Compositio Mathematica **139:** 263–295, 2003.
© 2003 Kluwer Academic Publishers. Printed in the Netherlands.

The Equation $f(X) = f(Y)$ in Rational Functions $X = X(t)$, $Y = Y(t)$

ROBERTO M. AVANZI[1] and UMBERTO M. ZANNIER[2]
[1] *Institut für Experimentelle Mathematik, Universität Essen, Ellernstraße 29, 45326 Essen, Germany. e-mail: mocenigo@exp-math.uni-essen.de*
[2] *Istituto Universitario di Architettura DCA, Santa Croce 191, 30135 Venice, Italy. e-mail: zannier@dimi.uniud.it*

(Received: 21 December 2001; accepted 1 July 2002)

Abstract. We determine all the complex polynomials $f(X)$ such that, for two suitable distinct, nonconstant rational functions $g(t)$ and $h(t)$, the equality $f(g(t)) = f(h(t))$ holds. This extends former results of Tverberg, and is a contribution to the more general question of determining the polynomials $f(X)$ over a number field K such that $f(X) - \lambda$ has at least two distinct K-rational roots for infinitely many $\lambda \in K$.

Mathematics Subject Classifications (2000). Primary: 14H45; Secondary: 11C08, 11D41, 11G30, 11R09, 12D05, 12E05.

Key words. diophantine equations, equations admitting rational functions as solutions, reducibility.

1. Introduction

In this paper the following classification problem is solved.

PROBLEM 1.1. Determine all the polynomials $f(X) \in \mathbb{C}[X]$ such that there exist two distinct rational functions $g(t), h(t) \in \mathbb{C}(t) \backslash \mathbb{C}$ with

$$f(g(t)) = f(h(t)).$$

This is equivalent to asking for which $f(X)$ the polynomial

$$F_f(X, Y) := \frac{f(X) - f(Y)}{X - Y}$$

has an absolutely irreducible factor whose associate curve has genus zero: such a factor will be in this paper always called a *genus zero factor*.

A more general question is that of determining the polynomials f over a number field K such that $f(X) - \lambda$ has at least *two* K-rational roots for infinitely many $\lambda \in K$. If these conditions are satisfied, then $F_f(X, Y)$ has a factor of genus at most one by Faltings' establishment of the Mordell Conjecture [Fa]. In this light, the present paper may be regarded as a contribution to this problem.

Some problems akin to ours have already been solved. They deal with particular cases of the question of determining all the pairs f, g of polynomials over a number

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

field K, such that their image sets over K have infinite intersection. Again, a factor of $f(X) - g(Y)$ must have genus zero or one. Necessary conditions for this to happen under the assumption $(\deg(f), \deg(g)) = 1$ are given in [R] for the genus zero case (see also [Z1]), and in [AZ] for the genus one case. The question regarding the intersection of the value sets of f and g over the ring of integers of K has been fully answered by Bilu and Tichy [BT].

Helge Tverberg determined in [Tv, Ch. 2] the polynomials $F_f(X, Y)$ over $\mathbb{C}$ with a linear or quadratic factor under the assumption that f is *indecomposable* (that is, f cannot be written as a composition of two polynomials of degree larger than 1). His result is that f is essentially a *cyclic* (i.e. of the form t^n) or a *Chebyshev* polynomial (see Section 2.2 below for a review of known facts about such polynomials). Similarly, Yuri Bilu [B] determined all the polynomials $f(X) - g(Y)$ with a quadratic factor.

Our Theorems 1 and 2 below represent a twofold extension of Tverberg's result: First, we impose a much weaker condition on the factor and, second, we remove the assumption that f is indecomposable. Theorem 1 deals with the polynomials $F_f(X, Y)$. We solve first the case where f is indecomposable (Proposition 4.1), then we turn to the general case. Now if $f = S(X)^r$ then $F_f(X, Y)$ has factors of the form $S(X) - c\,S(Y)$, where $c \neq 1$ is a root of unity. We must solve the two problems of their reducibility (the case of indecomposable S suffices, and is done in Theorem 3) and of their classification under the assumption they have a genus zero factor. We need only the case where c is a root of unity, but it does no harm to work under the more general assumption $c \in \mathbb{C}\backslash\{0, 1\}$. This is done in Theorem 2.

Moreover, we determine also the solutions $X = g(t)$ and $Y = h(t)$ to the equation $f(X) = cf(Y)$ (in both cases where $c = 1$ and $c \neq 1$): It will be clear upon reading the statements of Theorems 1 and 2 that it will both suffice and save space to write the solutions with $g \neq h$ and for the case of f indecomposable only. (They are given in Propositions 4.7 and 5.6.)

A noteworthy application of the polynomials $F_f(X, Y)$ is found in Fried's work [Fr1] on the Conjecture of Schur. We use many tools developed by him, in particular Proposition 2.4 below.

Before stating our results, let us spend a word on the notation used. The polynomials $P_1, \ldots, P_6$ are given later in Definition 2.1: There are polynomials of type P_1 of degree n for any integer $n \geqslant 3$, whereas the degrees of $P_2, \ldots, P_6$ are fixed. The cyclic polynomial of degree n is denoted by $Z_n(t)$, and T_n denotes the Chebyshev polynomial of degree n.

THEOREM 1. *Let $f(t) \in \mathbb{C}[t]$. The polynomial $F_f(X, Y)$ has a genus zero factor if and only if there exist a polynomial $A \in \mathbb{C}[t]$ and a linear polynomial $M \in \mathbb{C}[t]$ such that one of the following cases occur:*

(1) *$f = A \circ Z_m \circ S$ where $m > 2$, and $S \in \mathbb{C}[t]$ is such that $S(X) - \zeta S(Y)$ has a genus zero factor for some mth root of unity $\zeta \neq 1$.*

(2) *$f = A \circ T_n \circ M$ with $n > 2$.*

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

(3) $f = A \circ P_1 \circ M$ *with* $\deg(P_1) \geqslant 4$.
(4) $f = A \circ P_2 \circ M$.
(5) $f = A \circ P_3 \circ M$.

In the case (1) *if* $P(X, Y)$ *is a genus zero factor of* $F_f(X, Y)$ *there is a unique mth root of unity* $\zeta \neq 1$ *such that* $P(X, Y)$ *divides* $S(X) - \zeta S(Y)$. *Theorem* 2 *below characterises such* ζ *and* S.

Theorem 1 is completely explicit in the case where f is indecomposable. In this case A and S are linear. In other words, f is linearly related to one of Z_n, T_n, P_1, P_2 or P_3 according to the following definition.

DEFINITION 1.2. Two polynomials $f, g \in \mathbb{C}[t]$ are said to be linearly related (abbreviated: l.r.) if there exist two nonconstant linear polynomials ℓ_1 and ℓ_2 such that $g = \ell_2 \circ f \circ \ell_1$.

THEOREM 2. *Let* $f(t) \in \mathbb{C}[t]$ *and* $c \in \mathbb{C} \setminus \{0, 1\}$. *The polynomial* $f(X) - cf(Y)$ *has a genus zero factor if and only if either* f *is linear or we can find a decomposition* $f = f_0 \circ f_1$, *where* f_0 *is an indecomposable polynomial of degree* $n > 1$, *such that at least one of the following statements holds.*

(1) $f_0 = \alpha Z_n$ (*n a prime*) *and* f_1 *is such that* $f_1(X) - \zeta f_1(Y)$ *has a genus zero factor for some nth root of unity* $\zeta \in \mathbb{C}$.
(2) $f_0 = \alpha T_n$ (*n a prime*). *If* $c \neq -1$, *then* $n = 2$ *and* f_1 *is linear. If* $c = -1$, *then either* $f = \alpha T_{\deg(f)} \circ M$ *for a linear polynomial* M *or* $n > 2$ *and* $f_1(X) + f_1(Y)$ *has a genus zero factor.*
(3) $f_0 = t^r g(t^d)$ *which is not linearly related to a cyclic or a Chebyshev polynomial where* g *is a nonconstant polynomial with* $g(0) \neq 0$ *and* r, d *are coprime integers with* $r > 0$ *and* $d \geqslant 2$; *Also, c is a dth root of unity and* $f_1(X) - c^{r'} f_1(Y)$ *has a genus zero factor where* r' *is an integer satisfying* $rr' \equiv 1 \pmod{d}$.
(4) $f_0 = \alpha P_1$ *with* $c \neq 1$ *and* f_1 *is linear.*
(5) $f_0 = \alpha(T_3 + d)$ *where* $d \in \mathbb{C} \setminus \{0, \pm 2\}$, *with*

$$c = \frac{d+2}{d-2} \quad \text{or} \quad c = \frac{d-2}{d+2},$$

and f_1 *is linear.*
(6) $f_0 = \alpha P_4$ *with* $c = -1$ *and* f_1 *is linear.*
(7) $f_0 = \alpha P_5$ *with* $c = \omega$ *or* ω^2 *and* f_1 *is linear.*
(8) $f_0 = \alpha P_6$ *with* $c = -1$ *and* f_1 *is linear.*

Suppose $P(X, Y)$ *is a genus zero factor of* $f(X) - cf(Y)$. *In the case* (1), $P(X, Y)$ *divides* $f_1(X) - \zeta f_1(Y)$ *for a unique nth root of unity* $\zeta \in \mathbb{C}$. *In the case* (2) *with* $c = -1$ *and* $f \neq \alpha T_{\deg(f)} \circ M$, $n > 2$ *the polynomial* $P(X, Y)$ *divides* $f_1(X) + f_1(Y)$ *but not* $f(X) + f(Y)/f_1(X) + f_1(Y)$. *In the case* (3), $P(X, Y)$ *divides* $f_1(X) - c^{r'} f_1(Y)$.

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

Let us consider case (1) of Theorem 1 and suppose S is not linear. We may apply Theorem 2 below with S in place of f: the result is that there is a decomposition $S = f_0 \circ f_1$ where f_0 is an explicitly given indecomposable polynomial and f_1 also satisfies the assumptions of Theorem 2. Repeated application of Theorem 2 thus gives a functional decomposition of S, which, by Ritt's theory, is essentially unique (see for example [To]).

Consider now the polynomials of Theorem 2(3). It is an easy fact that $f(t) = t^r g(t^d)$ if and only if $f(t)$ satisfies an equation $f(\zeta t) = cf(t)$ where clearly $c = \zeta^{\deg(f)} = \zeta^r$ and ζ is a dth root of unity. Such a polynomial is not necessarily indecomposable, but all its composition factors are of the same type: this is easily seen by the argument of [Z2, Lemma 6].

THEOREM 3. *Let $f \in \mathbb{C}[t]$ be indecomposable and such that $f(X) - cf(Y) - c'$, where $c \in \mathbb{C}^*$ and $c' \in \mathbb{C}$, is reducible. If $c = 1$, then $c' = 0$. If $c \neq 1$, we may replace $f(t)$ by $f(t) + c'/(1-c)$ to assume $c' = 0$. Then we fall into one of the following cases.*

(1) $f(t) = a(t+b)^n$. *For some $a \in \mathbb{C}^*$, $b \in \mathbb{C}$. Now c can be any complex number.*
(2) $f(t) = aT_n(t+b)$ *(with n an odd prime) for some $a \in \mathbb{C}^*$, $b \in \mathbb{C}$. Now $c = -1$.*
(3) $f(t) = (t+b)^r g((t+b)^d)$ *for some $b \in \mathbb{C}$, for some coprime integers $r > 0$, $d \geqslant 2$ and some nonconstant $g \in \mathbb{C}[t]$. Also, c must be a dth root of 1.*

It is worth observing that in all three cases of the above theorem the polynomial $f(X) - cf(Y)$ is indeed reducible. To show this, observe that $\deg(f) > 1$. Case (1) is trivial, and the factorisation in case (2) is well known (see Proposition 2.2 below). In case (3) assume $b = 0$ for simplicity: Since $f(\zeta X) = cf(X)$ where $c = \zeta^r \neq 1$ for a suitable dth root of unity ζ, we see at once that $X - \zeta Y$ divides $f(X) - cf(Y)$.

We shall deduce Theorem 3 from a property of certain automorphisms of permutation groups for which we have found no reference: as far as we know this is a new result. We state it separately.

THEOREM 4. *Let G be a doubly transitive subgroup of Σ_n (the symmetric group on n letters) containing an n-cycle γ and let ϕ be an automorphism of G fixing γ. Denote by G_i the stabiliser of i in G. Then either $\phi(G_1)$ is transitive or ϕ is induced by a conjugation in Σ_n.*

It is possible to derive this result as a consequence of the Classification of the Finite Simple Groups (CFSG). However, we think it is worthwhile to provide CFSG-free proofs whenever possible. The combination of techniques used in our proof also seems to be new.

In Section 2 we shall set up some definitions, and summarize the relevant material on Chebyshev polynomials and a genus formula. Section 3 is devoted to the study of the reducibility of polynomials of the form $f(X) - cf(Y) - c'$ (Theorems 3 and 4),

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

necessary in the proofs of our first two theorems, which are presented in the last two sections.

2. Auxiliary Definitions and Results

2.1. THE SPORADIC POLYNOMIALS

We now define the polynomials $P_1,\dots,P_6$. As usual, ω denotes a fixed primitive cubic root of unity.

DEFINITION 2.1.

$P_1(t)=P_1(t;l,m):=t^l(t+1)^m$ with l and m coprime and $l+m\geqslant 3$.

$P_2(t)=P_2(t;a,b):=t(t+a)^2(t+b)^2$, where $a,b\in\mathbb{C}^*$ satisfy the equation $9a^2-2ab+9b^2=0$.

$P_3(t)=P_3(t;a,b):=t(t+a)^3(t+b)^3$, where $a,b\in\mathbb{C}^*$ satisfy $a^2-5ab+8b^2=0$.

$P_4(t)=P_4(t;a,b):=t^4-\frac{4}{3}(a+b)t^3+2abt^2$, where $a,b\in\mathbb{C}^*$ satisfy $a^2-\xi ab+b^2=0$ with $\xi^2-2\xi+2=0$.

$P_5(t)=P_5(t;a,b):=t^4-\frac{4}{3}(a+b)t^3+2abt^2+1$, where $(a+\bar{\omega})^3+2=0$ and $b+1=(1-a)\omega$.

$P_6(t)=P_6(t;a,b):=t(t+a)^2(t+b)^2$, where $a,b\in\mathbb{C}^*$ satisfy

$$a^2-\frac{22+5\xi}{9}ab+b^2=0 \quad\text{and}\quad \xi^2+\xi+4=0.$$

These polynomials define covers of the Riemann Sphere ramified over at most four points, as it will be clear from the proofs. Some of them have been already been found independently while investigating three points ramified covers: For example, Birch gives in [Schn, Page 41] the polynomial $t^3(t^2+5t+40)=(t-3)(t^2+4t+24)^2$ $+1728$, which is l.r. to $P_2(t)$. His $(t+3)^3(t-2)^2=t^2(t^3+5t^2-5t-45)+$ 108 is l.r. to $P_1(t;3,2)$.

2.2. CHEBYSHEV POLYNOMIALS

Following [Sch1] we define the *normalised Chebyshev polynomials* $T_d(X)$ by

$$T_0(X)=2,\quad T_1(X)=X,\quad T_{d+1}(X)=XT_d(X)-T_{d-1}(X).$$

They are precisely the polynomials such that

$$T_d(z+z^{-1})=z^d+z^{-d}.$$

They also satisfy the relation $T_d\circ T_e=T_{de}=T_e\circ T_d$.

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

PROPOSITION 2.2. *The polynomials* $T_n(X) \pm T_n(Y)$ *split into factors of degree at most two. More precisely, if we define*

$$\begin{aligned}\Upsilon_{n,k}(X, Y) &= X^2 - 2XY\cos(\pi k/n) + Y^2 - 4\sin^2(\pi k/n),\\ \Psi_n(X, Y) &= (X - Y) \prod_{1 \leqslant k \leqslant \frac{n-1}{2}} \Upsilon_{n,k}(X, Y)\end{aligned} \tag{1}$$

and

$$\Phi_n(X, Y) = \prod_{\substack{1 \leqslant k < n\\ k \equiv 1 \pmod 2}} \Upsilon_{n,k}(X, Y), \tag{2}$$

then

$$T_n(X) - T_n(Y) = \begin{cases} (X + Y)\Psi_n(X, Y) & \text{if } n \text{ is even},\\ \Psi_n(X, Y) & \text{if } n \text{ is odd};\end{cases} \tag{3}$$

and

$$T_n(X) + T_n(Y) = \begin{cases} \Phi_n(X, Y) & \text{if } n \text{ is even},\\ (X + Y)\Phi_n(X, Y) & \text{if } n \text{ is odd}.\end{cases} \tag{4}$$

The factors in the right-hand side of (1) *and of* (2) *are absolutely irreducible.*

We do not know the first instances of these formulae. A proof of (3) can be found in [Sch2]. Formula (4), which is an easy corollary of (3), is in [DLS].

