ISRAEL JOURNAL OF MATHEMATICS 85 (1994), 135–168

ON THE IRREDUCIBILITY OF SUMS OF RATIONAL FUNCTIONS WITH SEPARATED VARIABLES*

BY

WULF-DIETER GEYER**

Mathematisches Institut
Bismarckstraße $1\frac{1}{2}$, D–91054 Erlangen, Germany
email: geyer@pentheus.mi.uni-erlangen.de

ABSTRACT

A rational function with $n \geq 3$ separated variables, i.e. a sum $f_1(X_1) + f_2(X_2) + \cdots + f_n(X_n)$ with nonconstant f_i, is with exception of a special case in characteristic p always irreducible, i.e. has an irreducible numerator. This theorem was first proved by Schinzel. A different proof in characteristic 0 was given by Fried. We carry this proof to all characteristics. As an application we determine all rational functions f with an addition formula of type $f(x) + f(y) = f(h(x, y))$ for some rational function h.

1. Introduction

PROBLEM: *Let k be a field of characteristic $p \geq 0$, let $n \geq 3$ be a natural number. For $i = 1, \ldots, n$ let*

$$f_i = \frac{F_i}{H_i} \in k(X) \setminus k \qquad \gcd(F_i, H_i) = 1 \tag{1}$$

be nonconstant rational functions in one variable, whose degree is given by

$$\deg f_i := [k(X) : k(f_i)] = \max(\deg F_i, \deg H_i) \tag{2}$$

* This work was partially supported by a grant from G.I.F. (German Israeli Foundation for Scientific Research and Development). I thank Wolfgang Ruppert and Moshe Jarden for helpful comments on a preliminary version of this paper.

** The paper was written during a stay at the Institute for Advanced Studies at the Hebrew University in Jerusalem. The author thanks the Institute for the warm hospitality which made the stay so pleasant.
Received January 20, 1992 and in revised form June 1, 1992

We look at the sum of these functions, taken with separated variables, i.e. at the rational function

$$f(X_1, X_2, \ldots, X_n) = \sum_{i=1}^{n} f_i(X_i)$$

in n variables. The denominator of f is $H(X_1, \ldots, X_n) = \prod_{i=1}^{n} H_i(X_i)$, since the $H_i(X_i)$ are relatively prime. So the numerator of f is

$$F(X_1, X_2, \ldots, X_n) = \prod_{i=1}^{n} H_i(X_i) \cdot \sum_{i=1}^{n} f_i(X_i) = \sum_{i=1}^{n} F_i(X_i) \cdot {}_iH \tag{3}$$

with

$${}_iH(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n) = H/H_i(X_i) = \prod_{j \neq i} H_j(X_j)$$

and has the degrees

$$\deg_{X_i} F = \deg f_i, \qquad 1 \leq i \leq n$$

We ask if F is an irreducible polynomial, and formulate this question also as

$$\text{"Is } f = \sum_{i=1}^{n} f_i(X_i) \text{ irreducible?"}$$

Example: There is an **exceptional case**, where this is not the case. Let the characteristic p be positive and $L \in k[X]$ be an additive polynomial of degree > 1, i.e. $L(X + Y) = L(X) + L(Y)$ or equivalently, see [L] p. 343,

$$L(X) = \sum_{j=0}^{m} a_j X^{p^j}, \qquad a_j \in k, \quad m > 0, \quad a_m \neq 0 \tag{4}$$

We say that the given rational functions $(f_i)_{1 \leq i \leq n}$ are **composed** with the additive polynomial L, if there are rational functions $\tilde{f}_i \in k(X)$ such that

$$f_i(X) = L\big(\tilde{f}_i(X)\big)$$

In this case, the polynomial F in (3) is not irreducible: We have

$$f(X_1, \ldots, X_n) = L\Big(\sum_{i=1}^{n} \tilde{f}_i(X_i)\Big)$$

From this and $X \mid L(X)$ we get that $\tilde{f} = \sum_{i=1}^{n} \tilde{f}_i(X_i)$ is a factor of $f(X_1, \ldots, X_n)$ or more precisely (cf. §3, especially lemma 1): The numerator of $\tilde{f}$ is a proper divisor of the numerator F of f, so f is reducible. ∎

RESULTS. Geometrically this example is the only exception:

THEOREM A: *Let k be an algebraically closed field and $n \geq 3$. If for $1 \leq i \leq n$ the nonconstant rational functions f_i given in (1) are not composed with an additive polynomial of degree > 1, then the sum*

$$\sum_{i=1}^{n} f_i(X_i) = \frac{F(X_1, \ldots, X_n)}{H(X_1, \ldots, X_n)}$$

is irreducible, i.e. F is an irreducible polynomial.

