{at^2+b}{2a}\right)^2,$$

$$T_2(x^l;t) = ax^{5l} + bx^{4l} - \frac{b^5}{a^5} \cdot \frac{t^2(t-2)^4}{(t^2-3t+1)^5},$$

$$T_3(x^l;t) = ax^{8l} + bx^{6l} + \frac{b^8}{a^7} B^*_{8,6}(t),$$

where $t \in \mathbb{Q}$ and $\langle \alpha, \beta \rangle$ occurring in the definition of $B^*_{8,6}$ is a fixed rational solution of $\alpha^2 - 2\beta^2 = b/a$.

THEOREM 8. *For all $a, c \in \mathbb{Z} \setminus \{0\}$ and all n there exist only finitely many reducible trinomials $ax^n + bx^m + c$ where $2m \le n$, $b \in \mathbb{Z} \setminus \{0\}$ apart from the following*

$$T_4(x^l; t) = ax^{2pl} + aA^*_{2p,p}(t, b_1)x^{pl} + c, \qquad b_1^p = c/a\,,$$
$$T_5(x^l; t) = ax^{6l} + aA^*_{6,2}(t, b_1)x^{2l} + c, \qquad b_1^2 = -c/a\,,$$
$$T_6(x^l; t) = ax^{8l} + aA^*_{8,4}(t, b_1)x^{4l} + c, \qquad b_1^4 = c/a\,,$$

where $t, b_1 \in \mathbb{Q}$.

The exceptions given in Theorems 7 and 8 are genuine as follows from the identities

$$T_1(x; t) = a\left(x^2 + tx + \frac{at^2 + b}{2a}\right)\left(x^2 - tx + \frac{at^2 + b}{2a}\right),$$

$$T_2(x; t) = a\left(x^2 + \frac{b}{a} \cdot \frac{t(t-2)}{t^2 - 3t + 1} + \frac{b^2}{a^2} \cdot \frac{t(t-2)^2}{(t^2 - 3t + 1)^2}\right)$$
$$\times \left(x^3 + \frac{b}{a} \cdot \frac{-t+1}{t^2 - 3t + 1}x^2 + \frac{b^2}{a^2} \cdot \frac{t(t-2)}{(t^2 - 3t + 1)^2} + \frac{b^3}{a^3} \cdot \frac{-t(t-2)^2}{(t^2 - 3t + 1)^3}\right),$$

$$T_3(x; t)$$
$$= a\left(x^4 + a_1x^3 + (a_1^2 - b_1^2)x^2 + (a_1 + b_1)(a_1 - b_1)^2x + \frac{(a_1 + b_1)(a_1 - b_1)^3}{2}\right)$$
$$\times \left(x^4 - a_1x^3 + (a_1^2 - b_1^2)x^2 - (a_1 + b_1)(a_1 - b_1)^2x + \frac{(a_1 + b_1)(a_1 - b_1)^3}{2}\right),$$

where $a_1 = 2\alpha t^2 - 4\beta t + \alpha$, $b_1 = 2\beta t^2 - 2\alpha t + \beta$,

$$T_5(x^l; t) = a(x^3 + 2tx^2 + 2t^2x + b_1)(x^3 - 2tx^2 + 2t^2x - b_1)\,,$$
$$T_6(x^l; t) = a(x^4 + 2tx^3 + 2t^2x^2 + 2tb_1x + b_1^2)(x^4 + 2tx^3 + 2t^2x^2 - 2tb_1x + b_1^2)\,,$$

from the divisibility

$$x^2 - tx + b_1 \mid T_4(x; t)$$

and from the remark that $T_i(x; t) \in \mathbb{Z}[x]$ for infinitely many $t \in \mathbb{Q}$, at least if $2a \mid b$ $(1 \le i \le 3)$ and $a \mid c$ $(4 \le i \le 6)$. In particular, $T_2(x; t)$ furnishes a counterexample to an assertion of Fried [9] (statement 13), probably the same as mentioned in general terms by Fried himself in [10], p. 600.

Unfortunately, the finite sets of exceptional trinomials occurring in Theorems 7 and 8 cannot be effectively determined from the proofs of the theorems, since the latter use an ineffective theorem of Siegel [28]. In the special case $a = m = 1$ an effective determination has been achieved by Ribenboim [20]. In the case of Theorem 8 it is possible to achieve the same under a less stringent assumption $(m, n) = 1$. This follows from

THEOREM 9. *Let $a, b, c \in \mathbb{Z} \setminus \{0\}$, $(a, b, c) = 1$. If $ax^n + bx^m + c$ is reducible then at least one of the following four conditions is satisfied*:

(x) $|b| \le |a|^{m_1}|c|^{n_1-m_1}+1$;

(xi) $|b| < \dfrac{2m_1(n_1-m_1)}{\log 2m_1(n_1-m_1)}|a|^{m/n}|c|^{(n-m)/n}, \quad \min\{|a|,|c|\}=1$

and $\sqrt[p]{\max\{|a|,|c|\}} \in \mathbb{Z}$ *for some prime* $p \mid n_1$;

(xii) *for some* $q \mid (m,n)$, q *a prime or* $q=4$, $\sqrt[q]{|a|} \in \mathbb{Z}$, $\sqrt[q]{|c|} \in \mathbb{Z}$ *and if* $q=2$ *then* $(-1)^{n_1}ac>0$, *while if* $q=4$ *then* $ac>0$ *and* $n_1 \equiv 0 \bmod 2$;

(xiii) $4 \mid (m,n)$, $ac>0$, $n_1 \equiv 1 \bmod 2$ *and either* $\sqrt[4]{|a|} \in \mathbb{Z}$, $\sqrt[4]{4|c|} \in \mathbb{Z}$ *or* $\sqrt[4]{4|a|} \in \mathbb{Z}$, $\sqrt[4]{|c|} \in \mathbb{Z}$.

Theorem 9 can be regarded as a refinement of a theorem of Nagell [15], concerning trinomials $T(x;q,r)=x^n+qx^m+r$, $q,r \in \mathbb{Z}$. Nagell proves the following alternative as the necessary condition for reducibility of $T(x;q,r)$:

$$\text{either } |q| \le |r|^{n-1}+1 \text{ or } \sqrt[p]{|r|} \in \mathbb{Z} \text{ for some prime } p \mid n\,.$$

It is clear that (x) is stronger than the first term of the alternative and each of (xi), (xii), (xiii) is stronger than the second term. However, the proof of Theorem 9 is partly based on Nagell's idea.

Theorem 9 implies

Corollary 1. *For every positive integer* d *there exist only finitely many trinomials* $x^n+bx^m\pm1$, *where* $b\in\mathbb{Z}$, $|b|>2$, $n_1>d$, *with a factor of degree* d *and all of them can be found effectively. Indeed, they satisfy* $n \ll d\log d$, $b \ll d^2\log d$.

Corollary 1 gives a partial generalization of a result of Bremner [2], who determined all trinomials x^n+bx^m+1, $b \in \mathbb{Z}\setminus\{0\}$, with a cubic factor. Another generalization will be given below as Corollary 2 (to Theorem 10). The factorization found by Bremner

$$x^6+(4\mu^4-4\mu)x^2-1=(x^3+2\mu x^2+2\mu^2x+1)(x^3-2\mu x^2+2\mu^2x-1)$$

(a special case of the factorization given above for $T_5(x;t)$) shows that the condition $n_1>d$ cannot be omitted.

For the case of a,b or a,c fixed we have

Theorem 10. *There exist two effectively computable functions* $c_0(d)$ *and* $c_1(d)$ *with the following property. If* $a,b,c \in \mathbb{Z}\setminus\{0\}$, $(a,b,c)=1$,

$$a\xi^n+b\xi^m+c=0 \qquad \textit{and} \qquad [\mathbb{Q}(\xi):\mathbb{Q}] \le d$$

then either simultaneously

(xiv) $n < \max\left\{c_0(d),\, c_1(d)\log\dfrac{|ab|}{(a,b)}\right\}$,

(xv) $n < \max\left\{c_0(d),\, c_1(d)\log\dfrac{|bc|}{(b,c)}\right\}$,

(xvi) $n < \max\{c_0(d),\ 3c_1(d)\log|ac|\}$, *provided* $n \neq 2m$

or

(xvii) $\xi^{(n,m)} = q$, $(1 \pm i)q$, $(1 \pm \sqrt{-3})q$ *or* $(3 \pm \sqrt{-3})q$, $q \in \mathbb{Q}$.

COROLLARY 2. *For every positive integer d there exist only finitely many trinomials $x^n + bx^m + 1$, where $b \in \mathbb{Z}$, $|b| > 2$, $n \neq 2m$, with a proper factor of degree d.*

I conclude the introduction by expressing my thanks to Professor J. Browkin ([1]), Professor J.-L. Nicolas, Dr. A. Pokrzywa ([2]) and Dr. T. Regińska who performed computer calculations used in this or in the previous version of the paper. Professor Nicolas has moreover improved the original Lemma 12 and simplified the proof of Lemma 24. I thank him for the permission to include his proofs. I thank Professor K. Rubin for his contribution to the proof of Lemma 51. I also thank the organizers of the Austrian-Hungarian-Slovak Number-Theory-Colloquium Graz 1992 who let me present the above results there.

PART I

Reducibility over function fields

1. Auxiliary results from the theory of algebraic functions. Let $\overline{K}(t,x)$ be a finite separable extension of $\overline{K}(t)$ and let x be a zero of a polynomial $F(t,u)$ defined and irreducible over $\overline{K}$, of degree d with respect to u.

For every $\tau \in \overline{K}$ let

$$\mathbb{F}(\tau) = \bigcup_{e=1}^{\infty} \overline{K}(((t-\tau)^{1/e})) \quad \text{and} \quad \mathbb{F}(\infty) = \bigcup_{e=1}^{\infty} \overline{K}((t^{-1/e}))\,.$$

LEMMA 1. (a) *Assume that $F(t,u) = 0$ has exactly d distinct solutions in the field $\mathbb{F}(\tau)$, including e_1 solutions belonging to $\overline{K}(((t-\tau)^{1/e_1}))$ conjugate over $\overline{K}((t-\tau)), \dots, e_r$ solutions belonging to $\overline{K}(((t-\tau)^{1/e_r}))$ conjugate over $\overline{K}((t-\tau))$, where $e_i \not\equiv 0 \bmod \pi$, $e_1 + \dots + e_r = d$. Then the numerator of $t - \tau$ in $\overline{K}(t,x)$ has the factorization into prime divisors of the form $\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$.*

(b) *Assume that $F(t,u) = 0$ has exactly d distinct solutions in the field $\mathbb{F}(\infty)$, including f_1 solutions belonging to $\overline{K}((t^{-1/f_1}))$ conjugate over $\overline{K}((t^{-1})), \dots, f_s$ solutions belonging to $\overline{K}((t^{-1/f_s}))$ conjugate over $\overline{K}((t^{-1}))$. Then the denominator of t in $\overline{K}(t,x)$ has the factorization into prime divisors of the form $\mathfrak{q}_1^{f_1} \dots \mathfrak{q}_s^{f_s}$.*

([1]) He used the programme GP/PARI by C. Batut, D. Bernardi, H. Cohen and M. Olivier.

([2]) He used the programme MATHEMATICA, version 2.0, Wolfram Research, Inc., Champaign, Ill., 1991.

(c) *Under the assumptions of* (a) *and* (b) *the Galois group of the polynomial* F *over* $\overline{K}(t)$ *contains permutations of the type* $(e_1,\dots,e_r)$ *and* $(f_1,\dots,f_s)$, *respectively.*

P r o o f. (a) and (b) are proved in [8], Ch. III, §2 under the assumption that $\operatorname{char} K = 0$ formulated on p. 135. The proof, however, uses only the assumptions of (a) and (b). One can compare [5], Ch. IV, §6.

To prove (c) we take $e = \text{l.c.m.}_{1\le i\le r} e_i \not\equiv 0 \bmod \pi$ and consider the automorphism of the field $\overline{K}(((t-\tau)^{1/e}))$ given by

$$(t-\tau)^{1/e} \to \zeta_e (t-\tau)^{1/e}\,.$$

The zeros of F belonging to $\overline{K}(((t-\tau)^{1/e_i}))$ and conjugate over $\overline{K}((t-\tau))$ are cyclically permuted. This shows that the Galois group in question contains a permutation of the type $(e_1,\dots,e_r)$. For the type $(f_1,\dots,f_s)$ the proof is similar.

R e m a r k. The proof of (c) is modelled on the proof of a special case given by Turnwald [31].

Lemma 2. *Let* g *be the genus of* $\overline{K}(t,x)$.

(a) *If the assumptions of Lemma* 1(a) *and* (b) *are satisfied for all* $\tau \in \overline{K}$, *we have*

$$g = \frac{1}{2}\sum_{\tau\in\overline{K}}\sum_{i=1}^{r}(e_i-1) + \frac{1}{2}\sum_{j=1}^{s}(f_j-1) - d + 1\,.$$

(b) *If the field* $\overline{K}(t,x)$ *is rational,* $g = 0$.

(c) *If* L *is a field between* $\overline{K}(t)$ *and* $\overline{K}(t,x)$, *the genus of* L *does not exceed* g.

P r o o f. For (a) see [8], Ch. III, §2, formula (36) and §3, formula (8). For (b) see [5], Ch. II, §2, for (c) see [8], Ch. III, §3, formulae (9) and (10) or [5], Ch. VI, §2, Corollary 2.

2. Determination of the range of Tables 1 and 2 (Lemmas 3–27). In all this section except Lemmas 26 and 27 it is assumed that $(m,n) = 1$, $s(n-m) - rn = 1$, $s > 0$, $r \ge 0$.

Note that the condition $\pi \nmid nm(n-m)$ implies $\pi \ne 2$.

Lemma 3. *The algebraic function* $x(t)$ *defined by the equation*

$$T(x;t^r,t^s) := x^n + t^r x^m + t^s = 0$$

has just one branch point $t_1 \ne 0,\infty$ *with one two-cycle given by the Puiseux expansions*

$$x(t) = \xi_1 \pm (t-t_1)^{1/2} P_{11}(\pm(t-t_1)^{1/2})\,, \qquad \xi_1 \ne 0\,,$$

and the remaining expansions

$$x(t) = P_{1j}(t-t_1) \qquad (2 \le j \le n-1)\,.$$

Moreover, the branch point 0 *has one* m*-cycle given by the Puiseux expansions*

$$x(t) = \zeta_{2m}^{2i+1} t^{(s-r)/m} P_{01}(\zeta_{2m}^{(2i+1)n} t^{1/m}) \qquad (0 \le i < m)$$

and one $(n-m)$*-cycle given by the Puiseux expansions*

$$x(t) = \zeta_{2(n-m)}^{2i+1} t^{r/(n-m)} P_{02}(\zeta_{2(n-m)}^{-(2i+1)n} t^{1/(n-m)}) \qquad (0 \le i < n-m)\,,$$

and the branch point ∞ *has one* n*-cycle given by the Puiseux expansions*

$$x(t) = \zeta_{2n}^{2i+1} t^{s/n} P_{21}(\zeta_{2n}^{(2i+1)m} t^{-1/n}) \qquad (0 \le i < n)\,.$$

Here P_{ij} *are ordinary formal power series with* $P_{ij}(0) \ne 0$*.*

P r o o f. The standard argument gives

$$t_1 = \Big(-\frac{m}{n}\Big)^m \Big(-\frac{n-m}{n}\Big)^{n-m}, \qquad \xi_1 = \Big(-\frac{m}{n}\Big)^{s-r} \Big(-\frac{n-m}{n}\Big)^r,$$

$$P_{11}(0) = \Big(\frac{-2\xi_1^2}{nm(n-m)t_1}\Big)^{1/2}, \qquad \prod_{j=2}^{n-1} P_{1j}(0) = (-1)^n \frac{t_1^s}{\xi_1^2}\,,$$

$$P_{01}(0) = P_{02}(0) = P_{21}(0) = 1\,.$$

Lemma 4. *The Galois group of* $T(x; t^r, t^s)$ *over* $\overline{K}(t)$ *is the symmetric group* S_n*.*

P r o o f. By Lemmas 1(c) and 3 the Galois group in question contains the following permutations: a transposition, the product of an m-cycle and an $(n-m)$-cycle, and an n-cycle. By Theorem 14 of Chapter I of [30] the group is either S_n or imprimitive. We wish to eliminate the latter possibility.

Assume without loss of generality that $m \le n-m$. By a suitable numbering we can achieve that the product of the two cycles is $(1,\dots,m)(m+1,\dots,n)$. Further let $\mu, \nu_2, \dots, \nu_q$ be an imprimitivity system containing $\mu \le m$ with $\nu_i \le m$ for $i \le p$ exclusively. Since $(m,n) = 1$ the group also contains the cycle $(m+1, \dots, n)^m$. Then according to the definition of imprimitivity $(m+1,\dots,n)^m$ permutes the numbers $\nu_{p+1}, \dots, \nu_q$, therefore $\{\nu_{p+1}, \dots, \nu_q\} = \{m+1, \dots, n\}$ or $\emptyset$. In the first case, $q \ge n-m+p > n/2$ and since $q \mid n$, we have $q = n$. In the second case the imprimitivity system is contained in $\{1,\dots,m\}$ and since this holds for all $\mu \le m$, we have $q \mid m$. But $(m,n) = 1$ gives $q = 1$.

R e m a r k. In the course of the proof we have obtained a generalization of Theorem 20 of Chapter V of [30] corresponding to $m = 1$.

Definition 1. Let $T(x; t^r, t^s) = \prod_{i=1}^n (x - x_i(t))$. We set

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

where τ_j is the jth fundamental symmetric function.

R e m a r k. By Lemma 4 and since

$$T(x;t^{r+n-m},t^{s+n}) = t^n T\left(\frac{x}{t};t^r,t^s\right),$$

$L(k,m,n)$ and $L^*(k,m,n)$ are determined by k,m,n up to an isomorphism fixing $K(t)$ and $\overline{K}(t)$, respectively.

LEMMA 5. *In $L^*(k,m,n)$, the numerator of $t-t_1$ has $\binom{n-2}{k-1}$ prime divisors in the second power and none in the higher ones.*

P r o o f. By Lemma 1(a) the prime divisors of the numerator of $t-t_1$ are in one-to-one correspondence with the cycles of the Puiseux expansions of a generating element of $L^*(k,m,n)/\overline{K}(t)$ at $t=t_1$, provided the relevant condition is satisfied. For the generating element we take $y(t)=\sum_{j=1}^k a^j\tau_j(x_1,\dots,x_k)$, where $a\in\overline{K}$ 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 $\{i_1,\dots,i_k\}\subset\{1,\dots,n\}$ there is an automorphism of the field $\overline{K}(x_1(t),\dots,x_n(t))/\overline{K}(t)$ taking $x_1(t),\dots,x_k(t)$ into $x_{i_1}(t),\dots,x_{i_k}(t)$, respectively. Then at $t=t_1$ we obtain $\binom{n}{k}$ different expansions for y, including

$$\sum_{j=1}^k a^j((\xi_1+(t-t_1)^{1/2}P_{11}((t-t_1)^{1/2}))\tau_{j-1}(P_{1i_1}(t-t_1),\dots,P_{1i_{k-1}}(t-t_1)) + \tau_j(P_{1i_1}(t-t_1),\dots,P_{1i_{k-1}}(t-t_1))),$$

where $\{i_1,\dots,i_{k-1}\}$ is any subset of cardinality $k-1$ of $\{2,\dots,n-1\}$. Since the cofactor of $(t-t_1)^{1/2}P_{11}((t-t_1)^{1/2})$ equal to

$$\sum_{j=1}^k a^j\tau_{j-1}(P_{1i_1}(t-t_1),\dots,P_{1i_{k-1}}(t-t_1)) = a\prod_{j=1}^{k-1}(1+aP_{1i_j}(t-t_1))$$

is non-zero and $\pi\neq 2$, we have indeed $\binom{n-2}{k-1}$ prime divisors in the second power in the numerator of $t-t_1$. All other prime divisors appear in the first power at most.

LEMMA 6. *For every $d\,|\,n$ the number of subsets $\{i_1,\dots,i_k\}$ of $\{1,2,\dots,n\}$ of cardinality $k>0$ such that*

$$\{i_1+d,i_2+d,\dots,i_k+d\}\equiv\{i_1,i_2,\dots,i_k\} \bmod n$$

equals

$$\binom{d}{\frac{dk}{n}} \quad \text{if } n\mid dk$$

and 0 otherwise.

P r o o f. To every subset S in question we make correspond the set R of all positive integers $r\le d$ such that there exists an $s\in S$ with $s\equiv r \bmod d$. The condition $S+d\equiv S \bmod n$ implies that for every $r\in R$ we have $r+id\in S \bmod n$

for $i = 1, \dots, n/d$. Since for $r, r' \in R$, $r \neq r'$ we have $r + id \neq r' + i'd$ it follows that $\frac{n}{d} \mid k$, hence there are no subsets S in question if $n \nmid dk$. If $n \mid dk$ we may choose arbitrarily a subset R of $\{1, \dots, d\}$ of cardinality dk/n and obtain a set S satisfying $S + d \equiv S \bmod n$ on taking $S \equiv R + \{0, d, \dots, n-d\}$.

LEMMA 7. *For every $d \mid n$ the number $f(n,k,d)$ of subsets $\{i_1, \dots, i_k\}$ of $\{1, 2, \dots, n\}$ of cardinality k such that*

$$\{i_1 + \delta, i_2 + \delta, \dots, i_k + \delta\} \equiv \{i_1, i_2, \dots, i_k\} \bmod n$$

holds for $\delta = d$ but for no smaller δ, satisfies

$$f(n,k,d) = \begin{cases} \displaystyle\sum_{\delta \mid (d, dk/n)} \mu(\delta) \binom{d/\delta}{\frac{dk/\delta}{n}} & \text{if } n \mid dk, \\ 0 & \text{otherwise.} \end{cases}$$

P r o o f. By Lemma 6 we have

$$\sum_{\delta \mid d} f(n,k,\delta) = \begin{cases} \binom{d}{dk/n} & \text{if } n \mid dk, \\ 0 & \text{otherwise,} \end{cases}$$

and Lemma 7 follows by the Möbius inversion formula.

LEMMA 8. *The denominator of t in $L^*(k,m,n)$ has*

$$\frac{1}{n} \sum_{d \mid (n,k)} \varphi(d) \binom{n/d}{k/d}$$

distinct prime divisors.

P r o o f. The function $y(t)$ has the following Puiseux expansions at $t = \infty$:

$$Q(t; i_1, \dots, i_k) = \sum_{j=1}^{k} a^j \tau_j(\zeta_{2n}^{2i_1+1} t^{s/n} P_{21}(\zeta_{2n}^{(2i_1+1)m} t^{-1/n}), \dots, \zeta_{2n}^{2i_k+1} t^{s/n} P_{21}(\zeta_{2n}^{(2i_k+1)m} t^{-1/n})),$$

where $\{i_1, \dots, i_k\}$ runs through all subsets of $\{1, \dots, n\}$ of cardinality k. The conjugates of $t^{1/n}$ over $\overline{K}((t^{-1/d}))$, where $d \mid n$, are $\zeta_n^{de} t^{1/n}$, where $0 \leq e < n/d$. Therefore if P is an ordinary power series the conjugates of $P(t^{-1/n})$ over $\overline{K}((t^{-1/d}))$ are $P(\zeta_n^{-de} t^{-1/n})$, where $0 \leq e < n/d$. Therefore $Q(t; i_1, \dots, i_k) \in \overline{K}((t^{-1/d}))$ if and only if

$$Q(t; i_1, \dots, i_k) = Q(t; i_1 + ed, \dots, i_k + ed) \qquad (0 \leq e < n/d),$$

hence by the choice of a, if and only if

$$\{i_1 + d, \dots, i_k + d\} \equiv \{i_1, \dots, i_k\} \bmod n.$$

Thus

$$Q(t; i_1, \dots, i_k) \in \overline{K}((t^{-1/d})) \setminus \bigcup_{\substack{\delta \mid d \\ \delta < d}} \overline{K}((t^{-1/\delta}))$$

if and only if

$$\{i_1+\delta,\dots,i_k+\delta\}\equiv\{i_1,\dots,i_k\} \bmod n$$

for $\delta=d$, but for no smaller $\delta\,|\,d$. It follows by Lemma 7 that $y(t)$ has, at $t=\infty$, $f(n,k,d)$ expansions belonging to $\overline{K}((t^{-1/d}))\setminus\bigcup_{\delta|d,\,\delta<d}\overline{K}((t^{-1/\delta}))$. These expansions split into cycles of d conjugate expansions each, where $n\,|\,dk$, i.e. $d=e\frac{n}{(n,k)}, e\,|\,(n,k)$. Hence the number of distinct prime divisors of the denominator of t equals

$$\begin{aligned}(1)\qquad \frac{(n,k)}{n}\sum_{e|(n,k)}\frac{1}{e}f\Big(n,k,\frac{n}{(n,k)}e\Big)&=\frac{(n,k)}{n}\sum_{e|(n,k)}\frac{1}{e}\sum_{\delta|e}\mu(\delta)\binom{\frac{n}{(n,k)}\frac{e}{\delta}}{\frac{k}{(n,k)}\frac{e}{\delta}}\\&=\frac{1}{n}\sum_{\delta'|(n,k)}\binom{n/\delta'}{k/\delta'}\delta'\sum_{\delta|\delta'}\frac{\mu(\delta)}{\delta}\\&=\frac{1}{n}\sum_{\delta'|(n,k)}\varphi(\delta')\binom{n/\delta'}{k/\delta'},\end{aligned}$$

which proves the lemma.

Lemma 9. *The numerator of t in $L^*(k,m,n)$ has*

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

distinct prime divisors.

P r o o f. The function $y(t)$ has the following Puiseux expansions at $t=0$:

$$\begin{aligned}Q(t;l;i_1,\dots,i_k)=\sum_{j=1}^{k}a^j\tau_j(&\zeta_{2m}^{2i_1+1}t^{(s-r)/m}P_{01}(\zeta_{2m}^{(2i_1+1)n}t^{1/m}),\\&\dots,\zeta_{2m}^{2i_l+1}t^{(s-r)/m}P_{01}(\zeta_{2m}^{(2i_l+1)n}t^{1/m}),\ \zeta_{2(n-m)}^{2i_{l+1}+1}t^{r/(n-m)}P_{02}(\zeta_{2(n-m)}^{-(2i_{l+1}+1)n}t^{1/(n-m)}),\\&\dots,\zeta_{2(n-m)}^{2i_k+1}t^{r/(n-m)}P_{02}(\zeta_{2(n-m)}^{-(2i_k+1)n}t^{1/(n-m)})),\end{aligned}$$

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 $\{0,\dots,n-m-1\}$ of cardinality $k-l$.

If P is an ordinary power series, the conjugates of $P(t^{1/m})$ and $P(t^{1/(n-m)})$ over $\overline{K}((t^{1/dd_1}))$, where $d\,|\,m$, $d_1\,|\,n-m$, are $P(\zeta_m^{de}t^{1/m})$ $(0\le e<m/d)$ and $P(\zeta_{n-m}^{d_1e_1}t^{1/(n-m)})$ $(0\le e_1<(n-m)/d_1)$, respectively. Therefore,

$$Q(t;l;i_1,\dots,i_k)\in\overline{K}((t^{1/dd_1})),\qquad d\,|\,m,\ d_1\,|\,n-m\,,$$

if and only if

$$\begin{aligned}Q(t;l;i_1,\dots,i_k)=Q(t;l;i_1+ed,\dots,i_l+ed,i_{l+1}+e_1d_1,\dots,i_k+e_1d_1)\\(0\le e<m/d,\ 0\le e_1<(n-m)/d_1)\,,\end{aligned}$$

hence by the choice of a, if and only if

$$\{i_1,\dots,i_l\}+d\equiv\{i_1,\dots,i_l\} \bmod m\,,$$
$$\{i_{l+1},\dots,i_k\}+d_1\equiv\{i_{l+1},\dots,i_k\} \bmod (n-m)\,.$$

It follows from the definition of the function f in Lemma 7 that $y(t)$ has, at $t=0$, $\sum_{l=0}^{k} f(m,l,d)f(n-m,k-l,d_1)$ expansions belonging to

$$\overline{K}((t^{1/dd_1}))\setminus\bigcup_{\substack{\delta\mid dd_1\\ \delta<dd_1}}\overline{K}((t^{1/\delta}))\,,\qquad\text{where}\quad d\,|\,m,\ d_1\,|\,n-m\,.$$

These expansions split into cycles of dd_1 conjugate expansions each, where $m\,|\,dl$ and $n-m\,|\,d_1(k-l)$, i.e.

$$d=e\frac{m}{(m,l)},\qquad d_1=e_1\frac{n-m}{(n-m,k-l)}\,.$$

Hence the number of distinct prime divisors of the numerator of t is

$$\sum_{l=0}^{k}\frac{(m,l)}{m}\cdot\frac{(n-m,k-l)}{n-m}\Big(\sum_{e\mid(m,l)}\frac{1}{e}f\Big(m;l;\frac{m}{(m,l)}e\Big)\Big)\times\Big(\sum_{e_1\mid(n-m,k-l)}\frac{1}{e_1}f\Big(n-m;k-l;\frac{n-m}{(n-m,k-l)}e_1\Big)\Big)\,,$$

which by the formula (1) equals

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

Lemma 10. *The genus $g^*(k,m,n)$ of the field $L^*(k,m,n)$ equals*

$$\frac{1}{2}\binom{n-2}{k-1}-\frac{1}{2n}\sum_{d\mid(n,k)}\varphi(d)\binom{n/d}{k/d}$$
$$-\frac{1}{2m(n-m)}\sum_{l=0}^{k}\Big(\sum_{d\mid(m,l)}\varphi(d)\binom{m/d}{l/d}\Big)\Big(\sum_{d\mid(n-m,k-l)}\varphi(d)\binom{(n-m)/d}{(k-l)/d}\Big)+1\,.$$

Proof. By Lemma 3 the only ramification points of $y(t)$ may be t_1, 0 and ∞. The lemma follows now from Lemmas 2(a), 5, 8 and 9.