PROPOSITION 2.3 ([Sch 1, Lemma 9 on page 26]). *Let* K *be a field. The equation*

$$(Q(t) - q_1)(Q(t) - q_2) = (t - \xi_1)(t - \xi_2)R^2(t)$$

with $q_1, q_2, \xi_1, \xi_2 \in K$, $q_1 \neq q_2$, $\xi_1 \neq \xi_2$ *and* $Q, R \in K[t]$ *implies* $Q(t) = L \circ T_{\deg(Q)} \circ M^{-1}$, *where*

$$L(t) = \pm\frac{(q_1 - q_2)}{4}t + \frac{(q_1 + q_2)}{2} \quad \text{and} \quad M(t) = \frac{(\xi_1 - \xi_2)}{4}t + \frac{(\xi_1 + \xi_2)}{2}.$$

PROPOSITION 2.4 ([Fr1, Theorem 1]). *Let* $f(X) \in \mathbb{C}[X]$ *be an indecomposable polynomial. If* $f(X)$ *is not linearly related to a cyclic or a Chebyshev polynomial, then* $(f(X) - f(Y))/(X - Y)$ *is absolutely irreducible.*

2.3. THE GENUS FORMULA

A rational function $f(t) \in \mathbb{C}(t)$ is viewed as a map from $\mathbb{P}^1 := \mathbb{P}^1(\mathbb{C})$ to itself, and expressions like $f(\infty)$ and $f(t_0) = \infty$ are allowed.

Write $f = f_1/f_2$ where f_1 and f_2 are coprime polynomials. The *degree* of f is defined as $\max\{\deg(f_1), \deg(f_2)\}$. The degree so defined is multiplicative with respect to composition.

For any $f(t) \in \mathbb{C}(t)$ let Ω_f denote the splitting field of $f(t) - Z$ in a fixed algebraic closure of $\mathbb{C}(Z)$ (if we write $f = f_1/f_2$ as above, Ω_f is the splitting field of $f_1(t) - f_2(t)Z$).

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

For any extension $\Omega/\mathbb{C}(Z)$, an *infinite place* of Ω is a place lying above the place of $\mathbb{C}(Z)$ corresponding to $Z=\infty$ (which is the infinite place of $\mathbb{C}(Z)$).

DEFINITION 2.5. For $f(X)\in\mathbb{C}(X)$ and $\lambda\in\mathbb{P}^1$ let $h(\lambda)$ be the number of the distinct roots of $f(X)-\lambda$, and $r_1(\lambda),\dots,r_h(\lambda)$, with $h=h(\lambda)$, be their multiplicities. Let $\mu(\lambda)=\mu_f(\lambda)$ be the number of simple roots of $f(t)-\lambda^{\star}$.

For $g(Y)\in\mathbb{C}(Y)$, consider $g(Y)-\lambda$ and define $k(\lambda)$ and $s_1(\lambda),\dots,s_k(\lambda)$, $k=k(\lambda)$ in an analogous way.

PROPOSITION 2.6 ([Fr3, Proposition 2]). *Let $f(t)$, $g(t)\in\mathbb{C}(t)$ and define the numbers $h(\lambda)$, $k(\lambda)\,r_i(\lambda)$ and $s_j(\lambda)$ as in* 2.5 *for all $\lambda\in\mathbb{P}^1:=\mathbb{P}^1(\mathbb{C})$.*

If $f(X)-g(Y)$ is irreducible, then it defines a curve of genus $\mathfrak{g}$, where

$$2\,(\deg(f)+\mathfrak{g}-1)=\sum_{\lambda\in\mathbb{P}^1}\sum_{i=1}^{h(\lambda)}\sum_{j=1}^{k(\lambda)}\big(r_i(\lambda)-(r_i(\lambda),s_j(\lambda))\big). \tag{5}$$

If $(f(X)-f(Y))/(X-Y)$ is irreducible then it defines a curve of genus $\mathfrak{g}$, where

$$2\,(\deg(f)+\mathfrak{g}-2)=\sum_{\lambda\in\mathbb{P}^1}\sum_{i=1}^{h(\lambda)}\sum_{j=1}^{h(\lambda)}\big(r_i(\lambda)-(r_i(\lambda),r_j(\lambda))\big). \tag{6}$$

DEFINITION 2.7. Let $f(t)$ be a polynomial. We call λ a *special point* for f if and only if $\mu_f(\lambda)<n$ (i.e. if $f(t)-\lambda$ has a multiple root). We denote by $\Lambda(f)$ the set of the special points of f.

The special points of f are precisely the finite branch points of the cover $\mathbb{P}^1\to\mathbb{P}^1$ given by $X\mapsto f(X)$. Then formula (5) gives the genus of the fibred product of the covers f and g.

3. Reducibility of $f(X)-cf(Y)-c'$

In this Section we shall give proofs of Theorems 3 and 4.

Davenport, Lewis and Schinzel [DLS] posed the general problem of the reducibility of arbitrary polynomials $f(X)-g(Y)$. Fried [Fr2] solved the case where at least one of f, g is indecomposable, assuming a conjecture in group theory which has been later proved a consequence of the CFSG: Cassou-Noguès and Couveignes [CC] make Fried's results in some sense more explicit and review the required tools. The general case when f and g are not indecomposable is still open.

As already mentioned, the case that interests us can be solved without resorting to CFSG, the crucial step being provided by Theorem 4.

*We include notationally the case $\lambda=\infty$, where we formally replace $f(t)-\lambda$ by $f(t)^{-1}$, i.e. consider the poles of $f(X)$.

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

Proof of Theorem 4. We may assume $n \geqslant 3$. Suppose that $\phi(G_1)$ is intransitive. We have to prove that ϕ is induced by a conjugation in Σ_n.

The proof is divided in two parts. In the first part, we shall consider the natural representation ρ of G in $\mathrm{GL}_n(\mathbb{C})$: We shall show that ρ and $\rho \circ \phi$ are isomorphic, i.e. there exists a matrix M such that $M\rho(g)M^{-1} = \rho(\phi(g))$ for all g in G. We also find a matrix N closely related to M and of finite order. In the second part we shall use the eigenvalues of N to construct relations involving roots of unity, to which we shall apply certain arithmetical considerations to deduce that M can be replaced by a permutation matrix (i.e. the conclusion of the theorem).

Part 1: *permutation representations and matrix action*. We may assume that G acts on $\Omega := \{1, 2, \dots, n\}$, which we identify with $\mathbb{Z}/n\mathbb{Z}$, and that γ is the cycle $(1, 2, \dots, n)$. We shall use simple facts from the theory of linear representation of finite groups, for which we refer to [Se].

We consider the representation ρ of G in $\mathrm{GL}_n(\mathbb{C})$ associated to the action of G on Ω: If $e_1, \dots, e_n$ is the canonical basis of $\mathbb{C}^n$, we define $\rho(g)$, for $g \in G$, to be the linear map sending e_i to $e_{g(i)}$. It is well known (see, e.g. [Se, Section 2.4, Exercise 2.6]) that ρ is the sum of two irreducible representations. One is the unit representation and the corresponding space U is one dimensional generated by $v_1 := \sum e_i$. The other one is a degree $n-1$ representation ρ_1: The corresponding space consists of the vectors whose coordinates in the basis $\{e_i\}$ sum up to zero and a basis for it is given by the vectors $v_j := e_1 - e_j$ for $2 \leqslant j \leqslant n$.

Denote by H the orbit of $1 \in \Omega$ under $\phi(G_1)$ and define $H + t := \{x + t \,:\, x \in H\}$.

We can assume without loss of generality that 1 belongs to a *smallest* orbit of $\phi(G_1)$ on Ω, so $h := \#H \leqslant n/2$.

Let $\rho^* := \rho \circ \phi$. We proceed to show that ρ and ρ^* are isomorphic representations.

Define $e_t^* = \sum_{x \in H+(t-1)} e_x$ for $1 \leqslant t \leqslant n$. If $g \in G$ and $gs = t$, then we can write $g = \gamma^{t-1} g_1 \gamma^{-(s-1)}$ with $g_1 \in G_1$, which shows that $\phi(g)(H + (s-1)) = H + (t-1)$. Therefore the sets $H + t$ form one G-orbit. Equivalently, the vectors $\{e_t^*\}$ are conjugate under the action of $\rho(G)$. They span a $\rho(G)$-invariant subspace of $\mathbb{C}^n$ of dimension larger than 1 (since we assumed $\phi(G_1)$ intransitive, we may find t such that $1 \notin H + (t-1)$: thus e_1^* and e_t^* are linearly independent) and containing U, therefore they span the whole space and are linearly independent.

Moreover if $\rho(g)e_s = e_t$ then $\rho^*(g)e_s^* = e_t^*$, implying that the representation ρ^* is obtained from ρ by a change of representation module. In particular

$$M\rho(g)M^{-1} = \rho^*(g) = \rho(\phi(g)) \quad \text{for all g} \in G, \tag{7}$$

where M is the basis change matrix from the basis $\{e_i^*\}$ to the basis $\{e_i\}$, whose column vectors are the coordinates of the e_i^* with respect to the basis $\{e_i\}$. It is a so-called *circulant* matrix. (A matrix is called *circulant* if, for each column vector $(y_0, y_1, \dots, y_{n-1})^t$ the next column at its right is given by $(y_{n-1}, y_0, \dots, y_{n-2})^t$.) Each of its entries are either 0 or 1.

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

We note at once that if $h = 1$, then M is a permutation matrix and thus ϕ is induced by a conjugation by a suitable power of γ: it suffices to look at the position of the unique entry 1 in each of the columns.

Therefore we shall suppose from now on that $h \geqslant 2$ and derive a contradiction.

Let ϕ have order r. Then, by (7), $M^r\rho(g)M^{-r} = \rho(\phi^r(g)) = \rho(g)$ for $g \in G$, so M^r lies in the centraliser $\mathcal{C}$ of $\rho(G)$ in $\mathrm{GL}_n(\mathbb{C})$.

In view of the above decomposition of ρ, $\mathcal{C}$ is conjugate to the group $\mathcal{D}$ of diagonal $n \times n$ nonsingular matrices of the form $\mathrm{diag}(c, d, \ldots, d)$. (This follows from the irreducibility of ρ_1, taking into account e.g. Schur's Lemma [Se, Section 2.2, Prop. 4].) In fact $\mathcal{D} = X^{-1}\mathcal{C}X$ where X is the basis change matrix whose column vectors are the coordinates of $v_1, v_2, \ldots, v_n$ with respect to the canonical basis $\{e_i\}$. It follows that the elements of $\mathcal{C}$ have the form $aI + bJ$ where J is the matrix whose entries are all equal to 1 (it suffices to verify that $X\mathrm{diag}(c, d, \ldots, d) = (dI + (c-d)/(n)J)X$).

In particular $M^r = aI + bJ$ for some $a \in \mathbb{C}^*$, $b \in \mathbb{C}$.

Consider the equation $(yM + zJ)^r = I$ for unknowns $y \in \mathbb{C}^*$ and $z \in \mathbb{C}$. Using the fact that $JM = MJ = hJ$ and $J^2 = nJ$ we see that

$$(yM + zJ)^r = ay^rI + \left(by^r + \sum_{t=1}^{r}\binom{r}{t}(yh)^{r-t}n^{t-1}z^t\right)J.$$

Fix any y_0 such that $y_0^r = 1/a$ and observe that the coefficient of J in the above expansion, upon setting $y = y_0$, is a nonconstant polynomial in z, so it has a root z_0. Hence $(y_0M + z_0J)^r = I$. Put $N := y_0M + z_0J$.

Now N is a circulant matrix such that $N^r = I$ whose entries take only two values, namely z_0 and $y_0 + z_0$, the latter taken exactly h times in each column. It can be proved that N acts on $\rho(G)$ like M, i.e. that $M\rho(g)M^{-1} = N\rho(g)N^{-1}$ for all $g \in G$. As we shall not make use of this fact, its proof is omitted.

Part 2 : *constructing relations among roots of unity*. It is well known how to compute the eigenvalues of a $n \times n$ circulant matrix, e.g. by noting that, for a primitive nth root of unity θ, the nonsingular matrix $\Xi := (\theta^{ij})_{i,j=0}^{n-1}$ diagonalises it. The result is that the eigenvalues of a circulant matrix whose first column is the vector $(y_0, y_1, \ldots, y_{n-1})^t$, say, are the numbers $y_0 + \theta^k y_1 + \cdots + \theta^{(n-1)k}y_{n-1}$ for $0 \leqslant k < n$. In particular those of N, which are rth roots of unity, are given by $\xi_k = (y_0 + z_0)\sum_{t\in H}\theta^{tk} + y_0\sum_{t\notin H}\theta^{tk}$ for $0 \leqslant k < n$. Put

$$\sigma(k) := \sum_{t\in H}\theta^{tk} \quad \text{and} \quad \lambda := \frac{1}{z_0}.$$

Then

$$\sigma(k) = \xi_k\lambda \quad \text{for } k \not\equiv 0 \pmod{n} \quad \text{and} \quad \sigma(0) = h. \tag{8}$$

Multiplying N, and thus also y_0, z_0, by a suitable rth root of unity, we can assume without loss of generality that $\xi_1 = 1$, so $\lambda = \sigma(1) \in \mathbb{Z}[\theta]$.

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

We have, by Parseval's formula,

$$|\lambda|^2(n-1)=\sum_{k=1}^{n-1}|\sigma(k)|^2=\sum_{k=0}^{n-1}\sigma(k)\overline{\sigma(k)}-h^2=nh-h^2=h(n-h).$$

Put

$$m:=|\lambda|^2=\frac{h(n-h)}{n-1}$$

The number $\lambda=\sigma(1)$ being an algebraic integer, $m\in\mathbb{N}$. As $h\neq 1, n-1$ we have $m>1$.

If n is even, then $\sigma(n/2)$ is a rational integer, so the equation $m=|\lambda|^2=|\sigma(n/2)|^2$ implies that m is a square. This however holds also for odd n, as we shall now see.

If $k\not\equiv 0\,(\bmod\, n)$ we have $m=|\lambda|^2=|\sigma(k)|^2=\sigma(k)\sigma(-k)=\lambda^2\xi_k\xi_{-k}$. Also, $\lambda^2=\xi_k^{-2}\sigma(k)^2$, whence

$$m=\xi_k^{-1}\xi_{-k}\sigma(k)^2\in\mathbb{Z}[\theta^k].$$

This implies in particular that $\xi_k^{-1}\xi_{-k}$ is a root of unity in $\mathbb{Q}(\theta^k)$, whence it is ± a power of θ^k.

Let now p be a prime dividing n (so p is odd). We consider the last displayed relation, with $k=n/p$. In this case, one of the two numbers $\pm\xi_k^{-1}\xi_{-k}$ is a pth root of unity, so $\pm m$ is a square in $\mathbb{Q}(\theta^k)$, for a suitable choice of the sign. Since the unique quadratic subfield of $\mathbb{Q}(\theta^k)$ is (for $k=n/p$) one of the fields $\mathbb{Q}(\sqrt{\pm p})$, we deduce that either $m=u^2$ or $m=pu^2$ for some positive integer u.

If m is of the form pu^2, then n must be a power of p (otherwise we apply the above argument with two distinct prime factors of n to get a contradiction). But then the equality $m=\frac{h(n-h)}{n-1}$ implies that p divides m with even exponent: in fact, if p divides m, then it must divide h (because $(n-1)m=h(n-h)\equiv -h^2\,(\bmod\, p)$). And now, if $p^a\|h$ then $p^a\|n-h$, so $p^{2a}\|m$. This is a contradiction, thus in any case $m=u^2$ is a square and

$$\frac{h(n-h)}{n-1}=m=u^2. \tag{9}$$

Also, $\lambda=\pm u\theta^q$ for some integer q. In fact, equations (8) imply that

$$\lambda^2\xi_k\xi_{-k}=\sigma(k)\sigma(-k)=|\sigma(k)|^2=m=u^2,$$

so λ/u is a root of unity which lies in $\mathbb{Q}(\theta)$ (since λ does), and the conclusion follows.