Addenda: 1. In the case $n = 2$ the theorem does not hold as stated, the difference $f(X) - f(Y)$ e.g. always has the divisor $X - Y$. Indeed this case (cf. [F]) is more complicate than the case $n \geq 3$ and we do not enter here into its discussion.

2. the theorem shows that the polynomial F is always absolutely irreducible.

3. If k is an algebraically closed field of characteristic $p > 0$, every additive polynomial L of degree > 1 as in (4) has the shape

$$L(X) = L_o(X)^p + c \cdot L_o(X) \qquad \text{for some } c \in k$$

with some other (additive) polynomial L_o, see [T2]. Therefore in theorem A we need only to consider the special additive polynomials $X^p + cX$ and get as an equivalent formulation:

THEOREM A°: *Let k be an algebraically closed field. The polynomial F in (3) is reducible, iff $\operatorname{char} k = p > 0$ and there are $c \in k$ and $g_i \in k(X)$ such that*

$$f_i = g_i^p + cg_i, \qquad 1 \leq i \leq n$$

4. To formulate the correct analogue of theorem A in case of a non algebraically closed field affords the following

Definition: Let $f \in k(X)$ be a rational function. For each rational place $\xi \in \mathbb{P}_1(k) = k \cup \{\infty\}$ and each uniformizing element π, e.g. $\pi = X - \xi$ or $\pi = X^{-1}$, we have a power series expansion

$$f(X) = \sum_{i=\operatorname{ord}_\xi f}^{\infty} c_i \pi^i, \qquad c_i \in k$$

We call the zero$^{\text{th}}$ coefficient c_0 **represented by** the function f and denote it by

$$f(\xi;\pi) := c_0$$

If ξ is not a pole of f, we have of course $c_0 = f(\xi)$, but otherwise c_0 depends on the choice of π, not only on ξ. ∎

Remarks: a) For the properties of $f(\xi;\pi)$ cf. lemma 6.

b) If ξ is a pole of f of order prime to the characteristic, all elements in k are represented by f at this place.

c) For an infinite field k there are always $\xi \in k$ where $f(\xi)$ is finite; but for finite fields k we may have no finite value at a rational place, and therefore need this extended definition of represented elements in theorems B and C.

d) The elements represented by an additive polynomial L are exactly the values of L and form a subgroup k_L^+ of the additive group k^+; the elements represented by a rational function f_i of type (5) in theorem B are contained in a coset of this subgroup k_L^+.

e) A similar statement as d) holds for the functions ℓ in theorem C and the rational functions f_i of type (5*). ∎

5. THEOREM B: *Let k be a field and $n \geq 3$. Suppose that k is perfect if $\operatorname{char} k = 2$. For each $i = 1,\dots,n$ let $f_i \in k(X)$ be a nonconstant rational function and let $c_i \in k$ be an element represented by f_i. Then the sum $\sum_{i=1}^n f_i(X_i)$ is reducible iff there are an additive polynomial $L \in k[X]$ and rational functions $h_i \in k(X)$ such that*

$$f_i(X) - c_i = L\big(h_i(X)\big) \qquad \text{for } 1 \leq i \leq n \tag{5}$$

$$L(X) + \sum_{i=1}^{n} c_i \quad \text{is reducible} \tag{6}$$

More precisely: If the numerator F has two distinct prime factors, we find a separable L, otherwise we can take $L = aX^p$ with some $a \in k^\times$.

6. If k is algebraically closed, any nonconstant function has a rational zero, so we can take $c_i = 0$, moreover (6) is equivalent to $\deg L > 1$. So theorem A follows from theorem B.

7. THEOREM C: *Let k be an imperfect field of characteristic 2, and $n \geq 3$. For each $i = 1,\dots,n$ let $f_i \in k(X)$ be a nonconstant rational function and let $c_i \in k$*

be an element represented by f_i. *Then the sum* $\sum_{i=1}^{n} f_i(X_i)$ *is reducible iff there are rational functions* ℓ, $h_i \in k(X)$ *such that*

$$(5^*) \qquad f_i(X) - c_i = \ell\big(h_i(X)\big) \qquad \text{for } 1 \le i \le n$$

$$(6^*) \qquad \ell(X) + \sum_{i=1}^{n} c_i \text{ is reducible} \qquad \text{or} \qquad \sum_{i=1}^{n} c_i = 0$$

and ℓ *is of one of the following types:*

a) ℓ *is an additive polynomial of degree* > 1.

b) $\ell(X) = \dfrac{X}{X^2+b} + \displaystyle\sum_{j=1}^{m} \frac{a_j X}{(X^2+b)^{2^j}}$ *with* $a_j \in k$ *and* $b \in k \setminus k^2$.

c) $\ell(X) = \dfrac{a}{X^2+b}$ *with* $0 \ne a \in k$ *and* $b \in k \setminus k^2$. *In this case condition (6*) is equivalent to the fact that* $\sum c_i$ *is represented by* ℓ.