Lemma 11. *For all positive integers a, b, c with $a>b$ and $c\ge 2$ we have*

$$\binom{ac}{bc}\ge\frac{a}{4}\binom{a}{b}\binom{2c}{c}\,.$$

P r o o f. We assume without loss of generality that $a \ge 2b$. We have

$$\binom{ac}{bc}\binom{a}{b}^{-1} = c^{b-1}\frac{\prod_{i=a-b}^{a-1}\prod_{j=1}^{c-1}(ic+j)}{\prod_{i=0}^{b-1}\prod_{j=1}^{c-1}(ic+j)}, \qquad \binom{2c}{c} = 2\,\frac{\prod_{j=1}^{c-1}(c+j)}{(c-1)!}.$$

Hence

$$\binom{ac}{bc}\binom{a}{b}^{-1}\binom{2c}{c}^{-1} = \frac{1}{2}c^{b-1}\prod_{j=1}^{c-1}\frac{(a-b)c+j}{c+j}\cdot\frac{\prod_{i=a-b+1}^{a-1}\prod_{j=1}^{c-1}(ic+j)}{\prod_{i=1}^{b-1}\prod_{j=1}^{c-1}(ic+j)}$$

$$\ge \frac{1}{2}c^{b-1}\frac{(a-b)c+1}{c+1}.$$

If $b = 1$ the right hand side equals

$$\frac{(a-1)c+1}{2(c+1)} \ge \frac{2(a-1)+1}{6} \ge \frac{a}{4}.$$

If $b \ge 2$ the right hand side is greater than or equal to

$$c\frac{ac+2}{4(c+1)} > \frac{a}{4}\cdot\frac{c^2}{c+1} \ge \frac{a}{3}.$$

Lemma 12. *We have*

$$S = \sum_{c=2}^{\infty} c\varphi(c)\binom{2c}{c}^{-1} < 7/8.$$

P r o o f (following J.-L. Nicolas). We have

$$S = \sum_{c=2}^{6} c\varphi(c)\binom{2c}{c}^{-1} + \sum_{c=7}^{\infty} c\varphi(c)\binom{2c}{c}^{-1} = S_1 + S_2.$$

Now

$$S_1 = \frac{5821}{6930} < 0.84.$$

Since $\varphi(c) \le c-1$ and for $c \ge 7$,

$$\frac{c(c-1)\binom{2c}{c}^{-1}}{(c+1)c\binom{2c+2}{c+1}^{-1}} \ge \frac{45}{16},$$

we have

$$S_2 \le 7\cdot 6\cdot\binom{14}{7}^{-1}\cdot\frac{45}{29} < 0.02$$

and

$$S = S_1 + S_2 < 0.86 < 7/8.$$

LEMMA 13. *For all positive integers n and k we have*

$$\sum_{d|(n,k)} \varphi(d)\binom{n/d}{k/d} \le \left(1+\frac{3.5}{n}\right)\binom{n}{k}.$$

Proof. By Lemma 11 with $a=n/d$, $b=k/d$, $c=d$, for $d>1$ we have

$$\binom{n}{k} \ge \frac{n}{4d}\binom{n/d}{k/d}\binom{2d}{d},$$

hence

$$\begin{aligned}\binom{n}{k}^{-1}\sum_{d|(n,k)} \varphi(d)\binom{n/d}{k/d} &\le 1+\sum_{\substack{d|(n,k)\\ d>1}} \varphi(d)\frac{4}{d}\binom{2d}{d}^{-1}\\ &< 1+\frac{4}{n}\sum_{c\ge 2} c\varphi(c)\binom{2c}{c}^{-1} < 1+\frac{3.5}{n},\end{aligned}$$

by virtue of Lemma 12.

LEMMA 14. *For $n \ge 2k \ge 6$ we have*

$$g^*(k,m,n) \ge 1+\frac{1}{2n(n-1)}\binom{n}{k}p(k,m,n), \tag{2}$$

where

$$p(k,m,n) = k(n-k) - \frac{(n-1)(n+3.5)}{n} - \begin{cases} \dfrac{n(n+2.5)}{n-1} & \text{if } m=1,\ n-1,\\ \dfrac{n(n-1)(n+1.5)}{(n-2)^2} & \text{if } m=2,\ n-2,\\ \dfrac{(n+7)(m(n-m)+3.5)}{m(n-m)} & \text{if } 2<m<n-2.\end{cases}$$

Proof. By Lemma 10, $g^*(k,m,n) = g^*(k,n-m,n)$, thus it is enough to consider $m \le n/2$.

If $m=1$, by Lemmas 10 and 13 we have

$$\begin{aligned}g^*(k,1,n) \ge 1+\frac{1}{2}\binom{n-2}{k-1} - \frac{1}{2n}\left(1+\frac{3.5}{n}\right)\binom{n}{k}\\ -\frac{1}{2(n-1)}\sum_{l=0}^{1}\left(1+\frac{3.5}{n-1}\right)\binom{n-1}{k-l}\end{aligned}$$

and the right hand side equals the right hand side of (2).

If $m=2$, by Lemmas 10 and 13 we have

$$g^*(k,2,n) \ge 1+\frac{1}{2}\binom{n-2}{k-1} - \frac{1}{2n}\left(1+\frac{3.5}{n}\right)\binom{n}{k}$$

$$
\begin{aligned}
&- \frac{1}{4(n-2)} \sum_{l=0}^{2} \Bigg(\sum_{d \mid (2,l)} \binom{2/d}{l/d} \Bigg) \Big(1 + \frac{3.5}{n-2}\Big) \binom{n-2}{k-l} \\
&\geq 1 + \frac{1}{2}\binom{n-2}{k-1} - \frac{1}{2n}\Big(1 + \frac{3.5}{n}\Big)\binom{n}{k} \\
&\quad - \frac{1}{2(n-2)}\Big(1 + \frac{3.5}{n-2}\Big)\Big(\binom{n-2}{k} + \binom{n-2}{k-1} + \binom{n-2}{k-2}\Big) \\
&\geq 1 + \frac{1}{2}\binom{n-2}{k-1} - \frac{1}{2n}\Big(1 + \frac{3.5}{n}\Big)\binom{n}{k} - \frac{1}{2(n-2)}\Big(1 + \frac{3.5}{n-2}\Big)\binom{n}{k}
\end{aligned}
$$

and the right hand side equals the right hand side of (2).

If $m \geq 3$, by Lemmas 10 and 13 we have

$$
\begin{aligned}
g^*(k,m,n) &\geq 1 + \frac{1}{2}\binom{n-2}{k-1} - \frac{1}{2n}\Big(1 + \frac{3.5}{n}\Big)\binom{n}{k} - \frac{1}{2m(n-m)} \\
&\quad \times \Bigg\{ \Big(1 + \frac{3.5}{n-m}\Big)\binom{n-m}{k} \sum_{d \mid m} \varphi(d) \\
&\quad + \sum_{l=1}^{k-1} \Big(1 + \frac{3.5}{m}\Big)\binom{m}{l}\Big(1 + \frac{3.5}{n-m}\Big)\binom{n-m}{k-l} \\
&\quad + \Big(1 + \frac{3.5}{m}\Big)\binom{m}{k} \sum_{d \mid n-m} \varphi(d) \Bigg\} \\
&= 1 + \frac{1}{2}\binom{n-2}{k-1} - \frac{1}{2n}\Big(1 + \frac{3.5}{n}\Big)\binom{n}{k} - \frac{1}{2m(n-m)} \\
&\quad \times \Bigg\{ \Big(m - 1 - \frac{3.5}{m}\Big)\Big(1 + \frac{3.5}{n-m}\Big)\binom{n-m}{k} \\
&\quad + \Big(1 + \frac{3.5}{m}\Big)\Big(1 + \frac{3.5}{n-m}\Big) \sum_{l=0}^{k} \binom{m}{l}\binom{n-m}{k-l} \\
&\quad + \Big(n - m - 1 - \frac{3.5}{n-m}\Big)\Big(1 + \frac{3.5}{m}\Big)\binom{m}{k} \Bigg\}.
\end{aligned}
$$

Now we use the identity

$$
\sum_{l=0}^{k} \binom{m}{l}\binom{n-m}{k-l} = \binom{n}{k}
$$

and the inequalities

$$
\begin{aligned}
m - 1 - \frac{3.5}{m} > 0, \qquad \binom{n-m}{k} &\leq \frac{(n-m)(n-m-1)}{n(n-1)}\binom{n}{k}, \\
n - m - 1 - \frac{3.5}{n-m} > 0, \qquad \binom{m}{k} &\leq \frac{m(m-1)}{n(n-1)}\binom{n}{k}
\end{aligned}
$$

and we obtain

$$\begin{aligned} g^*(k,m,n) \ge 1 &+ \frac{1}{2}\binom{n-2}{k-1} - \frac{1}{2}\binom{n}{k}\Big\{\frac{1}{n}\Big(1+\frac{3.5}{n}\Big) \\ &+ \Big(m-1-\frac{3.5}{m}\Big)\Big(1+\frac{3.5}{n-m}\Big)\frac{(n-m)(n-m-1)}{n(n-1)} \\ &+ \Big(1+\frac{3.5}{m}\Big)\Big(1+\frac{3.5}{n-m}\Big) \\ &+ \Big(n-m-1-\frac{3.5}{n-m}\Big)\Big(1+\frac{3.5}{m}\Big)\frac{m(m-1)}{n(n-1)}\Big\}. \end{aligned}$$

The right hand side of this inequality coincides with the right hand side of (2).

LEMMA 15. *We have $g^*(k,m,n) \ge n/24$ for all integers n, m and k satisfying $n \ge 2m > 0$, $(n,m) = 1$ and $n \ge 2k \ge 6$ except for $k = 3$ and $\langle n,m\rangle = \langle 6,1\rangle$ or $\langle 7,1\rangle$. Moreover, $g^*(k,m,n) = 1$ if and only if either $k = 3$ and $\langle n,m\rangle = \langle 7,2\rangle$, $\langle 7,3\rangle$, $\langle 8,1\rangle$ or $\langle 9,1\rangle$, or $k = 4$ and $\langle n,m\rangle = \langle 8,1\rangle$.*

Proof. For $k=3$, $n \le 20$, for $k=4$, $n \le 13$, and for $k=5$, $n \le 12$ the lemma is proved by direct calculation of $g^*(k,m,n)$ from Lemma 10 kindly performed by J.-L. Nicolas. If $m = 1$ we have

$$p(k,1,n) = (k-2)n - k^2 - 6 - \frac{3.5}{n(n-1)} > (k-2)n - k^2 - 7\,.$$

We obtain $p(3,1,n) > 5$ for $n \ge 21$; $p(4,1,n) > 4$ for $n \ge 14$; $p(5,1,n) > 7$ for $n \ge 13$. For $k \ge 6$, $n \ge 2k$ we obtain $p(k,1,n) > k^2 - 4k - 7 \ge 5$.

If $m = 2$ we have

$$p(k,2,n) = (k-2)n - k^2 - 7 - \frac{9n^2 - 4n - 14}{n(n-2)^2}\,.$$

We obtain $p(3,2,n) > 4$ for $n \ge 21$; $p(4,2,n) > 4$ for $n \ge 14$; $p(5,2,n) > 4$ for $n \ge 13$; and $p(k,2,n) > k^2 - 4k - 9 \ge 3$ for $k \ge 6$, $n \ge 2k$.

If $m \ge 3$ we have

$$p(k,m,n) \ge (k-2)n - k^2 - \frac{32}{3} - \frac{49n+63}{6n(n-3)}\,.$$

This gives $p(3,m,n) > 0.8$ for $n \ge 21$; $p(4,m,n) > 0.5$ for $n \ge 14$; $p(5,m,n) > 2$ for $n \ge 13$; and $p(k,m,n) > k^2 - 4k - 11.7 \ge 0.3$ for $k \ge 6$, $n \ge 2k$.

The lemma follows now from (2).

LEMMA 16. *Let $T(x;t^r,t^s) = \prod_{i=1}^{n}(x - x_i(t))$. In the field $\overline{K}(t,x_1(t),x_2(t))$ we have the factorizations*

$$t \cong \frac{\prod_{i=1}^{m-1} \mathfrak{p}_i^m \prod_{j=1}^{n-m-1} \mathfrak{q}_j^{n-m} \mathfrak{r}^{m(n-m)} \mathfrak{s}^{m(n-m)}}{\prod_{k=1}^{n-1} \mathfrak{t}_k^n},$$

$$x_1(t) = \frac{\prod_{i=1}^{m-1} \mathfrak{p}_i^{s-r} \prod_{j=1}^{n-m-1} \mathfrak{q}_j^r \mathfrak{r}^{(s-r)(n-m)} \mathfrak{s}^{rm}}{\prod_{k=1}^{n-1} \mathfrak{t}_k^s},$$

$$x_2(t) = \frac{\prod_{i=1}^{m-1} \mathfrak{p}_i^{s-r} \prod_{j=1}^{n-m-1} \mathfrak{q}_j^r \mathfrak{r}^{rm} \mathfrak{s}^{(s-r)(n-m)}}{\prod_{k=1}^{n-1} \mathfrak{t}_k^s},$$

where $\mathfrak{p}_i$, $\mathfrak{q}_j$, $\mathfrak{r}$, $\mathfrak{s}$, $\mathfrak{t}_k$ $(1 \le i < m,\ 1 < j < n-m,\ 1 \le k < n)$ *are distinct prime divisors. For* t_1 *defined in Lemma* 3 *the numerator of* $t - t_1$ *has* $(n-2)(n-3)$ *prime factors in the first power only, the remaining factors are double.*

P r o o f. By Lemma 1(a), (b) 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 at $t = \infty$, respectively provided the relevant conditions are satisfied. 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 $i \le n$, $j \le n$, $i \ne j$ we have either $ax_i(t)+bx_j(t) \ne ax_1(t)+bx_2(t)$ or $\langle i, j\rangle = \langle 1, 2\rangle$. By Lemma 4 for each pair $\langle i, j\rangle$ with $i \le n$, $j \le n$, $i \ne j$ 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 $t = 0$ we obtain for $y(t)$ the expansions

$$a\zeta_{2m}^{2i+1} t^{(s-r)/m} P_{01}(\zeta_{2m}^{(2i+1)n} t^{1/m}) + b\zeta_{2m}^{2j+1} t^{(s-r)/m} P_{01}(\zeta_{2m}^{(2j+1)n} t^{1/m})$$
$$(0 \le i < m,\ 0 \le j < m,\ i \ne j),$$

$$a\zeta_{2m}^{2i+1} t^{(s-r)/m} P_{01}(\zeta_{2m}^{(2i+1)n} t^{1/m}) + b\zeta_{2(n-m)}^{2j+1} t^{r/(n-m)} P_{02}(\zeta_{2(n-m)}^{-(2j+1)n} t^{1/(n-m)})$$
$$(0 \le i < m,\ 0 \le j < n-m),$$

$$a\zeta_{2(n-m)}^{2i+1} t^{r/(n-m)} P_{02}(\zeta_{2(n-m)}^{-(2i+1)n} t^{1/(n-m)}) + b\zeta_{2m}^{2j+1} t^{(s-r)/m} P_{01}(\zeta_{2m}^{-(2j+1)n} t^{1/m})$$
$$(0 \le i < n-m,\ 0 \le j < m),$$

$$a\zeta_{2(n-m)}^{2i+1} t^{r/(n-m)} P_{02}(\zeta_{2(n-m)}^{-(2i+1)n} t^{1/(n-m)})$$
$$+ b\zeta_{2(n-m)}^{2j+1} t^{r/(n-m)} P_{02}(\zeta_{2(n-m)}^{-(2j+1)n} t^{1/(n-m)})$$
$$(0 \le i < n-m,\ 0 \le j < n-m,\ i \ne j).$$

The $m(m-1)$ expansions of the first set form $m-1$ m-cycles corresponding to the divisors $\mathfrak{p}_1, \dots, \mathfrak{p}_{m-1}$, which divide the numerators of $x_1(t)$, $x_2(t)$ in exactly the $(s-r)$th power. The $m(n-m)$ expansions of the second set form one $m(n-m)$-cycle corresponding to the divisor $\mathfrak{r}$ which divides $x_1(t)$ in the $(s-r)(n-m)$th power and $x_2(t)$ in the rmth power.

The $m(n-m)$ expansions of the third set form one $m(n-m)$-cycle corresponding to the divisor $\mathfrak{s}$ which divides $x_1(t)$ in the rmth power and $x_2(t)$ in the $(s-r)(n-m)$th power. The $(n-m)(n-m-1)$ expansions of the fourth set form $n-m-1$ $(n-m)$-cycles corresponding to divisors $\mathfrak{q}_1, \dots, \mathfrak{q}_{n-m-1}$ which divide the numerators of $x_1(t)$, $x_2(t)$ in exactly the rth power.

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

At $t = \infty$ we obtain for $y(t)$ the expansions

$$a\zeta_{2n}^{2i+1} t^{s/n} P_{21}(\zeta_{2n}^{(2i+1)m} t^{-1/n}) + b\zeta_{2n}^{2j+1} t^{s/n} P_{21}(\zeta_{2n}^{(2j+1)m} t^{-1/n}) \\ (0 \le i < n,\ 0 \le j < n, i \ne j)\,,$$

which form $n-1$ n-cycles corresponding to the divisors $\mathfrak{t}_1, \dots, \mathfrak{t}_{n-1}$ dividing the denominator of $x_1(t)$ and of $x_2(t)$ in exactly the sth power.

Since $x_1(t) = \infty$ implies $t = \infty$ we have found all factors of the denominator of $x_1(t)$ and similarly of $x_2(t)$.

At $t = t_1$ we obtain for $y(t)$ among others the expansions

$$aP_{1i}(t-t_1) + bP_{1j}(t-t_1) \qquad (2 \le i < n,\ 2 \le j < n,\ i \ne j)\,,$$

which form $(n-2)(n-3)$ 1-cycles corresponding to $(n-2)(n-3)$ simple factors of the numerator of $t - t_1$. All the remaining expansions contain $(t-t_1)^{1/2}$.

LEMMA 17. *For all primes p,*

$$\sqrt[p]{t} \notin \overline{K}\,(t, x_1(t), \dots, x_n(t)) = \Omega\,.$$

Proof. The argument used in the proof of Lemma 16 applied to the field Ω gives that the multiplicity of every prime divisor of the numerator and the denominator of t divides $m(n-m)$ and n, respectively. Since $(m,n) = 1$ we cannot have $t = \gamma^p, \gamma \in \Omega$.

LEMMA 18. *For every positive integer q prime to s, $q \not\equiv 0 \bmod \pi$, and every choice of q-th roots we have*

$$[\overline{K}(t, \sqrt[q]{x_1(t)}, \dots, \sqrt[q]{x_n(t)}) : \overline{K}(t, x_1(t), \dots, x_n(t))] = q^n\,.$$

Proof. By Theorem 1 of [25] it is enough to prove that for every prime $p \mid q$,

$$\prod_{j=1}^{n} x_j^{\alpha_j} = \gamma^p, \qquad \gamma \in \Omega = \overline{K}(t, x_1(t), \dots, x_n(t)) \tag{3}$$

implies $\alpha_j \equiv 0 \bmod p$ for all $j \le n$. Assume that (3) holds, but say $\alpha_1 \not\equiv 0 \bmod p$.

If for all j we have $\alpha_j \equiv \alpha_1 \bmod p$ it follows from (3) that

$$\Big(\prod_{j=1}^{n} x_j\Big)^{\alpha_1} = \gamma'^p\,, \qquad \gamma' \in \Omega\,,$$

and since $\prod_{j=1}^{n} x_j = (-1)^n t^s$ where $s\alpha_1 \not\equiv 0 \bmod p$ we obtain $\sqrt[p]{t} \in \Omega$, contrary to Lemma 17. Therefore, there exists an $i \le n$ such that $\alpha_i \not\equiv \alpha_1 \bmod p$. If $i \ne 2$, by Lemma 4 there exist automorphisms σ and τ of $\Omega/\overline{K}(t)$ such that $\sigma(x_2) = x_i$, $\sigma(x_i) = x_2$ and $\tau(x_1) = x_2$, $\tau(x_2) = x_i, \tau(x_i) = x_1$. Applying σ and τ to (3) we obtain

$$x_1^{\alpha_1} x_2^{\alpha_i} x_i^{\alpha_2} \prod_{j\ne 1,2,i}^{n} x_j^{\alpha_j} = (\gamma^\sigma)^p\,,$$

$$x_1^{\alpha_i} x_2^{\alpha_1} x_i^{\alpha_2} \prod_{j\ne 1,2,i}^{n} x_j^{\alpha_j} = (\gamma^\tau)^p\,,$$

hence on division

$$\left(\frac{x_1}{x_2}\right)^{\alpha_1-\alpha_i} = \left(\frac{\gamma^\sigma}{\gamma^\tau}\right)^p = \gamma'^p\,, \qquad \gamma' \in \Omega^*\,.$$

If $i = 2$ the same relation follows more simply on taking $\tau(x_1) = x_2, \tau(x_2) = x_1$. Since $\alpha_1 - \alpha_i \not\equiv 0 \bmod p$ we have $1 = a(\alpha_1 - \alpha_i) + bp, a, b \in \mathbb{Z}$, hence

$$\left(\frac{x_1}{x_2}\right) = \left(\gamma'^a \left(\frac{x_1}{x_2}\right)^b\right)^p = \delta^p\,, \qquad \delta \in \Omega^*\,. \tag{4}$$

The extension $\overline{K}(x_1, x_2, \delta)/\overline{K}(x_1, x_2)$ is a normal subextension of $\Omega/\overline{K}(x_1, x_2)$ and since the latter has the symmetric Galois group, we have either $\delta \in \overline{K}(x_1, x_2)$ or

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

Since the conjugates of δ with respect to $\overline{K}(x_1, x_2)$ are $\zeta_p^j \delta$, we have either $\delta \in \overline{K}(x_1, x_2)$ or $p = 2$ and $\delta = \varepsilon \prod_{\mu,\nu=3,\nu>\mu}^{n}(x_\nu - x_\mu)$, $\varepsilon \in \overline{K}(x_1, x_2)$.

In the former case we compare the divisors on both sides of (4) and obtain by Lemma 16

$$\delta^p \cong \frac{\mathfrak{r}}{\mathfrak{s}}\,,$$

a contradiction.

In the latter case we have

$$\delta = \varepsilon \prod_{\substack{\mu,\nu=1\\ \nu>\mu}}^{n} (x_\nu - x_\mu) \cdot \frac{x_1 - x_2}{\prod_{\nu>1}(x_\nu - x_1) \cdot \prod_{\nu\ne 2}(x_\nu - x_2)} = \eta \prod_{\substack{\mu,\nu=1\\ \nu>\mu}}^{n} (x_\nu - x_\mu)\,,$$

$$\eta \in \overline{K}(x_1, x_2)\,,$$

hence by (4),

$$\frac{x_1}{x_2} = \eta^2 \mathrm{disc}_x T(x; t^r, t^s) = \mathrm{const}\, \eta^2 t^{s(n-1)-1}(t - t_1)\,.$$

By Lemma 16 $t - t_1$ has at least one simple factor for $n > 3$, which occurs with a non-zero exponent on the right hand side, but not on the left, a contradiction. For $n = 3$ the divisor of the right hand side is a square, while that of the left hand side is not, a contradiction again.

LEMMA 19. *Let $n > 2$, $q \not\equiv 0 \bmod \pi$, $q \geq 2$, and $y_{iq}^q = x_i(t)$ $(1 \leq i \leq n)$. Then*

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

P r o o f. Suppose first that $(q, s) = 1$. By Lemmas 4 and 18 all isomorphic injections of the extension $\overline{K}(t, y_{1q}, \ldots, y_{nq})/\overline{K}(t)$ into $\overline{K(t)}/\overline{K}(t)$ are given by

$$y_{iq} \to \zeta_q^{\alpha_i} y_{\sigma(i)q} \qquad (1 \leq i \leq n) \tag{5}$$

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

$$[\alpha_1, \ldots, \alpha_n] \in (\mathbb{Z}/q\mathbb{Z})^n\,. \tag{6}$$

We shall show that there are exactly q^{n-1} distinct images of $(\sum_{i=1}^n y_{iq})^q$ under transformations (5). Indeed, if we apply (5) with $\sigma(i) = i$ to $(\sum_{i=1}^n y_{iq})^q$ we obtain

$$\Big(\sum_{i=1}^{n} \zeta_q^{\alpha_i} y_{iq}\Big)^q\,.$$

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

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

contrary to Lemma 18. Thus the number of distinct images is at least equal to the number of vectors satisfying (6) with $\alpha_1 = 0$, thus to q^{n-1}. On the other hand, $\sum_{i=1}^n y_{iq}$ is invariant under transformations (5) with $\alpha_1 = \alpha_2 = \ldots = \alpha_n$, which form a group, hence the number in question does not exceed q^{n-1}.

Suppose now that $(q, s) \neq 1$. Taking an integer solution $\sigma = s_1$, $\varrho = r_1$ of the equation $\sigma(n - m) - \varrho n = 1$ that satisfies $(q, s_1) = 1$ we have

$$T(x; t^r, t^s) = t^{s - s_1} T\Big(\frac{x}{t^{(s-s_1)/n}}; t^{r_1}, t^{s_1}\Big)\,,$$

hence if $T(x; t^{r_1}, t^{s_1}) = \prod_{i=1}^n (x - \overline{x}_i(t))$ one can renumber the $\overline{x}_i(t)$ so that

$$(t^{(s_1-s)/nq} y_{iq})^q = \overline{x}_i(t)\,.$$

Therefore, by the already proved case of the lemma

$$\Big[\overline{K}\Big(t, \Big(\sum_{i=1}^{n} t^{(s_1-s)/nq} y_{iq}\Big)^q\Big) : \overline{K}(t)\Big] = q^{n-1}$$

and the lemma follows in full generality.

Definition 2. Let $q \not\equiv 0 \bmod \pi$ and $y_{iq}^q = x_i(t)$, where $x_i(t)$ are defined in Lemma 16. We set

$$M(m,n,q) = K\Big(t, \Big(\sum_{i=1}^{n} y_{iq}\Big)^q\Big), \qquad M_*(m,n,q) = \overline{K}\Big(t, \Big(\sum_{i=1}^{n} y_{iq}\Big)^q\Big).$$

Remark. By Lemma 19 and the final argument in its proof $M(m,n,q)$ and $M_*(m,n,q)$ are determined by m, n, q up to an isomorphism which fixes $K(t)$ and $\overline{K}(t)$, respectively.

Lemma 20. *For $n > 2$ and $(q,2) = 1$ or $(q,s) = 1$ the numerator of $t - t_1$ has in $M_*(m,n,q)$ $(q^{n-1} - q^{n-2})/2$ factors in the second power.*

Proof. Let us fix

$$\overline{y}_{1q} = (\xi_1 + (t-t_1)^{1/2} P_{11}((t-t_1)^{1/2}))^{1/q},$$
$$\overline{y}_{2q} = (\xi_1 - (t-t_1)^{1/2} P_{11}(-(t-t_1)^{1/2}))^{1/q},$$

so that

$$\overline{y}_{1q} + \overline{y}_{2q} \in \overline{K}((t-t_1)), \tag{7}$$

$$(\overline{y}_{1q} - \overline{y}_{2q})(t-t_1)^{1/2} \in \overline{K}((t-t_1)) \tag{8}$$

and

$$\overline{y}_{jq} = (P_{i,j-1}(t-t_1))^{1/q} \in \overline{K}((t-t_1)) \qquad (2 < j \le n) \tag{9}$$

in an arbitrary way. Using Lemma 3 we obtain for $(\sum_{i=1}^n y_{iq})^q$ the following Puiseux expansions at $t = t_1$:

$$\Big(\overline{y}_{1q} + \zeta_q^{i_2}\overline{y}_{2q} + \sum_{j=3}^{n} \zeta_q^{i_j}\overline{y}_{jq}\Big)^q, \qquad [i_2, \dots, i_n] \in (\mathbb{Z}/q\mathbb{Z})^{n-1}.$$

If such an expansion belongs to $\overline{K}((t-t_1))$ then either

$$\overline{y}_{1q} + \zeta_q^{i_2}\overline{y}_{2q} + \sum_{j=3}^{n} \zeta_q^{i_j}\overline{y}_{jq} \in \overline{K}((t-t_1))$$

or

$$2 \,|\, q \quad \text{and} \quad \Big(\overline{y}_{1q} + \zeta_q^{i_2}\overline{y}_{2q} + \sum_{j=3}^{n} \zeta_q^{i_j}\overline{y}_{jq}\Big)(t-t_1)^{-1/2} \in \overline{K}((t-t_1)).$$

In the first case, by (7) and (9),

$$(1 - \zeta_q^{i_2})\overline{y}_{1q} \in \overline{K}((t-t_1))$$

and since $P_{11}(0) \neq 0$, $i_2 = 0$.