Since $\lambda\equiv 0\,(\bmod\, u)$, we have by (8) that $\sigma(k)\equiv 0\ (\bmod\, u)$ for $k\not\equiv 0\,(\bmod\, n)$. Pick now $s\in\Omega\backslash H$. Applying Fourier inversion to the defining expression for $\sigma(k)$ yields

$$\sum_{k=0}^{n-1}\sigma(k)\theta^{-sk}=\sum_{t\in H}\left(\sum_{k=0}^{n-1}\theta^{(t-s)k}\right)=0.$$

This implies that the congruence $\sigma(k)\equiv 0$ (mod) u holds in fact for all integers k.

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

Let now p be a prime factor of u (if $u = 1$, then $h = 1$ or $h = n - 1$ by (9), two cases which we exclude) and write $n = PQ$ where P is a power of p, say $P = p^a$ (possibly $P = 1$), and Q is a positive integer coprime to p. Also, write $\theta = \pi\chi$, where π (resp. χ) is a primitive Pth (resp. Qth) root of unity. Let x and y be arbitrary integers. By the Chinese Remainder Theorem we may find an integer $k = k(x, y)$ such that $k \equiv x \pmod P$ and $k \equiv y \pmod Q$. Then $\pi^k = \pi^x$ and $\chi^k = \chi^y$, so $\theta^{tk} = \pi^{tx}\chi^{ty}$. Therefore, for all pairs of integers x, y we have

$$\sigma(k) = \sum_{t\in H} \pi^{tx}\chi^{ty} \equiv 0 \pmod u.$$

By Fourier inversion with respect to y, we obtain that

$$Q \sum_{\substack{t\in H\\ t\equiv t_0 \pmod Q}} \pi^{tx} = \sum_{y=0}^{Q-1}\left(\sum_{t\in H} \pi^{tx}\chi^{ty}\right)\chi^{-t_0 y} \equiv 0 \pmod u,$$

for all pairs of integers t_0, x. Since p divides u and does not divide Q, we find

$$\sum_{\substack{t\in H\\ t\equiv t_0 \pmod Q}} \pi^{tx} \equiv 0 \pmod p. \tag{10}$$

Put now $x = 1$. We may pick t_0 such that the l.h.s. of (10) does not vanish, for otherwise $\sigma(k)$ would vanish for some k (actually for all $k \equiv 1 \pmod P$)). Also, no two terms in this sum can be equal, for they would correspond to distinct values $t, t' \in \Omega$ such that $t \equiv t'$ both modulo Q and modulo P. Hence, on putting $\epsilon_t = 1$ if t is congruent modulo P to some element of H and $t \equiv t_0 \pmod Q$, and $\epsilon_t = 0$ otherwise, equation (10) becomes

$$0 \neq T := \sum_{t=0}^{P-1} \epsilon_t \pi^t \equiv 0 \pmod p.$$

Now π has degree $f := \varphi(P) = (p-1)p^{a-1}$ over $\mathbb{Q}$, with minimal polynomial $\Phi(X) := (X^{p^a} - 1)/(X^{p^{a-1}} - 1) = 1 + X^{p^{a-1}} + \cdots + X^f$. We may use the equation $\Phi(\pi) = 0$ to express a power π^b, for $P > b \geqslant f$, as the sum $-\pi^{b-f} - \cdots - \pi^{b-p^{a-1}}$. In this way we obtain a (possibly) new expression for T, namely

$$T = \sum_{t=0}^{f-1} (\epsilon_t - \epsilon_{t_*})\pi^t,$$

where t_* is the unique integer $\equiv t \pmod{p^{a-1}}$ and such that $f \leqslant t_* < P$.

Further, every algebraic integer in $\mathbb{Q}(\theta)$ lies in $\mathbb{Z}[\theta]$, whence it may be written uniquely as a linear combination of $1, \pi, \ldots, \pi^{f-1}$ with coefficients in $\mathbb{Z}$. Upon writing $T = u\xi$, where ξ is an algebraic integer, we see that p divides $\epsilon_t - \epsilon_{t_*}$ (in $\mathbb{Z}$) for $t = 0, \ldots, f-1$. But $\epsilon_t - \epsilon_{t_*} \in \{0, \pm 1\}$ (and $p \geqslant 2$), so all these differences vanish and $T = 0$. This contradiction finally proves the Theorem. □

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

LEMMA 3.1. (i) *Let $f, g \in \mathbb{C}(X)$ with f indecomposable. If $f(X) - g(Y)$ is reducible, then $\Omega_g \supseteq \Omega_f$. Therefore if also g is indecomposable then $\Omega_f = \Omega_g$.*

(ii) *If, further, f and g are both indecomposable polynomials then they have the same degree and the same special points.*

Proof. (i) Let x_1 and y_1 be algebraic over $\mathbb{C}(Z)$ and satisfying $f(x_1) = g(y_1) = Z$. By assumption $p := [\mathbb{C}(x_1, y_1) : \mathbb{C}(x_1)] < n := \deg(g)$. As f is indecomposable, there are no fields properly intermediate between $\mathbb{C}(Z)$ and $\mathbb{C}(x_1)$ by Lüroth's Theorem. Thus $\Omega_g \cap \mathbb{C}(x_1)$ can only be one of these fields. If $\Omega_g \cap \mathbb{C}(x_1) = \mathbb{C}(Z)$ then, by simple Galois theory $g(Y) - Z$ remains irreducible over $\mathbb{C}(x_1)$, i.e. $p = n$. Hence we must have $\Omega_g \supseteq \mathbb{C}(x_1)$ and $\Omega_g \supseteq \Omega_f$ follows.

(ii) An infinite place of Ω_f (resp. Ω_g) has ramification index over $\mathbb{C}(Z)$ equal to $\deg(f)$ (resp. $\deg(g)$): the equality of degrees follows. Let x_1, y_1 algebraic be such that $f(x_1) = g(y_1) = Z$. Now, λ is a special point for f (resp. g) if and only if it corresponds to a place of $\mathbb{C}(Z)$ which ramifies in $\mathbb{C}(x_1)$ (resp. $\mathbb{C}(y_1)$). Every point of $\mathbb{C}(Z)$ ramified in $\mathbb{C}(x_1)$ must be ramified also in Ω_f, hence must be ramified in $\mathbb{C}(y_1)$. Then $\Lambda(f) \subseteq \Lambda(g)$. By symmetry we conclude. □

Proof of Theorem 3. Write $n := \deg f$. Let Z be an indeterminate over $\mathbb{C}$. Denote by Ω (resp. Ω^*) the splitting field of $f(X) - Z$ (resp. $cf(Y) + c' - Z$) in a fixed algebraic closure of $\mathbb{C}(Z)$. By Lemma 3.1 we know that $\Omega^* = \Omega$ and that $f(X)$ and $cf(Y) + c'$ have the same special points. Hence $c' = 0$ if $c = 1$, proving the first assertion. In the following assume then $c \neq 0, 1$, $c' = 0$. Now $c\Lambda = \Lambda$ and either $\Lambda = \{0\}$ or c must be a root of unity.

If $\Lambda = \{0\}$ we have $f(t) = a(t + b)^n$ and we fall in the first case.

Henceforth suppose that there is some nonzero special point. This already implies that c is a root of unity. Since $c \neq 1$, we see that $\#\Lambda \geqslant 2$. In particular f cannot be l.r. to a cyclic polynomial.

Assume that f is l.r. to T_n, so we may assume in fact $f(t) = T_n(t) + d$ (here n must be prime since f is indecomposable). Now, $\Lambda = \{d + 2, d - 2\}$. Therefore c has order 2, whence $c = -1$. Hence $d + 2 = -(d - 2)$, i.e. $d = 0$ and we fall in case (2). Note that T_n is odd for odd n, so in fact $T_n(X) + T_n(Y)$ is reducible in those cases.

Therefore it remains to prove that: *If f is an indecomposable polynomial not* l.r. *to a cyclic or to a Chebyshev one and $f(X) - cf(Y)$ is reducible, then $f(X) = cf(L(Y))$ for a suitable linear polynomial L.*

Let $\mathcal{X} = \{x_1, \ldots, x_n\}$ (resp. $\mathcal{Y} = \{y_1, \ldots, y_n\}$) be the set of the roots of $f(X) - Z$ (resp. $cf(Y) - Z$), and Γ (resp. Γ^*) the Galois group $\mathrm{Gal}(\Omega/\mathbb{C}(Z))$ (resp. $\mathrm{Gal}(\Omega^*/\mathbb{C}(Z))$). (For the moment we forget that $\Omega = \Omega^*$.)

We now embed $\Omega/\mathbb{C}(Z)$ into a Laurent series field. We use [V, Ch. 2] as a reference throughout. Choose an extension $\mathfrak{p}$ of the place of $\mathbb{C}(Z)$ corresponding to $Z = \infty$ to Ω, and denote by $G_\mathfrak{p}$ its inertial group, which is cyclic of order n. Let $\Omega_\mathfrak{p}$ be the $\mathfrak{p}$-adic completion of Ω. As the base field $\mathbb{C}$ is algebraically closed and of zero characteristic, an element $t \in \Omega_\mathfrak{p}$ can be found such that $\Omega_\mathfrak{p} = \mathbb{C}((t))$ and $t^n = Z^{-1}$. The Galois group of $\Omega_\mathfrak{p}/\mathbb{C}((1/Z))$ is $G_\mathfrak{p}$. The elements of $G_\mathfrak{p}$ are represented by $t \mapsto \xi t$ where $\xi^n = 1$ (more

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

precisely, $\sum_{i\geqslant N} b_i t^i \mapsto \sum_{i\geqslant N} b_i(\xi t)^i$. Now let g_∞ be a generator of $G_\mathfrak{p}$. It is (by restriction) an element of Γ and we can index the roots $\mathcal{X}$ so that

$$g_\infty(x_j)=x_{j+1}.$$

The place of $\mathbb{C}((t))/\mathbb{C}((\frac{1}{Z}))$ over $Z=\infty$ is ramified with index n. Let v be the associated valuation: The corresponding maximal ideal of $\mathbb{C}[[t]]$ is generated by the uniformising parameter t. Then $v(\frac{1}{Z})=n$ and $v(x_j^{-1})=1$ for all j. We can write

$$x_1^{-1}\equiv a_1 t \ (\mathrm{mod}\ t^2\mathbb{C}[[t]]),$$

with $a_1\neq 0$. Similar expressions hold for the other roots. Therefore there exists a nonzero $\zeta\in\mathbb{C}$ such that $x_2^{-1}\equiv a_1\zeta t\,(\mathrm{mod}\ t^2\mathbb{C}[[t]])$. Now $v(\zeta x_1^{-1}-x_2^{-1})>1$, whence $v(\zeta x_j^{-1}-x_{j+1}^{-1})=v\big(g_\infty^{j-1}(\zeta x_1^{-1}-x_2^{-1})\big)>1$. By simple induction this implies

$$x_j^{-1}\equiv a_1\zeta^{j-1}t \ (\mathrm{mod}\ t^2\mathbb{C}[[t]]).$$

This also proves that ζ is a primitive nth root of unity.

We know that $\Omega=\Omega^*$ and that the roots of $f(Y)-Z/c$ are obtained from those of $f(X)-Z$ by extending an automorphism $Z\to Z/c$ of $\mathbb{C}((\frac{1}{Z}))$ (which contains $\mathbb{C}(Z)$) to one of $\mathbb{C}((t))$. For a fixed nth root u of c such an automorphism (continuous with respect to the t-adic topology) is given by $t\mapsto ut$. We can index the elements of $\mathcal{Y}$ so that their expansions around $Z=\infty$ are

$$y_j^{-1}\equiv a_1 u\zeta^{j-1}t\,(\mathrm{mod}\ t^2\mathbb{C}[[t]]) \quad (1\leqslant j\leqslant n).$$

Define group monomorphisms Γ, $\Gamma^*\to\Sigma_n$ as follows

$$\tau:\Gamma\to\Sigma_n,\qquad g\mapsto\ \tau(g)\quad\text{where } \tau(g)(a)=b \text{ if } g(x_a)=x_b,$$

$$\tau^*:\Gamma^*\to\Sigma_n,\qquad g\mapsto\ \tau^*(g)\quad\text{where } \tau^*(g)(a)=b \text{ if } g(y_a)=y_b.$$

As we get the roots $\mathcal{Y}$ from the roots $\mathcal{X}$ by the variable change $t\mapsto ut$, it is clear now that the images of Γ and Γ^* in Σ_n are the same, in the sense that for every element $g\in\Gamma$ there exists an element $g^*\in\Gamma^*$ which induces on the indices of $\mathcal{Y}$ the same permutation as g on the indices of $\mathcal{X}$, that is: $\tau(g)=\tau^*(g^*)$. Therefore there exists an isomorphism $\psi\colon\Gamma\to\Gamma^*$ such that $\psi(g)=g^*=(\tau^*)^{-1}(\tau(g))$. For each $g\in\Gamma$, the image $\psi(g)$ sends y_a to y_b if $g(x_a)=x_b$. The image of g_∞ operates thus: $\psi(g_\infty)(y_j)=y_{j+1}$. As $\Omega=\Omega^*$, we also have that $\Gamma=\Gamma^*$ as automorphism groups, i.e.: Each element of Γ permute the $\mathcal{Y}$.

We are going to prove that g_∞ sends y_i to y_{i+1}. By the equality of the splitting fields, there is a relation

$$y_1=R(x_1,x_2,\ldots,x_n) \tag{11}$$

where $R(X_1,X_2,\ldots,X_n)$ is a rational function over $\mathbb{C}$. Now g_∞^r acts formally on the r.h.s. of (11) mapping x_i to x_{i+r}, and thus replacing t with $\zeta^r t$. As (11) is an identity of power series, g_∞^r acts also on the l.h.s. sending t to $\zeta^r t$, i.e. it maps y_1 to y_{1+r}. This proves that $g_\infty(y_i)=y_{i+1}$ for all i. In other words, *ψ is an automorphism of Γ fixing g_∞*.

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

Fried [Fr1, Lemma 9] proved that if the indecomposable polynomial f is not l.r. to a cyclic or to a Chebyshev polynomial, then $\Gamma = \mathrm{Gal}(\Omega/\mathbb{C}(Z))$ acts doubly transitively on the roots of $f(X) - Z$. (This is the key argument in his proof of the absolute irreducibility of $(f(X) - f(Y))/(X - Y)$.

As y_1 is transcendental over $\mathbb{C}$, the absolutely irreducible factors of $f(X) - cf(Y)$ are in one-to-one correspondence with those of $f(X) - cf(y_1)$, and thus correspond to the orbits of $\Gamma_{y_1} = \mathrm{Gal}(\Omega/\mathbb{C}(y_1))$ on $\mathcal{X}$. Now, as $f(X) - cf(Y)$ is reducible by assumption, $\Gamma_{y_1} = \psi(\Gamma_{x_1})$ is not transitive on $\mathcal{X}$.

We now apply Theorem 4, which shows that ψ is induced by a conjugation in the full symmetric group on $\mathcal{X}$. In turn this means that $\psi(\Gamma_{x_1})$ is the stabiliser of some root x_j. But if the stabilisers of y_1 and of x_j in the Galois group of $\Omega/\mathbb{C}(Z)$ coincide, then $\mathbb{C}(y_1) = \mathbb{C}(x_j)$, so $x_j = \ell(y_1)$ for some fractional linear function ℓ.

Then $f(\ell(Y)) = cf(Y)$, hence ℓ is a linear polynomial and we fall in case (3). □

4. Proof of Theorem 1

We consider first the case of indecomposable $f(t)$.

PROPOSITION 4.1. *Let $f \in \mathbb{C}[X]$ be indecomposable and let $g, h \in \mathbb{C}(t)$ be non-constant distinct rational functions satisfying $f(g(t)) = f(h(t))$. Then $f(X)$ is l.r. to one of the following polynomials:*

(1) X^n *(n a prime);*
(2) $T_n(X)$ *(n an odd prime);*
(3) $P_1(t; l, m)$ *for some coprime l, m such that $l + m > 3$;*
(4) $P_2(t; a, b)$ *for suitable a, b;*
(5) $P_3(t; a, b)$ *for suitable a, b.*

We give first some definitions, which will be often used in the following. Let $n = \deg(f)$. Adopt the notation of Section 2.3. Since in the proof of Theorem 2 we shall need to treat polynomials of the form $f(X) - g(Y)$, we consider this situation first, and then specialise the definitions and results to the relevant cases.

Put

$$a(\lambda) = \sum_{i=1}^{h}(r_i(\lambda) - 1) = \deg(f) - h(\lambda) \tag{12}$$

and

$$c(\lambda) := \sum_{i=1}^{h(\lambda)} c^{(i)}(\lambda), \qquad c^{(i)}(\lambda) = \sum_{j=1}^{k(\lambda)}(r_i(\lambda) - (r_i(\lambda), s_j(\lambda))). \tag{13}$$

Clearly

$$\deg(f) - 1 = \sum_{\lambda \in \mathbb{C}} a(\lambda). \tag{14}$$

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

We begin to derive some inequalities. We plainly have for every special λ

$$n-\mu(\lambda)-1 \geqslant a(\lambda) \geqslant \frac{n-\mu(\lambda)}{2}. \tag{15}$$

(Note that the inequality on the right-hand side holds actually for all λ.)

LEMMA 4.2. *If $r_i(\lambda)=1$ then $c^{(i)}(\lambda)=0$. If $r_i(\lambda)\geqslant 2$ and $g(Y)-\lambda$ is not a perfect power of a polynomial of smaller degree then*

$$c^{(i)}(\lambda) \geqslant r_i(\lambda)-1, \qquad c(\lambda) \geqslant a(\lambda) \tag{16}$$

and

$$c(\lambda) \geqslant a(\lambda)\mu_g(\lambda). \tag{17}$$

Proof. The first assertion is obvious. If $r_i(\lambda)\geqslant 2$ does not divide $s_j(\lambda)$, then $r_i(\lambda)-(r_i(\lambda), s_j(\lambda)) \geqslant r_i(\lambda)/2$. If this happens for two distinct indices j, then $c^{(i)}(\lambda)\geqslant r_i(\lambda)$. Otherwise $r_i(\lambda)$ divides $s_j(\lambda)$ for all j except at most one and in this case it cannot divide them all, for otherwise $g(Y)-\lambda$ would be a $r_i(\lambda)$-th power. So there is exactly one index j with $s_j(\lambda)$ not divisible by $r_i(\lambda)$. For the same reason as above we must have $(r_i(\lambda), s_j(\lambda))=1$. In conclusion $c^{(i)}(\lambda)\geqslant r_i(\lambda)-1$ and (16) follows summing over i. Also, observe that plainly $c^{(i)}(\lambda)\geqslant \mu_g(\lambda)(r_i(\lambda)-1)$, so we obtain (17). □

DEFINITION 4.3. For any polynomial $f(t)$ we define its *root type* at λ, denoted by $\mathcal{M}(f-\lambda)$ (or simply $\mathcal{M}(f)$ if $\lambda=0$) as the unordered list $[r_1, r_2, \ldots]$ of the multiplicities of the distinct roots of $f(t)-\lambda$ in $\mathbb{C}$. A short notation for n roots of multiplicity m is $m^{\times n}$.

Proof of Proposition 4.1. Put $F_f(X,Y)=(f(X)-f(Y))/(X-Y)$. If f is l.r. to a cyclic or to a Chebyshev polynomial then $F_f(X,Y)$ splits into genus zero factors and we fall in cases (1) or (2).

In the remainder of this proof we then assume that f is not l.r. to a cyclic or to a Chebyshev polynomial. Hence, f has degree larger than 3 and has at least two special points. By Proposition 2.4, $F_f(X,Y)$ is absolutely irreducible.

Put $\Lambda=\Lambda(f)=\{\lambda_1,\ldots,\lambda_{\#\Lambda}\}$, and define $a_i := a(\lambda_i)$, $c_i := c(\lambda_i)$, $\mu_i := \mu(\lambda_i)$ and so on. From (6) we get a formula for the genus $\mathfrak{g}$ of the curve associated to $F_f(X,Y)$:

$$2(\deg(f)+\mathfrak{g}-2)=\sum_{i=1}^{\#\Lambda} c_i, \tag{18}$$

where in the definition for $c_i=c(\lambda_i)$ one puts $s_j(\lambda_i)=r_j(\lambda_i)$.

Also, $f-\lambda$ is not a power of a smaller degree polynomial for all $\lambda\in\mathbb{C}$ and Lemma 4.2 holds with $g=f$ and $\mu_g(\lambda)=\mu(\lambda)$. By (14), (18) (with $\mathfrak{g}=0$) and (17), *there exists a special point, say λ_1, with $\mu_1\leqslant 1$.*

We may also assume that $\mu_1\leqslant\mu(\lambda)$ for every λ.

We first show that there cannot exist more than two special points.

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

Suppose on the contrary $\#\Lambda \geqslant 3$. By (18), (16) and (17) it is $2(n-2) \geqslant \sum_{i=1}^{3} c_i \geqslant a_1 + (\mu_2 + \mu_3)\min\{a_2, a_3\}$. By (14) and (15) we have $n-1 \geqslant \sum_{i=1}^{3}(n-\mu_i)/2$. Then, as $a_1 \geqslant (n-1)/2$ we obtain $\mu_2 + \mu_3 \geqslant n+1$. Hence $\min\{a_2, a_3\} = 1$. Say the minimum is $a_2 = 1$. Then we have $\mu_2 = n-2 = c_2$. In turn this implies $\mu_3 \geqslant 3$. As $c_3 \geqslant 3a_3$ by (17) and $a_2 = 1$, we have $2(n-2) = \sum_{i=1}^{\#\Lambda} c_i \geqslant c_1 + (n-2) + c_3 + \sum_{i \geqslant 3} a_i \geqslant (n-3)+ 2a_3 + \sum_{i=1}^{\#\Lambda} a_i = 2n - 4 + 2a_3$, which implies $a_3 = 0$, a contradiction. Hence $\#\Lambda = 2$ as claimed.

We cannot have $\mu_2 = 0$, otherwise $a_1, a_2 \geqslant n/2$, contrary to (14). By a similar argument, if $\mu_2 = 1$ then also $\mu_1 = 1$. Therefore $\mu_2 \geqslant 1 \geqslant \mu_1$. If $h_1 \leqslant 2$ then $f(X) - \lambda_1$ has at most two roots, hence exactly two or we would fall in case (1). Write $\mathcal{M}(f(X) - \lambda_1) = [l, m]$: since $\deg(f) > 3$ we fall in case (3).

So suppose from now on that $h_1 \geqslant 3$.

We are going to prove that $\mu_2 \leqslant 3$. We have $(n-\mu_2)/2 \leqslant a_2 = n-1-a_1 = n-1-(n-h_1) = h_1 - 1$, so $n+2-2h_1 \leqslant \mu_2$ and $c_2 \geqslant \mu_2 a_2 = \mu_2(h_1-1)$, by (17). Using (18) with $\mathfrak{g} = 0$ and $c_1 \geqslant a_1 = n - h_1$ we thus get

$$n + 2 - 2h_1 \leqslant \mu_2, \quad \text{and} \quad (\mu_2 - 1)(h_1 - 1) - 3.$$

Combination of these inequalities gives $(n+1-2h_1)(h_1-1) \leqslant n-3$, that is $(h_1-2)n \leqslant (h_1-1)(2h_1-1) - 3 = (h_1-2)(2h_1+1)$, whence $n \leqslant 2h_1 + 1$ (recall $h_1 \geqslant 3$). Finally,

$$\mu_2 - 1 \leqslant \frac{n-3}{h_1-1} \leqslant \frac{2h_1-2}{h_1-1} = 2.$$

We have thus $\mu_2 \leqslant 3$ as desired.

Suppose $\mu_2 = 1$. Then also $\mu_1 = 1$, and $a_1, a_2 \geqslant (n-1)/2$, where equality must hold because $a_1 + a_2 = n-1$. In other words, $f(X) - \lambda_1$ and $f(X) - \lambda_2$ have both exactly one simple root, all other ones being double. By Proposition 2.3 f would be l.r. to a Chebyshev polynomial, a case which we exclude.

Let then in the following be $\mu_2 = 2$ or 3. We show that, in this case, $\mu_1 = 1$. If $\mu_1 = 0$, $f(X) - \lambda_1$ has no simple root, and not all the roots can be double, since $f(X)$ is indecomposable. Hence, $a_1 \geqslant (n+1)/2$ (holding with equality if and only if there is exactly one triple root and the remaining ones are double), whence $a_2 \leqslant (n-3)/2$. Since $a_2 \geqslant (n-\mu_2)/2$ we deduce that $\mu_2 = 3$ and all such inequalities are in fact equalities. In particular $f(X) - \lambda_2$ has three simple roots and all remaining roots double. These facts give $c_1 = \frac{3}{2}(n-3) = c_2$, whence $2n - 4 = 3n - 9$ and $n = 5$, $h_1 = 2$, a contradiction. Therefore $\mu_1 = 1$.

Let $\mathcal{M}(f - \lambda_1) = [r_1, \ldots, r_{h_1}]$ (recall $h_1 \geqslant 3$) and put $M := \max\{r_i\} > 1$. Let q be the number of roots (of $f - \lambda_1$) of multiplicity M. If $0 \neq r < M$ then $M - (M, r) \geqslant M - \max\{d : d \mid M, d < M\} =: M^*$, say. We then get $\sum_{1 < r_j < M}\big(M - (M, r_j)\big) \geqslant M^*(h_1 - 1 - q)$ whence, directly from (13),

$$c_1 \geqslant \sum_{i=1}^{h_1}(r_i - 1) + qM^*(h_1 - 1 - q) = n - h_1 + M^* q(h_1 - 1 - q). \tag{19}$$

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

Since $\mu_1=1$ and $h_1 \geqslant 3$, we have $n \geqslant 5$, so $c_2 \geqslant \mu_2(n-\mu_2)/2 \geqslant \min(n-2, \frac{3}{2}(n-3)) \geqslant n-2$ whence $c_1 \leqslant n-2$. By (19), $h_1 \geqslant 2+M^*q(h_1-1-q)$. If $q \neq h_1-1$ then $q(h_1-1-q) \geqslant h_1-2$, so $M^*=1$. However $M^*=1$ if and only if $M=2$, which implies $q=h_1-1$. Therefore in any case we have $q=h_1-1$ and $a_1=(M-1)/M(n-1)$, $a_2=(n-1)/M$. Since $a_2 \geqslant (n-3)/2$ by (15), we see that $M=2$ or $n \leqslant 7$.

If $M=2$ then $a_2=a_1=(n-1)/2$ and $h_1=h_2=(n+1)/2$. It is now easy to see that if $\mu_2=2$ the root type at λ_2 must be $[1,1,2^{\times\frac{n-5}{2}},3]$, while if $\mu_2=3$ it must be $[1,1,1,2^{\times\frac{n-9}{2}},3,3]$ or $[1,1,1,2^{\times\frac{n-7}{2}},4]$. A quick verification shows that the only case compatible with (18) is $n=5$ with root types $[1,1,3]$, resp. $[1,2,2]$ at λ_2, resp. λ_1. Replacing f with a l.r. polynomial we may assume that $\lambda_1=0$ and $f(t):=t(t+a)^2(t+b)^2$, where $ab(a-b)\neq 0$. Also, $f(t)-\lambda_2$ has a triple zero, say ξ. This zero ξ must be a double zero of $f'(t)$, $\xi \neq -a,-b$. The discriminant of $(f'(t))/((t+a)(t+b))=5t^2+3(a+b)t+ab$ which is $9(a+b)^2-20ab$ must then vanish. Hence we fall in case (4).

Last, let $n \leqslant 7$ and $M \geqslant 3$. Recall $h_1 \geqslant 3$ and $q=h_1-1$, so $n \geqslant 1+3(h_1-1) \geqslant 7$, hence in fact $n=7$, with root type at λ_1, resp. λ_2 equal to $[1,3,3]$, resp. $[1,1,1,2,2]$. Replacing f with a l.r. polynomial we may assume that $f(t)=t(t+a)^3(t+b)^3$, $ab(a-b)\neq 0$. Now we must impose that f takes the same value at the two zeros of f' distinct from $-a,-b$. We have $f'(t)=(t+a)^2(t+b)^2(7t^2+4(a+b)t+ab)$. Solving $7t^2+4(a+b)t+ab=0$ and substituting into f we obtain an equation which leads to the equations $8a^2-5ab+b^2=0$ and $a^2-5ab+8b^2=0$ (here we used a computer), hence we fall in the last case. □

Remark 4.4. Consider now cases (3)–(5) of the Proposition just proved. The root types of the special points of P_1 (with degree at least 4), P_2 and P_3 show that they cannot be l.r. to cyclic or Chebyshev polynomials. Also, they are indecomposable. This is clear for P_2 and P_3 since they have prime degree. The following Lemma settles the question for P_1.

LEMMA 4.5. *$P_1(t;p,q)$ is indecomposable.*

Proof. Suppose that $P_1(t)=t^p(t+1)^q=f_1(f_2(t))$ with $\deg(f_1), \deg(f_2) \geqslant 2$. As p and q are coprime, f_1 is not a power of a linear polynomial and has $N \geqslant 2$ distinct roots. Write $f_1(t)=\prod_{j=1}^N (t-\xi_j)^{m_j}$ with $\xi_j \neq \xi_k$ if $j \neq k$. Thus $t^p(t+1)^q=\prod_{j=1}^N (f_2(t)-\xi_j)^{m_j}$ and the factors $f_2(t)-\xi_j$ being pairwise coprime, we have $N \leqslant 2$, hence $N=2$. At least one of the polynomials $f_2(t)-\xi_1$ and $f_2(t)-\xi_2$ has at least two distinct roots, which implies that $P_1(t)$ must have at least *three* distinct roots, which is a contradiction. □

Remark 4.6. Let us consider now the *sporadic* polynomials $P_2(t;a,b)$ and $P_3(t;a,b)$ and the corresponding curves $(f(X)-f(Y))/(X-Y)$. It is clear that l.r. polynomials define isomorphic curves.

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

We prove that the polynomials $P_2(t; a, b)$ form only one l.r.-class. First observe that $P_2(t; ca, cb) = c^5 P_2(t/c; a, b)$. Let a_1 and a_2 be the roots of $9a^2 - 2a + 9$: It is easily seen that $a_2^5 P_2(t; a_1, 1) = P_2(a_2 t; a_2, 1)$, so we have only one class.

On the other hand, we have two l.r.-classes of polynomials $P_3(t; a, b)$. As above assume $b = 1$, let a_1 and a_2 be the two roots of $a^2 - 5a + 8$ and consider the equation $\big(pP_3(t; a_1, 1) + q\big) - P_3(ct + d; a_2, 1) = 0$: This is a system of 8 equations in c, d, p and q (corresponding to the coefficients of t^j, $0 \leqslant j \leqslant 7$) which has, however, no solutions.

PROPOSITION 4.7. *Suppose that f is one of the polynomials given in Proposition* 4.1 (1)–(5). *Then there exist distinct nonconstant rational functions $g(t), h(t)$ with $f(g(t)) = f(h(t))$ and all pair of such functions are given by the formulae $g(t) = g_1(r(t))$ and $h(t) = h_1(r(t))$, where $r(t)$ is a rational function, and respectively in cases* (1)–(5)*:*

(1) *$g_1(t) = t$ and $h_1(t) = \zeta t$ where $\zeta^n = 1$, $\zeta \neq 1$.*
(2) *$g_1(t) = t + \frac{1}{t}$, $h_1(t) = \zeta t + \frac{1}{\zeta t}$, where $\zeta^n = 1$, $\zeta \neq 1$.*
(3) *$g_1(t) = \frac{1-t^l}{t^{l+m}-1}$, $h_1(t) = t^m g_1(t)$.*
(4) *Put $\sigma := a + b$ and $\delta := a - b$. Also, put $U = U(t) := \frac{1}{2}(t^2 + \frac{15}{64})$, $Z = Z(t) = \frac{1}{2}(t^2 - \frac{7}{4}t - \frac{15}{64})$. Then*

$$g_1(t) = \frac{-2abt^2}{\sigma(Z^2 + tZ + t^2) + \delta(Z - t)U} \quad \text{and} \quad h_1(t) = g_1(t)\frac{Z^2}{t^2}.$$

(5) *Define σ, δ as before. Also, define $e = \frac{a}{4b}$, $f = 1 - \frac{e^2}{4}$, Finally, put $U = U(t) := \frac{1}{2}(t^2 + f)$, $Z = Z(t) := \frac{1}{2}(t^2 - et - f)$. Then*

$$g_1(t) = \frac{-2abt^3}{\sigma\dfrac{Z^4 - t^4}{Z - t} + \delta(Z^2 + 4(1 - e)tZ + t^2)U} \quad \text{and} \quad h_1(t) = g_1(t)\frac{Z^3}{t^3}.$$

In cases (2)–(5) *the expressions for g_1 are reduced* (*i.e. numerator and denominator are coprime*) *and with square-free denominator.*

Proof. The case (1) is trivial.