In the second case, by (8),

$$\Big(\frac{1 + \zeta_q^{i_2}}{2}(\overline{y}_{1q} + \overline{y}_{2q}) + \sum_{j=3}^{n} \zeta_q^{i_j}\overline{y}_{jq}\Big)(t-t_1)^{-1/2} \in \overline{K}((t-t_1))$$

and since

$$\frac{1+\zeta_q^{i_2}}{2}(\overline{y}_{1q}+\overline{y}_{2q})+\sum_{j=3}^{n}\zeta_q^{i_j}\overline{y}_{jq}\in\overline{K}((t-t_1))$$

by (7) and (9), we obtain

$$\frac{1+\zeta_q^{i_2}}{2}(\overline{y}_{1q}+\overline{y}_{2q})+\sum_{j=3}^{n}\zeta_q^{i_j}\overline{y}_{jq}=0\,,$$

which contradicts Lemma 18 unless $(s,q)>1$.

Therefore if $(q,2)=1$ or $(q,s)=1$ we obtain $q^{n-1}-q^{n-2}$ expansions for $(\sum_{i=1}^{n}y_{iq})^q$ belonging to $\overline{K}(((t-t_1)^{1/2}))\setminus\overline{K}((t-t_1))$, which correspond to $(q^{n-1}-q^{n-2})/2$ distinct prime divisors of the numerator of $t-t_1$ in $M_*(m,n,q)$.

Lemma 21. *For every positive integer l the number of vectors $[i_1,\dots,i_l]\in(\mathbb{Z}/q\mathbb{Z})^l$ such that*

$$\sum_{j=1}^{l}\zeta_q^{i_j}\zeta_{ql}^{j-1}=0 \tag{10}$$

does not exceed $q^{l-\varphi(lq)/\varphi(q)}$.

P r o o f. We have

$$[\mathbb{Q}(\zeta_{ql}):\mathbb{Q}(\zeta_q)]=\frac{\varphi(lq)}{\varphi(q)}=\varrho\,,$$

hence ζ_{lq} has ϱ conjugates over $\mathbb{Q}(\zeta_q)$. Let them be $\zeta_{lq}^{r_k}$ $(k\le\varrho)$. It follows from (10) that

$$\sum_{j=1}^{l}\zeta_q^{i_j}\zeta_{ql}^{(j-1)r_k}=0$$

and since

$$\det\left(\zeta_{ql}^{(j-1)r_k}\right)_{j,k\le\varrho}=\prod_{\substack{\mu,\nu=1\\ \nu>\mu}}^{\varrho}(\zeta_{ql}^{r_\nu}-\zeta_{ql}^{r_\mu})\neq 0$$

$\zeta_q^{i_j}$ $(j\le\varrho)$ are determined by $\zeta_q^{i_j}$ $(\varrho<j\le l)$, which gives the lemma.

Lemma 22. *The denominator of t in $M_*(m,n,q)$ has at most*

$$q^{n-1}\left(\frac{1}{n}+\frac{n-1}{nq^{\varphi(nq)/\varphi(q)}}\right)$$

distinct prime divisors.

P r o o f. By Lemma 1(b) the prime divisors of the denominator of t correspond to the cycles of the Puiseux expansions of $(\sum_{i=1}^{n}y_{iq})^q$ at $t=\infty$, provided the relevant condition is satisfied. By Lemma 3 we obtain for $(\sum_{i=1}^{n}y_{iq})^q$ the following

expansions at $t=\infty$:

$$\Big(\sum_{j=1}^{n}\zeta_q^{i_j}\zeta_{2qn}^{2j-1}t^{s/qn}P_{21}(\zeta_n^{(2j-1)m}t^{-1/n})^{1/q}\Big)^q \tag{11}$$

where $[i_1,\dots,i_n]\in(\mathbb{Z}/q\mathbb{Z})^n$, $i_1=0$. Note that $qn\not\equiv 0 \bmod \pi$.

Let S be the set of vectors $[i_2,\dots,i_n]\in(\mathbb{Z}/q\mathbb{Z})^{n-1}$ such that

$$1+\sum_{j=2}^{n}\zeta_q^{i_j}\zeta_{qn}^{j-1}=0\,.$$

By Lemma 21 with $l=n$,

$$\operatorname{card} S\le q^{n-\varphi(qn)/\varphi(q)-1}\,. \tag{12}$$

If $[i_2,\dots,i_n]\notin S$ the coefficient of $t^{s/n}$ in the expansion (11) equals

$$\zeta_{2n}\Big(1+\sum_{j=2}^{n}\zeta_q^{i_j}\zeta_{qn}^{j-1}\Big)^q P_{21}(0)\ne 0\,,$$

hence we obtain an n-cycle. The number of cycles thus obtained is $\frac{1}{n}(q^{n-1}-\operatorname{card} S)$. The number of the remaining cycles does not exceed $\operatorname{card} S$. Therefore the total number of cycles does not exceed

$$\frac{1}{n}(q^{n-1}-\operatorname{card} S)+\operatorname{card} S=\frac{q^{n-1}}{n}+\Big(1-\frac{1}{n}\Big)\operatorname{card} S\le\frac{q^{n-1}}{n}\Big(\frac{1}{n}+\frac{n-1}{q^{\varphi(qn)/\varphi(q)}}\Big)$$

by (12).

Lemma 23. *The numerator of t in $M_*(m,n,q)$ has at most*

$$\frac{q^{n-2}}{m(n-m)}\Big(1+\frac{m-1}{q^{\varphi(mq)/\varphi(q)}}\Big)\Big(1+\frac{n-m-1}{q^{\varphi((n-m)q)/\varphi(q)}}\Big)$$

distinct prime divisors.

Proof. By Lemma 1(a) the prime divisors of the numerator of t correspond to the cycles of the Puiseux expansions of $(\sum_{i=1}^{n}y_{iq})^q$ at $t=0$, provided the relevant condition is satisfied. By Lemma 3 we obtain the expansions

$$\begin{aligned}\Big(\sum_{j=1}^{m}\zeta_q^{i_j}\zeta_{2mq}^{2j-1}t^{(s-r)/qm}P_{01}(\zeta_{2m}^{(2j-1)n}t^{1/m})^{1/q}\\ +\sum_{j=m+1}^{n}\zeta_q^{i_j}\zeta_{2(n-m)q}^{2j-1}t^{r/q(n-m)}P_{02}(\zeta_{2(n-m)}^{-(2j-1)n}t^{1/n-m})^{1/q}\Big)^q,\end{aligned} \tag{13}$$

where $[i_1,\dots,i_n]\in(\mathbb{Z}/q\mathbb{Z})^n$, $i_1=0$. Note that $qm(n-m)\not\equiv 0 \bmod \pi$.

Let S be the set of vectors $[i_2,\dots,i_m]\in(\mathbb{Z}/q\mathbb{Z})^{m-1}$ such that

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

and T the set of vectors $[i_{m+1}, \dots, i_n] \in (\mathbb{Z}/q\mathbb{Z})^{n-m}$ such that

$$\sum_{j=m+1}^{n} \zeta_q^{i_j} \zeta_{q(n-m)}^{j-1} = 0\,.$$

By Lemma 21,

$$\operatorname{card} S \le q^{m-\varphi(qm)/\varphi(q)-1}\,, \qquad \operatorname{card} T \le q^{n-m-\varphi(q(n-m))/\varphi(q)}\,.$$

If $[i_2, \dots, i_m] \notin S$ and $[i_{m+1}, \dots, i_n] \notin T$ the least two powers of t occurring with non-zero coefficients in the (outer) parentheses in (13) are

$$t^{(s-r)/qm} \quad \text{and} \quad t^{r/q(n-m)}\,.$$

Hence the expansion (13) contains with non-zero coefficients

$$t^{(s-r)/qm+(q-s)r/q(n-m)} \quad \text{and} \quad t^{(q-1)(s-r)/qm+r/q(n-m)}\,.$$

The least common denominator of the two exponents is $qm(n-m)$, hence we obtain

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

$qm(n-m)$-cycles.

If $[i_2, \dots, i_m] \notin S$ and $[i_{m+1}, \dots, i_n] \in T$ the least powers of t occurring with non-zero coefficients in the parentheses of (13) are

$$t^{(s-r)/qm}, \quad t^{(s-r)/qm+\mu/m} \quad \text{and} \quad t^{r/q(n-m)+\nu/(n-m)}$$

for some positive integers $\mu \in M$ (M may be empty) and a positive integer ν satisfying

$$\frac{s-r}{qm} + \frac{\mu}{m} < \frac{r}{q(n-m)} + \frac{\nu}{n-m} \qquad (\mu \in M)\,.$$

Hence the expansion (13) contains with non-zero coefficients

$$t^{(s-r)/m} \quad \text{and} \quad t^{(q-1)(s-r)/qm+r/q(n-m)+\nu/(n-m)}\,.$$

The least common denominator of the two exponents is divisible by

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

hence we obtain at most

$$\frac{(q^m - \operatorname{card} S)\operatorname{card} T}{qm}$$

qm-cycles.

If $[i_2, \dots, i_m] \in S$ and $[i_{m+1}, \dots, i_n] \notin T$ the least powers of t occurring with non-zero coefficients in the parentheses of (13) are

$$t^{(s-r)/qm+\mu/m}\,, \quad t^{r/q(n-m)} \quad \text{and} \quad t^{r/q(n-m)+\nu/(n-m)}$$

for a positive integer μ and some positive integers $\nu \in N$ (N may be empty), satisfying

$$\frac{r}{q(n-m)} + \frac{\nu}{n-m} < \frac{s-r}{qm} + \frac{\mu}{m} \qquad (\nu \in N)\,.$$

Hence the expansion (13) contains with non-zero coefficients

$$t^{r/(n-m)} \qquad \text{and} \qquad t^{(q-1)r/q(n-m)+(s-r)/qm}\,.$$

The least common denominator of the two exponents is divisible by

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

hence we obtain at most

$$\frac{\operatorname{card} S(q^{n-m} - \operatorname{card} T)}{q(n-m)}$$

$q(n-m)$-cycles.

Finally, if $[i_2,\dots,i_m] \in S$ and $[i_{m+1},\dots,i_n] \in T$ the least powers of t occurring in the parentheses in (13) with non-zero coefficients are either

$$t^{(s-r)/qm+\mu/m} \qquad (\mu \in M)\,, \qquad t^{r/q(n-m)+\nu/(n-m)}$$

or

$$t^{(s-r)/qm+\mu/m}\,, \qquad t^{r/q(n-m)+\nu/(n-m)} \qquad (\nu \in N)\,,$$

where the sets M and N are non-empty and

$$\frac{s-r}{qm} + \frac{\mu}{m} < \frac{r}{q(n-m)} + \frac{\nu}{n-m} \qquad (\mu \in M)$$

or

$$\frac{r}{q(n-m)} + \frac{\nu}{n-m} < \frac{s-r}{qm} + \frac{\mu}{m} \qquad (\nu \in N)\,,$$

respectively. In view of symmetry it suffices to consider the first case. Then the expansion (13) contains with a non-zero coefficient

$$t^{(q-1)(s-r)/qm+(q-1)\mu/m+\nu/q(n-m)+\nu/m}\,.$$

Since the exponent in its reduced form has q in the denominator we obtain at most

$$\frac{\operatorname{card} S \operatorname{card} T}{q}$$

q-cycles. Therefore the total number of distinct cycles does not exceed

$$\frac{(q^{m-1} - \operatorname{card} S)(q^{n-m} - \operatorname{card} T)}{qm(n-m)} + \frac{(q^{m-1} - \operatorname{card} S)\operatorname{card} T}{qm} + \frac{\operatorname{card} S(q^{n-m} - \operatorname{card} T)}{q(n-m)} + \frac{\operatorname{card} S \cdot \operatorname{card} T}{q}$$

$$= \frac{q^{n-1}}{qm(n-m)} + \operatorname{card} S\left(\frac{q^{n-m}}{q(n-m)} - \frac{q^{n-m}}{qm(n-m)}\right) + \operatorname{card} T\left(\frac{q^{m-1}}{qm} - \frac{q^{m-1}}{qm(n-m)}\right)$$

$$+\operatorname{card} S \operatorname{card} T\left(\frac{1}{qm(n-m)}-\frac{1}{qm}-\frac{1}{q(n-m)}+\frac{1}{q}\right).$$

Since the coefficients are non-negative we can apply Lemma 21 and obtain the desired estimate for the number of distinct cycles.

LEMMA 24. *For all positive integers l and q with $q \geq 2$ we have*

$$q^{\varphi(ql)/\varphi(q)} \geq q(l-1).$$

Proof (following J.-L. Nicolas). We observe first that

$$\varphi(l) \geq \frac{l \log 2}{\log 2l}.$$

Indeed, if l has k distinct prime factors $p_1, \dots, p_k$ we have $l \geq 2^k$, and so $k \leq \log l / \log 2$. Hence

$$\frac{\varphi(l)}{l} = \prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right) \geq \prod_{i=1}^{k}\left(1-\frac{1}{i+1}\right) = \frac{1}{k+1} \geq \frac{\log 2}{\log 2l}.$$

Suppose now that

$$q^{\varphi(ql)/\varphi(q)} < q(l-1).$$

Since $\varphi(ql) \geq \varphi(q)\varphi(l)$ we obtain

$$2^{\varphi(l)-1} \leq q^{\varphi(l)-1} < l-1$$

and thus

$$\frac{l \log 2}{\log 2l} \leq \varphi(l) < \frac{\log(l-1)}{\log 2} + 1 < \frac{\log 2l}{\log 2}.$$

However, for all $x > 0$, $\log x = 4 \log \sqrt[4]{x} \leq (4/e)\sqrt[4]{x}$. Hence

$$l < \left(\frac{\log 2l}{\log 2}\right)^2 \leq \left(\frac{4}{e \log 2}\right)^2 \sqrt{2l},$$

and thus

$$l < 2\left(\frac{4}{e \log 2}\right)^4 < 41.$$

Since $l > 2$, $\varphi(l) > 1$ and

$$q < (l-1)^{1/(\varphi(l)-1)}$$

we find that either $l \in \{4, 6, 10, 12\}$, $q = 2$ or $l = 6$, $q \in \{3, 4\}$. In each of the six cases we have

$$q^{\varphi(ql)/\varphi(q)} \geq q(l-1),$$

which proves the lemma.

LEMMA 25. *For all positive integers m, n and q where $n > 2m$, $(m, n) = 1$, $qnm(n-m) \not\equiv 0 \bmod \pi$ and $q \geq 2$ the genus $g_*(m, n, q)$ of $M_*(m, n, q)$ is greater*

than $nq/24$ *unless*

$$\langle q,n,m\rangle \in \{\langle 2,3,1\rangle,\ \langle 2,4,1\rangle,\ \langle 2,5,1\rangle,\ \langle 2,5,2\rangle,\ \langle 2,6,1\rangle,\ \langle 3,3,1\rangle,\ \langle 3,4,1\rangle,\ \langle 4,3,1\rangle,\ \langle 5,3,1\rangle\}\,, \tag{14}$$

and is greater than 1 *unless* (14) *holds or*

$$\langle q,n,m\rangle \in \{\langle 2,7,1\rangle,\ \langle 6,3,1\rangle,\ \langle 7,3,1\rangle\}\,. \tag{15}$$

If (14) *or* (15) *holds and* $\langle q,n,m\rangle \neq \langle 6,3,1\rangle$ *we have* $g_*(m,n,q) = 0$ *or* 1, *respectively.*

P r o o f. By Lemma 2(a) and by Lemmas 21–23 together with Remark after Definition 2 we have

$$g_*(m,n,q) \geq 1 + \frac{q^{n-2}}{2}\left(\frac{q-1}{2} - \frac{q}{n}\left(1 + \frac{n-1}{q^{\varphi(qn)/\varphi(q)}}\right) - \frac{1}{m(n-m)}\left(1 + \frac{m-1}{q^{\varphi(qm)/\varphi(q)}}\right)\left(1 + \frac{n-m-1}{q^{\varphi(q(n-m))/\varphi(q)}}\right)\right). \tag{16}$$

Hence by Lemma 24,

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

where

$$\gamma(q,n,m) = \begin{cases} \dfrac{q-1}{2} - \dfrac{q+1}{n} - \dfrac{1}{n-1}\left(1+\dfrac{1}{q}\right) & \text{if } m = 1,\\[2ex] \dfrac{q-1}{2} - \dfrac{q+1}{n} - \dfrac{1}{m(n-m)}\left(1+\dfrac{1}{q}\right)^2 & \text{otherwise.}\end{cases}$$

It is easy to check using (16) that the lemma holds if

$$\langle q,n,m\rangle \in \{\langle 2,7,2\rangle,\ \langle 2,7,3\rangle,\ \langle 2,8,1\rangle,\ \langle 2,8,3\rangle,\ \langle 2,9,1\rangle,\ \langle 3,5,1\rangle,\ \langle 3,5,2\rangle,\ \langle 4,4,1\rangle,\ \langle 5,4,1\rangle,\ \langle 8,3,1\rangle\}\,. \tag{17}$$

If $\langle q,n,m\rangle$ satisfies neither (14) nor (15) nor (17) we have one of the following cases:

$q = 2$, $m = 1$, $n \geq 10$, $\gamma(q,n,m) \geq 1/30$,

$$g_*(m,n,q) \geq 1 + \frac{2^{n-2}}{60} > \frac{n}{12}\,;$$

$q = 2$, $m \geq 2$, $n \geq 9$, $\gamma(q,n,m) \geq 1/168$,

$$g_*(m,n,q) \geq 1 + \frac{2^{n-2}}{336} > \frac{n}{12}\,;$$

$q = 3$, $m = 1$, $n \geq 6$, $\gamma(q,n,m) \geq 1/15$,

$$g_*(m,n,q) \geq 1 + \frac{2^{n-2}}{30} > \frac{n}{8}\,;$$

$q = 3$, $m \geq 2$, $n \geq 7$, $\gamma(q,n,m) \geq 1/4$,

$$g_*(m,n,q) \geq 1 + \frac{2^{n-2}}{8} > \frac{n}{8}\,;$$

$q \in \{4,5\}$, $n \geq 5$, $\gamma(q,n,m) \geq 1/5$,

$$g_*(m,n,q) \geq 1 + \frac{2^{n-2}}{10} > \frac{5n}{24}\,;$$

$q \in \{6,7,8\}$, $n \geq 4$, $\gamma(q,n,m) \geq 1/3$,

$$g_*(m,n,q) \geq 1 + \frac{2^{n-2}}{6} > \frac{n}{3}\,;$$

$q \geq 9$, $n \geq 3$, $\gamma(q,n,m) = (q^2-8q-3)/6q$,

$$g_*(m,n,q) \geq 1 + \frac{q^{n-3}}{12}(q^2-8q-3) > \frac{qn}{24}\,.$$

The last assertion of the lemma is proved by a direct use of Lemma 2(a).

LEMMA 26. *Let $n \geq 2m$ and $A, B \in K(\mathbf{y})^*$, $A^{-n}B^{n-m} \notin K$. Then $x^n + Ax^m + B$ is reducible over $K(\mathbf{y})$ if and only if one of the following cases holds*:

(18) *$x^{n_1} + Ax^{m_1} + B$ has a proper linear or quadratic factor over $K(\mathbf{y})$.*

(19) *There exists an integer l such that*

$$\left\langle \frac{n}{l}, \frac{m}{l} \right\rangle := \langle \nu, \mu \rangle \in S_0 := \bigcup_{p \text{ prime}} \{\langle 2p, p\rangle\} \cup \{\langle 6,1\rangle, \langle 6,2\rangle, \langle 7,1\rangle\,,$$

$$\langle 8,2\rangle, \langle 8,4\rangle, \langle 9,3\rangle, \langle 10,2\rangle, \langle 10,4\rangle, \langle 12,2\rangle, \langle 12,3\rangle, \langle 12,4\rangle, \langle 15,5\rangle\}$$

and $x^\nu + Ax^\mu + B$ is reducible over $K(\mathbf{y})$.

Proof. The sufficiency is obvious. We proceed to prove the necessity.

If $x^n + Ax^m + B$ is reducible over $K(\mathbf{y})$ then by Capelli's lemma (see e.g. [18], p. 662 or [26], p. 89) either

(20) $$x^{n_1} + Ax^{m_1} + B \text{ is reducible over } K(\mathbf{y})$$

or

(21) $x^{(m,n)} - \xi$ is reducible over $K(\mathbf{y}, \xi)$, where ξ is a zero of $x^{n_1} + Ax^{m_1} + B$.

In the former case either (18) holds or $x^{n_1} + Ax^{m_1} + B$ has a factor of degree k, where $n \geq 2k \geq 6$. In this case let us choose non-negative integers r and s such that

$$s(n_1 - m_1) - rn_1 = 1\,.$$

We have

(22) $$A^{-n_1 s}B^{n_1 r}(x^{n_1} + Ax^{m_1} + B)$$
$$= (A^{-s}B^r x)^{n_1} + (A^{-n_1}B^{n_1-m_1})^r (A^{-s}B^r x)^{m_1} + (A^{-n_1}B^{n_1-m_1})^s\,,$$

hence $x^{n_1} + (A^{-n_1}B^{n_1-m_1})^r x^{m_1} + (A^{-n_1}B^{n_1-m_1})^s$ also has a factor of degree k over $K(\mathbf{y})$.

Therefore the field $L^*(k, m_1, n_1)$ defined in Definition 1 is a rational function field and by Lemma 2(b), $g^*(k, m_1, n_1) = 0$. It follows by Lemma 15 that $k = 3$ and $\langle n_1, m_1\rangle = \langle 6, 1\rangle$ or $\langle 7, 1\rangle$, hence (19) holds with $l = (m, n)$ and $\langle \nu, \mu\rangle = \langle 6, 1\rangle$ or $\langle 7, 1\rangle$.

Assume now that we have (21), but not (20). It follows by Capelli's theorem that either

$$\xi = \eta^p\,, \qquad \text{where } p \text{ is a prime, } p \,|\, (m, n),\ \eta \in K(\mathbf{y}, \xi)\,, \tag{23}$$

or

$$\xi = -4\eta^4, \qquad \text{where } 4 \,|\, n,\ \eta \in K(\mathbf{y}, \xi). \tag{24}$$

If (23) or (24) holds then $x^{pn_1} + Ax^{pm_1} + B$ or $x^{4n_1} + Ax^{4m_1} + B$, respectively, is reducible over $K(\mathbf{y})$. Let

$$x^{n_1} + t^r x^{m_1} + t^s = \prod_{i=1}^{n_1}(x - x_i)\,, \qquad y_{iq}^q = x_i\,.$$

It follows from (22) that if $t = A^{-n_1}B^{n_1-m_1}$ one can take

$$\begin{aligned} &q = p\,, \quad && y_{iq} = (A^{-s}B^r)^{1/p}\eta_i && \text{if (23) holds,}\\ &q = 4, && y_{iq} = (A^{-s}B^r)^{1/4}(1 + \zeta_4)\eta_i && \text{if (24) holds,} \end{aligned}$$

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

$$M_*(m_1, n_1, q) = \overline{K}(t, (y_{1q} + \ldots + y_{n_1q})^q)$$

is parameterized as follows:

$$t = A^{-n_1}B^{n_1-m_1}\,,$$

$$(y_{1q} + \ldots + y_{n_1q})^q = \begin{cases} A^{-s}B^r(\eta_1 + \ldots + \eta_{n_1})^p & \text{if (23) holds,}\\ -4A^{-s}B^r(\eta_1 + \ldots + \eta_4)^4 & \text{if (24) holds.} \end{cases}$$

It follows by Lemma 2(b) that $g_*(m_1, n_1, q) = 0$ and by Lemma 25 either $\langle n_1, m_1\rangle = \langle 2, 1\rangle$ or

$$\langle q, n_1, m_1\rangle \in \{\langle 2,3,1\rangle, \langle 2,4,1\rangle, \langle 2,5,1\rangle, \langle 2,5,2\rangle, \langle 2,6,1\rangle, \langle 3,3,1\rangle, \langle 3,4,1\rangle, \langle 4,3,1\rangle, \langle 5,3,1\rangle\}\,.$$

In the former case (19) holds, with $\langle \nu, \mu\rangle = \langle 2p, p\rangle$, $l = (m, n)/p$ or $\langle \nu, \mu\rangle = \langle 8, 4\rangle$, $l = (m, n)/4$. In the latter case (19) holds with $\langle \nu, \mu\rangle = \langle n_1 q, m_1 q\rangle$, $l = (m, n)/q$.

LEMMA 27. *Let $n > 2m$, L be a finite extension of $K(y_1)$ with $\overline{K}L$ of genus $g > 0$, and A, $B \in L^*$, $A^{-n}B^{n-m} \notin \overline{K}$. The trinomial $x^n + Ax^m + B$ is reducible over L if and only if either*

$$x^{n_1} + Ax^{m_1} + B \text{ has a proper linear or quadratic factor over } L \tag{25}$$

or there exists an integer l such that

$$\left\langle \frac{n}{l}, \frac{m}{l} \right\rangle := \langle \nu, \mu\rangle \in \mathbb{Z}^2, \quad \nu < 24g \text{ and } x^\nu + Ax^\mu + B \text{ is reducible over } L. \tag{26}$$

If $g = 1$ the latter condition can be made more precise as follows: there exists an integer l such that

$$\left\langle \frac{n}{l}, \frac{m}{l} \right\rangle := \langle \nu, \mu \rangle \in S_0 \cup S_1, \tag{27}$$

$x^\nu + Ax^\mu + B$ is reducible over L and for $\langle \nu, \mu \rangle = \langle 9, 1 \rangle$ it has a cubic factor over L.

P r o o f. The sufficiency of the condition is obvious. The proof of the necessity is similar to that of Lemma 26.

If $x^n + Ax^m + B$ is reducible over L then either

$$x^{n_1} + Ax^{m_1} + B \text{ is reducible over } L \tag{28}$$

or

$$x^{(m,n)} - \xi \text{ is reducible over } L(\xi), \text{ where } \xi \text{ is a zero of } x^{n_1} + Ax^{m_1} + B. \tag{29}$$

In the former case either (25) holds or $x^{n_1} + Ax^{m_1} + B$ has a factor of degree k, where $n \geq 2k \geq 6$. In this case we infer from (22) that $x^{n_1} + (A^{-n_1} B^{n_1 - m_1})^r x^{m_1} + (A^{-n_1} B^{n_1 - m_1})^s$ has a factor of degree k over L. Therefore the field $L^*(k, m_1, n_1)$ defined in Definition 1 is isomorphic to a subfield of $\overline{K}L$ and by Lemma 2(c), $g^*(k, m_1, n_1) \leq g$.

It follows by Lemma 15 that $n_1 < 24g$ and if $g = 1$ then $\langle n_1, m_1 \rangle \in S_0 \cup S_1$ with the proviso that for $\langle n_1, m_1 \rangle = \langle 9, 1 \rangle$ we have $k = 3$, hence (26) and (27) hold with $l = (m, n)$ and $\langle \nu, \mu \rangle = \langle 6, 1 \rangle$, $\langle 7, 1 \rangle$, $\langle 8, 1 \rangle$ or $\langle 9, 1 \rangle$.

Assume now that we have (29), but not (28).

Then in the same way as in the proof of Lemma 26 we infer that for a suitable $q \,|\, (m, n)$, $q = 4$ or a prime, $x^{n_1 q} + Ax^{m_1 q} + B$ is reducible over L and the field $M_*(m, n, q)$ is isomorphic to a subfield of $\overline{K}L$. Hence by Lemma 2(c) we have $g_*(m, n, q) \leq g$. Since $\langle n_1, m_1 \rangle \neq \langle 2, 1 \rangle$ it follows by Lemma 25 that either $\langle q, n_1, m_1 \rangle \in \{\langle 2, 3, 1 \rangle, \langle 2, 4, 1 \rangle, \langle 2, 5, 1 \rangle, \langle 2, 6, 1 \rangle, \langle 3, 3, 1 \rangle, \langle 3, 4, 1 \rangle, \langle 4, 3, 1 \rangle, \langle 5, 3, 1 \rangle\}$ or $n_1 q < 24g$. Moreover, if $g = 1$ the last inequality can be replaced by $\langle q, n_1, m_1 \rangle \in \{\langle 2, 7, 1 \rangle, \langle 6, 3, 1 \rangle, \langle 7, 3, 1 \rangle\}$ and the case $\langle q, n_1, m_1 \rangle = \langle 6, 3, 1 \rangle$ is impossible because of the restriction on q. Thus (26) and (27) follow with $l = (m, n)/q$, $\langle \nu, \mu \rangle = \langle n_1 q, m_1 q \rangle$.