Consider case (2) and assume that $T_n(g(t)) = T_n(h(t))$. Write, in an algebraic closure of $\mathbb{C}(t)$, $g(t) = \alpha + \frac{1}{\alpha}$, $h(t) = \beta + \frac{1}{\beta}$. Then the defining equation for T_n gives

$$\alpha^n + \frac{1}{\alpha^n} = \beta^n + \frac{1}{\beta^n}$$

which we rewrite as $(\alpha^n - (1/\beta^n))(1 - (\beta^n/\alpha^n)) = 0$. So $\alpha = \zeta\beta^\epsilon$ for some nth root of unity ζ and some $\epsilon = \pm 1$. Replacing β with $1/\beta$ if necessary, we may assume that $\epsilon = 1$. Now observe that $\zeta g(t) - h(t) = (\zeta^2 - 1)\beta$, that $\zeta \neq -1$ because n is odd and that $\zeta \neq 1$ since g and h are assumed distinct. Then $\beta = r(t)$, say, is a rational function and, by the above formulae, we are done.

In the remaining cases $F_f(X, Y)$ is absolutely irreducible by Proposition 2.4, since, by Remark 4.4, f is indecomposable in those cases. Let $\Phi := \mathbb{C}(x, y)$ where $F_f(x, y) = 0$. Suppose we find rational functions $g_1(u), h_1(u) \in \mathbb{C}(u)$ with $F_f(g_1(u), h_1(u)) = 0$ and

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

$\mathbb{C}(g_1(u), h_1(u)) = \mathbb{C}(u)$. Then $\Phi = \mathbb{C}(u)$. Now, if $g(t), h(t)$ are distinct and satisfy $F_f(g(t), h(t)) = 0$, we have $\Phi = \mathbb{C}(g(t), h(t)) \subset \mathbb{C}(t)$. Also, $g(t) = g^*(u)$, $h(t) = h^*(u)$ for certain rational functions g^*, h^*. Since $x = g_1(u) = g(t) = g^*(u)$ we have $g_1 = g^*$ and similarly $h_1 = h^*$. Moreover $u \in \mathbb{C}(t)$, so $u = r(t)$ for a rational function r. Hence, to complete the proof it suffices to find g_1, h_1 as above, in each of the cases (3)–(5).

In case (3) we verify by direct substitution that the given formulae satisfy the relevant equation. Observe that $t^m = h_1/g_1 \in \mathbb{C}(g_1, h_1)$. Hence $t^l = (1 + g_1)/(t^m g_1 + 1)$ also lies in $\mathbb{C}(g_1, h_1)$, which thus contains t, since l, m are coprime.

In case (4), rather than verifying by brute force that the displayed formulae satisfy the relevant conditions, we reconstruct in several steps the formulae themselves. Put $\Phi = \mathbb{C}(x, y)$, where $F_f(x, y) = 0$. Put $z := (x + a)(x + b)/((y + a)(y + b))$, so $y = z^2 x$. We have $\mathbb{C}(x, z) = \Phi$. Substituting $y = z^2 x$ in the right side of the formula defining z we get

$$(z^5 - 1)x^2 + (a + b)(z^3 - 1)x + ab(z - 1) = 0. \tag{20}$$

Let $\Delta = \Delta(z) = (a + b)^2(z^3 - 1)^2 - 4ab(z - 1)(z^5 - 1)$ be the discriminant of this quadratic equation in x. We have $\Phi = \mathbb{C}(x, z) = \mathbb{C}(z, \sqrt{\Delta})$.

If we can find nonconstant g_1 and h_1 with $F_f(g_1(t), h_1(t)) = 0$ then the field Φ has genus zero, and the latter condition, as is well known, means that Δ has at most two roots of odd multiplicity. In fact, it can be easily verified (for example using `maple`) that if $9a^2 - 2ab + 9b^2 = 0$ and $\delta = a - b$, then $\Delta = \delta^2(z - 1)^4(z^2 + \frac{7}{4}z + 1)$. Hence

$$\Phi = \mathbb{C}(z, \sqrt{\Delta}) = \mathbb{C}(z, \sqrt{z^2 + \frac{7}{4}z + 1}).$$

Put $u^2 = z^2 + \frac{7}{4}z + 1$. It is well known how to parametrise this type of equation. On completing the square we obtain $(u - z - \frac{7}{8})(u + z + \frac{7}{8}) = \frac{15}{64}$. Now the parametrisation comes by setting $t := u + z + \frac{7}{8}$, so $\frac{15}{64t} = u - z - \frac{7}{8}$ and we obtain $z = z(t) = \frac{1}{2}(t - \frac{15}{64t} - \frac{7}{4})$ and $u = u(t) := \frac{1}{2}(t + \frac{15}{64t})$.

The roots of a quadratic equation $\alpha X^2 + \beta X + \gamma = 0$ can be also given by $\frac{-2\gamma}{\beta \mp \eta}$, $\eta = \sqrt{\Delta}$. Using these formulae to solve equation (20) for x, we can express x (and also y) as a rational function of t and thus obtain

$$g_1(t) = \frac{-2ab}{\sigma(z^2 + z + 1) + \delta(z - 1)u} \quad \text{and} \quad h_1(t) = g_1(t)z^2.$$

Putting $Z := tz$, $U := tu$ we obtain the formulae given in the statement. By construction $\Phi = \mathbb{C}(t)$. The expression for g_1 is a fraction with both denominator and numerator polynomial and it is reduced, as the denominator does not vanish for $t = 0$. We compute (with `maple`) the greatest common divisor of the denominator and its derivative with respect to t. Since the result is 1, we conclude that the denominator is square-free.

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

The procedure to obtain case (5) is similar to the preceding one. Defining z by the same formula we have $y = z^3 x$ and again $\Phi = \mathbb{C}(x, z)$. Again we obtain a quadratic equation for x, namely $(z^7 - 1)x^2 + \sigma(z^4 - 1)x + ab(z - 1) = 0$ with discriminant $\Delta := \sigma^2(z^4 - 1)^2 - 4ab(z - 1)(z^7 - 1)$. By verification as before we find that $\Delta(z) = \delta^2(z^2 + 4(1 - e)z + 1)^2(z - 1)^2(z^2 + ez + 1)$. As in the previous case we parametrise $z^2 + ez + 1 = u^2$, solve the quadratic equation for x, put $U = ut, Z = Zt$ and get the formulae displayed in the statement. The formula for g_1 also in this case is reduced and with square-free denominator. □

In [Fr2, p. 141] Fried stated that, for (unspecified) applications, it would have been of interest to consider the reducibility of rational functions $f(X) - g(Y)$ where f is a polynomial but g is a rational function. Our next theorem is one such result, which will be needed in the proof of Theorem 1.

THEOREM 5. *Let $S(X)$, $p(X)$ and $q(X)$ be polynomials over $\mathbb{C}$, with $S(X)$ indecomposable, $\deg(S) \geqslant 2$, $\deg(q) \geqslant 1$, $\deg(p) \leqslant \deg(q) + 1$ and $(p, q) = 1$. Put $\phi(X, Y) := S(X) - p(Y)/q(Y)$. Then the rational function $\phi(X, Y)$ is irreducible (as a rational function in 2 variables) and, if q is square-free and $\deg(q) \geqslant 3$, it defines a curve of positive genus.*

Proof. Suppose that $\phi(X, Y)$ is reducible. Hence $S(X)q(Y) - p(Y)$ splits in at least two absolutely irreducible factors (which are bivariate, q and p being coprime). Put $H(Y) = p(Y)/q(Y)$. By Lemma 3.1 $\Omega_S \subseteq \Omega_H$. The infinite places of Ω_S over $\mathbb{P}^1$ are ramified with index $\deg(S) > 1$, contradicting the fact that those of Ω_H are unramified.

Assume now q square-free and $\deg(q) \geqslant 3$. Put $m := \deg(S)$. The genus formula (5) with $f = S$ and $g = H$ implies $2(m + \mathfrak{g} - 1) \geqslant 3(m - 1)$ (just considering the contributions at infinity), i.e. $\mathfrak{g} > 0$. □

Proof of Theorem 1. If f is one of the polynomials given in cases (1)–(5), then $F_f(X, Y)$ has a genus zero factor by Proposition 4.7.

Conversely, suppose that $F_f(X, Y)$ has a genus zero factor $P(X, Y)$. The function field of the associate curve is $\Phi(x, y)$ with $P(x, y) = 0$. It is of the form $\mathbb{C}(t)$ and $x = \widehat{g}(t)$, $y = \widehat{h}(t)$, where $\widehat{g}$ and $\widehat{h}$ are distinct rational functions. Also, $f(\widehat{g}(t)) = f(\widehat{h}(t))$.

Let f now be a composite polynomial

$$f = R_1 \circ R_2 \circ \cdots \circ R_p,$$

where the polynomials $R_1, \ldots, R_p$ have degrees $\geqslant 2$.

Then there exists $j, 1 \leqslant j \leqslant p$ such that $S \circ \widehat{g} \neq S \circ \widehat{h}$ where $S = R_{j+1} \circ \cdots \circ R_p$ (it is understood that S has degree 1 if $j = p$) but $R_j \circ S \circ \widehat{g} = R_j \circ S \circ \widehat{h}$. Let $A = R_1 \circ R_2 \circ \cdots \circ R_{j-1}$. Setting $R = R_j$ and $\widehat{f} = R \circ S$ we have that $R(S \circ \widehat{g}) = R(S \circ \widehat{h})$ with $S \circ \widehat{g} \neq S \circ \widehat{h}$, so by Proposition 4.7 (of which we adopt the notation in the following) we conclude that $(S \circ \widehat{g}, S \circ \widehat{h})$ must be one of the pairs

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

(g,h) described there. Possibly exchanging $\widehat{g}$ with $\widehat{h}$, we can assume that $S\circ\widehat{g} = g_1\circ r$. In other words, the equation

$$R_{j+1}(X) - g_1(Y) = 0 \tag{21}$$

defines an algebraic set with at least one genus zero component.

If we fall in cases (3)–(5) note that the rational function $g_1(t)$ has square-free denominator coprime to the numerator, of degree at least 3 and always larger than that of the numerator. By Theorem 5, if $\deg(S)\geqslant 2$ (and thus $j<p$ and $\deg(R_{j+1})\geqslant 2$) then (21) defines a curve of positive genus: This contradiction proves S linear. Moreover $A = R_1\circ R_2\circ\cdots\circ R_{j-1}$ and $M=S$.

If we fall in case (2) then we can assume (composing R to the right and S to the left with suitable linear polynomials) that R is a Chebyshev polynomial.

It easy to see that $S(X)-g_1(Y)=0$ is irreducible: indeed $Y^2 - YS(X)+1$ splits into factors (which, by Gauss' Lemma, must be polynomials in Y and X, linear in Y) only if $S(X)$ is a constant. Now we want to determine all the polynomials $S(X)$ such that the genus is 0. If $Z = Y - \frac{S(X)}{2}$, we get $Z^2 = \frac{1}{4}(S(X)^2-4)$ which has genus zero if and only if $S=\epsilon T_{\deg(S)}\circ M$ where $\epsilon=\pm 1$ and M is a linear polynomial by Proposition 2.3. Hence $R\circ S = T_{\deg(R)\cdot\deg(S)}\circ M$, and, if $\deg(R)$ is odd and $\epsilon=-1$, we replace $A(X)$ with $A(-X)$.

Last, consider case (1). If $R(X)=X^m$ then

$$S(X)^m - S(Y)^m = \prod_{k=0}^{m-1}\big(S(X)-\zeta_m^k S(Y)\big),$$

where ζ_m is a mth primitive root of unity. It follows that $P(X,Y)$ divides one of the factors $S(X)-\zeta_m^k S(Y)$. Plainly, $P(X,Y)$ can divide only one polynomial of the form $S(X)-\zeta S(Y)$, $\zeta\in\mathbb{C}$, for otherwise it would divide $S(X)$ and $S(Y)$, and it would be a constant. As $S\circ\widehat{g}\neq S\circ\widehat{h}$, it must be $k\neq 0$. Hence $S(X)-\zeta_m^k S(Y)$ is given by Theorem 2. □

5. Proof of Theorem 2

As in the proof of Theorem 1, we adopt the notation of Section 2.3. Also, (12)–(15) and Lemma 4.2 hold. From (5) we deduce a formula for the genus $\mathfrak{g}$ of the curve associated to an absolutely irreducible polynomial $f(X)-g(Y)$ where $\deg(f)\mid\deg(g)$, namely:

$$2(\deg(f)+\mathfrak{g}-1) = \sum_{\lambda\in\Lambda(f)} c(\lambda). \tag{22}$$

We shall mainly deal with polynomials of the form $f(X)-cf(Y)$, in which case

$$\begin{aligned} &g(t) = cf(t), && \mu_g(\lambda) = \mu(\lambda/c),\\ &k(\lambda) = h(\lambda/c) \quad\text{and} && s_i(\lambda) = r_i(\lambda/c). \end{aligned}$$

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

Beside the definition of linear relation, in this section we shall need a stronger equivalence relation:

DEFINITION 5.1. We say that two polynomials P and Q are similar if there exist a linear polynomial ℓ and a nonzero constant α with $P = \alpha Q \circ \ell$.

PROPOSITION 5.2. *An indecomposable polynomial $f(t) \in \mathbb{C}[t]$ of degree n is such that an absolutely irreducible factor of $f(X) - cf(Y)$ with $c \neq 1$ defines a curve of genus zero if and only if either $n = 1$ or it is similar to one of the following polynomials:*

(1) *Z_n, with n prime.*
(2) *T_n, with n prime. If $c \neq -1$ then $n = 2$.*
(3) *A polynomial of the form $t^r g(t^d)$ which is not l.r. to a cyclic or a Chebyshev polynomial, where $g \in \mathbb{C}[t]$, r and d are coprime integers with $r > 0$ and $d \geqslant 2$. In this case c is a dth root of unity.*
(4) *P_1. Then $c \neq 1$.*
(5) *$T_3 + d$ where $d \neq 0, \pm 2$, with $c = (d+2)/(d-2)$ or $c = (d-2)/(d+2)$.*
(6) *P_4. Then $c = -1$.*
(7) *P_5. Then $c = \omega$ or ω^2.*
(8) *P_6. Then $c = -1$.*

Observe that in cases (1), (3) and in case (2) with n odd (so $c = -1$) the polynomial $f(X) - cf(Y)$ is reducible, whereas in the remaining cases it is absolutely irreducible.

Proof. If $f(X) - cf(Y)$ is reducible then by Theorem 3 we obtain cases (1)–(3). In the first case it splits in linear factors. In the second case one sees that by Proposition 2.2 the absolutely irreducible factors of $T_n(X) + T_n(Y)$ define curves of genus zero. In the third case it is clear that a linear factor exists.

From now on let $f(X) - cf(Y)$ be irreducible. Put $\Lambda := \Lambda(f)$, $n := \deg(f)$. Either $\#\Lambda = 1$, that is f is l.r. to a cyclic polynomial, or $\#\Lambda > 1$, in which case $f(X) - \lambda$ is not a perfect power of a polynomial of smaller degree for any λ and $n > 2$. In the first case we can assume up to similarity that $f(t) = t^n + \lambda$ with $n > 1$. Then $X^n - cY^n - c'$ is irreducible and defines a curve of genus zero (where $c' = (c-1)\lambda$). Clearly it must be $c' \neq 0$, which implies $\lambda \neq 0$ (so we can even assume $\lambda = -2$) and $n = 2$. We have thus $f(t) = T_2$, and fall in case (2).

Henceforth we work under the assumption $\#\Lambda > 1$.

Putting $\tilde{\mu}(\lambda) := \mu_{cf}(\lambda) = \mu(c^{-1}\lambda)$, inequalities (16) and (17) give

$$c(\lambda) \geqslant a(\lambda) \max(1, \tilde{\mu}(\lambda)). \tag{23}$$

We show now that $\#\Lambda \in \{2, 3\}$. From (14) and the r.h.s. of (15) both applied to cf in place of f we obtain

$$n - 1 \geqslant \sum_{\lambda \in \mathbb{C}} \frac{n - \tilde{\mu}(\lambda)}{2} \geqslant \sum_{\lambda \in \Lambda} \frac{n - \tilde{\mu}(\lambda)}{2}.$$

(Note that the second sum is over Λ, not over $c\Lambda$.) On the other hand by equations (22) with $\mathfrak{g} = 0$ and (17) it is $2(n-1) \geqslant \sum_{\lambda \in \Lambda} \tilde{\mu}(\lambda)$. Adding twice the first of these

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

inequalities to the second one gives $4(n-1)\geqslant n\#\Lambda$, whence $\#\Lambda\leqslant 3$. (In other words, f defines a Riemann Sphere cover ramified over the point at infinity and at most three finite points.)

We consider two cases: (i) $\tilde{\mu}(\lambda)>1$ for all $\lambda\in\Lambda$ and (ii) there exists $\lambda\in\Lambda$ with $\tilde{\mu}(\lambda)\leqslant 1$. These will be further divided into two subcases according to $\#\Lambda$.

We warn the reader that, due to the nature of our result, the remainder of the proof consists mainly of several verifications, which lead to the various sporadic polynomials.

- *Case* (i): $\tilde{\mu}(\lambda)>1$ *for all* $\lambda\in\Lambda$.

As $2(n-1)=\sum_{\lambda\in\Lambda}c(\lambda)\geqslant\sum_{\lambda\in\Lambda}a(\lambda)\tilde{\mu}(\lambda)\geqslant 2\sum_{\lambda\in\Lambda}a(\lambda)=2(n-1)$, we infer that equality must hold throughout, so $\tilde{\mu}(\lambda)=2$ and $c(\lambda)=2a(\lambda)$ for all $\lambda\in\Lambda$. But $n\geqslant 3$ and this implies that, in fact, $n\geqslant 4$ and $\lambda\in\Lambda(cf)$ for $\lambda\in\Lambda$, whence $\Lambda=c\Lambda$. This implies that c is a root of unity. Furthermore, $\mu(\lambda)=2$ for all $\lambda\in\Lambda$. Let then be $r_i(\lambda)=s_i(\lambda)=1$ for $i\leqslant 2$.

Fix now $\lambda\in\Lambda$. Should one of the $r_i(\lambda)$ not divide $s_j(\lambda)$ where $i,j\geqslant 3$, it would be $2(n-h(\lambda))=2a(\lambda)=c(\lambda)>\sum_{i=3}^{h(\lambda)}2(r_i(\lambda)-1)=2(n-h(\lambda))$ (the inequality holds strictly because there is at least one more non-vanishing summand in the sum for $c(\lambda)$). Hence $r_i(\lambda)\,|\,s_j(\lambda)$ for all $i,j\geqslant 3$. By symmetry also $s_j(\lambda)\,|\,r_i(\lambda)$, whence $r_i(\lambda)=s_j(\lambda)$. Therefore there exists an integer $r(\lambda)$ such that $r_i(\lambda)=s_j(\lambda)=r(\lambda)$ for $i,j\geqslant 3$. In other words, for all $\lambda\in\Lambda$, both $f(X)-\lambda$ and $cf(Y)-\lambda$ have two simple roots, all the other ones having multiplicity $r(\lambda)$. Hence $a(\lambda)=(n-2)(r(\lambda)-1)/r(\lambda)$ and, by (14),

$$n-1=(n-2)\sum_{\lambda\in\Lambda}\frac{r(\lambda)-1}{r(\lambda)}. \tag{24}$$

- *Subcase* (i, a): $\#\Lambda=3$.

Clearly $n\geqslant 4$. Equation (24) implies $n-1\geqslant\frac{3}{2}(n-2)$, i.e. $n\leqslant 4$, which forces $n=4$. It follows that $\mathcal{M}(f(X)-\lambda)=[2,1,1]$ for all $\lambda\in\Lambda$. Now c is an mth root of unity with $m\leqslant 3$ and $c\neq 1$.

If $c=-1$ then $\Lambda=\{0,\pm\beta\}$ with $\beta\neq 0$: Replacing f with a suitable similar polynomial we can assume that f is monic and $f(0)=0$. Write $f(t)=t^4-\frac{4}{3}(a+b)t^3+2abt^2$, with $ab(a-b)\neq 0$, so that $f'(t)=4t(t-a)(t-b)$. The condition $f(a)+f(b)=0$ gives $a^4-2a^3b-2ab^3+b^4=0$, the left-hand side of which splits into factors as $\prod_{j=1}^{2}(a^2-\xi_j ab+b^2)$ where ξ_1 and ξ_2 are the roots of $\xi^2-2\xi+2=0$. We then fall case (6). We have to prove that $P_4(X)+P_4(Y)$ is irreducible and defines a curve of genus zero. First of all note that P_4 is indecomposable[★]. The verification that $P_4(X)+P_4(Y)$ is irreducible is done by the method described in the next remark:

Remark 5.3. Let $f(X)$ be an indecomposable polynomial which is not l.r. to a cyclic or a Chebyshev polynomial. Assume $f(X)-cf(Y)$ reducible. Theorem 3(3)

[★] If it were decomposable, it would be the composition of two degree 2 polynomials, and $P_4(t)+\eta$ would be a square for some $\eta\in\mathbb{C}$, which it is not.

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

implies that $cf(Y) = f(M(Y))$ where M is linear, so $(x - M(Y)) \mid (f(X) - cf(Y))$. To verify the irreducibility of $f(X) - cf(Y)$ we may thus consider $cf(Y) - f(AY + B) = 0$ as a system of $\deg(f) + 1$ equations in the letters A and B, and check whether it admits solutions: in the cases we shall encounter this is straightforward. □

Since the root types of P_4 are known, it is easily verified that the genus of the curve associated to $P_4(X) + P_4(Y)$ is zero. In fact, as an example, by using (22) with $f(X) = P_4(X)$ and $g(Y) = -P_4(Y)$, we see that $c(\lambda) = 2$ for all special λ's and thus $\mathfrak{g} = 0$.

Consider now the case $c^3 = 1$. Let ρ_j, for $0 \leqslant j \leqslant 2$, be the three roots of f'. Then we can assume $f(\rho_0) = \omega f(\rho_1) = \bar{\omega} f(\rho_2)$. Up to similarity we can take f monic, with $\rho_0 = 0$, $f(0) = 1$. Write $f(t) = f(t; a, b) = t^4 - \frac{4}{3}(a + b)t^3 + 2abt^2 + 1$ with $a, b \in \mathbb{C}$. Then $f'(t) = 4t(t - a)(t - b)$ with $ab(a - b) \neq 0$. Solving $f(a) = \omega$ for b we obtain $b = (a^4 - 3(1 - \omega))/2a^3$. The condition $f(b) = \bar{\omega}$ implies $b^4 - 2ab^3 - 3(1 - \bar{\omega}) = 0$: In it we substitute the above relation for b and obtain $a^{16} - 24\bar{\omega}a^{12} - 54\omega a^8 - 243\bar{\omega} = 0$, whose l.h.s. is equal to $(a^4 + 3\bar{\omega}) \prod_{t=0}^{3} (a^3 + 3i^{3t}\bar{\omega}a^2 + 3i^{2t}\omega a + 3i^t)$. Multiplying a by i has the effect of multiplying also b by i, so we get $f(it; a, b) = f(t; ia, ib)$. Therefore we need only to consider (up to similarity of f) $a = \omega(-3)^{1/4}$ and $a^3 + 3\bar{\omega}a^2 + 3\omega a + 3 = (a + \bar{\omega})^3 + 2 = 0$. In the latter case $b = (1 - a)\omega - 1$ holds[★]. This shows we are in case (7).

The indecomposability of f, the reducibility of both $f(X) - \omega f(Y)$ and $f(X) - \bar{\omega} f(Y)$ precisely when $a = \bar{\omega}(-3)^{1/4}$ and their irreducibility otherwise, and that in that case they define genus zero curves, are proved exactly as for $c = -1$ (f, ωf and $\bar{\omega} f$ by construction have the same three special points and all have root type [2, 1, 1] as above).

- *Subcase* (i, b): $\#\Lambda = 2$.

As $c \neq 1$ it is $c = -1$ and $r := r(\lambda) = r(-\lambda)$. Plainly $n \geqslant r + 2$. If $r = 2$ then (24) yields at once the contradiction $n - 1 = n - 2$, whereas if $r > 3$ then $n > 5$, but (24) implies $n \leqslant 4$, a contradiction. Thus $r = 3$, $n = 5$ and $\mathcal{M}(f \mp \lambda) = [3, 1, 1]$ whence f' has two double roots. Replacing f with a similar polynomial we assume that $f'(t) = 5(t - 1)^2(t + 1)^2$. Integrating and using the condition $f(1) = -f(-1)$ we obtain $f(t) = t^5 - \frac{10}{3}t^3 + 5t$. Now $X + Y$ divides $f(X) + f(Y)$, so we do not find new polynomials.

- *Case* (ii): *there exists* $\lambda \in \Lambda$ *with* $\tilde{\mu}(\lambda) \leqslant 1$.

Note that $\Lambda \cap c\Lambda \neq \emptyset$, because $\tilde{\mu}(\lambda) \leqslant 1$ implies $\lambda \in c\Lambda$. (Recall that $n > 2$.)

As in the proof of Proposition 4.1 it will be convenient to define $\Lambda = \{\lambda_1, \ldots, \lambda_{\#\Lambda}\}$ and $a_i := a(\lambda_i)$, $c_i := c(\lambda_i)$, $\mu_i := \mu(\lambda_i)$, $\tilde{\mu}_i := \tilde{\mu}(\lambda_i)$ and so on.

[★] Use the equation for a to verify that $(a^4 - 3(1 - \omega))/2a^3 = (1 - a)\omega - 1$.

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

- *Subcase* (ii, a): $\#\Lambda = 3$.

Let $\tilde{\mu}_1 \leqslant 1$, so $\lambda_1 \in c\Lambda$. We can also assume that $\tilde{\mu}_1 \leqslant \tilde{\mu}_i$ for all i.

Being $\tilde{\mu}_1 \leqslant 1$, from $n - 1 \geqslant \sum_{i=1}^{3} (n - \tilde{\mu}_i)/2$ (obtained applying (14) and (15) to cf) we get $\tilde{\mu}_2 + \tilde{\mu}_3 \geqslant n + 1$ and also $\tilde{\mu}_2, \tilde{\mu}_3 \geqslant 3$.

Put $m = \min\{a_2, a_3\}$. Clearly $m \geqslant 1$ and

$$2(n-1) = c_1 + c_2 + c_3 \geqslant a_1 + (\tilde{\mu}_2 + \tilde{\mu}_3)m > (n+1)m,$$

so $m = 1$.

We can thus assume without loss of generality that $a_3 = 1$, i.e. $f(X) - \lambda_3$ has root type $[2, 1, \dots, 1]$. Using (14) again we infer that $a_1 + a_2 = n - 2$.

As $\mu_3 = n - 2$ it cannot be $\lambda_1 = c\lambda_3$. Suppose that $\lambda_1 = c\lambda_2$, which implies $\mu_2 = \tilde{\mu}_1 \leqslant 1$. Recall that $\tilde{\mu}_2 \geqslant 3$. Since $a_1 + a_2 = n - 2$ and $a_2 \geqslant (n-1)/2$, by (22) and (23) we obtain $2(n-1) \geqslant a_1 + 3a_2 + 3 = (n-2) + 2a_2 + 3 \geqslant 2n$, which is a contradiction. Therefore $\lambda_1 = c\lambda_1$. This implies $\lambda_1 = 0$ and $\mu_1 = \tilde{\mu}_1$.

We are going to prove that $\Lambda = c\Lambda$. Suppose first that $\lambda_3 \notin c\Lambda$, that is $\mathcal{M}(cf - \lambda_3) = [1, \dots, 1]$ and $c_3 = n$. Thus, using (22) and (23) we obtain the contradiction $2(n-1) = \sum_{i=1}^{3} c_i \geqslant a_1 + 3a_2 + n \geqslant (n-2) + 2a_2 + n \geqslant 2n$. Hence $\lambda_3 \in c\Lambda$, and it must be $\lambda_3 = c\lambda_2$ (because $c \neq 1$). Suppose now that $\lambda_2 \notin c\Lambda$. Then $\mathcal{M}(cf - \lambda_2) = [1, \dots, 1]$ and $c_2 = n$. Note that $a_2 = 1$ otherwise it would be $2(n-1) \geqslant a_2\tilde{\mu}_2 \geqslant 2n$. Hence $\mathcal{M}(f - \lambda_2) = [2, 1, \dots, 1]$. Being $a_3 = 1$, (14) implies $a_1 = n - 3$. Now $2(n-1) \geqslant a_1 + c_2 + \tilde{\mu}_3 \geqslant (n-3) + n + 3 = 2n$ which is absurd. Therefore also $\lambda_2 \in c\Lambda$.

Summarising, $\lambda_1 = 0$, $c = -1$ and $\lambda_2 = -\lambda_3$ so $n - 2 = \mu_3 = \tilde{\mu}_2 \geqslant 3$, i.e. $n \geqslant 5$. If it were $a_2 \geqslant 2$ then $2(n-1) \geqslant 1 + 2(n-2) + 3 = 2n$. Hence $a_2 = 1$, which implies that $\mu_2 = n - 2 = \tilde{\mu}_3$ and $c_2 = c_3 = n - 2$. By (22) it is now $c_1 = 2$. By (14) we get $a_1 = n - 3$. Thus $2 = c_1 \geqslant a_1 = n - 3$, so $n = 5$. We conclude that $\mathcal{M}(f) = [1, 2, 2]$.

Up to similarity we can assume $f(t) = t(t+a)^2(t+b)^2$. Then

$$f'(t) = (t-a)(t-b)\big(5t^2 - 3(a+b)t + ab\big).$$

Let χ_1 and χ_2 be the roots of $5t^2 - 3(a+b)t + ab$. The condition $f(\chi_1) + f(\chi_2) = 0$ implies $(a+b)(27a^4 - 117a^3b + 212a^2b^2 - 117ab^3 + 27b^4) = 0$, that is $(a+b) \times \prod_{j=1}^{2}(a^2 - \frac{22+5\xi_j}{9}ab + b^2) = 0$ where ξ_1 and ξ_2 are the roots of $\xi^2 + \xi + 4 = 0$. If $a = -b$ then $f(X) + f(Y)$ is reducible. In the other cases, by the method of Remark 5.3, it is easily verified that $f(X) + f(Y)$ is irreducible. We then fall in case (8).

To verify that the curve associated to $P_6(X) + P_6(Y)$ has genus zero, we first recall that the special points of P_6 are 0 and $\pm\lambda_2$. The root type of P_6 at 0 is $[1, 2, 2]$ and the root types at $\pm\lambda_2$ are both $[1, 1, 1, 2]$. We use (22) with $f(X) = P_6(X)$ and $g(Y) = -P_6(Y)$: we already know that $c_1 = c(0) = 2$ and $c_2 = c_3 = c(\pm\lambda_2) = 3$, so that $\mathfrak{g} = 0$.

- *Subcase* (ii, b): $\#\Lambda = 2$.

Suppose first that $\#(\Lambda \cap c\Lambda) = 1$. We can assume without loss of generality that $\lambda_1 \in c\Lambda$ and $\lambda_2 \notin c\Lambda$. Then $c_2 \geqslant \tilde{\mu}_2 = n$. Now, $a_2 = 1$ (in fact, if $a_2 \geqslant 2$ then

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

$c_2 \geqslant 2n$, contradicting (22)), so $a_1 = n-2$. It follows that $\mathcal{M}(f-\lambda_1) = [p, q]$, with p and q coprime. Now there are two possibilities: $\lambda_1 = c\lambda_1$ or $\lambda_1 = c\lambda_2$.

If $\lambda_1 = c\lambda_1$ then $\lambda_1 = 0$ and f is similar to $P_1(t; p, q)$. As $P_1(X)$ and $cP_1(Y)$ are indecomposable (see Lemma 4.5) and have different sets of special points, by Lemma 3.1 the polynomial $P_1(X) - cP_1(Y)$ must be irreducible: A simple application of formula (5) proves that it has genus zero. We fall thus in case (4).

If $\lambda_1 = c\lambda_2$, then $\tilde{\mu}_1 = \mu_2 = n-2$, whence, by (22) and (23), it is $n = 3$. Also, $f(X) - cf(Y)$ is irreducible and defines a genus zero curve as in case (4). In this case it is notationally convenient to express f in term of a Chebyshev polynomial (which is also l.r. to $P_1(t; 1, 2)$) and we fall in case (5).

Let now be $\Lambda = c\Lambda$. Plainly $c = -1$ i.e. $\lambda_1 = -\lambda_2$. Set $t := \mu_1 + \mu_2$. By (14) and (15), $2 \leqslant t \leqslant n-1$. If $t = 2$ then f is l.r. to a Chebyshev polynomial by Proposition 2.3. The special points being symmetric, f is similar to $T_{\deg(f)}$ and $f(X) + f(Y)$ is reducible (see Proposition 2.2). Therefore we can assume $t \geqslant 3$, so that $n \geqslant 4$.