3. Determination of the content of Table 1 (Lemmas 28–40)

Lemma 28. *Let K be any field of characteristic different from 2, and $A, B \in K^*$. The trinomial $x^{2m} + Ax^m + B$ is reducible over K if and only if either $\sqrt{A^2 - 4B} \in K$ or for some prime $p \,|\, m$,*

$$A = u^p A_{2p,p}(v), \qquad B = u^{2p} B_{2p,p}(v), \qquad u, v \in K, \tag{30}$$

or $4 \,|\, m$ and

$$A = u^4 A_{8,4}(v), \qquad B = u^8 B_{8,4}(v), \qquad u, v \in K. \tag{31}$$

P r o o f. The condition is necessary. Indeed, if x^2+Ax+B is reducible over K then $\sqrt{A^2-4B} \in K$. If x^2+Ax+B is irreducible over K, but $x^{2m}+Ax^m+B$ is reducible it follows by Capelli's lemma that $x^m-(-A+\sqrt{A^2-4B})/2$ is reducible over $K(\sqrt{A^2-4B})$, hence by Capelli's theorem either there is a prime $p \mid m$ such that

$$\frac{-A+\sqrt{A^2-4B}}{2} = \vartheta^p\,, \qquad \vartheta \in K(\sqrt{A^2-4B})\,, \tag{32}$$

or $4 \mid m$ and

$$\frac{-A+\sqrt{A^2-4B}}{2} = -4\vartheta^4\,, \qquad \vartheta \in K(\sqrt{A^2-4B}). \tag{33}$$

Since ϑ is of degree 2 over K it can be written in the form

$$\vartheta = \frac{A_1+\sqrt{A_1^2-4B_1}}{2}\,, \qquad A_1, B_1 \in K\,. \tag{34}$$

Substituting (34) into (32) and taking traces and norms of both sides we obtain (30) with $u = A_1$, $v = B_1/A_1^2$. Substituting (34) into (33) and taking traces and norms of both sides we obtain (31) with $u = A_1$, $v = 2B_1/A_1^2$.

The condition is sufficient. If $\sqrt{A^2-4B} \in K$ this is obvious. If (30) holds $x^{2m}+Ax^m+B$ is divisible by $x^{2m/p}-ux^{m/p}+u^2v$, while if (31) holds it is equal to

$$(x^m+2ux^{3m/4}+2u^2x^{m/2}+2u^3vx^{m/4}+u^4v^2) \times(x^m-2ux^{3m/4}+2u^2x^{m/2}-2u^3vx^{m/4}+u^4v^2)\,.$$

Lemma 29. *Let K be any field, $f \in K[x]$, f irreducible over K, and n a positive integer. Then $f(x^n)$ is reducible over K if and only if either for a prime $p \mid n$,*

$$f(x^p) = c\prod_{j=0}^{p-1} g(\zeta_p^j x)\,,$$

or $4 \mid n$, $\operatorname{char} K \neq 2$, and

$$f(-4x^4) = c\prod_{j=0}^{3} g(\zeta_4^j x)\,,$$

where $g \in K[x]$ is monic and $\zeta_p = 1$ if $p = \operatorname{char} K$.

P r o o f. The condition is necessary. Indeed, let $f(\eta) = 0$. By Capelli's lemma $x^p-\eta$ is reducible over $K(\eta)$. By Capelli's theorem we have $\eta = \vartheta^p$, $\vartheta \in K(\eta)$ or $\operatorname{char} K \neq 2$, $\eta = -4\vartheta^4$, $\vartheta \in K(\eta)$. Let $\vartheta_1, \dots, \vartheta_n$ be all the conjugates of ϑ with respect to K. We take

$$g(x) = \prod_{i=1}^{n}(x-\vartheta_i) \in K[x]$$

and find in the first case

$$f(x^p) = a\prod_{i=1}^{n}(x^p - \vartheta_i^p) = a\prod_{i=1}^{n}\prod_{j=0}^{p-1}(x - \zeta_p^{-j}\vartheta_i)$$
$$= a(-1)^{(p-1)n}\prod_{j=0}^{p-1}\prod_{i=0}^{n}(\zeta_p^j x - \vartheta_i) = c\prod_{j=0}^{p-1} g(\zeta_p^j x)\,,$$

in the second case

$$f(-4x^4) = a\prod_{i=1}^{n}(-4x^4 + 4\vartheta_i^4) = a(-4)^n\prod_{i=1}^{n}\prod_{j=0}^{3}(x - \zeta_4^{-j}\vartheta_i)$$
$$= a\cdot 4^n\prod_{j=0}^{3}\prod_{i=0}^{n}(\zeta_4^j x - \vartheta_i) = c\prod_{j=0}^{3} g(\zeta_4^j x)\,.$$

The condition is sufficient, since in the first case it gives $g(x^n)$ as a proper factor of $f(x^n)$ in $K[x]$.

In the second case we have

$$f(x^4) = c\prod_{j=0}^{3} g(\tfrac{1}{2}\zeta_4^j(1-\zeta_4)x)\,.$$

If $\zeta_4 \notin K$ then $\zeta_4^j(1-\zeta_4)$ for $j = 0$ and 1 are conjugate to each other over K, hence

$$h(x) = \prod_{j=0}^{1} g(\tfrac{1}{2}\zeta_4^j(1-\zeta_4)x) \in K[x]\,,$$

and $h(x^{n/4})$ is a proper factor of $f(x^n)$ in $K[x]$.

Remark. For $n = 2$ the lemma was proved by Selmer [27].

Lemma 30. *Let K be a field of characteristic different from 2, and $A, B \in K^*$. The trinomial $x^6 + Ax + B$ has a cubic factor in $K[x]$ if and only if*

$$A = u^5 A_{6,1}(v)\,, \qquad B = u^6 B_{6,1}(v)\,, \tag{35}$$

where $u, v \in K$.

Proof. The condition (35) is sufficient, since it implies

$$x^6 + Ax + B = (x^3 + 2ux^2 + 2u^2(1+v)x + u^3(-v^2+4v+1))$$
$$\times (x^3 - 2ux^2 + 2u^2(1-v)x + u^3(v^2+4v-1)).$$

On the other hand, if

$$x^6 + Ax + B = (x^3 + a_1x^2 + b_1x + c_1)(x^3 + a_2x^2 + b_2x + c_2)$$

we have

$$a_2 + a_1 = 0\,,$$

$$b_2 + a_1a_2 + b_1 = 0\,, \qquad c_2 + a_1b_2 + b_1a_2 + c_1 = 0\,,$$
$$a_1c_2 + b_1b_2 + c_1a_2 = 0\,, \qquad b_1c_2 + c_1b_2 = A\,, \qquad c_1c_2 = B\,.$$

If $a_1 = 0$ we obtain $a_2 = 0$, $b_1 + b_2 = b_1b_2 = 0$, hence $b_1 = b_2 = 0$ and $A = 0$, contrary to $A \in K^*$. If $a_1 \neq 0$, we take $a_1 = 2u$, $b_1 = 2u^2(1 + v)$ and find $a_2 = -2u$, $b_2 = 2u^2(1 - v)$, $c_1 = u^3(-v^2 + 4v + 1)$, $c_2 = u^3(v^2 + 4v - 1)$, which gives (35).

LEMMA 31. *Let K be a field of characteristic different from 2, and $A, B \in K^*$. The trinomial $x^6 + Ax^2 + B$ is reducible over K if and only if either $x^3 + Ax + B$ is reducible over K or*

$$A = u^4A_{6,2}(v)\,, \qquad B = u^6B_{6,2}(v)\,, \tag{36}$$

where $u, v \in K$.

Proof. The condition (36) is sufficient, since it implies

$$x^6 + Ax^2 + B = (x^3 + 2ux^2 + 2u^2x - u^3v)(x^3 - 2ux^2 + 2u^2x + u^3v)\,.$$

On the other hand, if $x^6 + Ax^2 + B$ is reducible and $x^3 + Ax + B$ is irreducible over K we have, by Lemma 29,

$$x^6 + Ax^2 + B = (x^3 + ax^2 + bx + c)(x^3 - ax^2 + bx - c)\,,$$

hence

$$2b - a^2 = 0\,, \qquad b^2 - 2ac = A\,, \qquad -c^2 = B\,.$$

If $a = 0$ we obtain $b = 0$, hence $A = 0$, contrary to $A \in K^*$. If $a \neq 0$ we take $a = 2u$, $c = -u^3v$ and obtain (36).

LEMMA 32. *Let K be a field of characteristic different from 2, and $A, B \in K^*$. The trinomial $x^7 + Ax + B$ has a cubic factor in $K[x]$ if and only if*

$$A = u^6A_{7,1}(v)\,, \qquad B = u^7B_{7,1}(v)\,, \tag{37}$$

where $u, v \in K$.

Proof. The condition (37) is sufficient, since it implies

$$\begin{aligned} x^7 + Ax + B &= (x^4 + u(2v + 1)x^3 + u^2(2v + 1)^2vx^2 + u^3(2v + 1)^2(v^2 + 2v - 1)x \\ &\quad + u^4(2v - 1)(2v + 1)^3(v^2 - v - 1)) \\ &\quad \times (x^3 - u(2v + 1)x^2 + u^2(1 - v)(2v + 1)^2x + u^3v(2v + 1)^2(3v - 2))\,. \end{aligned}$$

On the other hand, if

$$x^7 + Ax + B = (x^4 + a_1x^3 + b_1x^2 + c_1x + d_1)(x^3 + a_2x^2 + b_2x + c_2)$$

we have

$$a_2 + a_1 = 0\,, \qquad b_2 + a_1a_2 + b_1 = 0\,, \qquad c_2 + a_1b_2 + b_1a_2 + c_1 = 0\,,$$
$$a_1c_2 + b_1b_2 + c_1a_2 + d_1 = 0\,, \qquad b_1c_2 + c_1b_2 + d_1a_2 = 0\,,$$

$$c_1c_2 + d_1b_2 = A\,, \qquad d_1c_2 = B\,.$$

If $a_1 = 0$ we obtain $b_2 = -b_1$, $c_2 = -c_1$, $d_1 = b_1^2$, $2b_1c_1 = 0$, hence $B = 0$, contrary to $B \in K^*$. If $a_1 \neq 0$ and $b_1 = -\frac{1}{2}a_1^2$ we obtain $b_2 = \frac{3}{2}a_1^2$, $c_2 + c_1 = -2a_1^3$, $a_1^2(c_2 + c_1) = \frac{3}{2}a_1^5$, a contradiction. If $a_1 \neq 0$ and $b_1 \neq -\frac{1}{2}a_1^2$ we take $v = b_1/a_1^2$, $u = a_1/(2v + 1)$ and obtain (37) by a simple elimination.

LEMMA 33. *Let K be a field of characteristic different from 2, and $A, B \in K^*$. The trinomial $x^8 + Ax^2 + B$ is reducible over K if and only if either $x^4 + Ax + B$ is reducible over K or*

$$A = u^6A_{8,2}(v)\,, \qquad B = u^8B_{8,2}(v)\,, \tag{38}$$

where $u, v \in K$.

Proof. The condition (38) is sufficient, since it implies

$$\begin{aligned} x^8 + Ax^2 + B = {} & (x^4 + 2ux^3 + 2u^2x^2 + u^3vx + u^4(2v - 2)) \\ & \times (x^4 - 2ux^3 + 2u^2x^2 - u^3vx + u^4(2v - 2))\,. \end{aligned}$$

On the other hand, if $x^8 + Ax^2 + B$ is reducible and $x^4 + Ax + B$ irreducible over K we have, by Lemma 29,

$$x^8 + Ax^2 + B = (x^4 + ax^3 + bx^2 + cx + d)(x^4 - ax^3 + bx^2 - cx + d)\,,$$

hence

$$2b - a^2 = 0\,, \qquad 2d + b^2 - 2ac = 0\,, \qquad bd - c^2 = A\,, \qquad d^2 = B\,.$$

If $a = 0$ we obtain $b = 0$, $d = 0$, $B = 0$, contrary to $B \in K^*$. If $a \neq 0$ we take $a = 2u$, $c = u^3v$ and obtain (38).

LEMMA 34. *Let K be a field of characteristic different from 3, and $A, B \in K^*$. The trinomial $x^9 + Ax^3 + B$ is reducible over K if and only if either $x^3 + Ax + B$ is reducible over K or*

$$A = u^6A_{9,3}(v)\,, \qquad B = u^9B_{9,3}(v)\,, \tag{39}$$

where $u, v \in K$.

Proof. The condition (39) is sufficient, since it implies

$$\begin{aligned} & x^9 + Ax^3 + B \\ & \quad = (x^3 + 3ux^2 + u^2vx + u^3(3v - 9))(x^3 + 3u\zeta_3^2x^2 + u^2v\zeta_3x + u^3(3v - 9)) \\ & \qquad \times (x^3 + 3u\zeta_3x^2 + u^2v\zeta_3^2x + u^3(3v - 9))\,. \end{aligned}$$

On the other hand, if $x^9 + Ax^3 + B$ is reducible and $x^3 + Ax + B$ irreducible over K we have, by Lemma 29,

$$\begin{aligned} x^9 + Ax^3 + B &= (x^3 + ax^2 + bx + c)(x^3 + a\zeta_3^2x^2 + b\zeta_3x + c) \\ &\quad \times (x^3 + a\zeta_3x^2 + b\zeta_3^2x + c) \\ &= (x^3 + c)^3 + a^3x^6 + b^3x^3 - 3(x^3 + c)abx^3\,, \end{aligned}$$

hence

$$3c + a^3 - 3ab = 0\,, \qquad 3c^2 + b^3 - 3abc = A\,, \qquad c^3 = B\,.$$

If $a = 0$ we obtain $c = 0$, $B = 0$, contrary to $B \in K^*$. If $a \neq 0$ we take $a = 3u$, $b = u^2 v$ and obtain (39).

LEMMA 35. *Let K be a field of characteristic different from 2, and $A, B \in K^*$. The trinomial $x^{10} + Ax^2 + B$ is reducible over K if and only if either $x^5 + Ax + B$ is reducible over K or*

$$A = u^8 A_{10,2}(v)\,, \qquad B = u^{10} B_{10,2}(v)\,, \tag{40}$$

where $u, v \in K$.

Proof. The condition (40) is sufficient, since it implies

$$\begin{aligned} &x^{10} + Ax^2 + B \\ &\quad = (x^5 + 2ux^4 + 2u^2x^3 + 2u^3vx^2 + u^4(4v-2)x + u^5(-v^2+4v-2)) \\ &\qquad \times (x^5 - 2ux^4 + 2u^2x^3 - 2u^3vx^2 + u^4(4v-2)x - u^5(-v^2+4v-2))\,. \end{aligned}$$

On the other hand, if $x^{10} + Ax^2 + B$ is reducible and $x^5 + Ax + B$ irreducible over K we have, by Lemma 29,

$$x^{10} + Ax^2 + B = (x^5 + ax^4 + bx^3 + cx^2 + dx + e)(x^5 - ax^4 + bx^3 - cx^2 + dx - e)\,,$$

hence

$$\begin{gathered} 2b - a^2 = 0\,, \qquad 2d + b^2 - 2ac = 0\,, \qquad 2bd - 2ae - c^2 = 0\,, \\ d^2 - 2ce = A\,, \qquad -e^2 = B\,. \end{gathered}$$

If $a = 0$, we obtain $b = c = d = 0$, $A = 0$, contrary to $A \in K^*$. If $a \neq 0$ we take $a = 2u$, $c = 2u^3 v$ and obtain (40).

LEMMA 36. *Let K be a field of characteristic different from 2, and $A, B \in K^*$. The trinomial $x^{10} + Ax^4 + B$ is reducible over K if and only if either $x^5 + Ax^2 + B$ is reducible over K or*

$$A = u^8 A_{10,4}(v)\,, \qquad B = u^{10} B_{10,4}(v)\,, \tag{41}$$

where $u, v \in K$.

Proof. The condition (41) is sufficient, since it implies

$$\begin{aligned} &x^{10} + Ax^4 + B \\ &\quad = (x^5 + 2uvx^4 + 2u^2v^2x^3 + u^3v^4x^2 + u^4v^4(2v-2)x + 2u^5v^4(v-1)^2) \\ &\qquad \times (x^5 - 2uvx^4 + 2u^2v^2x^3 - u^3v^4x^2 + u^4v^4(2v-2)x - 2u^5v^4(v-1)^2)\,. \end{aligned}$$

On the other hand, if $x^{10} + Ax^4 + B$ is reducible and $x^5 + Ax^2 + B$ irreducible over K we have, by Lemma 29,

$$x^{10} + Ax^4 + B = (x^5 + ax^4 + bx^3 + cx^2 + dx + e)(x^5 - ax^4 + bx^3 - cx^2 + dx - e)\,,$$

hence

$$2b-a^2=0\,,\qquad 2d+b^2-2ac=0\,,\qquad 2bd-2ae-c^2=A\,,$$
$$d^2-2ce=0\,,\qquad -e^2=B\,.$$

If $a=0$, we obtain $b=d=0$, $ce=0$ and $AB=0$, contrary to $A,B\in K^*$. If $a\neq 0$, $c=0$ we obtain $d=0$, $b=0$, $a^2=0$, a contradiction. If $a\neq 0$, $c\neq 0$ we take $v=8c/a^3$, $u=a/2v$ and obtain (41).

LEMMA 37. *Let K be a field of characteristic different from 2, and $A,B\in K^*$. The trinomial $x^{12}+Ax^2+B$ is reducible over K if and only if either x^6+Ax+B is reducible over K or*

$$A=u^{10}A_{12,2}(v),\qquad B=u^{12}B_{12,2}(v)\,, \tag{42}$$

where $u,v\in K$.

Proof. The condition (42) is sufficient, since it implies

$$\begin{aligned}x^{12}+Ax^2+B=(&x^6+4u(v-4)x^5+8u^2(v-4)^2x^4+8u^3v(v-4)^3x^3\\&+32u^4(v-1)(v-4)^4x^2+32u^5(v-4)^4(3v^2-12v+10)x\\&+32u^6(v-4)^5(v^3-8v+8))(x^6-4u(v-4)x^5+8u^2(v-4)^2x^4\\&-8u^3v(v-4)^3x^3+32u^4(v-1)(v-4)^4x^2\\&-32u^5(v-4)^4(3v^2-12v+10)x+32u^6(v-4)^5(v^3-8v+8))\,.\end{aligned}$$

On the other hand, if $x^{12}+Ax^2+B$ is reducible, but x^6+Ax+B irreducible over K we have, by Lemma 29,

$$\begin{aligned}&x^{12}+Ax^2+B\\&=(x^6+ax^5+bx^4+cx^3+dx^2+ex+f)(x^6-ax^5+bx^4-cx^3+dx^2-ex+f)\,,\end{aligned}$$

hence

$$2b-a^2=0\,,\qquad 2d+b^2-2ac=0\,,\qquad 2f-2bd-2ae-c^2=0\,,\qquad 2bf+d^2-2ce=0\,,$$
$$2df-e^2=A\,,\qquad f^2=B\,.$$

If $a=0$, we obtain $b=0$, $d=0$, $ce=0$, $AB=0$, contrary to $A,B\in K^*$. If $a\neq 0$, $c=\frac{1}{2}a^3$ we obtain $b=\frac{1}{2}a^2$, $d=\frac{3}{8}a^4$, $f-ae=-\frac{1}{16}a^6$, $a^2f-a^3e=-\frac{9}{64}a^8$, a contradiction. If $a\neq 0$, $c\neq\frac{1}{2}a^3$ we take $v=8c/a^3$, $u=a/4(v-4)$ and obtain (42).

LEMMA 38. *Let K be a field of characteristic different from 3, and $A,B\in K^*$. The trinomial $x^{12}+Ax^3+B$ is reducible over K if and only if either x^4+Ax+B is reducible over K or*

$$A=u^9A_{12,3}(v)\,,\qquad B=u^{12}B_{12,3}(v)\,, \tag{43}$$

where $u,v\in K$.

P r o o f. The condition (43) is sufficient, since it implies

$$x^{12}+Ax^3+B = \prod_{i=0}^{2}(\zeta_3^i x^4+3u(v-1)x^3+9u^2v(v-1)^2\zeta_3^{2i}x^2+9u^3(v-1)^3(3v-1)\zeta_3^i x + 9u^4(v-1)^3(3v^3-3v+1))\,.$$

On the other hand, if $x^{12}+Ax^3+B$ is reducible and x^4+Ax+B irreducible over K we have, by Lemma 29,

$$x^{12}+Ax^3+B = \prod_{i=0}^{2}(\zeta_3^i x^4+ax^3+b\zeta_3^{2i}x^2+c\zeta_3^i x+d) = (x^4+cx)^3+(ax^3+d)^3b^3x^6-3bx^2(x^4+cx)(ax^3+d)\,.$$

Hence

$$3c+a^3-3ab=0\,,\qquad 3c^2+3a^2d+b^3-3abc-3bd=0\,,$$
$$c^3+3ad^2-3bcd=A\,,\qquad B=d^3\,.$$

If $a=0$, we obtain $c=0$, $A=0$, contrary to $A\in K^*$. If $a\neq 0$, $b=a^2$ we obtain $c=\frac{2}{3}a^3$, $\frac{1}{3}a^6=0$, a contradiction. If $a\neq 0$, $b\neq a^2$ we take $v=b/a^2$, $u=a/3(v-1)$ and obtain (43).

Lemma 39. *Let K be a field of characteristic different from 2, and $A,B\in K^*$. The trinomial $x^{12}+Ax^4+B$ is reducible over K if and only if either x^6+Ax^2+B is reducible over K or*

$$A=u^8A_{12,4}(v)\,,\qquad B=u^{12}B_{12,4}(v)\,, \tag{44}$$

where $u,v\in K$.

P r o o f. The condition (44) is sufficient, since it implies

$$\begin{aligned}x^{12}+Ax^4+B = {}&(x^6+4ux^5+8u^2x^4+8u^3(2v^2+1)x^3+64u^4v^2x^2\\ &+64u^5v(-2v^2+4v-1)x+32u^6(-2v^2+4v-1)^2)\\ &\times(x^6-4ux^5+8u^2x^4-8u^3(2v^2+1)x^3+64u^4v^2x^2\\ &-64u^5v(-2v^2+4v-1)x+32u^6(-2v^2+4v-1)^2)\,.\end{aligned}$$

On the other hand, if $x^{12}+Ax^4+B$ is reducible and x^6+Ax^2+B irreducible over K we have, by Lemma 29,

$$-64x^{12}+Ax^4+B = -64\prod_{i=0}^{3}(\zeta_4^i x^3+a\zeta_4^{2i}x^2+b\zeta_4^i x+c) = -64((x^3+bx)^2-(ax^2+c)^2)((-x^3+bx)^2+(-ax^2+c)^2)\,.$$

Hence

$$2b^2-4ac-(2b-a^2)^2=0\,,\qquad 16((b^2-2ac)^2+2(2b-a^2)c^2)=A\,,\qquad 64c^4=B\,.$$

If $a=0$, we obtain $b=0$, $A=0$, contrary to $A\in K^*$. If $a\neq 0$ we take $a=2u$, $b=4u^2v$ and obtain (44).

LEMMA 40. *Let K be a field of characteristic different from 5, and $A,B\in K^*$. The trinomial $x^{15}+Ax^5+B$ is reducible over K if and only if either x^3+Ax+B is reducible over K or*

$$A=u^{10}A_{15,5}(v)\,,\qquad B=u^{15}B_{15,5}(v)\,, \tag{45}$$

where $u,v\in K$.

Proof. The condition (45) is sufficient, since it implies

$$x^{15}+Ax^5+B=\prod_{i=0}^{4}(\zeta_5^{3i}x^3+u(5v-5)\zeta_5^{2i}x^2+u^2v(5v-5)^2\zeta_5^ix + u^3(5v-5)^2(5v^2-5v+1))\,.$$

On the other hand, if $x^{15}+Ax^5+B$ is reducible and x^3+Ax+B irreducible over K we have, by Lemma 29,

$$x^{15}+Ax^5+B=\prod_{i=0}^{4}(\zeta_5^{3i}x^3+a\zeta_5^{2i}x^2+b\zeta_5^ix+c)\,.$$

Hence

$$\begin{gathered}-5bc+5a^2c+5ab^2-5a^3b+a^5=0\,,\\ -5ac^3-5ab^3c+5a^2bc^2+5b^2c^2+b^5=A\,,\qquad c^5=B\,.\end{gathered}$$

If $a=0$, we obtain $bc=0$, $AB=0$, contrary to $A,B\in K^*$. If $a\neq 0$, $b=a^2$ we obtain $a^5=0$, a contradiction. If $a\neq 0$, $b\neq a^2$ we take $v=b/a^2$, $u=a/(5v-5)$ and obtain (45).

4. Determination of the content of Table 2 (Lemmas 41–48)

LEMMA 41. *Let K be a field of characteristic different from 2. The curve*

$$y^2=x^4+a_1x^3+3a_2x^2+a_3x+a_4=R(x), \tag{46}$$

where $R\in K[x]$ is not a square, is equivalent to the curve

$$w^2=v^3-(4a_4-a_1a_3+3a_2^2)v-(8a_2a_4+a_1a_2a_3-a_4a_1^2-a_3^2-2a_2^3) \tag{47}$$

under the following birational transformation over K:

$$\begin{aligned}v&=2y+2x^2+a_1x+a_2\,,\\ w&=4xy+a_1y+4x^3+3a_1x^2+6a_2x+a_3\,;\end{aligned}$$

$$x=\frac{(v-a_2)^2-4a_4}{2w+a_1(v-a_2)+2a_3}\,, \tag{48a}$$

$$y=\frac{1}{2}v-x^2-\frac{a_1}{2}x-\frac{a_2}{2}\,.$$

The zeros of the denominator in the above formula for x, lying on (47), *correspond to the point at infinity on* (46) *and to the points $\langle x, y\rangle$, where*

$$x = \frac{4(a_3 + a_1\sqrt{a_4})}{a_1^2 - 12a_2 - 8\sqrt{a_4}}\,, \qquad y = \frac{1}{2}v - x^2 - \frac{a_1}{2}x - \frac{a_2}{2}$$

with any choice of the square root.

Moreover, if $R(x_0) = 0$, $R'(x_0) \neq 0$ for an $x_0 \in K$ there is a simpler birational transformation over K:

$$\begin{aligned} v &= \frac{\frac{1}{3}R''(x_0)x + (2R'(x_0) - \frac{1}{3}R''(x_0)x_0)}{2(x - x_0)}\,, \\ w &= \frac{R'(x_0)y}{(x - x_0)^2}\,; \\ x &= \frac{2x_0v + (2R'(x_0) - \frac{1}{3}R''(x_0)x_0)}{2v - \frac{1}{3}R''(x_0)}\,, \\ y &= \frac{4R'(x_0)w}{(2v - \frac{1}{3}R''(x_0))^2}, \end{aligned} \tag{48b}$$

where $\frac{1}{3}R''(x_0) = 4x_0^2 + 2a_1x_0 + 2a_2$. The two zeros of the denominator in the above formula for x, lying on (47), *correspond to the double point at infinity on* (46).

R e m a r k. Note that $4(a_3 + a_1\sqrt{a_4})$ and $a_1^2 - 12a_2 - 8\sqrt{a_4}$ are not simultaneously 0 since otherwise $R(x) = (x^2 + \frac{1}{2}a_1x - \sqrt{a_4})^2$.

P r o o f. The curve (46) is equivalent to the curve

$$y_1^2 = a_4x_1^4 + a_3x_1^3 + 3a_2x_1^2 + a_1x_1 + 1 = R(x_1) \tag{49}$$

via the involution I:

$$x_1 = \frac{1}{x}\,, \qquad y_1 = \frac{y}{x^2}\,.$$

On the other hand, the curve (49) has the rational point $\langle 0, 1\rangle$. Applying to (49) the transformation of Weierstraß as described in Theorem 3 of [16] with $x_0 = 0$, $y_0 = 1$ we find that it is equivalent to the curve

$$Y^2 = 4X^3 - g_2X - g_3\,, \tag{50}$$

where

$$g_2 = \frac{1}{4}(4a_4 - a_1a_3 + 3a_2^2)\,, \qquad g_3 = \frac{1}{16}(8a_2a_4 + a_1a_2a_3 - a_4a_1^2 - a_3^2 - 2a_2^3)\,,$$

via the birational transformation T:

$$X = \frac{y_1 + 1 + \frac{1}{2}a_1x_1 + 3a_2}{2x_1^2}\,,$$

$$Y = \frac{y_1^2}{x_1^3} - \frac{1}{4}\frac{R'(x_1)}{x_1^2} + \left(\frac{1}{x_1^3} + \frac{1}{4}\frac{a_1}{x_1^2}\right)y_1\,;$$

$$x_1 = \frac{Y + \frac{1}{2}a_1(X - \frac{3}{2}a_2) + \frac{1}{4}a_3}{2(X - \frac{3}{2}a_2)^2 - \frac{1}{2}a_4}\,,$$

$$y_1 = 2Xx_1^2 - 1 - \frac{1}{2}a_1x_1 - 3a_2x_1^2\,.$$

Finally, the curve (50) is equivalent to the curve (47) via the linear transformation L:

$$v = 4X\,, \qquad w = 4Y\,.$$

The birational transformation (48a) given in the lemma is the composition of I, T and L.

The birational transformation (48b) is obtained directly from Theorem 3 in [16] by setting $y_0 = 0$.

LEMMA 42. *Let K be a field of characteristic different from 2, and $A, B \in K^*$. The trinomial $x^7 + Ax^2 + B$ has a cubic factor in $K[x]$ if and only if either*

$$A = -2u^5, \qquad B = u^7\,, \qquad u \in K \tag{51}$$

or

$$A = u^5A_{7,2}(v, w)\,, \qquad B = u^7B_{7,2}(v, w)\,, \tag{52}$$

where $u \in K$ and

$$\langle v, w\rangle \in E_{7,2}(K)\,. \tag{53}$$

Proof. The condition is sufficient, since if (51) holds we have

$$x^7 + Ax^2 + B = (x^4 - u^2x^2 - u^3x + u^4)(x^3 + ux^2 + u^3)$$

and if (52) and (53) hold we have

$$\begin{aligned} x^7 + Ax^2 + B &= (x^4 + 2ux^3 - u^2vx^2 + u^3(w + 4)x + u^4(v^2 + 12v + 4w + 32)) \\ &\quad \times (x^3 - 2ux^2 + u^2(v + 4)x + u^3(-4v - w - 12))\,. \end{aligned}$$

On the other hand, if $x^7 + Ax^2 + B$ has a cubic factor we have

$$x^7 + Ax^2 + B = (x^4 + a_1x^3 + b_1x^2 + c_1x + d_1)(x^3 + a_2x^2 + b_2x + c_2)\,,$$

hence

$$\begin{gathered} a_2 + a_1 = 0\,, \qquad b_2 + a_1a_2 + b_1 = 0\,, \qquad c_2 + a_1b_2 + b_1a_2 + c_1 = 0\,, \\ a_1c_2 + b_1b_2 + c_1a_2 + d_1 = 0\,, \qquad b_1c_2 + c_1b_2 + d_1a_2 = A\,, \\ c_1c_2 + d_1b_2 = 0\,, \qquad d_1c_2 = B\,. \end{gathered}$$

If $a_1 = 0$ we obtain $a_2 = 0$, $b_2 = -b_1$, $c_2 = -c_1$, $d_1 = b_1^2$, $c_1^2 + b_1^3 = 0$ and on taking $b_1 = -u^2$ we obtain (51).

If $a_1 \neq 0$ we take $a_1 = 2u$, $b_1 = -u^2 v$, $c_1 = u^3(w+4)$ and obtain (52)–(53).

LEMMA 43. *Let K be a field of characteristic different from 2, 3, and $A, B \in K^*$. The trinomial $x^7 + Ax^3 + B$ has a cubic factor in $K[x]$ if and only if*

$$A = u^4 A_{7,3}(v,w)\,, \qquad B = u^7 B_{7,3}(v,w)\,, \tag{54}$$

where $u \in K$ and

$$\langle v, w\rangle \in E_{7,3}(K)\,. \tag{55}$$

Proof. The condition is sufficient, since if it is satisfied we have

$$\begin{aligned} x^7 &+ Ax^3 + B \\ &= (x^4 + u(v-39)x^3 - 36u^2(v-39)x^2 + 6u^3(v-39)(-w+3v+99)x \\ &\quad + 6u^4(v-39)(-w(v+33) + 9v^2 + 162v - 4455)) \\ &\quad \times (x^3 - u(v-39)x^2 + u^2(v-3)(v-39)x + u^3(6w - v^2 - 12v + 693))\,. \end{aligned}$$

On the other hand, if

$$x^7 + Ax^3 + B = (x^4 + a_1x^3 + b_1x^2 + c_1x + d_1)(x^3 + a_2x^2 + b_2x + c_2)$$

we have

$$\begin{gathered} a_2 + a_1 = 0\,, \qquad b_2 + a_1a_2 + b_1 = 0\,, \qquad c_2 + a_1b_2 + b_1a_2 + c_1 = 0\,, \\ a_1c_2 + b_1b_2 + c_1a_2 + d_1 = A\,, \qquad b_1c_2 + c_1b_2 + d_1a_2 = 0\,, \\ c_1c_2 + d_1b_2 = 0, \qquad d_1c_2 = B\,. \end{gathered}$$

If $a_1 = 0$ we obtain $a_2 = 0$, $b_2 = -b_1$, $c_2 = -c_1$, $b_1c_1 = 0$, $B = 0$, contrary to $B \in K^*$.

If $a_1 \neq 0$ we take $x = 2b_2/a_1^2$, $y = 4c_2a_1^{-3} + 4b_2^2a_1^{-4} + 2b_2a_1^{-2} - 2$ and obtain

$$y^2 = x^4 - 2x^3 + x^2 - 4x + 4 = R(x)\,.$$

If $x = 2$ we obtain $b_2 = a_1^2$, $b_1 = 0$, $c_2 = -a_1^3$, $c_1 = 0$, $d_1 = 0$, $B = 0$, contrary to $B \in K^*$. Since $R(2) = 0$, if $x \neq 2$ we put

$$v = \frac{39x - 6}{x - 2}\,, \qquad w = \frac{216y}{(x-2)^2}\,.$$

By Lemma 41 we have (55) and $v \neq 39$. On taking $u = a_1/(v-39)$ we obtain (54).

LEMMA 44. *Let K be a field and $A, B \in K^*$. The trinomial $x^8 + Ax + B$ has a cubic factor in $K[x]$ if and only if either*

$$A = -3u^7\,, \qquad B = 2u^8\,, \qquad u \in K \tag{56}$$

or

$$\begin{aligned} A &= ((3v^2 - 12v - 10)w - 8v^3 + 20v^2 + 8v - 32)u^7\,, \\ B &= (w - 3v + 5)((2v-5)w - 3v^2 + 15v - 17)u^8, \end{aligned} \tag{57}$$

where $u, v, w \in K$ *and*

$$w^2 = v^3 - 10v + 12\,. \tag{58}$$

P r o o f. The condition is sufficient, since if (56) holds then

$$x^8 + Ax + B = (x^5 - u^2x^3 + u^3x^2 + u^4x + 2u^5)(x^3 + u^2x + u^3)$$

and if (57) and (58) hold then

$$\begin{aligned} x^8 + Ax + B &= (x^5 - ux^4 + u^2(2-v)x^3 + u^3(-w+v-2)x^2 + u^4(-2w+v^2+v-5)x \\ &\quad + u^5((2v-5)w - 3v^2 + 15v - 17))(x^3 - ux^2 + (v-1)x + (w-3v+5))\,. \end{aligned}$$

On the other hand, if

$$x^8 + Ax + B = (x^5 + a_1x^4 + b_1x^3 + c_1x^2 + d_1x + e_1)(x^3 + a_2x^2 + b_2x + c_2)$$

we have

$$\begin{gathered} a_2 + a_1 = 0\,, \quad b_2 + a_1a_2 + b_1 = 0\,, \quad c_2 + a_1b_2 + b_1a_2 + c_1 = 0\,, \\ a_1c_2 + b_1b_2 + c_1a_2 + d_1 = 0\,, \quad b_1c_2 + c_1b_2 + d_1a_2 + e_1 = 0\,, \\ c_1c_2 + d_1b_2 + e_1a_2 = 0\,, \quad d_1c_2 + e_1b_2 = A\,, \quad e_1c_2 = B\,. \end{gathered}$$

If $a_1 = 0$ we obtain $a_2 = 0$, $b_2 = -b_1$, $c_2 = -c_1$, $d_1 = b_1^2$, $e_1 = 2b_1c_1$, $c_1^2 + b_1^3 = 0$, and (56) follows on taking $u = c_1/b_1$. If $a_1 \neq 0$, (57) and (58) follow on taking

$$u = a_1\,, \quad v = 2 - \frac{b_1}{a_1^2}\,, \quad w = -\frac{b_1}{a_1^2} - \frac{c_1}{a_1^3}\,.$$

Lemma 45. *Let* K *be a field of characteristic different from* 2, *and* $A, B \in K^*$. *The trinomial* $x^8 + Ax + B$ *has a quartic factor in* $K[x]$ *if and only if either*

$$A = 3u^7\,, \quad B = 2u^8\,, \quad u \in K \tag{59}$$

or

$$\begin{aligned} A &= 128(w - 2v - 8)^4(v+2)(v^2 + 12v + 4) \\ &\quad \times (2w - v^2 + 4v + 4)(4w - v^2 - 12)\,, \\ B &= 64(w - 2v - 8)^4 \\ &\quad \times (9v^4 + 8v^3 - 8v^2 + 288v + 272 - w(v^3 + 18v^2 + 76v + 24)) \\ &\quad \times (v^4 + 24v^3 + 152v^2 + 96v + 16 + w(v^3 - 22v^2 - 52v - 72))\,, \end{aligned} \tag{60}$$

where $u, v, w \in K$ *and*

$$w^2 = v^3 - 20v - 16\,. \tag{61}$$

P r o o f. The condition is sufficient, since if (59) holds we have

$$x^8 + Ax + B = (x^4 + ux^3 + u^2x^2 + 2u^3x + u^4)(x^4 - ux^3 - u^3x + 2u^4)\,.$$

If (60) and (61) hold we have

$$\begin{aligned}x^8+Ax+B=(&x^4+4(w-2v-8)x^3+4(w-2v-8)(v^2-8v-20)x^2\\&+8(w-2v-8)^2(-20v-24+w(v-2))x\\&+8(w-2v-8)^2(9v^4+8v^3-8v^2+288v+272\\&-w(v^3+18v^2+76v+24)))\\&\times(x^4-4(w-2v-8)x^3+4(w-2v-8)(4w-v^2-12)x^2\\&+8(w-2v-8)^2(4v^2+4v+8-w(v+6))x\\&+8(w-2v-8)^2(v^4+24v^3+152v^2+96v+16\\&+w(v^3-22v^2-52v-72)))\,.\end{aligned}$$

On the other hand, if

$$x^8+Ax+B=(x^4+a_1x^3+b_1x^2+c_1x+d_1)(x^4+a_2x^3+b_2x^2+c_2x+d_2)$$

we have

$$\begin{gathered}a_2+a_1=0\,,\qquad b_2+a_1a_2+b_1=0\,,\qquad c_2+a_1b_2+b_1a_2+c_1=0\,,\\d_2+a_1c_2+b_1b_2+c_1a_2+d_1=0\,,\qquad a_1d_2+b_1c_2+c_1b_2+d_1a_2=0\,,\\b_1d_2+c_1c_2+d_1b_2=0\,,\qquad c_1d_2+d_1c_2=A\,,\qquad d_1d_2=B\,.\end{gathered}$$

If $a_1=0$ we obtain $a_2=0$, $b_2=-b_1$, $c_2=-c_1$, $d_2=b_1^2-d_1$, $2b_1c_1=0$, $b_1^3-2b_1d_1-c_1^2=0$, $A=0$, contrary to $A\in K^*$.

If $a_1\neq0$ we take $x_1=2b_1/a_1^2$, $y_1=4c_1/a_1^3-4b_1^2/a_1^4-1$ and obtain

$$y_1^2=x_1^4-4x_1^3+12x_1^2-16x_1+9=R(x_1)\,.$$

If $x_1=2$ we obtain $y_1=\pm3$ hence either $b_1=a_1^2$, $c_1=2a_1^3$, $b_2=0$, $c_2=-a_1^3$, $d_1=a_1^4$, $d_2=2a_1^4$ and (59) holds with $u=-a_1$ or $b_1=a_1^2$, $c_1=\frac12a_1^3$, $b_2=0$, $c_2=\frac12a_1^3$, $d_1=\frac14a_1^4$, $d_2=-\frac14a_1^4$, $A=0$, contrary to $A\in K^*$.

If $x_1\neq2$ we put

$$\begin{aligned}v&=2y_1+2x_1^2-4x_1+4\,,\\w&=4x_1y_1-4y_1+4x_1^3-12x_1^2+24x_1-16\end{aligned}$$

and using Lemma 41 we obtain (61) with $w-2v-8\neq0$. Now (60) follows on taking

$$u=\frac{a_1}{4(w-2v-8)}\,.$$

Lemma 46. *Let K be a field of characteristic different from 2 and 3, and $A,B\in K^*$. The trinomial x^9+Ax+B has a cubic factor in $K[x]$ if and only if either $\sqrt{13}\in K$ and*

$$\begin{aligned}A&=(-480053919711226727\pm66936076602084894\sqrt{13})u^8\,,\\B&=\tfrac12(-5712685878317063725\pm66644985243629014605\sqrt{13})u^9\,,\end{aligned}\tag{62}$$

where $u\in K$,

or

$$A = u^8 A_{9,1}(v,w)\,, \qquad B = u^9 B_{9,1}(v,w)\,, \tag{63}$$

where $u \in K$ *and*

$$\langle v,w\rangle \in E_{9,1}(K)\,. \tag{64}$$

P r o o f. The condition is sufficient, since if (62) is satisfied we have, with a suitable value of $\sqrt{13}$,

$$\begin{aligned}
&x^9 + Ax + B\\
&= \left(x^3 + 183ux^2 + (41175 + 549\sqrt{13})u^2x + \frac{9879255 - 1774917\sqrt{13}}{2}u^3\right)\\
&\quad\times\left(x^6 - 183ux^5 - (7686 + 549\sqrt{13})u^2x^4 + \frac{8003871 + 2176785\sqrt{13}}{2}u^3x^3\right.\\
&\quad + (491986899 - 334756044\sqrt{13})u^4x^2\\
&\quad + \frac{-461897936703 + 20279163483\sqrt{13}}{2}u^5x\\
&\quad\left. + \frac{34367850319995 + 19666467995175\sqrt{13}}{2}u^6\right)
\end{aligned}$$

and if (63) and (64) hold we have

$$\begin{aligned}
x^9 + Ax + B = {}&(x^3 + 3(w - 2v - 9)ux^2 + 3(w - 2v - 9)(v^2 - 9v - 9)u^2x\\
&+ 3(w - 2v - 9)^2(6v^2 - 21v - 9 - w(v + 3))u^3)\\
&\times (x^6 - 3(w - 2v - 9)ux^5\\
&+ 3(w - 2v - 9)(-v^2 + 3v - 18 + 3w)u^2x^4\\
&+ 3(w - 2v - 9)^2(-15v + 36 + w(v - 6))u^3x^3 + 9(w - 2v - 9)^2\\
&\times (-v^4 - 21v^3 + 30v^2 - 117v + 351 + w(7v^2 + 33v - 45))u^4x^2\\
&+ 9(w - 2v - 9)^3(12v^4 + 48v^3 - 153v^2 + 135v - 567\\
&+ w(-2v^3 - 24v^2 - 90v + 54))u^5x + 9(w - 2v - 9)^3\\
&\times (v^6 + 219v^5 - 9v^4 - 792v^3 - 2916v^2\\
&+ 6804v - 6804 + w(v^5 - 60v^4 - 228v^3\\
&- 81v^2 - 972v + 1134))u^6)\,.
\end{aligned}$$

On the other hand, if

$$x^9 + Ax + B = (x^6 + a_1x^5 + b_1x^4 + c_1x^3 + d_1x^2 + e_1x + f_1)(x^3 + a_2x^2 + b_2x + c_2)$$

we find

$$\begin{aligned}
&a_2 + a_1 = 0\,, \quad b_2 + a_1a_2 + b_1 = 0\,, \quad c_2 + a_1b_2 + b_1a_2 + c_1 = 0\,,\\
&a_1c_2 + b_1b_2 + c_1a_2 = 0\,, \quad b_1c_2 + c_1b_2 + d_1a_2 + e_1 = 0\,,\\
&c_1c_2 + d_1b_2 + e_1a_2 + f_1 = 0\,, \quad d_1c_2 + e_1b_2 + f_1a_2 = 0\,,
\end{aligned}$$

$$e_1c_2 + f_1b_2 = A\,, \qquad f_1c_2 = B\,.$$

If $a_1 = 0$ we obtain $a_2 = 0$, $b_2 = -b_1$, $c_2 = -c_1$, $d_1 = b_1^2$, $e_1 = 2b_1c_1$, $f_1 - b_1^3 - c_1^2 = 0$, $3b_1e_1 = 0$ and either $b_1 = 0$, which gives $A = 0$, or $c_1 = 0$, which gives $B = 0$, contrary to the assumption.

If $a_1 \neq 0$ we take

$$x_1 = 3b_2/a_2^2\,, \qquad y_1 = -18c_2/a_2^3 - 15 + 36b_2/a_2^2 - 9b_2^2/a_2^4$$

and obtain

$$y_1^2 = x_1^4 - 8x_1^3 + 54x_1^2 - 144x_1 + 117\,.$$

If

$$\langle x_1, y_1\rangle = \left\langle \frac{225 \pm 3\sqrt{13}}{61}, \frac{11478 \pm 10545\sqrt{13}}{61^2} \right\rangle$$

(62) follows on taking $u = a_2/183$.

If

$$\langle x_1, y_1\rangle \neq \left\langle \frac{225 \pm 3\sqrt{13}}{61}, \frac{11478 \pm 10545\sqrt{13}}{61^2} \right\rangle$$

we put

$$v = \frac{y_1}{2} + \frac{x_1^2}{2} - 2x_1 + \frac{9}{2}\,, \qquad w = \frac{x_1y_1}{2} - y_1 + \frac{x_1^3}{2} - 3x_1^2 + \frac{27}{2}x_1 - 18\,.$$

By Lemma 41 we obtain (64) and $w - 2v - 9 \neq 0$. Hence (63) follows on taking $u = a_2/183(w - 2v - 9)$.

LEMMA 47. *Let K be a field of characteristic different from 2, and $A, B \in K^*$. The trinomial $x^{14} + Ax^2 + B$ is reducible over K if and only if either $x^7 + Ax + B$ is reducible over K or*

$$A = u^{12}A_{14,2}(v, w)\,, \qquad B = u^{14}B_{14,2}(v, w)\,, \tag{65}$$

where $u \in K$ and

$$\langle v, w\rangle \in E_{14,2}(K)\,. \tag{66}$$

P r o o f. The condition is sufficient, since it yields

$$\begin{aligned} x^{14} + Ax^2 + B = \prod_{\varepsilon=\pm1} (&x^7 + 2\varepsilon u(v-2)x^6 + 2u^2(v-2)^2x^5 \\ &+ 2\varepsilon u^3(v-2)^2(v-1)x^4 + 2u^4(v-2)^3vx^3 \\ &+ 2\varepsilon u^5(v-2)^3(w+v^2-3)x^2 \\ &+ 2u^6(v-2)^4(2w+v^2+2v-5)x \\ &+ \varepsilon u^7(v-2)^4((2v-6)w+v^3-12v+14))\,. \end{aligned}$$

On the other hand, if $x^{14} + Ax^2 + B$ is reducible, but $x^7 + Ax + B$ irreducible over K we have, by Lemma 29,

$$x^{14}+Ax^2+B=\prod_{\varepsilon=\pm1}(x^7+\varepsilon ax^6+bx^5+\varepsilon cx^4+dx^3+\varepsilon ex^2+fx+\varepsilon g)$$
$$=(x^7+bx^5+dx^3+fx)^2-(ax^6+cx^4+ex^2+g)^2\,.$$

Hence (cf. [1])

$$2b-a^2=0\,,\quad 2d+b^2-2ac=0\,,\quad 2f+2bd-2ae-c^2=0\,,$$
$$2bf+d^2-2ag-2ce=0\,,\quad 2df-2cg-e^2=0\,,$$
$$f^2-2eg=A\,,\quad -g^2=B\,.$$

If $a=0$ we obtain $b=0$, $d=0$, $2f-c^2=0$, $2ce=0$, $2cg+e^2=0$, $e=0$, $AB=0$, contrary to $A,B\in K^*$.

If $a\neq0$ we put $x_1=4c/a^3$, $y_1=16e/a^5-8c/a^3-16c^2/a^6+2$ and obtain

$$y_1^2=x_1^4+2x_1^3-6x_1^2+3x_1\,.$$

If $x_1=1$ we obtain $y_1=0$, $c=a^3/4$, $e=a^5/16$, $b=a^2/2$, $d=a^4/8$, $f=a^6/32$, $g=a^7/128$, $A=0$, contrary to $A\in K^*$.

If $x_1\neq1$ we put

$$v=\frac{2x_1-1}{x_1-1}\,,\qquad w=\frac{y_1}{(x_1-1)^2}$$

and using Lemma 41 obtain (66) with $v\neq2$. Now (65) follows on taking $u=a/2(v-2)$.

LEMMA 48. *Let K be a field of characteristic different from 2, 7, and $A,B\in K^*$. The trinomial $x^{21}+Ax^7+B$ is reducible over K if and only if either x^3+Ax+B is reducible over K or*

$$A=2\cdot7^{13}u^{14}\,,\qquad B=7^{14}\left(\frac{7\pm\sqrt{21}}{2}\right)^7u^{21}\,,\qquad u\in K \tag{67}$$

or

$$A=u^{14}A_{21,7}(v,w)\,,\qquad B=u^{21}B_{21,7}(v,w)\,, \tag{68}$$

where $u\in K$ and

$$\langle v,w\rangle\in E_{21,7}(K)\,. \tag{69}$$

Proof. The conditions are sufficient since if (67) holds we have

$$x^{21}+Ax^7+B=\prod_{i=0}^{6}\left(\zeta_7^{3i}x^3+7\zeta_7^{2i}ux^2+49\zeta_7^iu^2x+49u^3\left(\frac{7\pm\sqrt{21}}{2}\right)\right).$$

If (68) and (69) hold, we have

$$x^{21}+Ax^7+B=\prod_{i=0}^{6}(\zeta_7^{3i}x^3+14\zeta_7^{2i}u(w-7v-343)x^2$$
$$+14\zeta_7^iu^2(w-7v-343)(v^2-98v-1715)x$$
$$+14u^3(w-7v-343)^2(-(49+v)w+21v^2-686v-7203))\,.$$

On the other hand, if $x^{21}+Ax^7+B$ is reducible and x^3+Ax+B irreducible over K we have, by Lemma 29,

$$\begin{aligned}
&x^{21}+Ax^7+B\\
&=\prod_{i=0}^{6}(\zeta_7^{3i}x^3+a\zeta_7^{2i}x^2+b\zeta_7^i x+c)\\
&=x^{21}+(a^7-7a^5b+7a^4c+14a^3b^2-21a^2bc-7ab^3+7ac^2+7b^2c)x^{14}\\
&\quad+(b^7-7b^5ac+7b^4c^2+14b^3a^2c^2-21b^2ac^3-7ba^3c^3+7bc^4+7a^2c^4)x^7+c^7\,.
\end{aligned}$$

Hence

$$a^7-7a^5b+7a^4c+14a^3b^2-21a^2bc-7ab^3+7ac^2+7b^2c=0\,.$$

If $a=0$ we have $bc=0$ and $AB=0$, contrary to $A,B\in K^*$.

If $a\neq 0$ we put

$$x_1=7\frac{b}{a^2}\,,\qquad y_1=-98\frac{c}{a^3}-49\frac{b^2}{a^4}+147\frac{b}{a^2}-49$$

and obtain

$$y_1^2=x_1^4-14x_1^3+147x_1^2-686x_1+1029\,.$$

If $x_1=7$ we obtain $y_1=\pm 7\sqrt{21}$, $b=a^2$, $c=\frac{7\pm\sqrt{21}}{14}a^3$ and (67) follows on taking $u=a/7$.

If $x_1\neq 7$ we put

$$\begin{aligned}
v&=2y_1+2x_1^2-14x_1+49\,,\\
w&=4x_1y_1-14y_1+4x_1^3-42x_1^2+294x_1-686\,.
\end{aligned}$$

By Lemma 41 we obtain (69) and $w-7v-343\neq 0$. Hence (68) follows on taking $u=a/14(w-7v-343)$.

5. Proof of Theorems 1, 2 and 3

Proof of Theorem 1. The theorem follows from Lemmas 26, 28 and 30–40.

Proof of Theorem 2. For $n>2m$ the theorem follows from Lemmas 27, 30–40 and 42–48. For $n=2m$ it follows from Lemma 28.

For the proof of Theorem 3 we need two lemmas.

Lemma 49. *Let L be a finite separable extension of $K(\mathbf{y})$ and let $L\cap\overline{K}=K_0$. Then $[L:\overline{K}(\mathbf{y})]=[L:K_0(\mathbf{y})]$.*

Proof. Let $L=K_0(\mathbf{y},z)$ and let F be the minimal polynomial of z over $K_0(\mathbf{y})$, of degree d. Suppose that $[L:\overline{K}(\mathbf{y})]<[L:K_0(\mathbf{y})]$. Then F is reducible over $\overline{K}(\mathbf{y})$, hence over $K_1(\mathbf{y})$, where $[K_1:K_0]<\infty$. Since the coefficients of any monic factor of F belong to the normal closure of L over $\overline{K}(\mathbf{y})$, which is separable over $\overline{K}(\mathbf{y})$, we may assume without loss of generality that K_1/K_0 is separable. Then $K_1=K_0(\vartheta)$. Let f be the minimal polynomial of ϑ over K_0. Then f is

irreducible over L; indeed, the coefficients of its problematic monic factors over L would have to belong to $L \cap \overline{K} = K_0$. Hence

$$[L(\vartheta) : L] = [K_1 : K_0]$$

and since $L(\vartheta) = K_1(\mathbf{y}, z)$ we have

$$[K_1(\mathbf{y}, z) : K_0(\mathbf{y})] = [K_1(\mathbf{y}, z) : K_0(\mathbf{y}, z)][K_0(\mathbf{y}, z) : K_0(\mathbf{y})] = d[K_1 : K_0]\,.$$

On the other hand, $[K_1(\mathbf{y}) : K_0(\mathbf{y})] = [K_1 : K_0]$, hence

$$\begin{aligned}[K_1(\mathbf{y}, z) : K_0(\mathbf{y})] &= [K_1(\mathbf{y}, z) : K_1(\mathbf{y})][K_1(\mathbf{y}) : K_0(\mathbf{y})] \\ &= [K_1(\mathbf{y}, z) : K_1(\mathbf{y})][K_1 : K_0]\,.\end{aligned}$$

By comparison of the above two formulae,

$$[K_1(\mathbf{y}, z) : K_1(\mathbf{y})] = d\,,$$

hence F is irreducible over K_1. The obtained contradiction completes the proof.

LEMMA 50. *Under the assumptions of Theorem* 3, *if* $C_0 \in L^*$, $C_0 = c_1 C_1^q$, *where* $c_1 \in \overline{K}$, $C_1 \in \overline{K}L$, $q \not\equiv 0 \bmod \pi$ *then there exist* $c \in K_0$ *and* $C \in L^*$ *such that* $C_0 = cC^q$.

Proof. Let K_1 be the separable closure of K_0 in $\overline{K}$ and consider first the case where $c_1 \in K_1$ and $C_1 \in K_1 L$.

Since $K_0 = L \cap \overline{K}$ we have, by Lemma 49,

$$L = K_0(\mathbf{y}, z)\,,$$

where z is a zero of a polynomial over $K_0(\mathbf{y})$ irreducible over $\overline{K}(\mathbf{y})$, of degree d, say.

Let $G = \mathrm{Gal}(K_1/K_0)$. We extend the action of G to $K_1 L$ by putting $\mathbf{y}^\sigma = \mathbf{y}$, $z^\sigma = z$ for all $\sigma \in G$.

We have

$$C_1 = \sum_{j=0}^{d-1} f_j z^j\,, \qquad f_j \in K_1(\mathbf{y})\,,$$

hence

$$C_1^\sigma = \sum_{j=0}^{d-1} f_j^\sigma z^j \qquad \text{for all } \sigma \in G\,.$$

On the other hand,

$$c_1^\sigma (C_1^\sigma)^q = C_0^\sigma = C_0 = c_1 C_1^q\,,$$

hence

$$C_1^\sigma = e_\sigma C_1\,, \qquad e_\sigma \in K_1\,.$$

Since z is of degree d over $K_1(\mathbf{y})$ we obtain

$$f_j^\sigma = e_\sigma f_j \qquad (0 \le j < d)\,.$$

Let i be the least index such that $f_i \neq 0$,

$$f_i = \frac{g}{h}\,, \qquad \text{where} \quad g, h \in K_1[\mathbf{y}]\,,$$

and let γ, χ be the coefficients of the first term in the antilexicographic order of g and h, respectively.

We have

$$\left(\frac{\gamma}{\chi}\right)^{\sigma} = e_\sigma \frac{\gamma}{\chi}\,,$$

hence

$$\left(C_1 \frac{\chi}{\gamma}\right)^{\sigma} = C_1 \frac{\chi}{\gamma} \qquad \text{for all } \sigma \in G\,.$$

It follows that

$$C := C_1 \frac{\chi}{\gamma} \in L$$

and the assertion holds with $c = c_1(\gamma/\chi)^q$.