One of μ_1, μ_2 is $\leqslant 1$, so $\mu_1\mu_2 \leqslant t-1$. It is

$$2(n-1) = c_1 + c_2 \geqslant \frac{n-\mu_1}{2}\mu_2 + \frac{n-\mu_2}{2}\mu_1 = \frac{tn}{2} - \mu_1\mu_2 \tag{25}$$

which implies that $2(n-1) \geqslant n(t/2) - (t-1)$ and thus $t \leqslant 4 + 2/(n-2)$. If $n \geqslant 5$ then $t \leqslant 4$, whereas if $n = 4$ it is $t = 3$.

For any $\xi \in \mathbb{C}$, denote by $\mathrm{mult}_f(\xi)$ the multiplicity of the root ξ of $f(X) - f(\xi)$.

LEMMA 5.4. *Let* $\#\Lambda = 2$. *Put* $\sigma := \sum_{\xi : \mathrm{mult}_f(\xi) > 2} (\mathrm{mult}_f(\xi) - 2)$. *Then* $\sigma = t - 2$.

Proof. Let R be the number of distinct roots of f'. Note that $2n = \deg((f-\lambda_1)(f-\lambda_2)) = t + 2R + \sigma$ and $n - 1 = \deg(f') = R + \sigma$, then eliminate n and R from the last two equalities. □

Suppose $t = 3$. By Lemma 5.4, $(f-\lambda_1)(f-\lambda_2)$ has exactly one triple root, all the other roots being simple or double. We can thus assume that $\mathcal{M}(f-\lambda_1) = [3, 2^{\times a}, 1^{\times \mu_1}]$ and $\mathcal{M}(f-\lambda_2) = [2^{\times b}, 1^{\times \mu_2}]$, where

$$a = \frac{n-3-\mu_1}{2} \quad \text{and} \quad b = \frac{n-\mu_2}{2}.$$

By (22) we then obtain

$$\begin{aligned} 2(n-1) &= c_1 + c_2 = b(3+\mu_1) + (a+2)\mu_2 \\ &= (3+\mu_1)\frac{n-\mu_2}{2} + \mu_2\frac{n-(3+\mu_1)}{2} + 2\mu_2 = 3n - (1+\mu_1)\mu_2 \geqslant 3n-4, \end{aligned}$$

which, under our assumptions, is impossible.

Last, let $t = 4$. Here $n \geqslant 5$. Inequality (25) implies $\mu_1\mu_2 \neq 0$ and thus one of μ_1, μ_2 must be equal to 1 (recall that we are in case (ii) and $\Lambda = c\Lambda$), so $\mu_1\mu_2 = 3$.

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

Lemma 5.4 shows that $(f - \lambda_1)(f - \lambda_2)$ has either one root of multiplicity four or two roots of multiplicity three, all other roots being either simple or double. There are now three possibilities:

(a) $\mathcal{M}(f - \lambda_1) = [4, 2^{\times\frac{n-4-\mu_1}{2}}, 1^{\times\mu_1}]$ and $\mathcal{M}(f - \lambda_2) = [2^{\times\frac{n-\mu_2}{2}}, 1^{\times\mu_2}]$;
(b) $\mathcal{M}(f - \lambda_1) = [3, 3, 2^{\times\frac{n-6-\mu_1}{2}}, 1^{\times\mu_1}]$ and $\mathcal{M}(f - \lambda_2) = [2^{\times\frac{n-\mu_2}{2}}, 1^{\times\mu_2}]$; and
(c) $\mathcal{M}(f - \lambda_1) = [3, 2^{\times\frac{n-3-\mu_1}{2}}, 1^{\times\mu_1}]$ and $\mathcal{M}(f - \lambda_2) = [3, 2^{\times\frac{n-3-\mu_2}{2}}, 1^{\times\mu_2}]$.

By the same method used in the case $t = 3$ (that is, by a direct application of formula (22) with $\mathfrak{g} = 0$) we easily arrive at contradictions in all three cases, thus completing the proof of Proposition 5.2. □

Remark 5.5. Consider now the polynomials given up to similarity in cases (6)–(8) of Proposition 5.2: We ask how many similarity classes they form.

By the method of Remark 4.6 it can be seen that there are two similarity classes of polynomials P_4 and P_6. It suffices to prove that the two given representants for each of P_4 and P_6 are not similar: The equation to solve is analogous to that for P_3 in the mentioned Remark, but with $q = 0$.

We are going to prove that the polynomials P_5 form only one similarity class. Let $a_j = -2^{1/3}\omega^{j-1} - \bar{\omega}$, $1 \leqslant j \leqslant 3$ be the roots of $(a + \bar{\omega})^3 + 2$ and $b_j = (1 - a_j)\omega - 1$. It is

$$\bar{\omega}P_5(t; a_1, b_1) = P_5(\bar{\omega}(t - a_1); a_2, b_2).$$

Letting the Galois group of $\mathbb{Q}(\omega, 2^{1/3})/\mathbb{Q}(\omega)$ act on the displayed equation, the indices of the a_j, b_j are permuted cyclically, thus proving our claim. Note also that, for fixed a, b, the equation $P_5(X) - \bar{\omega}P_5(Y)$ is obtained from $P_5(X) - \omega P_5(Y)$ exchanging X and Y and multiplying by $\bar{\omega}$, so that in case (7) there is up to isomorphism only one curve. □

PROPOSITION 5.6. *Suppose that f, is one of the polynomials given in Proposition* 5.2 (1)–(8), *with $n = \deg(f)$. Let $g(t), h(t)$ be distinct nonconstant rational functions with $f(g(t)) = cf(h(t))$.*

Then there exists a rational function $r(t)$ with $g(t) = g_1(r(t))$, $h(t) = h_1(r(t))$ and respectively in cases (1)–(8)*:*

(1) *$g_1(t) = t$, $h_1(t) = \gamma t$ where $\gamma^n = c$.*
(2) *If $c = -1$ then either $g_1(t) = t$, $h_1(t) = -t$ and $n > 2$, or $g_1(t) = t + \frac{1}{t}$, $h_1(t) = \zeta t + \frac{1}{\zeta t}$, where ζ is a primitive 2nth root of unity* (n *a prime*).
If $c \neq -1$ (*with $n = 2$*), *then $g_1(t) = \frac{1}{2}(t + \frac{2(1-c)}{t})$ and $h_1(t) = \frac{1}{2\sqrt{c}}(t - \frac{2(1-c)}{t})$.*
(3) *$g_1(t) = t$, $h_1(t) = \gamma t$ where $\gamma^r = c$.*
(4) *$g_1(t) = \frac{1-\gamma t^l}{\gamma t^{l+m}-1}$ and $h_1(t) = t^m g_1(t)$ where γ satisfies $c = \gamma^m$.*
(5) *If $c = \frac{d+2}{d-2}$, then $g_1(t) = 3\frac{ct^2+1}{ct^3+1} - 1$ and $h_1(t) = 1 - tg_1(t) - t$. If $c = \frac{d-2}{d+2}$, exchange g_1 with h_1.*

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

(6) *Replace f with a similar polynomial to assume that $b = 1$ in order to simplify the expressions. Put $d := -6a$, $k := 2(2a^2 - 5a + 2)$, $U := U(t) = \frac{1}{6}(t + \frac{d}{t})$ and $Z := Z(t) = \frac{-1}{2\sqrt{k}}(t - \frac{d}{t}) - (a + \frac{1}{a})$. Then*

$$g_1(t) = \frac{(Z-a)(Z-\frac{1}{a})U + \frac{2}{3}(a+1)(Z^3+1)}{Z^4+1} \quad \textit{and} \quad h_1(t) = g_1(t)Z.$$

(7) *Define $d := -\omega(a^2 - i\sqrt{3}a + 3\omega)$ and $e := \sqrt{-3(a-1)/2}$. Also define $p_0 := \frac{i}{\sqrt{3}}a^2 - \omega(a-1)$, $p_1 := -\frac{i\omega}{\sqrt{3}}a^2 - \omega(a-1)$ and $P(s) := s^2 + p_1 s + p_0$. Put $U := U(t) = (t + \frac{d}{t})/(2e)$ and $Z := Z(t) = (t - \frac{d}{t})/2 + p_1$. Finally*

$$g_1(t) = \frac{P(Z)U - \frac{2}{3}(\omega - \bar{\omega})((a-1)Z^3 - \omega(a-\omega))}{Z^4 - 1} + a \quad \textit{and}$$
$$h_1(t) = \bar{\omega}(g_1(t) - a)Z.$$

(8) *Put $\sigma := a + b$, $\delta := a - b$ and $e := 251 + 7\xi$ ($\xi^2 + \xi + 4 = 0$ as in Definition 2.1). Define also $U := U(t) = \frac{1}{2}(t + e/t)$ and $Z := Z(t) = \frac{1}{32}(t - \frac{e}{t} + 6 - 2\xi)$. Then*

$$g_1(t) = \frac{\sigma(Z^3+1) + \delta(Z^2 - \xi Z + 1)U}{2(Z^5-1)} \quad \textit{and} \quad h_1(t) = -g_1(t)Z^2.$$

Proof. The case (1) is trivial.

(2) If $c \neq -1$, then $n = 2$, so we use the usual parametrisations of quadrics.

If $T_n(g(t)) + T_n(h(t)) = 0$ then $T_{2n}(g(t)) - T_{2n}(h(t)) = 0$ because

$$T_n(X) + T_n(Y) = \frac{T_{2n}(X) - T_{2n}(Y)}{T_n(X) - T_n(Y)}.$$

In an algebraic closure of $\mathbb{C}(t)$, we write $g(t) = \alpha + \frac{1}{\alpha}$, $h(t) = \beta + \frac{1}{\beta}$, and by the defining equation for T_{2n} we obtain, replacing β with $1/\beta$ if necessary, $\alpha = \zeta\beta$ for some $2n$th root of unity ζ. If it were $\zeta^n = 1$ we would have $T_n(g(t)) - T_n(h(t)) = 0$ and thus $T_n(g(t)) = 0$, which is absurd, $g(t)$ being assumed nonconstant. If $g(t) \neq -h(t)$ then also $\zeta \neq -1$ and we continue as in the proof of Proposition 4.7 (2) getting the result of the statement. If $g(t) = -h(t)$ clearly $n > 2$.

(3) The proof of Theorem 2 (3) shows that $X - \gamma Y$ is the only genus zero factor of $f(X) - cf(Y)$.

In cases (4)–(8), note that $f(X) - cf(Y)$ is irreducible and therefore it suffices to find g_1, h_1 as in the statement, as remarked in the proof of Proposition 4.7.

Case (4) is verified by substitution as in Proposition 4.7(3).

(5) Let $c = (d+2)/(d-2)$. The equation can be rewritten as

$$(X-2)(X+1)^2 = c(Y+2)(Y-1)^2.$$

Upon putting $X = -3X_1 - 1$ and $Y = 3Y_1 + 1$ we get the equation $X_1^2(X_1 + 1) = -cY_1^2(Y_1 + 1)$. We thus fall in case (4) with $l = 2$, $m = 1$ and $-c$ in place of c.

If $c = (d-2)/(d+2)$ then we exchange X with Y and divide by c the equation in order to fall in the previous case.

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

(6) Put $P(X, Y) := P_4(X) + P_4(Y)$. The singular points on the curve $P(X, Y) = 0$ are $(X, Y) = (0, 0), (1, a)$ and $(a, 1)^{\star}$. A singular point is the origin, which is easily blown up via the birational morphism defined by $Y = ZX$. So we obtain an equation

$$(Z^4 + 1)X^2 - \tfrac{4}{3}(a + 1)(Z^3 + 1)X + 2a(Z^2 + 1) = 0. \tag{26}$$

Consider the discriminant of the above equation with respect to X:

$$\Delta := \Delta(Z) = \tfrac{16}{9}(a + 1)^2(Z^3 + 1)^2 - 8a(Z^4 + 1)(Z^2 + 1).$$

It can be verified that $\Delta = k(\frac{2}{3}(Z - a)(Z - \frac{1}{a}))^2(Z + a^2)(Z + \frac{1}{a^2})$ where k is as in the statement. We parametrise $U^2 = k(Z^2 + (a^2 + \frac{1}{a^2})Z + 1)$ in the usual way. We are then able to extract a square root of Δ, so we can solve (26) for $X = X(t) = g_1(t)$ in rational functions, and thus express also $Y = h_1(t)$.

Case (7) is obtained in a similar way, but the details are more intricate. We begin with $P_5(X) - \omega P_5(Y) = 0$ where $P_5(t) = P_5(t; a, b)$ and a, b satisfy the conditions $a^3 + 3\bar{\omega}a^2 + 3\omega a + 3 = 0$ and $b = (1 - a)\omega - 1$ given in Definition 2.1. Upon putting $Y = \bar{\omega}Y_1$ consider the equation $P_5(X) - \omega P_5(\bar{\omega}Y_1) = 0$, and as in Case (6) we see that the singular points on the associated curve are $(X, Y_1) = (a, 0), (0, \omega b)$ and $(b, \omega a)$. We translate the first of these points to the origin: Putting $X = X_1 + a$ in we see that X_1^2 divides the constant term with respect to Y_1 of the resulting equation, and that the coefficient of Y_1 is 0. We then put $Y_1 = ZX_1$ and get

$$\begin{aligned}&(Z^4 - 1)X_1^2 - \tfrac{4}{3}(\omega - \bar{\omega})((a - 1)Z^3 - \omega(a - \omega))X_1\\&\quad - 2a((a - 1 + \bar{\omega})Z^2 - \bar{\omega}(a - \omega + \bar{\omega})) = 0.\end{aligned}$$

Let $\Delta = \Delta(Z)$ be the discriminant of this quadratic equation in X_1. It can be verified that, defining $Q(s) := s^2 - 2p_1s + p_0$ where p_0, p_1 and $P(s)$ are as in the statement:

$$\Delta = \frac{-8}{3(a - 1)}P(Z)^2Q(Z).$$

Therefore, as in case (6), we parametrise $U^2 = -2/(3(a - 1))Q(Z)$, we express X_1 using U and $P(Z)$, and finally obtain the formulae displayed.

(8) We use (essentially) the method of Proposition 4.7 (4) and (5). Put $\Phi = \mathbb{C}(x, y)$, where $P_6(x; a, b) + P_6(y; a, b) = 0$. Put $Z := (x + a)(x + b)/((y + a)(y + b))$, so $y = -Z^2x$: Upon substituting this in the right side of the formula defining Z, we get a quadratic equation for x, namely $(Z^5 - 1)x^2 - (Z^3 + 1)(a + b)x + ab(Z - 1)$. By direct verification we see that the discriminant of this equation in x is $\Delta{=}(a - b)^2(Z^2 - \xi Z + 1)^2(Z^2 - \frac{3-\xi}{8}Z + 1)$. Upon parametrising $U^2{=}Z^2 - \frac{3-\xi}{8}Z + 1$, we express first U and Z, then x and y, as rational functions of t. □

[⋆] They are obtained upon solving the system $\partial P/\partial X = \partial P/\partial Y = P(X, Y) = 0$. Alternatively we could observe that the curve $\mathcal{D}$ defined by $P(X, Y) = 0$ is the fibred product of the two covers of the Riemann sphere by itself given by $X \mapsto Z = P_4(X)$ and by $Y \mapsto Z = -P_4(Y)$. By Abhyankhar's Lemma, over a point $(x_0, y_0) \in \mathcal{D}$ there are (r, s) distinct places where $r = \mathrm{mult}_{P_4}(x_0)$ and $s = \mathrm{mult}_{-P_4}(y_0)$. Now it is straightforward to detemine the singular points on $\mathcal{D}$, as the special points of P_4 are known.

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

Proof of Theorem 2. If f is one of the polynomials given in cases (1)–(8), then $f(X)-cf(Y)$ has a genus zero factor by Propositions 5.2 and 2.2.

Conversely, suppose from now on that $f(X)-cf(Y)$ has a genus zero factor $P(X, Y)$.

Write $f=f_0\circ f_1$ with f_0 indecomposable of degree n greater than 1. The map $(X, Y)\mapsto(f_1(X), f_1(Y))$ defines a nontrivial morphism of the curve associated to $P(X, Y)$ onto the curve associated to some factor of $f_0(X)-cf_0(Y)$, which must then have genus zero.

Hence we can apply Proposition 5.2 to $f_0(X)-cf_0(Y)$: We get at once the statements of the theorem regarding the types of f_0. Replace f_0 and f_1 with $f_0\circ\ell^{-1}$ and $\ell\circ f_1$ for a suitable linear ℓ to assume, without loss of generality, that f_0 is one of the polynomials displayed in cases (1)–(8); we can further assume f_0 monic. We consider now these cases one by one.

(1) If $f_0=Z_n$ then there is nothing to prove.