Consider now the general case. Since the extension $\overline{K}/K_1$ is purely inseparable there exists an exponent e such that $c_1^{\pi^e} \in K_1$ and $C_1^{\pi^e} \in K_1 L$.

Since $\pi \nmid q$ there exist integers r and s such that $\pi^e r - qs = 1$ and we obtain

$$C_0 = c_1^{\pi^e r} \left(\frac{C_1^{\pi^e r}}{C_0^s}\right)^q = c_2 C_2^q\,, \qquad \text{where } c_2 \in K_1,\ C_2 \in K_1 L\,.$$

The assertion follows by the already proved part of the lemma.

P r o o f o f T h e o r e m 3. The condition given in the theorem is sufficient, since if

$$x^{n_1 q} + a x^{m_1 q} + b = f(x) g(x)\,, \qquad f, g \in K_0[x] \setminus K_0\,,$$

we have

$$x^n + A x^m + B = C^{n_1 q} f\left(\frac{x^{(m,n)/q}}{C}\right) g\left(\frac{x^{(m,n)/q}}{C}\right).$$

On the other hand, $A^{-n} B^{n-m} \in \overline{K}$ implies $A^{-n} B^{n-m} \in K_0$,

$$A = a_0 C_0^{m_1 - m_1}\,, \qquad B = b_0 C_0^{m_1}\,, \qquad a_0, b_0 \in K_0\,, \qquad C_0 \in L\,,$$

and

$$C_0^{-n_1}(x^n + A x^m + B) = \left(\frac{x^{(m,n)}}{C_0}\right)^{n_1} + a_0 \left(\frac{x^{(m,n)}}{C_0}\right)^{m_1} + b_0\,.$$

Thus if $x^n + A x^m + B$ is reducible over L we infer by Capelli's lemma that either $x^{n_1} + a_0 x^{m_1} + b_0$ is reducible over L or else

$$\frac{x^{(m,n)}}{C_0} - \xi$$

is reducible over $L(\xi)$, where ξ is a zero of $x^{n_1} + a_0 x^{m_1} + b_0$. In the former case the condition is satisfied with $a = a_0$, $b = b_0$, $C = C_0$, $q = 1$. In the latter case

by Capelli's theorem there exists a $q \mid (m,n)$, $q=4$ or a prime, such that

$$C_0 = c_1 C_1^q\,, \qquad c_1 \in \{\xi^{-1}, -4\xi^{-1}\}\,, \qquad C_1 \in L(\xi)\,,$$

and

$$\frac{x^q}{C_0} - \xi \text{ is reducible over } L(\xi)\,.$$

By Lemma 50 we have $C_0 = cC^q$, $c \in K_0$, $C \in L$ and $x^q - c\xi$ is reducible over $L(\xi)$. This implies, again by Capelli's lemma, that $x^{n_1 q} + a_0 c^{n_1 - m_1} x^{m_1 q} + b_0 c^{n_1}$ is reducible over L, hence over K_0 and the condition follows with $a = a_0 c^{n_1 - m_1}$, $b = b_0 c^{n_1}$.

6. Proof of Theorems 4 and 5

Proof of Theorem 4. According to Theorem 1, if $n \geq 2m$, $a \in K^*$, $B \in K(\mathbf{y}) \setminus K$ and $x^n + ax^m + B(\mathbf{y})$ is reducible over $K(\mathbf{y})$ we have either (i) or (ii). In case (i), no matter whether $n \geq 2m$ or $n < 2m$, if $x^{n_1} + ax^{m_1} + B(\mathbf{y})$ has a linear factor over $K(\mathbf{y})$, say $x - t$, $t \in K(\mathbf{y})$, we have $B(\mathbf{y}) = -t^{n_1} - at^{m_1}$. If $n_1 \geq 4$ and the factor is quadratic of the form $x^2 - t$, we find $t^{n_1/2} + at^{m_1/2} + B(\mathbf{y}) = 0 = (-1)^{n_1} t^{n_1/2} + (-1)^{m_1} t^{m_1/2} + B(\mathbf{y})$ and since at least one of the numbers n_1, m_1 is odd, we have $t^{1/2} \in K(\mathbf{y})$, hence $x^{n_1} + ax^{m_1} + B(\mathbf{y})$ has a linear factor over $K(\mathbf{y})$.

If $n_1 \geq 4$ and the quadratic factor has the middle coefficient different from zero we can write the factor in the form

$$x^2 - ux + u^2 v = \left(x - u\frac{1+\sqrt{1-4v}}{2}\right)\left(x - u\frac{1-\sqrt{1-4v}}{2}\right), \qquad u, v \in K(\mathbf{y})\,,$$

and thus we obtain

$$u^{n_1}\left(\frac{1 \pm \sqrt{1-4v}}{2}\right)^{n_1} + au^{m_1}\left(\frac{1 \pm \sqrt{1-4v}}{2}\right)^{m_1} + B(\mathbf{y}) = 0\,,$$

whence

$$a = -u^{n_1 - m_1}\frac{f_{n_1}(v)}{f_{m_1}(v)}\,, \qquad B(\mathbf{y}) = u^{n_1} v^{m_1}\frac{f_{n_1 - m_1}(v)}{f_{m_1}(v)}\,.$$

The first of the above equations implies that the irreducible curve it describes is of genus 0. We have

$$f_k(v) = \text{const}\prod_{j=1}^{[(k-1)/2]}\left(v - \frac{1}{2 + 2\cos(2j\pi/k)}\right) \tag{70}$$

hence $(f_{m_1}, f_{n_1}) = 1$ and the condition on the genus implies that either $n_1 - m_1 = 1$ or

$$\left[\frac{n_1 - 1}{2}\right] = 1 \tag{71}$$

or $n_1 - m_1 = 2$ and $[\frac{n_1-1}{2}] + [\frac{m_1-1}{2}] = 2$. The last condition gives $2[\frac{n_1-1}{2}] = 3$, which is impossible, hence we have either $n_1 - m_1 = 1$ or, from (71), $n_1 = 4$,

$m_1 = 1$. In the first case we take $t = v$ and obtain

$$u = -a\frac{f_{n_1-1}(t)}{f_{n_1}(t)}\,, \qquad B = \frac{u^{n_1}t^{n_1-1}}{f_{n_1-1}(t)} = (-a)^{n_1}t^{n_1-1}\frac{f_{n_1-1}(t)^{n_1-1}}{f_{n_1}(t)^{n_1}}\,.$$

In the second case we take $t = u^{-1}$ and find $B = B^*_{4,1}(t)$.

In case (ii) we infer that the curve $a = u^{\nu-\mu}A_{\nu,\mu}(v)$ must have at least one irreducible component of genus 0. Examining all the 13 cases we find that this condition is satisfied if and only if $\langle\nu,\mu\rangle = \langle 4,2\rangle$, $\langle 6,2\rangle$ or $\langle 6,3\rangle$.

In each case we take $t = u$ and obtain

- for $\langle\nu,\mu\rangle = \langle 4,2\rangle$,
$$v = \frac{t^2+a}{2t^2}\,, \qquad B = u^4v^2 = B^*_{4,2}(t)\,;$$
- for $\langle\nu,\mu\rangle = \langle 6,2\rangle$,
$$v = \frac{-4t^4+a}{4t^4}\,, \qquad B = -u^6v^2 = B^*_{6,2}(t)\,;$$
- for $\langle\nu,\mu\rangle = \langle 6,3\rangle$,
$$v = \frac{t^3+a}{3t^3}\,, \qquad B = u^6v^3 = B^*_{6,3}(t)\,.$$

It remains to consider the case where $n < 2m$ and $x^{n_1} + ax^{m_1} + B(\mathbf{y})$ has no proper linear or quadratic factor. Then

$$x^n + \frac{a}{B(\mathbf{y})}x^{n_1-m_1} + \frac{1}{B(\mathbf{y})}$$

satisfies (ii), hence there exists an integer l and $\langle\nu,\mu\rangle \in S_0$ such that $n = \nu l$, $n - m = \mu l$ and

$$\frac{a}{B(\mathbf{y})} = u^{\nu-\mu}A_{\nu,\mu}(v)\,, \qquad \frac{1}{B(\mathbf{y})} = u^{\nu}B_{\nu,\mu}(v)\,, \qquad u, v \in K(\mathbf{y})\,.$$

It follows that $au^\mu = A_{\nu,\mu}(v)/B_{\nu,\mu}(v)$ and thus the curve in question has at least one irreducible component of genus 0. Examining all the 13 cases we find that this holds if and only if $\langle\nu,\mu\rangle = \langle 6,1\rangle$, $\langle 6,2\rangle$, $\langle 7,1\rangle$ or $\langle 8,2\rangle$.

If $\langle\nu,\mu\rangle = \langle 6,1\rangle$ or $\langle 7,1\rangle$ we take $t = v$ and obtain

$$u = \frac{A_{\nu,\mu}(t)}{aB_{\nu,\mu}(t)}\,, \qquad B = u^{-\nu}B_{\nu,\mu}(v)^{-1} = B^*_{\nu,\nu-\mu}(t)\,.$$

If $\langle\nu,\mu\rangle = \langle 6,2\rangle$ we take $t = uv$ and obtain

$$v = -\frac{at^2+4}{4}\,, \qquad u = \frac{-4t}{at^2+4}\,, \qquad B = -u^{-6}v^{-2} = B^*_{6,4}(t)\,.$$

Finally, if $\langle\nu,\mu\rangle = \langle 8,2\rangle$ and

$$au^2 = \frac{-v^2+8v-8}{(2v-2)^2}$$

we have

$$a = \left(\frac{v}{u(2v-2)}\right)^2 - 2\left(\frac{v-2}{u(2v-2)}\right)^2,$$

hence

$$a = \alpha^2 - 2\beta^2\,, \qquad \alpha, \beta \in K\,.$$

Taking

$$t = \frac{(v-2) - \beta u(2v-2)}{v - \alpha u(2v-2)}$$

we find

$$\frac{v}{u(2v-2)} = \alpha + \frac{2\alpha - 4\beta t}{2t^2-1}\,, \qquad \frac{v-2}{u(2v-2)} = \beta + t\frac{2\alpha - 4\beta t}{2t^2-1}\,,$$

hence

$$u^{-1} = \alpha + \beta + (t+1)\frac{2\alpha - 4\beta t}{2t^2-1}\,, \qquad v^{-1} = \left(2\left(\alpha + \frac{2\alpha - 4\beta t}{2t^2-1}\right)u - 1\right)^{-1},$$

$$B = u^{-8}(2v-2)^{-2} = B^*_{8,6}(t)\,.$$

Proof of Theorem 5. According to Theorem 1, if $n \geq 2m$, $A \in K(\mathbf{y})\setminus K$, $b \in K^*$ and $x^n + A(\mathbf{y})x^m + b$ is reducible over $K(\mathbf{y})$ we have either (i) or (ii). In case (i) if $x^{n_1} + A(\mathbf{y})x^{m_1} + b$ has a linear factor over $K(\mathbf{y})$, say $x - t$, $t \in K(\mathbf{y})^*$, we have $A(\mathbf{y}) = -t^{n_1-m_1} - bt^{-m_1}$. If $n_1 \geq 4$ and the factor in question is quadratic of the form $x^2 - t$ we find

$$t^{n_1/2} + A(\mathbf{y})t^{m_1/2} + b = 0 = (-1)^{n_1}t^{n_1/2} + A(\mathbf{y})(-1)^{m_1}t^{m_1/2} + b$$

and since at least one of the numbers n_1, m_1 is odd, we have $t^{1/2} \in K(\mathbf{y})$, hence $x^{n_1} + A(\mathbf{y})x^{m_1} + b$ has a linear factor over $K(\mathbf{y})$.

If $n_1 \geq 4$ and the quadratic factor has the middle coefficient different from zero we can write the factor in the form $x^2 - ux + u^2v$ and thus we obtain

$$u^{n_1}\left(\frac{1 \pm \sqrt{1-4v}}{2}\right)^{n_1} + A(\mathbf{y})u^{m_1}\left(\frac{1 \pm \sqrt{1-4v}}{2}\right)^{m_1} + b = 0\,,$$

whence

$$A(\mathbf{y}) = -u^{n_1-m_1}\frac{f_{n_1}(v)}{f_{m_1}(v)}\,, \qquad b = u^{n_1}v^{m_1}\frac{f_{n_1-m_1}(v)}{f_{m_1}(v)}\,.$$

The second of the above equations implies that the irreducible curve it describes is of genus 0. In view of the formula (70) we have $(f_{m_1}(v), vf_{n_1-m_1}(v)) = 1$ and the condition on the genus implies that

$$m_1 + \left[\frac{n_1 - m_1}{2}\right] = 1\,,$$

which is impossible for $n_1 \geq 4$.

In the case (ii) we infer that the curve $b = u^\nu B_{\nu,\mu}(v)$ must have at least one irreducible component of genus 0. Examining all the 13 cases we find that this

condition is fulfilled if and only if $\langle \nu, \mu \rangle = \langle 2p, p \rangle$ (p a prime), $\langle 6, 2 \rangle$, $\langle 8, 2 \rangle$, $\langle 8, 4 \rangle$, $\langle 9, 3 \rangle$.

- If $\langle \nu, \mu \rangle = \langle 2p, p \rangle$ we have $b = (u^2 v)^p$, hence
$$b_1 := u^2 v \in K(\mathbf{y}) \cap \overline{K} = K\,, \qquad v = b_1 u^{-2}\,.$$
- If $\langle \nu, \mu \rangle = \langle 6, 2 \rangle$ we have $b = -(u^3 v)^2$, hence
$$b_1 := u^3 v \in K(\mathbf{y}) \cap \overline{K} = K, \qquad v = b_1 u^{-3}\,.$$
- If $\langle \nu, \mu \rangle = \langle 8, 2 \rangle$ we have $b = (u^4(2v-2))^2$, hence
$$b_1 := u^4(2v-2) \in K(\mathbf{y}) \cap \overline{K} = K\,, \qquad v = 1 + \frac{b_1}{2u^4}\,.$$
- If $\langle \nu, \mu \rangle = \langle 8, 4 \rangle$ we have $b = (u^2 v)^4$, hence
$$b_1 := u^2 v \in K(\mathbf{y}) \cap \overline{K} = K\,, \qquad v = b_1 u^{-2}\,.$$
- If $\langle \nu, \mu \rangle = \langle 9, 3 \rangle$ we have $b = (3u^2(v-3))^3$, hence
$$b_1 := 3u^3(v-3) \in K(\mathbf{y}) \cap \overline{K} = K\,, \qquad v = 3 + \frac{b_1}{3u^3}\,.$$

In every case we take $t = u$ and obtain
$$A(\mathbf{y}) = u^{\nu-\mu} A_{\nu,\mu}(v) = A^*_{\nu,\mu}(t, b_1)\,.$$

PART II

Reducibility over algebraic number fields and, in particular, over $\mathbb{Q}$

7. Proof of Theorem 6 and of the subsequent remarks

Proof of Theorem 6. We begin by defining the sets $F_{\nu,\mu}(K)$ for $\nu \geq 2\mu$. This is done in several steps. First we put $q = (\mu, \nu)$, $\nu_1 = \nu/q$, $\mu_1 = \mu/q$, choose the least non-negative integers ϱ, σ satisfying the equation $\sigma(\nu_1 - \mu_1) - \varrho\nu_1 = 1$ and introduce the fields $L(k, \mu_1, \nu_1)$ and $M(\mu_1, \nu_1, q)$. By Lemma 19 the function $(y_{1q} + \ldots + y_{\nu_1 q})^q$ generating $M(\mu_1, \nu_1, q)$ over $K(t)$ is determined up to a conjugacy. We put

$$S_{\nu,\mu}(K) = \begin{cases} \bigcup_{2<k\leq\nu/2, g^*(k,\mu_1,\nu_1)>1} \{t_0 \in K : t - t_0 \\ \text{is either ramified in } L(k,\mu_1,\nu_1) \\ \text{or has there a prime divisor} \\ \text{of degree 1}\} & \text{if } q = 1, \\ \{\langle t_0, u_0\rangle \in K^2 : \text{ there exists a prime} \\ \text{divisor } \mathfrak{p} \text{ of} \\ M(\mu_1,\nu_1,q) \text{ such that } t \equiv t_0 \bmod \mathfrak{p}, \\ (y_{1q} + \ldots + y_{\nu_1 q})^q \equiv u_0 \bmod \mathfrak{p}\}, & \text{if } q > 1,\ g_*(\mu_1,\nu_1,q) > 1, \\ \emptyset \quad \text{otherwise.} \end{cases}$$

It follows from Lemmas 4 and 19 that $[L(k,\mu_1,\nu_1) : K(t)] = [L^*(k,\mu_1,\nu_1) : \overline{K}(t)]$ and $[M(\mu_1,\nu_1,q) : K(t)] = [M_*(\mu_1,\nu_1,q) : \overline{K}(t)]$, hence K is the exact constant field of $L(k,\mu_1,\nu_1)$ and $M(\mu_1,\nu_1,q)$. Therefore the conditions $t \equiv t_0$, $(y_{1q} + \ldots + y_{\nu q})^q \equiv u_0 \bmod \mathfrak{p}$ and $\langle t_0, u_0\rangle \in K^2$ imply that $\mathfrak{p}$ is either of degree 1 or a ramification divisor. By the Faltings theorem there are only finitely many prime divisors of degree 1 in $L(k,\mu_1,\nu_1)$ or $M(\mu_1,\nu_1,q)$ if $g^*(k,\mu_1,\nu_1) > 1$ or $g_*(\mu_1,\nu_1,q) > 1$, respectively. Hence the sets $S_{\nu,\mu}(K)$ are finite.

Now we introduce auxiliary sets

$$T_{\nu,\mu}(K) = \begin{cases} \bigcup_{t_0 \in S_{\nu,\mu}(K)} \{\langle t_0^{\varrho}, t_0^{\sigma}\rangle\} & \text{if } q = 1, \\ \bigcup_{\langle t_0,u_0\rangle \in S_{\nu,\mu}(K)} \{\langle t_0^{\varrho} u_0^{(\mu-\nu)/q}, t_0^{\sigma} u_0^{-\nu/q}\rangle\} & \text{if } q \text{ is a prime}, \\ \bigcup_{\langle t_0,u_0\rangle \in S_{\nu,\mu}(K)} \{\langle t_0^{\varrho}(-u_0/4)^{(\mu-\nu)/4}, t_0^{\sigma}(-u_0/4)^{-\nu/4}\rangle\} & \text{if } q = 4, \\ \emptyset \quad \text{otherwise.} \end{cases}$$

Finally, we put

$$F_{\nu,\mu}(K) = \begin{cases} \{\langle a,b\rangle \in T_{\nu,\mu}(K) : x^{\nu} + ax^{\mu} + b \text{ is reducible over } K\} & \\ \qquad \text{if } \langle \nu,\mu\rangle \notin S_0 \cup S_1 \text{ or } \langle \nu,\mu\rangle = \langle 9,1\rangle,\ \sqrt{13} \notin K, & \\ \{\langle a,b\rangle \in T_{9,1}(K) : x^9 + ax + b \text{ is reducible over } K\} \cup & \\ \bigcup_{\varepsilon=\pm 1} \{\langle -480053919711226727 + \varepsilon 66936076602084894\sqrt{13}, & \\ \quad \tfrac{1}{2}(-57126885878317063725 + \varepsilon 66644985243629014605\sqrt{13})\rangle\} & \\ \qquad \text{if } \langle \nu,\mu\rangle = \langle 9,1\rangle,\ \sqrt{13} \in K, & \\ \left\{\left\langle 2\cdot 7^{13}, 7^{14}\left(\frac{7+\sqrt{21}}{2}\right)^7\right\rangle, \left\langle 2\cdot 7^{13}, 7^{14}\left(\frac{7-\sqrt{21}}{2}\right)^7\right\rangle\right\} & \\ \qquad \text{if } \langle \nu,\mu\rangle = \langle 21,7\rangle,\ \sqrt{21} \in K, & \\ \emptyset \quad \text{otherwise.} & \end{cases}$$

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

Assume that $x^n + ax^m + b$ is reducible over K. There are two possibilities:

$$x^{n_1} + ax^{m_1} + b \text{ is reducible over } K \tag{72}$$

and

$$x^{n_1} + ax^{m_1} + b \text{ is irreducible over } K. \tag{73}$$

In the case (72), $x^{n_1} + ax^{m_1} + b$ has a proper factor over K of degree $k \le n_1/2$. If $k \le 2$ we have (vi). If $k > 2$ and $g^*(k,m_1,n_1) \le 1$, by Lemmas 15 and 30, 31, 42–46 we have (vii) or (viii) with $l = (m,n)$, $\nu = n_1$, $\mu = m_1$ or one of the exceptional cases (51), (56), (59), (62) with $A = a$, $B = b$. In the cases (51), (56), (59), $x^{n_1} + ax^{m_1} + b$ has the linear factor $x - u \in K[x]$, hence (vi) holds. In the case (62) we obtain (ix) with $l = (m,n)$, $\nu = 9$, $\mu = 1$ by the definition of $F_{\nu,\mu}(K)$.

Now, suppose that $k > 2$ and $g^*(k, m_1, n_1) > 1$. Then by Lemma 15, $\langle n_1, m_1\rangle \notin S_0 \cup S_1 \setminus \{\langle 9, 1\rangle\}$. Put

$$t_0 = a^{-n_1} b^{n_1 - m_1}\,. \tag{74}$$

If r, s are the least non-negative integers satisfying $s(n_1 - m_1) - rn_1 = 1$, by the identity (22) the trinomial $x^{n_1} + t_0^r x^{m_1} + t_0^s$ has a factor of degree k over K. Hence there exists a prime divisor $\mathfrak{P}$ of $L^*(k, m_1, n_1)$ such that $t \equiv t_0$, $y(t) \equiv y_0 \bmod \mathfrak{P}$, where $y(t)$ is the function defined in the proof of Lemma 5 and $y_0 \in K$. Let $\mathfrak{p}$ be a prime divisor of $L(k, m_1, n_1)$ divisible by $\mathfrak{P}$. Since $t_0, y_0 \in K$, $\mathfrak{p}$ is either of degree 1 or a ramification divisor. Thus $t_0 \in S_{n_1,m_1}(K)$, $\langle t_0^r, t_0^s\rangle \in F_{n_1,m_1}(K)$ and (ix) holds with $l = (m, n)$, $\nu = n_1$, $\mu = m_1$, $a_0 = t_0^r$, $b_0 = t_0^s$, $u = a^s b^{-r}$.

In the case (73) by Capelli's lemma

$$x^{(m,n)} - \xi \text{ is reducible over } K(\xi),$$

where $\xi^{n_1} + a\xi^{m_1} + b = 0$.

Further, by Capelli's theorem, there exists a $q \mid (m, n)$ such that either q is a prime and $\xi = \eta^q$, $\eta \in K(\xi)$ or $q = 4$ and $\xi = -4\eta^4$, $\eta \in K(\xi)$. In both cases

$$x^{n_1 q} + ax^{m_1 q} + b \text{ is reducible over } K. \tag{75}$$

If $g_*(m_1, n_1, q) \le 1$, by Lemmas 25 and 31, 33–40, 47, 48 we have either (vii) or (viii) with $l = (m, n)/q$, $\nu = n_1 q$, $\mu = m_1 q$ or (67) with $A = a$, $B = b$. In the last case we have (ix) with $l = (m, n)/7$, $\nu = 21$, $\mu = 7$, by the definition of $F_{\nu,\mu}(K)$.

Now, suppose that $g_*(m_1, n_1, q) \ge 2$ and (74) holds. Then by Lemma 25, $\langle n_1 q, m_1 q\rangle \notin S_0 \cup S_1$. If $\eta_1, \ldots, \eta_{n_1}$ are all the conjugates of η over K we have

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

and by (22),

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

Hence there exists a prime divisor $\mathfrak{P}$ of $M_*(m_1, n_1, q)$ such that

$$t \equiv t_0\,, \qquad (y_{1q} + \ldots + y_{n_1 q})^q \equiv u_0 \bmod \mathfrak{P}\,,$$

where

$$u_0 = \begin{cases} a^{-s} b^r (\eta_1 + \ldots + \eta_{n_1})^q & \text{if } q \text{ is a prime,} \\ -4a^{-s} b^r (\eta_1 + \ldots + \eta_{n_1})^4 & \text{if } q = 4. \end{cases} \tag{76}$$

Let $\mathfrak{p}$ be a prime divisor of $M(m_1, n_1, q)$ divisible by $\mathfrak{P}$. Since $t_0, u_0 \in K$ we have

$$t \equiv t_0\,, \qquad (y_{1q} + \ldots + y_{n_1 q})^q \equiv u_0 \bmod \mathfrak{p}\,.$$

Hence $\langle t_0, u_0\rangle \in S_{n_1q,m_1q}$ and

$$\begin{aligned} &\langle t_0^r u_0^{m_1-n_1}, t_0^s u_0^{-n_1}\rangle \in T_{\nu,\mu}(K) \quad \text{if } q \text{ is a prime,}\\ &\left\langle t_0^r\left(\frac{-u_0}{4}\right)^{m_1-n_1}, t_0^s\left(\frac{-u_0}{4}\right)^{-n_1}\right\rangle \in T_{\nu,\mu}(K) \quad \text{if } q=4\,. \end{aligned} \tag{77}$$

By (74) and (76) the above pairs equal $\langle a(\eta_1+\ldots+\eta_{n_1})^{qm_1-qn_1}, b(\eta_1+\ldots+\eta_{n_1})^{-qn_1}\rangle$ and since

$$\begin{aligned} &x^{qn_1}+a(\eta_1+\ldots+\eta_{n_1})^{qm_1-qn_1}x^{m_1q}+b(\eta_1+\ldots+\eta_{n_1})^{-qn_1}\\ &\quad=(\eta_1+\ldots+\eta_{n_1})^{-qn_1}((x(\eta_1+\ldots+\eta_{n_1}))^{qn_1}+a(x(\eta_1+\ldots+\eta_{n_1}))^{qm_1}+b)\,, \end{aligned}$$

$T_{\nu,\mu}(K)$ can be replaced in (77) by $F_{\nu,\mu}(K)$, by virtue of (75). Thus (ix) holds with

$$l=\frac{(m,n)}{q}\,,\qquad \nu=n_1q\,,\qquad \mu=m_1q\,,\qquad u=\eta_1+\ldots+\eta_{n_1}\,.$$

Assume now that one of the cases (vi)–(ix) holds. (vi) and (ix) imply the reducibility of x^n+ax^m+b in an obvious way, and so do (vii) and (viii) by Lemmas 30–40 and 42–48, respectively.

The proof of Theorem 6 is complete.

The remark following Theorem 6 can be summarized as

LEMMA 51. *For $\langle\nu,\mu\rangle \in S_1$ the sets $E_{\nu,\mu}(\mathbb{Q})$ are infinite, except that*

$$E_{7,2}(\mathbb{Q})=\{\langle -4,4\rangle,\langle -4,-4\rangle\}\,,\qquad E_{21,7}(\mathbb{Q})=\{\langle -49,0\rangle\}\,.$$

Proof. The curve $E_{7,2}$ is equivalent via an affine transformation to a curve listed in the tables [17A] as curve 35A (I owe this information to Professor Karl Rubin). The curves $E_{7,3}$, $E_{9,1}$ and $E_{14,2}$ have rational points of infinite order $\langle 3,108\rangle$, $\langle 16,62\rangle$ and $\langle 5,10\rangle$, respectively. Also the two curves to be taken as $E_{8,1}$, namely $w^2=v^3-10v+12$ and $w^2=v^3-20v-16$ have rational points of infinite order $\langle 3,3\rangle$ and $\langle 5,3\rangle$, respectively. It remains to find all rational points on the curve

$$E_{21,7}: w^2=v^3-1715v+33614\,.$$

The discriminant of the cubic on the right hand side is $-2^8\cdot 7^9$ and using Nagell's theorem (see [4], Theorem 22.1) we easily find that the only rational point of finite order is $\langle -49,0\rangle$. In order to show that there are no rational points of infinite order we notice that by Lemma 41 the curve $E_{21,7}$ is birationally equivalent over $\mathbb{Q}$ to the curve

$$y^2=x^4+294x^2-343\,.$$

By Theorem 8 of [19] the number of generators of infinite order of the group of rational points on the above curve equals $\varrho_1+\varrho_2-2$ where 2^{ϱ_1} is the number of solvable equations

$$s(x^4-588sx^2y^2+s^2\cdot 87808y^4)=z^2 \tag{78}$$

and 2^{ϱ_2} the number of solvable equations

$$t(t^2x^4 + 294tx^2y^2 - 343y^4) = z^2 \tag{79}$$

where s and t run through the squarefree divisors of 87808 and of 343 respectively. The left hand side of (78) is negative for negative s, hence the only relevant values of s are 1, 2, 7 and 14, while the relevant values of t are ± 1, ± 7. For $s = 1$ and 7 the equation (78) has solutions $\langle x, y, z\rangle = \langle 1, 0, 1\rangle$ and $\langle 0, 1, 5488\rangle$, respectively. For $t = 1$ and -7 the equation (79) has solutions $\langle 1, 0, 1\rangle$ and $\langle 0, 1, 49\rangle$, respectively. However, (78) for $s = 2$ and (79) for $t = -1$ are insoluble in $\mathbb{Z}_2$ hence $\varrho_1 = \varrho_2 = 1$ and $\varrho_1 + \varrho_2 - 2 = 0$.

8. Deduction of Consequences 1–3 from Conjecture. Consequence 1 is immediate. In order to deduce Consequence 2 we prove

LEMMA 52. *For every field K and every polynomial $f \in K[x]$ of degree d, $f(x^n)$ has over K an irreducible factor with at most $2d+1$ non-zero coefficients.*

Remark. A special case of this lemma with $K = \mathbb{Q}$ and $d = 1$ was proved in [21].

Proof. Let $g(x)$ be a factor of $f(x)$ irreducible over $K(\zeta_4)$, let $g(\xi) = 0$ and let e be the maximal exponent dividing n such that $\xi = \eta^e$, $\eta \in K(\zeta_4, \xi)$. By Capelli's theorem $x^{n/e} - \eta$ is irreducible over $K(\zeta_4, \xi)$, hence by Capelli's lemma

$$g(x) = N_{K(\zeta_4,\xi)/K(\zeta_4)}(x^{n/e} - \eta)$$

is irreducible over $K(\zeta_4)$ and has at most $[K(\zeta_4, \xi) : K(\zeta_4)] + 1 \le d + 1$ non-zero coefficients. If $g \in K[x]$ we have more than asserted. If $g(x) \notin K[x]$, g and its conjugate $\overline{g}$ over K are coprime and $f_1 = g\overline{g} \in K[x]$ is irreducible over K. Moreover, the number of non-zero coefficients of f_1 does not exceed $2d + 1$.

Deduction of Consequence 2. Suppose that $x^n + ax^m + b$ is reducible over K. Then by Consequence 1, $n_1 \le C_1(K)$. Hence by Lemma 52, $x^n + ax^m + b = (x^{(m,n)})^{n_1} + a(x^{(m,n)})^{m_1} + b$ has an irreducible factor with at most $2C_1(K) + 1$ non-zero coefficients. Hence one can take $C_2(K) = 2C_1(K) + 1$.

From this point onwards reducibility means reducibility over $\mathbb{Q}$. In order to deduce Consequence 3 we show

LEMMA 53. *The trinomial $x^n + bx^m \pm 1$, where $(n, m) = 1$, $n > 2$, $b \in \mathbb{Z}$, $|b| > 2$, has no linear or quadratic factor.*

Proof. In view of symmetry we may assume $n < 2m$, $m > 1$. Linear factors being excluded by $|b| > 2$ we write a supposed quadratic factor as $(x - \alpha)(x - \beta)$, where α, β are conjugate units. It follows that

$$b = \frac{\alpha^n - \beta^n}{\beta^m - \alpha^m}$$

and since $(\alpha^n-\beta^n, \alpha^m-\beta^m) = (\alpha^{(m,n)}-\beta^{(m,n)}) = \alpha-\beta$ and $b \in \mathbb{Z}$ we obtain

$$\frac{\alpha^m-\beta^m}{\alpha-\beta} = \pm 1\,. \tag{80}$$

Since $|b|>2$, α and β cannot be roots of unity, thus they are real and

$$\max\{|\alpha|,|\beta|\} \geq \frac{1+\sqrt{5}}{2}\,, \qquad \min\{|\alpha|,|\beta|\} \leq \frac{\sqrt{5}-1}{2}\,.$$

Hence (80) implies $m=2$, $n=3$ and the existence of a quadratic factor would imply the existence of a linear factor, a contradiction.

Deduction of Consequence 3. By Theorem 6, Lemma 53 and Conjecture the existence of infinitely many integers b with $x^n+bx^m \pm 1$ reducible for some $n \neq 2m$ would imply the existence of fixed $n \neq 2m$ and infinitely many integers b with x^n+bx^m+1 reducible. This, however, is impossible by Theorem 8, since for $a=c=1$ the condition $b_1^2 = -c/a$ is not satisfied by any rational b_1.

Remark. The proof of Theorem 8 to be given in §9 is independent of the present section, thus there is no danger of a vicious circle.

9. Proof of Theorems 7 and 8

Lemma 54. *If $g(t) \in \mathbb{Q}(t)$ takes infinitely many integer values for rational values of t, then*

$$\text{either } g \in \mathbb{Q}[t] \quad \text{or} \quad g(t) = \frac{P(t)}{Q(t)},\ P,Q \in \mathbb{Q}[t],\ \deg P \leq \deg Q\,, \tag{81}$$

where Q is a power of a linear polynomial or of an irreducible quadratic polynomial with a positive discriminant.

Proof. This is the result of [13].

Lemma 55. *Let $F \in \mathbb{Q}[x,y] \setminus \mathbb{Q}$. There exists a finite (possibly empty) subset $S(F)$ of $\mathbb{Q}(t)$ with the following properties*:

(82) *If $g \in S(F)$ then $F(x,g(t))$ has a zero in $\mathbb{Q}(t)$ and (81) holds.*

(83) *The set of integers $y^* \notin \bigcup_{g\in S(F)} g(\mathbb{Q})$ such that $F(x,y^*)$ has an integer zero is finite.*

Proof. Assume first that F is irreducible over $\mathbb{C}$. If the genus of the curve $F(x,y)=0$ is positive we take $S(F)=\emptyset$ and (83) follows from Siegel's theorem. If the genus is zero, by the Hilbert–Hurwitz theorem all but finitely many rational points on the curve are given by $x^*=f(t^*)$, $y^*=g(t^*)$, where $f,g \in \mathbb{Q}(t)$, $t^* \in \mathbb{Q}$. We take $S(F)=\{g(t)\}$ if g satisfies (81), $S(F)=\emptyset$ otherwise and (83) follows from Lemma 54.

Assume now that F is reducible over $\mathbb{C}$, but irreducible over $\mathbb{Q}$. Then the number of rational points on $F(x,y)$ is finite (see [4], p. 196), hence it suffices to take $S=\emptyset$.

Assume finally that $F = \prod_{i=1}^{k} F_i$, where F_i are irreducible over $\mathbb{Q}$. Then we take $S(F) = \bigcup_{i=1}^{k} S(F_i)$.

LEMMA 56. *Let $F \in \mathbb{Q}[x,y]$ be irreducible over $\mathbb{Q}$. Then there exists a finite (possibly empty) subset $R(F)$ of $\mathbb{Q}(t)$ with the following properties*:

(84) *If $g \in R(F)$ then $F(x,g(t))$ is reducible over $\mathbb{Q}(t)$ and* (81) *holds.*

(85) *The set of integers $y^* \notin \bigcup_{g\in R(F)} g(\mathbb{Q})$ such that $F(x,y^*)$ is reducible over $\mathbb{Q}$ is finite.*

P r o o f. This follows from Lemma 55 in the same way as Theorem 33 of [25] follows from Lemma 1 there for $K = \mathbb{Q}$, $r = s = 1$.

R e m a r k. Similar results are stated without proof by M. Fried: in [9] in the special case $F(x,y) = f(x) - y$, in [10] in general. In the former case the possibility $g \notin \mathbb{Q}[t]$ is omitted by mistake (acknowledged in [10], p. 600), in the latter case the condition $\deg P \le \deg Q$ in (81) is replaced by $\deg P = \deg Q$, the possibility of Q being a power of a linear form is omitted and there is no restriction on the discriminant of Q. These changes are permissible, since if Q is a power of a linear form, we may replace g by $g(a + t^{-1})$, where $Q(a) = 0$; if Q is a power of an irreducible quadratic form and $\deg P \le \deg Q$, we may replace g by $g(a + t^{-1})$, where $P(a) \ne 0$.

P r o o f o f T h e o r e m 7. Applying Lemma 56 with $F(x,y) = ax^n + bx^m + y$ we infer from (84) and Theorem 4 that if $n_1 = 5$, $m_1 = 4$ then

$$R(F) = \left\{ -at^5 - bt^4, a\left(\frac{b}{a}\right)^5 \frac{t^2(t-2)^4}{(t^2-3t+1)^5} \right\};$$

if $n_1 = 2$, $m_1 = 1$ and $2 \,|\, (m,n)$ then

$$R(F) = \left\{ -at^2 - bt, a\left(\frac{at^2+b}{2a}\right)^2 \right\};$$

if $n_1 = 4$, $m_1 = 3$ and $2 \,|\, (m,n)$ then

$$R(F) = \left\{ -at^4 - bt^3, \right.$$
$$\left. a\frac{((2\alpha-2\beta)t^2 + (2\alpha-4\beta)t + (\alpha-\beta))^6((2\alpha+2\beta)t^2 - (2\alpha+4\beta)t + (\alpha+\beta))^2}{4(2t^2-1)^8} \right\},$$

where $\alpha^2 - 2\beta^2 = b/a$, $\alpha, \beta \in \mathbb{Q}$ fixed; otherwise

$$R(F) = \{-at^{n_1} - bt^{m_1}\}$$

and (85) implies the theorem. The only point which requires a proof is that the function

$$g(t) = \left(-\frac{b}{a}\right)^{n_1} t^{n_1-1} \frac{f_{n_1-1}(t)^{n_1-1}}{f_{n_1}(t)^{n_1}}$$

occurring in Theorem 4 satisfies the condition (81) only for $n_1 = 5$. To see this let us observe that by (78),

$$(tf_{n_1-1}(t), f_{n_1}(t)) = 1\,,$$

hence $g(t)$ in a reduced form has the denominator

$$f_{n_1}(t)^{n_1} = \prod_{j=1}^{[(n_1-1)/2]} \left(t - \frac{1}{2+2\cos(2j\pi/n_1)}\right)^{n_1}.$$

Therefore for $n_1 > 5$, $g(t)$ has at least three different poles, and for $n_1 = 4$ its numerator is of greater degree than the denominator.

Proof of Theorem 8. Applying Lemma 56 with $F(x,y) = ax^n + yx^m + c$ we infer from (84) and Theorem 5 that if $n = 2m$ then

$$R(F) = \bigcup_{\substack{p\mid m\\ p \text{ prime}\\ b_1 = \sqrt[p]{c/a}\in\mathbb{Q}}} \left\{ -a\left(\frac{t+\sqrt{t^2-4b_1}}{2}\right)^p - a\left(\frac{t-\sqrt{t^2-4b_1}}{2}\right)^p \right\}$$

$$\cup \{a(4t^4 - 8t^2b_1 + 2b_1^2)\}\,,$$

where the last summand occurs only if $4 \mid m$ and $b_1 = \sqrt[4]{c/a} \in \mathbb{Q}$; if $n_1 = 3$, $m_1 = 1$, $2 \mid (m,n)$ and $\sqrt{-ac} \in \mathbb{Q}$ then

$$R(F) = \{4at^4 - 4t\sqrt{-ac}\}\,;$$

otherwise, $R(F) = \emptyset$ and (85) implies the theorem.

10. Proof of Theorem 9 and of Corollary 1

Lemma 57. *Let $A \in \mathbb{C}$ and $T(x) = x^n + Ax^m + 1$. If $|A| > 2$, exactly m zeros of $T(x)$ (counting multiplicities) satisfy the inequality*

$$\left|\log|x| + \frac{1}{m}\log|A|\right| < \frac{1}{m}\log\frac{|A|}{|A|-1} \tag{86}$$

and the remaining $n-m$ zeros satisfy the inequality

$$\left|\log|x| - \frac{1}{n-m}\log|A|\right| < \frac{1}{n-m}\log\frac{|A|}{|A|-1}\,. \tag{87}$$

Remark. Under the conditions of the lemma all zeros of $T(x)$ are simple, but we do not need this in the sequel.

Proof. Since $|Ax^m + 1| \geq |A| - 1 > 1 = |x|^n$ for $|x| = 1$, by Rouché's theorem $T(x)$ has as many zeros inside the unit circle as $Ax^m + 1$, hence m. For each of these zeros we have

$$\pm|Ax^m| \leq |x|^n \pm 1 \leq |x|^n \pm 1\,,$$

hence

$$\frac{1}{|A|+1} \le |x|^m \le \frac{1}{|A|-1}\,,$$

and

$$\log\frac{|A|}{|A|+1} \le m\log|x| + \log|A| \le \log\frac{|A|}{|A|-1}\,,$$

which gives (86). The remaining $n-m$ zeros of $T(x)$ are outside the unit circle and satisfy

$$\pm|x^n| \le \pm|Ax^m| + 1 < \pm|Ax^m| + |x|^m\,,$$

hence

$$|A| - 1 \le |x|^{n-m} \le |A| + 1\,,$$

$$\log\frac{|A|-1}{|A|} \le (n-m)\log|x| - \log|A| \le \log\frac{|A|+1}{|A|}\,,$$

which gives (87).

Lemma 58. *In the notation of Lemma* 57, *if* $(m,n)=1$ *and*

$$|A| \ge \frac{2m(n-m)}{\log 2m(n-m)}\,, \tag{88}$$

then the trinomial $T(x)$ *has no proper monic factor* $f \in \mathbb{C}[x]\setminus\mathbb{C}$ *with* $|f(0)|=1$.

Proof. The condition (88) implies $|A| \ge e$, hence $T(x)$ has no zero on the unit circle, which settles the case $n<4$. Since $|f(0)|=1$ implies $|T(0)f^{-1}(0)|=1$ it is enough to consider the case where $n\ge 4$, $\deg f \le n/2$. Let

$$f(x) = \prod_{j=1}^{r}(x-\xi_j)\prod_{k=1}^{s}(x-\eta_k)\,,$$

where ξ_j satisfy (86) and η_k satisfy (87). The condition $|f(0)|=1$ gives

$$\sum_{j=1}^{r}\log|\xi_j| + \sum_{k=1}^{s}\log|\eta_k| = 0\,,$$

hence by (86) and (87),

$$\left|\frac{r}{m} - \frac{s}{n-m}\right|\log|A| \le \left(\frac{r}{m} + \frac{s}{n-m}\right)\log\frac{|A|}{|A|-1}\,. \tag{89}$$

Since $(m,n)=1$ we have $(m,n-m)=1$, and $r(n-m)-sm=0$ would imply $r\equiv 0 \bmod m$, $s\equiv 0 \bmod (n-m)$, hence either $r=s=0$ or $r=m$, $s=n-m$, $\deg f = n$ contrary to the assumption. Hence

$$|r(n-m)-sm| \ge 1\,. \tag{90}$$

Moreover, if $r \ge (m+1)/2$ we have

$$r(n-m)-sm = rn-(r+s)m \ge \frac{m+1}{2}n - \frac{mn}{2} = \frac{n}{2} \ge 2\,,$$

and similarly if $s \geq (n-m+1)/2$ we have

$$r(n-m) - sm = (r+s)(n-m) - sn$$
$$\leq \frac{n(n-m)}{2} - \frac{n(n-m+1)}{2} = -\frac{n}{2} \leq -2\,.$$

Thus

$$|r(n-m) - sm| \geq 2\,, \qquad \text{unless } r \leq m/2 \text{ and } s \leq (n-m)/2\,. \tag{91}$$

The inequalities (89)–(91) give

$$\frac{\log|A|}{m(n-m)} \leq \log\frac{|A|}{|A|-1}\,. \tag{92}$$

However, $t \log \frac{t}{t-1}$ is a decreasing function of $t > 1$, hence

$$|A| \log\frac{|A|}{|A|-1} \leq e \log\frac{e}{e-1}$$

and (92) gives

$$\frac{|A|\log|A|}{m(n-m)} \leq e\log\frac{e}{e-1}\,.$$

Thus, by (91),

$$2\left(1 - \frac{\log\log 2m(n-m)}{\log 2m(n-m)}\right) \leq e\log\frac{e}{e-1}$$

and

$$2(1-e^{-1}) \leq e\log\frac{e}{e-1}\,,$$

which is false.

Lemma 59. *If $a,b,c \in \mathbb{Z}\setminus\{0\}$, $n > m$ are positive integers and $|b| > |a|^m|c|^{n-m}+1$ then every monic factor $f \in \mathbb{Q}[x]\setminus\mathbb{Q}$ of ax^n+bx^m+c satisfies $|f(0)| = |c/a|^{(\deg f)/n}$.*

Proof. Assume first that $2m \leq n$. Let $f(x) = \prod_{j=1}^{d}(x-\vartheta_j)$. For every j we have

$$a\vartheta_j^{n-m} = -b - c\vartheta_j^{-m}$$

and both sides are algebraic integers since the left hand side may have in the denominator only those prime ideals $\mathfrak{p}$ of $\mathbb{Q}(\vartheta_j)$ for which $\operatorname{ord}_{\mathfrak{p}}\vartheta_j < 0$, and the right hand side only those for which $\operatorname{ord}_{\mathfrak{p}}\vartheta_j > 0$. Hence

$$a\vartheta_j^{n-m} \equiv -c\vartheta_j^{-m} \bmod b \qquad (1 \leq j \leq d)\,,$$

where the congruence is taken in the ring of algebraic integers. Multiplying the obtained congruences we obtain

$$a^d((-1)^d f(0))^{n-m} \equiv (-1)^d e^d((-1)^d f(0))^{-m} \bmod b\,.$$

If both sides of the congruence are equal then

$$|f(0)| = \left|\frac{c}{a}\right|^{d/n}, \tag{93}$$

otherwise

$$|a|^d|f(0)|^{n-m} + |c|^d|f(0)|^{-m} \geq |b|\,. \tag{94}$$

By the same argument applied to the polynomial

$$g(x) = \frac{ax^n + bx^n + c}{af(x)}$$

we infer that either

$$\left|\frac{c}{af(0)}\right| = \left|\frac{c}{a}\right|^{(n-d)/n} \tag{95}$$

or

$$|a|^{n-d}\left|\frac{c}{af(0)}\right|^{n-m} + |c|^{n-d}\left|\frac{c}{af(0)}\right|^{-m} \geq |b|\,. \tag{96}$$

However, (95) implies (93), hence we have either (93), i.e. the assertion of the lemma, or simultaneously (94) and (96). Let us put, for $t > 0$,

$$\varphi_d(t) = |a|^d t^{n-m} + |c|^d t^{-m}\,.$$

The conjunction of (94) and (96) can be written as

$$\min\left\{\varphi_d(|f(0)|),\, \varphi_{n-d}\left(\left|\frac{c}{f(0)}\right|\right)\right\} \geq |b|\,. \tag{97}$$

On the other hand, we have $af(0) \in \mathbb{Z}$ and $cf(0)^{-1} \in \mathbb{Z}$, hence $|a|^{-1} \leq |f(0)| \leq |c|$ and we infer from (97) that

$$M := \max_{|a|^{-1} \leq t \leq |c|} \min\{\varphi_d(t), \varphi_{n-d}(|c/a|t^{-1})\} \geq |b|\,. \tag{98}$$

Now, the function $\varphi_d(t)$ has no local maximum in $(0, \infty)$, and the same applies to $\varphi_{n-d}(|c/a|t^{-1})$.

Consider first the case $d \leq m$. The inequality (98) with the above remark implies that

$$\max\{\varphi_d(|a|^{-1}), \varphi_d(|c|)\} \geq M \geq |b|\,.$$

In view of $d \leq m \leq n - m$ we have

$$\begin{aligned} \varphi_d(|a|^{-1}) &= |a|^{d+m-n} + |c|^d|a|^m \leq 1 + |c|^{n-m}|a|^m\,, \\ \varphi_d(|c|) &= |a|^d|c|^{n-m} + |c|^{d-m} \leq |a|^m|c|^{n-m} + 1\,, \end{aligned} \tag{99}$$

hence

$$|a|^m|c|^{n-m} + 1 \geq |b|\,, \tag{100}$$

contrary to the assumption.

Consider now the case $m < d < n - m$. The equation

$$\varphi_d(t) = \varphi_{n-d}(|c/a|t^{-1})$$

implies

$$t^{n-2m} = |c|^{n-m-d}|a|^{m-d};$$

moreover, denoting the positive root of the latter equation by t_0, we have

$$|a|^{-1} \le t_0 \le |c|\,,$$
$$\varphi_d(t) < \varphi_{n-d}(|c/a|t^{-1}) \quad \text{for } t < t_0\,,$$
$$\varphi_d(t) > \varphi_{n-d}(|c/a|t^{-1}) \quad \text{for } t > t_0\,.$$

Hence, by (98) and the subsequent remark,

$$M = \max\{\varphi_d(|a|^{-1}), \varphi_d(t_0), \varphi_{n-d}(|a|^{-1})\} \ge |b|\,.$$

Now

$$\begin{aligned}
\varphi_d(|a|^{-1}) &= |a|^{d+m-n} + |c|^d|a|^m \le 1 + |c|^{n-m}|a|^m\,,\\
\varphi_d(t_0) &= (|a|^m|c|^{n-m})^{(n-m-d)/(n-2m)} + (|a|^m|c|^{n-m})^{(d-m)/(n-2m)}\\
&\le |a|^m|c|^{n-m} + 1\,,\\
\varphi_{n-d}(|a|^{-1}) &= |a|^{m-d} + |c|^{n-d}|a|^m \le 1 + |c|^{n-m}|a|^m
\end{aligned}$$

hence (100), contrary to the assumption.

Consider next the case $d \ge n - m$. Then

$$\max\{\varphi_{n-d}(|c|),\ \varphi_{n-d}(|a|^{-1})\} \ge M \ge |b|$$

and since $n - d \le m$, by (99) we have again (100), contrary to the assumption.

Finally, assume that $2m > n$. Then $2(n - m) < n$ and since $f(0)^{-1}x^d f(x^{-1})$ is a monic factor of $cx^n + bx^{n-m} + a$ we infer from the already proved case of the lemma that

$$|f(0)^{-1}| = \left|\frac{a}{c}\right|^{d/n},$$

which gives the assertion.

Lemma 60. *If $a, b, c \in \mathbb{Z} \setminus \{0\}$, $n > m$ are positive integers, $(m, n) = 1$ and $ax^n + bx^m + c$ is reducible then either*

$$|b| \le |a|^m|c|^{n-m} + 1 \tag{101}$$

or simultaneously

$$\min\{|a|, |c|\} = 1\,, \qquad |b| \le \frac{2m(n-m)}{\log 2m(n-m)}|a|^{m/n}|c|^{(n-m)/n}$$

and

$$\sqrt[p]{\max\{|a|, |c|\}} \in \mathbb{Z} \quad \textit{for some prime } p \mid n\,.$$

Proof. Suppose that

$$ax^n + bx^m + c = f(x)g(x)\,, \quad \text{where } f, g \in \mathbb{Q}[x] \setminus \mathbb{Q} \text{ and } f \text{ is monic}\,. \tag{102}$$

If (101) does not hold we have, by Lemma 59,

$$|f(0)| = \left|\frac{c}{a}\right|^{(\deg f)/n}, \quad \text{hence } \left|\frac{c}{a}\right|^{1/p} \in \mathbb{Q} \text{ for some prime } p \mid n\,. \tag{103}$$

Choose any value of $(c/a)^{1/n}$ and put

$$A = bc^{-1}\left(\frac{c}{a}\right)^{m/n}. \tag{104}$$

By (102) we have

$$c(x^n + Ax^m + 1) = f\left(\left(\frac{c}{a}\right)^{1/n} x\right) g\left(\left(\frac{c}{a}\right)^{1/n} x\right).$$

The polynomial

$$f_1(x) = \left(\frac{c}{a}\right)^{-(\deg f)/n} f\left(\left(\frac{c}{a}\right)^{1/n} x\right)$$

is a proper monic factor of $x^n + Ax^m + 1$ and by (103),

$$|f_1(0)| = \left|\left(\frac{c}{a}\right)^{-(\deg f)/n} f(0)\right| = 1\,.$$

Hence by Lemma 58,

$$|A| \le \frac{2m(n-m)}{\log 2m(n-m)}$$

and by (104),

$$|b| \le \frac{2m(n-m)}{\log 2m(n-m)} |a|^{m/n} |c|^{(n-m)/n}\,.$$

If $\min\{|a|, |c|\} \ge 2$, then

$$\frac{|a|^m |c|^{n-m} + 2}{|a|^{m/n} |c|^{(n-m)/n}} \ge \frac{2^n + 2}{2} > \frac{n^2/2}{\log n^2/2} \ge \frac{2m(n-m)}{\log 2m(n-m)}\,,$$

thus $|b| < |a|^n |c|^{n-m} + 2$ and (101) holds. If $\min\{|a|, |c|\} = 1$, (103) gives $\sqrt[p]{\max\{|a|, |c|\}} \in \mathbb{Z}$ for some prime $p \mid n$.

Lemma 61. *If $f \in \mathbb{Z}[x]$ is a primitive irreducible polynomial with leading coefficient l,*

$$f(\xi) = 0 \quad \textit{and} \quad \xi = \eta^p, \quad \eta \in \mathbb{Q}(\xi)\,,$$

then $\sqrt[p]{|l|} \in \mathbb{Z}$, $\sqrt[p]{|f(0)|} \in \mathbb{Z}$; moreover, if $p = 2$ then

$$(-1)^{\deg f}\, l f(0) > 0\,. \tag{105}$$

Proof. Let $(\eta) = \mathfrak{a}/\mathfrak{b}$, where $\mathfrak{a}$, $\mathfrak{b}$ are integral ideals of $\mathbb{Q}(\xi)$, $(\mathfrak{a}, \mathfrak{b}) = 1$. We have $(\xi) = \mathfrak{a}^p/\mathfrak{b}^p$ and $\mathfrak{b}^{-p}$ is the content of $x - \xi$, hence $|l|(N\mathfrak{b})^{-p}$ is the content of

f and since f is primitive, $|l| = (N\mathfrak{b})^p$, $\sqrt[p]{|l|} = N\mathfrak{b} \in \mathbb{Z}$, N denoting the absolute norm in $\mathbb{Q}(\xi)$. Now

$$(-1)^{\deg f}\frac{f(0)}{l} = N\xi = (N\eta)^p\,, \tag{106}$$

hence $\sqrt[p]{|f(0)|} = |N\eta|\sqrt[p]{|l|} \in \mathbb{Q}$. Moreover, if $p = 2$ then (106) implies (105).

Lemma 62. *In the notation of Lemma* 61, *if*

$$f(\xi) = 0 \quad \textit{and} \quad \xi = -4\eta^4, \quad \eta \in \mathbb{Q}(\xi), \quad \deg f \equiv 1 \bmod 2 \tag{107}$$

then $lf(0) > 0$ *and either* $\sqrt[4]{|l|} \in \mathbb{Z}$, $\sqrt[4]{4|f(0)|} \in \mathbb{Z}$ *or* $\sqrt[4]{4|l|} \in \mathbb{Z}$, $\sqrt[4]{|f(0)|} \in \mathbb{Z}$.

Proof. Let

$$(2) = \prod_{j=1}^{k}\mathfrak{p}_j^{e_j}\,, \qquad N\mathfrak{p}_j = 2^{f_j}\,,$$

be the factorization of (2) into prime ideals of $\mathbb{Q}(\xi)$.

The equality $(\xi) = (4\eta^4)$ implies that

$$(\xi) = \prod_{j=1}^{k}\mathfrak{p}_j^{a_j}\frac{\mathfrak{a}}{\mathfrak{b}}\,, \qquad a_j \equiv 2e_j \bmod 4 \quad (1 \le j \le k)\,,$$

where $\mathfrak{a}$, $\mathfrak{b}$ are integral ideals of $\mathbb{Q}(\xi)$, $(\mathfrak{a},\mathfrak{b}) = 1$ and $(2,\mathfrak{ab}) = 1$. Arguing as in the proof of Lemma 61 we infer that

$$|l| = 2^{\Sigma'|a_j|f_j}(N\mathfrak{b})^4$$

where the sum $\sum'$ is taken over all j with $a_j < 0$, and

$$\frac{f(0)}{l} = (-1)^{\deg f}N\xi = 4^{\deg f}(N\eta)^4\,.$$

Hence $lf(0) > 0$ and if $\sum' a_jf_j \equiv 0 \bmod 4$ we have

$$\sqrt[4]{|l|} \in \mathbb{Z}\,, \qquad \sqrt[4]{4|f(0)|} = 2^{(\deg f+1)/2}|N\eta|\sqrt[4]{|l|} \in \mathbb{Q}\,.$$

If $\sum' a_jf_j \equiv 2 \bmod 4$ we have

$$\sqrt[4]{4|l|} \in \mathbb{Z}\,, \qquad \sqrt[4]{|f(0)|} = 2^{(\deg f-1)/2}|N\eta|\sqrt[4]{4|l|} \in \mathbb{Q}\,.$$

Proof of Theorem 9. If $t(x) := ax^{n_1} + bx^{m_1} + c$ is reducible then by Lemma 60 we have either (x) or (xi). If $t(x)$ is irreducible we apply Capelli's lemma to $t(x^{(m,n)}) = ax^m + bx^n + c$ and we infer that it is reducible if and only if

$$x^{(m,n)} - \xi \text{ is reducible over } \mathbb{Q}(\xi)\,,$$

where $t(\xi) = 0$. However, by Capelli's theorem the last binomial is reducible if and only if either

$$\xi = \eta^p\,, \qquad \text{where } \eta \in \mathbb{Q}(\xi),\ p \text{ a prime, } p\,|\,(m,n)\,,$$

or

$$\xi = -4\eta^4\,, \qquad \text{where } \eta \in \mathbb{Q}(\xi)\,,\ 4 \,|\, n\,.$$

These conditions give (xii) and (xiii) in virtue of Lemmas 61 and 62.