(2) Let first $c=-1$. Let $\widehat{g}(t)$, $\widehat{h}(t)$ be nonconstant rational functions such that $P(\widehat{g}(t), \widehat{h}(t))=0$. Then $f_1\circ\widehat{g}$ and $f_1\circ\widehat{h}$ parametrise a genus zero factor of $T_n(X)+T_n(Y)$. We apply Proposition 5.6(2) and infer that either $f_1\circ\widehat{g}=-f_1\circ\widehat{h}$ and $n>2$ or, possibly exchanging $\widehat{g}$ with $\widehat{h}$, that $f_1(\widehat{g}(t))=g_1(r(t))$ with $g_1(t)=t+\frac{1}{t}$.

In the first case $P(X, Y)$ must divide $f_1(X)+f_1(Y)$. In fact, under the notation of Proposition 2.2, if $P(X, Y)$ divided $\Upsilon_{n,k}(f_1(X), f_1(Y))$ for some k with $1\leqslant k<n$, $k\equiv 1 (\mathrm{mod}\ 2)$, then $\Upsilon_{n,k}(f_1(\widehat{g}(t)), f_1(\widehat{h}(t)))=0$. Since $f_1\circ\widehat{g}=-f_1\circ\widehat{h}$, the polynomial $\Upsilon_{n,k}(X, -X)$ would vanish for infinitely many values taken by the variable X, so it would be zero. On the other hand $\Upsilon_{n,k}(X, -X)=2(1+\cos(\pi k/n))X^2-4\sin^2(\pi k/n)\neq 0$ the coefficient of X^2 being nonzero.

In the second case we have that the curve $f_1(X)-g_1(Y)$ is irreducible and has genus zero, implying $f_1=\epsilon T_{\deg(f_1)}\circ M$ where $\epsilon=\pm 1$ and M is a linear polynomial: the argument is the same as in the proof of Theorem 1(2), with R replaced here by f_1. Hence $T_n\circ f_1=T_{n\deg(f_1)}\circ M$.

Consider next the case $c\neq -1$. Now $f_0=T_2$. For $c\neq 0, \pm 1$ the polynomial $T_2(X)-cT_2(Y)=X^2-2-c(Y^2-2)$ is irreducible. If the curve $W^2=cf(Y)-2$ were reducible, then $f(Y)-\frac{2}{c}$ would be a square of a polynomial, but as $f(Y)+2$ is a square, this cannot happen. Thus $W^2=cf(Y)-2$ defines an irreducible curve $\mathcal{C}$. For the same reason also the curve $\mathcal{C}' : f(X)+2c=Z^2$ is irreducible. All the components of the algebraic set $f(X)-cf(Y)=0$ map onto $\mathcal{C}$, resp. $\mathcal{C}'$, via $X\mapsto W=f(X)$, resp. $Y\mapsto Z=f(Y)$. Therefore $\mathcal{C}$ and $\mathcal{C}'$ have genus zero. This means that there exist polynomials R, S with $f(Y)+\frac{2}{c}=(Y-\eta_1)(Y-\eta_2)R(Y)^2$ and $f(X)+2c=(X-\xi_1)\ (X-\xi_2)S(X)^2$. Moreover $f(X)+2=f_1(X)^2$. As R, S and f_1 are pairwise coprime factors of f', the sum of their degrees is $\leqslant\deg(f')=\deg(f)-1$. This implies $\deg(f)\leqslant 2$, hence f_1 is linear.

(3) It suffices to prove that *the only genus zero factor of* $\Phi(X, Y):=f_0(X)-cf_0(Y)$ *is* $X-\zeta Y$ *where* ζ *is a dth root of unity with* $\zeta^r=c$ (in which case $\zeta=c^{r'}$ where $rr'\equiv 1\ (\mathrm{mod}\ d)$). By Proposition 2.4, $F_{f_0}(X, \zeta Y)=\frac{f_0(X)-cf_0(Y)}{X-\zeta Y}$ is absolutely

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

irreducible. Our claim shall follow from Proposition 4.1 and obvious transformations after we have proved that $f_0(t)$ is not l.r. to either P_1, P_2 or P_3.

Observe that $f_0(\zeta^j t)=\zeta^{jr}f_0(t)$ for all j, so

$$\text{the root types of } f_0(t) \text{ at } \lambda \text{ and } \lambda/\zeta^{jr} \text{ are the same for all } j. \tag{27}$$

In particular $a(\lambda)=a(\lambda/\zeta^{jr})$ and $\mu(\lambda)=\mu(\lambda/\zeta^{jr})$.

- Assume first f_0 l.r. to P_1. Write $f_0(t)=(t+\alpha)^l(t+\beta)^m+\lambda$ with $\alpha\neq\beta$. If $\lambda=0$ then, possibly exchanging α and β, it is $\alpha=0$, and $l=r$, $g(t^d)=(t+\beta)^m$, which is not possible. Then $\lambda\neq 0$ and, by (27), $a(\lambda)=a(\lambda/\zeta^r)=(l-1)+(m-1)=n-2$ with $\zeta^r\neq 1$. Formula (14) yields $n-1\geqslant a(\lambda)+a(\lambda/\zeta^r)=2(n-2)$ i.e. $n\leqslant 3$, contradicting the assumption that $n=l+m\geqslant 4$.
- Suppose now f_0 l.r. to P_2. Plainly we can write $f_0(t)=(t+u)(t+u+\alpha)^2(t+u+\beta)^2+\lambda$ for some $u\in\mathbb{C}$ and with $\alpha,\beta\in\mathbb{C}^*$ satisfying

$$9\alpha^2-2\alpha\beta+9\beta^2=0. \tag{28}$$

There are three possibilities for d and r: $d=2$ with $r=1$, i.e. $f_0=tg(t^2)$ where $\deg(g)=2$; $d=3$ with $r=2$, i.e. $f_0=t^2(t^3-v)$; and $d=4$ with $r=1$, i.e. $f_0=t(t^4-v)$.

Assume $\lambda=0$. Only in the first of the three listed possibilities it can be $\mathcal{M}(f_0)=[1,2,2]$ and since $f_0(-t)=-f_0(t)$ (because $\zeta=-1$), we also have $u=0$ and $g(t)=(t-v)^2$ (with $v\neq 0$). Thus $f_0(t)=t(t^2-v)^2$, and $\alpha=-\beta$, contrary to (28).

Hence $\lambda\neq 0$. Now (27) holds, and $a(\lambda)=a(\lambda/\zeta^r)=a(\lambda/\zeta^{2r})=\cdots=2$. This and formula (14) (where $n=5$) imply that $d=2$ and thus $\zeta=-1$. Also, the root types at λ and $-\lambda$ are equal, therefore $\mathcal{M}(f_0-\lambda)=\mathcal{M}(f_0+\lambda)=[1,2,2]$. By Proposition 2.3 we infer that f_0 is l.r. to T_5, which is a contradiction.
- Last, suppose f_0 l.r. to P_3. Write $f_0(t)=(t+u)(t+u+\alpha)^3(t+u+\beta)^3+\lambda$ where $8\alpha^2-5\alpha\beta+\beta^2=0$. If $\lambda=0$ then, by an argument similar to that for the case f_0 l.r. P_2, we see that it has to be $\alpha=-\beta$, contradicting the relation defining α and β. If $\lambda\neq 0$ we arrive at $\mathcal{M}(f_0-\lambda)=\mathcal{M}(f_0-\lambda/\zeta^r)=[1,3,3]$ with $\zeta^r\neq 1$, i.e. $a(\lambda)=a(\lambda/\zeta^r)=4$, and (14) (recall that $n=7$) yields again a contradiction.

For the next cases we need some auxiliary results. The following Lemma can be derived using Ritt's Theory [R, To]. For a simple proof follow [Z2, Lemma 6].

LEMMA 5.7. *Let A,B,C,D be nonconstant polynomials over a field K of zero characteristic with* $\deg A=\deg C$ *and $A\circ B=C\circ D$. Then there is a nonconstant K-linear polynomial ℓ such that $A\circ\ell=C$ and $B=\ell\circ D$.*

PROPOSITION 5.8. *Let f,g be polynomials of the same degree over the complex field, with f indecomposable and $f(X)-g(Y)$ irreducible.*

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

Then $f(X) - g(h(Y))$ is irreducible for all $h(Y) \in \mathbb{C}[Y]$.

Proof. Suppose $f(X) - g(h(Y))$ is reducible. Now [Fr2, Prop. 2] (or [BT, Prop. 8.1]) implies that there exist polynomials $\tilde{g}$ and $\tilde{h}$ with $g \circ h = \tilde{g} \circ \tilde{h}$, such that $f(X) - \tilde{g}(Y)$ is reducible and $\Omega_{\tilde{g}} = \Omega_f$. Thus, $\deg(\tilde{g}) = \deg(f) = \deg(g)$. Now $g = \tilde{g} \circ \ell$ with ℓ linear by Lemma 5.7. This clearly implies that $f(X) - g(Y)$ is reducible. □

We handle cases (4) and (5) together. We are in the following situation: f_0 is an indecomposable polynomial with $\Lambda(f_0) = \{\lambda_1, \lambda_2\}$ and $\lambda_1 \in \Lambda(cf_0)$ (in case (4) it is $\lambda_1 = c\lambda_1$, so $\lambda_1 = 0$, whereas in case (5) it is $\lambda_1 = c\lambda_2$) but $\lambda_2 \notin \Lambda(cf_0)$. From the proof of Proposition 5.2 we know that $f_0(X) - cf_0(Y)$ is irreducible and that its associated curve has genus zero. Also $\mathcal{M}(f_0 - \lambda_1) = \mathcal{M}(cf_0 - \lambda_1) = [p, q]$ with p, q coprime, $p > 1$.

Let now f_1 be a polynomial of degree m. We know by Proposition 5.8 that $\mathcal{D}$: $f_0(X) - cf_0(f_1(Y)) = 0$ is an irreducible curve.

Write $cf_0(Y) - \lambda_1 = c_0(Y - \eta_1)^p(Y - \eta_2)^q$ and $cf_0(Y) - \lambda_2 = c_0 \prod_{j=1}^{n}(Y - \xi_j)$ with the η_i, ξ_j pairwise distinct. Let v_1 (resp. $v_{2,j}$ for $1 \leqslant j \leqslant n$), be the number of simple roots of $f_1(Y) - \eta_2$ (resp. $f_1(Y) - \xi_j$). Therefore the number of simple roots of $cf_0(f_1(Y)) - \lambda_1$ (resp. $cf_0(f_1(Y)) - \lambda_2$) is at least v_1 (resp. $\sum_{j=1}^{n} v_{2,j}$). By (14) and (15) with f_1 in place of f we have

$$m - 1 \geqslant \frac{m - v_1}{2} + \sum_{j=1}^{n} \frac{m - v_{2,j}}{2},$$

whence $v_1 + \sum_{j=1}^{n} v_{2,j} \geqslant m(n-1) + 2$. By the genus formula (22) with f_0 and $cf_0 \circ f_1$ in place of f and g we have $2(n + \mathfrak{g} - 1) = c(\lambda_1) + c(\lambda_2) \geqslant v_1 + \sum_{j=1}^{n} v_{2,j}(n-1) + 2$, whence $\mathfrak{g} > 0$ if $m > 1$.

Each of the absolutely irreducible factors of $f(X) - cf(Y)$ define coverings of $\mathcal{D}$ in an obvious way, so they all define curves of genus $\geqslant \mathfrak{g}$. Thus f_1 must be linear.

Cases (6)–(8) are dealt with an argument similar to that for cases (4)–(5), by virtue of the following Lemma (recall that $f_0(t) = P_j(t)$ with $4 \leqslant j \leqslant 6$ is indecomposable and that $f_0(X) - cf_0(Y)$ is irreducible).

LEMMA 5.9. *Suppose $f(t) \in \mathbb{C}[t]$ is an indecomposable polynomial with at least 3 special points (and thus of degree at least 4) and $c \in \mathbb{C}\backslash\{0\}$ is such that $f(X) - cf(Y)$ is irreducible (thus $c \neq 1$) and defines a curve of genus zero. Let $h(t) \in \mathbb{C}[t]$ be of degree greater than 1.*

Then $f(X) - cf(h(Y))$ is irreducible and defines a curve of positive genus. In particular, and thus of degree at least 4 this holds if f is one of $P_4(t; a, b)$, $P_5(t; a, b)$ and $P_6(t; a, b)$.

Proof. The irreducibility of $f(X) - cf(h(Y))$ follows from Proposition 5.8. Set $n = \deg(f)$ and $p = \deg(h)$. Let $\lambda_1, \lambda_2, \lambda_3$ be distinct special points of f, and η_i be the number of simple roots of $cf(h(Y)) - \lambda_i$ for $1 \leqslant i \leqslant 3$. By formula (22) with $\mathfrak{g} = 0$

https://doi.org/10.1023/B:COMP.0000018136.23898.65 Published online by Cambridge University Press

and $g = cf \circ h$ we have $2(n-1) = \sum_{i=1}^{3} c(\lambda_i) \geqslant \sum_{i=1}^{3} \eta_i$ whereas by (14) and (15) applied to g in place of f we obtain $np - 1 \geqslant \sum_{i=1}^{3} \frac{np-\eta_i}{2} \geqslant \frac{3}{2}np - \sum_{i=1}^{3} \frac{\eta_i}{2}$, so $np + 2 \leqslant \sum_{i=1}^{3} \eta_i \leqslant 2(n-1)$, which implies $p \leqslant 1$, a contradiction.

This concludes the proof of Theorem 2. □

Acknowledgements

The authors thank Yuri Bilu, Gerhard Frey and Helge Tverberg for stimulating discussions on different aspects of this work. Their gratitude goes also to an anonymous referee whose comments considerably improved the paper.

Many computations have been performed using Maple [CGG$^+$].

References

[AZ] Avanzi, R. M. and Zannier, U. M.: Genus one curves defined by separated variable polynomials and a polynomial Pell equation, *Acta Arith.* **99** (2001), 227–256.

[B] Bilu, Y. F.: Quadratic factors of $f(x) - g(y)$, *Acta Arith.* **90** (1999), 341–355.

[BT] Bilu, Y. F. and Tichy, R. F.: The diophantine equation $f(x) - g(y)$, *Acta Arith.* **95** (2000), 261–288.

[CC] Cassou-Noguès P. and Couveignes, J.-M.: Factorisations explicites de $g(y) - h(z)$, *Acta Arith.* **87** (1999), 291–317.

[CGG$^+$] Char, B. W., Geddes, K. O., Gonnet, G. H., Leong, B. L., Monagan, M. B. and Watt, S. M.: *Maple V Language Reference Manual*, Springer, New York, 1991.

[DLS] Davenport, H., Lewis, D. J., and Schinzel, A.: Equations of the form $f(x) = g(y)$, *Quart. J. Math. Oxford* (2), **12** (1961), 304–312.

[Fa] Faltings, G.: Endlichkeitssātze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73** (1983), 349–366.

[Fr1] Fried, M.: On a conjecture of Schur, *Michigan Math. J.* **17** (1970), 41–55.

[Fr2] Fried, M.: The field of definition of function fields and a problem in the reducibility of polynomials in two variables, *Illinois J. Math.* **17** (1973), 128–146.

[Fr3] Fried, M.: Arithmetical properties of function fields (II), *Acta Arith.* **25** (1974), 225–258.

[R] Ritt, J. F.: Prime and composite polynomials, *Trans. Amer. Math. Soc.* **23** (1922), 51–66.

[Sch1] Schinzel, A. *Selected Topics on Polynomials*, Ann Arbor, 1982.

[Sch2] Schinzel, A. *Polynomials with Special Regard to Reducibility*, Encyclop. Math. Appl. 77, Cambridge Univ. Press, New York, 2000.

[Schn] Schneps, L. (ed.), *The Grothendieck Theory of Dessins d'Enfants*, London Math. Soc. Lecture Note Ser. 200, Cambridge Univ. Press, 1994.

[Se] Serre, J.-P.: *Linear Representations of Finite Groups*, Springer, New York, 1977.

[To] Tortrat, P.: Sur la composition des polynomes, *Colloq. Math.* **55** (1988), 329–353.

[Tv] Tverberg, H.: *A Study in Irreducibility of Polynomials*, PhD Thesis, Univ. Bergen, 1968.

[V] Völklein, H.: *Groups as Galois Groups*, Cambridge Stud. Adv. Math. 53, Cambridge Univ. Press, 1996.

[Z1] Zannier, U.: Ritt's second theorem in arbitrary characteristic, *J. Reine Angew. Math.* **445** (1993), 175–203.

[Z2] Zannier, U.: On a functional equation relating a Laurent series $f(X)$ to $f(X^m)$, *Aequationes Math.* **55** (1998), 15–43.