Proof of Corollary 1. Replacing x by x^{-1}, if necessary, we may assume $n \geq 2m$. Since $n_1 > d$ and $x^n + bx^m \pm 1$ has a factor of degree d, by Capelli's lemma $x^{n_1} + bx^{m_1} \pm 1$ is reducible. Hence by Theorem 9,

$$|b| < \frac{2m_1(n_1 - m_1)}{\log 2m_1(n_1 - m_1)} \leq \frac{2(n-m)^2}{\log 2(n-m)^2}\,. \tag{108}$$

On the other hand, since $|b| > 2$, $x^n + bx^m \pm 1$ has no cyclotomic factors, and also no reciprocal factors since $x^n + bx^m \pm 1 - (x^n \pm bx^{n-m} \pm 1) = b(x^m \pm x^{n-m})$. Therefore by Smyth's result [29] at least one zero ϑ of the factor of degree d satisfies the inequality

$$\log \vartheta \geq \frac{\log \vartheta_0}{d}\,, \qquad \text{where } \vartheta_0^3 - \vartheta_0 - 1 = 0\,.$$

Hence by Lemma 55,

$$\frac{\log \vartheta_0}{d} \leq \frac{1}{n-m} \log \frac{|b|^2}{|b|-1}\,,$$

and by (108),

$$\frac{\log \vartheta_0}{d} \ll \frac{\log(n-m)}{n-m}\,.$$

This gives $n \leq 2(n-m) \ll d \log d$ and by (108), $|b| \ll d^2 \log d$. The constants in the Vinogradov symbols are effective.

11. Proof of Theorem 10 and of Corollary 2

Lemma 63. *Let K be an algebraic number field, $\xi, \eta \in K^*$ and $(\xi, \eta) = \mathfrak{c}/\mathfrak{d}$, where $\mathfrak{c}$, $\mathfrak{d}$ are integral ideals of K. Then*

$$(\xi^n - \eta^n, \xi^m - \eta^m) \,\Big|\, \frac{\mathfrak{c}^{n-(m,n)}}{\mathfrak{d}^{m-(m,n)}} (\xi^{(m,n)} - \eta^{(m,n)})\,.$$

Proof. Let K_1 be an extension of K such that $\mathfrak{c} = (\gamma)$ and $\mathfrak{d} = (\delta)$ are principal ideals of K_1. We then have

$$\xi = \frac{\gamma}{\delta}\xi_1\,, \qquad \eta = \frac{\gamma}{\delta}\eta_1\,,$$

where ξ_1, η_1 are integers of K_1 and $(\xi_1, \eta_1) = 1$. Clearly

$$(\xi^n - \eta^n, \xi^m - \eta^m) \,\Big|\, \frac{\gamma^n}{\delta^m} (\xi_1^n - \eta_1^n,\, \xi_1^m - \eta_1^m)\,. \tag{109}$$

Let $(m,n) = rn - sm$, where r, s are positive integers. We have

$$\xi_1^n - \eta_1^n \,|\, \xi_1^{rn} - \eta_1^{rn}\,, \qquad \xi_1^m - \eta_1^m \,|\, \xi_1^{sm} - \eta_1^{sm}\,,$$

hence

$$(\xi_1^n-\eta_1^n,\xi_1^m-\eta_1^m)\,|\,\xi_1^{rn}-\eta_1^{rn}-\xi_1^{(m,n)}(\xi_1^{sm}-\eta_1^{sm})=\eta_1^{sm}(\xi_1^{(m,n)}-\eta_1^{(m,n)})$$

and by symmetry

$$(\xi_1^n-\eta_1^n,\,\xi_1^m-\eta_1^m)\,|\,\xi_1^{sm}(\xi_1^{(m,n)}-\eta_1^{(m,n)})\,.$$

Since $(\xi_1,\eta_1)=1$ it follows that

$$(\xi_1^n-\eta_1^n,\,\xi_1^m-\eta_1^m)\,|\,\xi_1^{(m,n)}-\eta_1^{(m,n)}=\frac{\delta^{(m,n)}}{\gamma^{(m,n)}}(\xi^{(m,n)}-\eta^{(m,n)})\,,$$

and the lemma follows from (109).

Lemma 64. *In the notation of Lemma* 63 *let* $l=[K:\mathbb{Q}]$, $l_0=[\mathbb{Q}(\xi/\eta):\mathbb{Q}]$. *If* ξ/η *is not a root of unity we have*

$$\log|N(\xi^n-\eta^n)|=n\log\frac{N\mathfrak{c}}{N\mathfrak{d}}+n\frac{l}{l_0}\log M(\xi/\eta)+O\bigg(\frac{l}{l_0}\log M(\xi/\eta)+l_0\bigg)\log n$$

where N *is the absolute norm in* K, $M(\xi/\eta)$ *is the Mahler measure of* ξ/η *and the constant in the* O *symbol depends only on* l_0.

Proof. Let $\xi/\eta=\alpha/\beta$, where $\alpha,\beta\in\mathbb{Q}(\xi/\eta)=K_0$, α, β are integers and $(\alpha,\beta)=\mathfrak{d}_0$. Let S be the set of all isomorphic injections of K_0 into $\mathbb{C}$ and N_0 be the absolute norm in K_0.

In the notation of [24] we have

$$\begin{aligned}w(\alpha/\beta)&:=\log\prod_{\sigma\in S}\max\{|\alpha^\sigma|,|\beta^\sigma|\}-\log N_0\mathfrak{d}_0\\&=\log M(\alpha/\beta)=\log M(\xi/\eta)\,,\end{aligned}\tag{110}$$

since $N_0\mathfrak{d}_0^{-1}\prod_{\sigma\in S}\beta^\sigma$ is the leading coefficient of the primitive irreducible polynomial $N_0\mathfrak{d}_0^{-1}\prod_{\sigma\in S}(\beta^\sigma-\alpha^\sigma)$ which has α/β as a zero. Therefore, by Lemmas 1 and 2 from [24], for all $\sigma\in S$ we have

$$\log|(\alpha^\sigma)^n-(\beta^\sigma)^n|=n\log\max\{|\alpha^\sigma|,\,|\beta^\sigma|\}+O(l_0+\log M(\xi/\eta))\,,$$

where the constant in the O symbol depends only on l_0 and is effectively computable. This gives

$$\log|N_0(\alpha^n-\beta^n)|=n\log\prod_{\sigma\in S}\max\{|\alpha^\sigma|,\,|\beta^\sigma|\}+O(l_0+\log M(\xi/\eta))\log n$$

and by (110),

$$\log|N_0(\alpha^n-\beta^n)|=n\log N_0\mathfrak{d}_0+n\log M(\xi/\eta)+O(l_0+\log M(\xi/\eta))\log n\,,$$

which gives at once

$$\log|N_0(\alpha^n-\beta^n)|=n\log N_0\mathfrak{d}_0+n\frac{l}{l_0}\log M(\xi/\eta)+O\bigg(l+\frac{l}{l_0}\log M(\xi/\eta)\bigg)\log n\,.$$

On the other hand,

$$\left(\frac{\xi^n-\eta^n}{\alpha^n-\beta^n}\right)=\frac{(\xi,\eta)^n}{(\alpha,\beta)^n}=\frac{\mathfrak{c}^n}{\mathfrak{d}^n\mathfrak{d}_0^n}\,,$$

hence

$$\log|N(\xi^n-\eta^n)|=n\log\frac{N\mathfrak{c}}{N\mathfrak{d}}+n\frac{l}{l_0}\log M(\xi/\eta)+O\left(l+\frac{l}{l_0}\log M(\xi/\eta)\right)\log n\,.$$

Proof of Theorem 10. Suppose that the minimal polynomial of ξ, say $f(x)$, is of degree $e\le d$. If for every zero η of f we have ξ/η equal to a root of unity then $\xi^e/N\xi$ is a root of unity and

$$\xi^{(m,n)}=\sqrt[r]{g}\zeta_s\,,$$

where g is a positive integer, not a power with exponent greater than 1 and dividing r. If $\xi^{(m,n)}\in\mathbb{Q}$ we have (xvii); otherwise $\xi^{(m,n)}$ has a conjugate

$$\eta^{(m,n)}=\xi^{(m,n)}\zeta_t^j\,,\qquad j\not\equiv 0 \bmod t\,.$$

Since

$$a\xi^n+b\xi^m+c=a\eta^n+b\eta^m+c=0 \tag{111}$$

and $\zeta_t^{jn/(m,n)}=\zeta_t^{jm/(m,n)}=1$ is impossible we obtain

$$\xi^{(m,n)}\in\mathbb{Q}(\zeta_t),\qquad\text{hence}\qquad\sqrt[r]{g}\in\mathbb{Q}(\zeta_s,\zeta_t)\,.$$

It follows (see [17]) that $r=1$ or 2. If $r=1$ then by Mann's theorem [14], $s\mid 6$ and we have (xvii). If $r=2$ the equation

$$a(\sqrt{g}\zeta_s)^{n/(m,n)}+b(\sqrt{g}\zeta_s)^{m/(m,n)}+c=0$$

gives a representation of $\sqrt{g}$ as a linear combination of two roots of unity. Hence squaring and using Mann's theorem again we obtain $s=8$, $g=2q^2$ or $s=12$, $g=3q^2$, $q\in\mathbb{Q}$, which gives (xvii).

It remains to consider the case where for a certain zero η of f we have ξ/η different from roots of unity. Let $K=\mathbb{Q}(\xi,\eta)$ be of degree l and let $(\xi,\eta)=\mathfrak{c}/\mathfrak{d}$, where $\mathfrak{c}$, $\mathfrak{d}$ are integral ideals of K, $(\mathfrak{c},\mathfrak{d})=1$. We infer from (111) that

$$\mathfrak{c}^m\mid c\,,\qquad\mathfrak{d}^{n-m}\mid a\,,$$

hence

$$m\log N\mathfrak{c}\le l\log|c|\,,\qquad(n-m)\log N\mathfrak{d}\le l\log|a|\,. \tag{112}$$

On the other hand,

$$a(\xi^n-\eta^n)=b(\eta^m-\xi^m)\,, \tag{113}$$

hence

$$\xi^n-\eta^n\,\Big|\,\frac{b}{(a,b)}(\eta^m-\xi^m)$$

and

$$\xi^n-\eta^n\,\Big|\,\frac{b}{(a,b)}(\xi^n-\eta^n,\,\xi^m-\eta^m)\,.$$

By Lemma 63 this gives

$$(\xi^n-\eta^n)\,\Big|\,\frac{b}{(a,b)}\,\frac{\mathfrak{c}^{n-(m,n)}}{\mathfrak{d}^{m-(m,n)}}(\xi^{(m,n)}-\eta^{(m,n)})\,,$$

hence

$$\begin{aligned}\log|N(\xi^n-\eta^n)| &\le l\log\frac{|b|}{(a,b)}+(n-(m,n))\log N\mathfrak{c}\\ &\quad-(m-(m,n))\log N\mathfrak{d}+\log|N(\xi^{(m,n)}-\eta^{(m,n)})|\,.\end{aligned}$$

Now we apply Lemma 64 and obtain

$$\begin{aligned}&n(\log N\mathfrak{c}-\log N\mathfrak{d})+n\frac{l}{l_0}\log M(\xi/\eta)+O\bigg(\frac{l}{l_0}\log M(\xi/\eta)+l\bigg)\log n\\ &\qquad\le l\log\frac{|b|}{(a,b)}+(n-(m,n))\log N\mathfrak{c}-(m-(m,n))\log N\mathfrak{d}\\ &\qquad\quad+(m,n)(\log N\mathfrak{c}-\log N\mathfrak{d})+(m,n)\frac{l}{l_0}\log M(\xi/\eta)\\ &\qquad\quad+\bigg(\frac{l}{l_0}\log M(\xi/\eta)+l\bigg)\log(m,n)\end{aligned}$$

and thus by (112),

$$\begin{aligned}(n-(m,n))\log M(\xi/\eta) &\le l_0\log\frac{|b|}{(a,b)}+(n-m)\frac{l_0}{l}\log N\mathfrak{d}\\ &\quad+O(\log M(\xi/\eta)+l_0)\log n\\ &\le l_0\log\frac{|ab|}{(a,b)}+O(\log M(\xi/\eta)+l_0)\log n\,.\end{aligned}\tag{114}$$

Let $B_0(l_0)$ be the constant in the O-symbol, and

$$B_1(l_0)=\inf\log M(\theta)\,,$$

where the infimum is taken over all algebraic numbers θ of degree l_0 different from roots of unity. By Dobrowolski's theorem [7] or by earlier results $B_1(l_0)>0$. Let $c_0(d)$ be the unique solution of the equation

$$\frac{n}{\log n}=4\sup_{l_0\le d(d-1)}B_0(l_0)\bigg(1+\frac{l_0}{B_1(l_0)}\bigg)\,.$$

Since $(m,n)\le\frac12 n$ and $l_0\le d(d-1)$, for $n>c_0(d)$ the inequality (114) implies

$$\frac12 n\log M(\xi/\eta)\le l_0\log\frac{|ab|}{(a,b)}+\frac14 n\log M(\xi/\eta)\,,$$

hence (xiv) holds with

$$c_1(d)=\sup_{l_0\le d(d-1)}\frac{4l_0}{B_1(l_0)}\,.$$

(xv) is obtained from (xiv) on replacing ξ by ξ^{-1}, with c taking the role of a.

In order to obtain (xvi) we assume without loss of generality that $n < 2m$. (If $n > 2m$ we replace ξ by ξ^{-1}, then m is replaced by $n - m$.) We infer from (113) that

$$\xi^m - \eta^m \mid a(\xi^n - \eta^n)$$

and since $\xi^m - \eta^m \mid a(\xi^m - \eta^m)$ we have

$$\xi^m - \eta^m \mid a(\xi^n - \eta^n,\ \xi^m - \eta^m)\,.$$

By Lemma 63 this gives

$$(\xi^m - \eta^m) \,\Big|\, (a)\frac{\mathfrak{c}^{n-(m,n)}}{\mathfrak{d}^{m-(m,n)}}(\xi^{(m,n)} - \eta^{(m,n)})\,,$$

hence

$$\begin{aligned}\log|N(\xi^m - \eta^m)| &\le l\log|a| + (n-(m,n))\log N\mathfrak{c}\\ &\quad - (m-(m,n))\log N\mathfrak{d} + \log|N(\xi^{(m,n)} - \eta^{(m,n)})|\,.\end{aligned}$$

Now we apply Lemma 64 and obtain

$$\begin{aligned}m\log N\mathfrak{c} - m\log N\mathfrak{d} + m\frac{l}{l_0}\log M(\xi/\eta) + O\Big(\frac{l}{l_0}\log M(\xi/\eta) + l\Big)\log m&\\ \le l\log|a| + (n-(m,n))\log N\mathfrak{c} - (m-(m,n))\log N\mathfrak{d}&\\ + (m,n)\log N\mathfrak{c} - (m,n)\log N\mathfrak{d} + (m,n)\frac{l}{l_0}\log M(\xi/\eta)&\\ + O\Big(\frac{l}{l_0}\log M(\xi/\eta) + l\Big)\log(m,n)\,,&\end{aligned}$$

thus by (112),

$$\begin{aligned}(m-(m,n))\log M(\xi/\eta) &\le l_0\log|a| + (n-m)\frac{l_0}{l}\log N\mathfrak{c}\\ &\quad + O(\log M(\xi/\eta) + l_0)\log m\\ &\le l_0\log|ac| + O(\log M(\xi/\eta) + l_0)\log n\,.\end{aligned}$$

Since $n < 2m$, by considering a few cases we find $m - (m,n) \ge n/3$, hence for $n > c_0(d)$ we obtain

$$\frac{1}{3}\log M(\xi/\eta) \le l_0\log|ac| + \frac{1}{4}n\log M(\xi/\eta)\,,$$

which implies (xvi) by the definition of $c_1(d)$.

Proof of Corollary 2. If ξ is a zero of the factor in question, then ξ is an algebraic unit, hence (xvii) would imply that ξ is a root of unity, impossible for $|b| > 2$. Therefore by Theorem 10 we have (xvi), which for $a = c = 1$ gives $n < c_0(d)$. However, by Theorem 8, for every n there exist only finitely many reducible trinomials $x^n + bx^m + 1$ with $n \ne 2m$.

Table 5. Sporadic trinomials over $\mathbb{Q}$

The table contains all reducible trinomials $x^n + Ax^m + B$, $n \geq 2m$, $A, B \in \mathbb{Z} \setminus \{0\}$, known to the author, which satisfy neither (vi) nor (vii) nor (viii) and have the following properties: 1) for every divisor $d > 1$ of (n, m), $x^{n/d} + Ax^{m/d} + B$ is irreducible, 2) (A^n, B^{n-m}) is free from $n(n-m)$th powers, 3) if $n - m$ is odd then $A > 0$, if n, m are both odd, then $B > 0$.

Number	Trinomial	Factor	Discoverer
1	$x^8 + 3x^3 - 1$	$x^3 + x - 1$	Łutczyk
2	$x^8 + 2^3 \cdot 3x^3 + 2^5$	$x^3 - 2x^2 + 4$	Nicolas
3	$x^8 + 2^2 \cdot 3^3 x^3 + 3^5$	$x^3 + 3x^2 + 9x + 9$	Nicolas
4	$x^8 + 3 \cdot 5 \cdot 7^3 \cdot 59x^3 - 2^3 \cdot 7^5 \cdot 11^3$	$x^3 - 7x^2 - 98x + 2156$	Schinzel
5	$x^9 - 2^2 \cdot 19x + 2^5 \cdot 3$	$x^4 - 2x^2 - 4x + 6$	Schinzel
6	$x^9 + 2^5 x^2 - 2^6$	$x^3 - 2x^2 + 4x - 4$	Nicolas
7	$x^9 + 3^4 x^2 - 2 \cdot 3^3$	$x^3 + 3x + 3$	Nicolas
8	$x^9 + 3^6 x^2 - 2 \cdot 3^6$	$x^3 - 3x^2 + 9$	Browkin
9	$x^9 + 3^5 x^4 + 2^2 \cdot 3^6$	$x^3 - 3x^2 + 18$	Browkin
10	$x^9 + 2^4 \cdot 3^5 x^4 - 2^8 \cdot 3^6$	$x^3 + 6x^2 + 36x + 72$	Nicolas
11	$x^{10} + 3^3 \cdot 11x - 3^5$	$x^3 + 3x - 3$	Schinzel
12	$x^{10} + 2^6 \cdot 3^3 \cdot 5^6 \cdot 11x - 2^7 \cdot 3^5 \cdot 5^5 \cdot 19$	$x^4 - 60x^2 - 300x + 5400$	Browkin
13	$x^{10} + 3x^3 - 2^3$	$x^4 + x^3 - x - 2$	Morain
14	$x^{10} + 2^5 x^3 - 2^6$	$x^5 - 2x^4 + 8x - 8$	Morain
15	$x^{10} + 3^2 \cdot 11x^3 + 2 \cdot 3^3$	$x^3 + 3x + 3$	Nicolas
16	$x^{11} + 2^2 \cdot 3x + 2^3$	$x^5 - 2x^4 + 2x^3 - 2x^2 + 2$	Nicolas
17	$x^{11} + 2^3 \cdot 3^3 \cdot 23x^2 - 2^4 \cdot 3^5$	$x^3 + 6x - 6$	Browkin
18	$x^{11} + 2^2 \cdot 23x^3 + 2^3 \cdot 3$	$x^3 + 2x^2 + 4x + 2$	Morain
19	$x^{11} + x^4 + 2^2$	$x^5 - x^3 - x^2 + 2$	Jonassen

Table 5 (cont.)

Number	Trinomial	Factor	Discoverer
20	$x^{11} - 3^3 \cdot 5^2 \cdot 23x^5 + 3^8 \cdot 5^4$	$x^3 - 15x - 45$	Browkin
21	$x^{12} + 2^6 \cdot 3^2 x + 2^4 \cdot 23$	$x^3 + 2x^2 + 4x + 2$	Browkin–Schinzel
22	$x^{12} + 2^5 \cdot 3^4 \cdot 13x + 2^4 \cdot 3^4 \cdot 23$	$x^3 + 6x + 6$	Browkin
23	$x^{12} + 2^6 x^5 - 2^8$	$x^3 - 2x^2 + 4x - 4$	Morain
24	$x^{13} + 2^8 \cdot 3x + 2^{10}$	$x^3 + 2x^2 + 4x + 4$	Browkin
25	$x^{13} + 2^8 \cdot 3 \cdot 53x - 2^{12} \cdot 7$	$x^3 - 4x^2 + 8x - 4$	Browkin–Schinzel
26	$x^{13} + 2^8 \cdot 3 \cdot 5^6 \cdot 53x + 2^{11} \cdot 5^7 \cdot 13$	$x^3 + 20x + 100$	Browkin
27	$x^{13} - 2^6 \cdot 3 \cdot 5^5 \cdot 53x^3 + 2^8 \cdot 5^8 \cdot 11$	$x^3 + 20x - 100$	Browkin
28	$x^{13} + 3x^4 - 1$	$x^3 + x^2 - 1$	Coray
29	$x^{13} + 2^6 \cdot 3x^4 - 2^9$	$x^3 + 2x^2 + 4x + 4$	Browkin
30	$x^{13} + 3^3 \cdot 53x^4 - 2^2 \cdot 3^6$	$x^3 - 3x^2 + 6$	Browkin
31	$x^{13} + 3x^6 + 1$	$x^4 - x + 1$	Coray
32	$x^{13} + 2^4 \cdot 3x^6 - 2^8$	$x^3 - 2x^2 + 4x - 4$	Browkin
33	$x^{14} + 2^2 x + 3$	$x^3 - x^2 + 1$	Bremner
34	$x^{14} + 2^2 x^5 - 1$	$x^3 + x^2 - 1$	Bremner
35	$x^{14} + 2^2 \cdot 3^6 x^5 + 3^{11}$	$x^4 - 3x^3 + 9x^2 - 18x + 27$	Morain
36	$x^{15} - 3^7 \cdot 5^6 \cdot 31x + 2^2 \cdot 3^8 \cdot 5^5 \cdot 29$	$x^3 + 15x - 45$	Browkin
37	$x^{15} - 2^4 \cdot 7^3 \cdot 31x^7 + 2^{11} \cdot 3 \cdot 7^5$	$x^3 - 14x - 28$	Browkin
38	$x^{16} + 7x^3 + 3$	$x^3 - x^2 + 1$	Bremner
39	$x^{16} + 2^3 \cdot 7x^3 - 3^2$	$x^3 + x^2 + x - 1$	Bremner
40	$x^{16} + 2^8 x^7 + 2^{12}$	$x^4 - 2x^3 + 4x^2 - 8x + 8$	Morain
41	$x^{16} + 2^8 \cdot 7x^7 - 2^{15}$	$x^3 + 2x^2 - 8$	Bremner
42	$x^{17} + 103x + 2^3 \cdot 7$	$x^3 - x^2 + x + 1$	Bremner

Table 5 (cont.)

Number	Trinomial	Factor	Discoverer
43	$x^{17} + 2^{12} \cdot 103x^4 - 2^{16} \cdot 3^2$	$x^3 + 2x^2 + 4x - 8$	Browkin
44	$x^{21} + 2^{11} \cdot 13x^5 + 2^{14} \cdot 3$	$x^3 - 2x^2 + 4$	Browkin
45	$x^{22} + 2^{14} \cdot 23x - 2^{15} \cdot 13$	$x^3 + 2x^2 - 4$	Browkin
46	$x^{24} + 2^{11} \cdot 7x + 2^8 \cdot 47$	$x^3 - 2x^2 + 2$	Browkin–Schinzel
47	$x^{26} + 2^7 \cdot 3 \cdot 53x^3 + 2^8 \cdot 47$	$x^3 - 2x^2 + 2$	Browkin–Schinzel
48	$x^{33} + 67x^{11} + 1$	$x^3 + x + 1$	Bremner
49	$x^{39} + 2^9 \cdot 3 \cdot 157x^{13} + 2^{13}$	$x^3 + 2x + 2$	Browkin
50	$x^{46} + 2^{26} \cdot 47x^7 - 2^{31} \cdot 3^2$	$x^3 - 2x^2 + 4x - 4$	Browkin
51	$x^{51} - 2^{31} \cdot 103x^5 + 2^{34} \cdot 47$	$x^3 - 2x^2 + 4x - 4$	Browkin
52	$x^{52} + 2^{34} \cdot 3 \cdot 53x + 2^{35} \cdot 103$	$x^3 + 2x^2 + 4x + 4$	Browkin

References

[1] A. Bremner, *On reducibility of trinomials*, Glasgow Math. J. 27 (1981), 155–156.

[2] —, *On trinomials of type* $x^n + Ax^m + 1$, Math. Scand. 49 (1981), 145–155.

[3] A. Capelli, *Sulla riduttibilità delle equazioni algebriche*, *Nota prima*, Rend. Accad. Sci. Fis. Mat. Soc. Napoli (3) 3 (1897), 243–252.

[4] J. W. S. Cassels, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. 41 (1966), 193–291.

[5] C. Chevalley, *Introduction to the Theory of Algebraic Functions of One Variable*, New York, 1951.

[6] A. Choudhry and A. Schinzel, *On the number of terms in the irreducible factors of a polynomial over* $\mathbb{Q}$, Glasgow Math. J. 34 (1992), 11–15.

[7] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. 34 (1979), 391–401.

[8] M. Eichler, *Einführung in die Theorie der algebraischen Zahlen und Funktionen*, Birkhäuser, Basel–Stuttgart, 1963.

[9] M. Fried, *On the Diophantine equation* $f(y) - x = 0$, Acta Arith. 19 (1971), 79–87.

[10] —, *Exposition on an arithmetic-group theoretic connection via Riemann's existence theorem*, in: Proc. Sympos. Pure Math. 37, Amer. Math. Soc., 1980, 571–602.

[11] M. Fried and A. Schinzel, *Reducibility of quadrinomials*, Acta Arith. 21 (1972), 153–171.

[12] K. Győry and A. Schinzel, *On a conjecture of Posner and Ramsey*, J. Number Theory, to appear.

[13] E. Maillet, *Détermination des points entiers des courbes algébriques unicursales à coefficients entiers*, C. R. Acad. Sci. Paris 168 (1919), 217–220.
[14] H. Mann, *On linear relations between roots of unity*, Mathematika 12 (1965), 107–117.
[15] T. Nagell, *Sur la réductibilité des trinômes*, in: Comptes rendus du 8. congrès des mathématiciens scandinaves, Stockholm, 1934, 273–275.
[16] —, *Sur la classification des cubiques planes du premier genre par des transformations birationnelles dans un domaine de rationalité quelconque*, Nova Acta Regiae Soc. Sci. Upsaliensis (4) 12 (1941), No. 8.
[17] —, *Contributions à la théorie des corps et des polynômes cyclotomiques*, Ark. Mat. 5 (1963), 153–192.
[17A] *Numerical tables on elliptic curves*, in: Modular Functions of One Variable IV, Lecture Notes in Math. 476, Springer, Berlin, 1975.
[18] L. Rédei, *Algebra. Erster Teil*, Akad. Verlagsges. Geest & Portig K.-G., Leipzig, 1959.
[19] H. Reichardt, *Über die Diophantische Gleichung* $ax^4+bx^2y^2+cy^4 = ez^2$, Math. Ann. 117 (1940), 235–276.
[20] P. Ribenboim, *On the factorization of* $x^n - Bx - A$, Enseign. Math. 37 (1991), 191–200.
[21] A. Schinzel, *Some unsolved problems on polynomials*, in: Neki nerešeni problemi u matematici, Mat. Bibl. 25, Zavod Izd. Udžb., Belgrade, 1963, 63–70.
[22] —, *Reducibility of lacunary polynomials I*, Acta Arith. 16 (1969), 123–159.
[23] —, *Reducibility of polynomials*, in: Computers in Number Theory, Academic Press, London, 1971, 73–75.
[24] —, *Primitive divisors of the expression* $A^n - B^n$ *in algebraic number fields*, J. Reine Angew. Math. 268/269 (1974), 27–33.
[25] —, *On linear dependence of roots*, Acta Arith. 28 (1975), 161–175.
[26] —, *Selected Topics on Polynomials*, University of Michigan Press, Ann Arbor, 1982.
[27] E. S. Selmer, *On the irreducibility of certain trinomials*, Math. Scand. 4 (1956), 287–302.
[28] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Preuß. Akad. Wiss., Phys.-math. Kl. 1929 Nr 1.
[29] C. J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*, Bull. London Math. Soc. 3 (1971), 169–175.
[30] N. Tschebotarëw und H. Schwerdtfeger, *Grundzüge der Galois'schen Theorie*, Noordhoff, Groningen–Djakarta, 1950.
[31] G. Turnwald, *On Schur's conjecture*, J. Austral. Math. Soc. Ser. A, to appear.
[32] K. Th. Vahlen, *Über reductible Binome*, Acta Math. 19 (1895), 195–198.