In the inseparable quadratic extension field $k_1 = k\big(\sqrt{b}\big)$ *the cases* b) *and* c) *can be converted to* a), *since* $\ell\big(T^{-1} + \sqrt{b}\big)$ *is an additive polynomial.*

From the representation (5*) follows in cases b) and c) that the poles of the rational functions f_i have residue fields containing k_1, especially there is no rational pole. Schinzel gave in [S3] no explicit description of ℓ in case b), but remarked that in this case there is no pole at ∞. So he could regain his earlier result about polynomials [S2, p.53] as special case of his version of theorems B and C.

8. As an application of theorems B and C we determine all rational functions f having an addition formula of type $f(x) + f(y) = f\big(h(x,y)\big)$ for some rational function h. These are, up to a Moebius transformation, essentially the functions L resp. ℓ occurring in theorem B resp. C. The precise formulation is theorem D in §9.

The paper is organized as follows: In §2 we give an account of the history of theorems A – C, in §3 we prove the sufficiency of the conditions. §§4–8 show that the conditions are necessary. In §4 we develop some tools from the theory of composita of algebraic field extensions, used in the proof of the key lemma, in §5 we gather other ingredients. In §6 the key lemma in the proofs by Tverberg, Schinzel and Fried is shown extending ideas of [F]. In §7 we give a proof of theorem B, in §8 we complement §7 to a proof of theorem C. In §9 we determine all rational functions with an addition formula.

2. Historical Remarks

Ehrenfeucht [E] showed that for $n \geq 2$ a complex polynomial of the form

$$F(X_1, \ldots, X_n) = \sum_{i=1}^{n} F_i(X_i), \qquad F_i \in \mathbb{C}[X] \setminus \mathbb{C}, \ \gcd(\deg F_i) = 1$$

is always irreducible. According to [S3] A. Ehrenfeucht and A. Pełczyński proved this for $n = 3$ without a condition on the degrees, but the first published proofs for this more general result in case $n \geq 3$ seem to be those of Schinzel [S1] and Tverberg [T1]. Their proofs carry over to arbitrary fields of characteristic zero. In [T2] Tverberg extended resp. modified this result in the case $n = 3$ for algebraically closed fields of positive characteristic, giving theorem A° in the case of polynomials f_i.

In his book [S2, p.53] Schinzel proved for an arbitrary field k the following generalization: If for given polynomials $F_i \in k[T] \setminus k$ for $i = 1, 2, 3$ the sum $F_1(X) + F_2(Y) + F_3(Z)$ is reducible in $k[X, Y, Z]$, then there are an additive polynomial $L \in k[T]$ and polynomials $F_i^\circ \in k[T]$ such that

$$F_i(T) - F_i(0) = L(F_i^\circ(T)), \qquad i = 1, 2, 3$$

Jarden asked (and used the answer in [HJ], p.194), if such a result would be true if the polynomials are replaced by rational functions, a rational function being called irreducible, if its numerator is irreducible. In [S3] Schinzel gave a precise answer with a rather long and mainly computational proof, stating theorem B with special c_i, coming from the expansion of the f_i in $k((X^{-1}))$, and stating theorem C in a weaker form. Fried [F] gave in the simpler case of characteristic zero another proof, using concepts from Galois theory applied to composita of fields. In this paper his ideas are used to settle the general case using a pure theory of composita which also settles the inseparable case.

3. The conditions are sufficient for the reducibility of F

Definition: For a rational function $f \in k(X)$, say $f = A/B$ with $A, B \in k[X]$, we denote the **order** of f **at infinity** as

$$\operatorname{ord}_\infty f = \deg B - \deg A \qquad \blacksquare$$

LEMMA 1: *Let $R = k[X_1, \dots, X_n]$ be the polynomial ring in n variables over the field k. Let $U, V \neq 0$ be relatively prime polynomials in R with $U/V \notin k$. For a polynomial $A \in k[X]$ in one variable define*

$$A(U,V) := A(U/V) \cdot V^{\deg A}$$

which obviously is in R. Then the following holds:

a) *If $A(U,V)$ is constant, then A is constant or there are $a, b \in k$ with $A = a(X-b)^d$ and $U - bV$ a constant.*

b) *The substitution $A \mapsto A(U,V)$ preserves products:*

$$A, B \in k[X] \implies (A \cdot B)(U,V) = A(U,V) \cdot B(U,V)$$

c) *If $A \neq 0$, then $A(U,V)$ is relatively prime to V. If $A, B \in k[X]$ are relatively prime, then $A(U,V)$ and $B(U,V)$ are relatively prime.*

d) *If $f = A/B$ and $g = U/V$ are representations of the rational functions $f \in k(X)$ and $g \in k(X_1, \dots, X_n) \setminus k$ as quotients of relatively prime polynomials, and if $d = \operatorname{ord}_\infty f$, then*

$$f(g) = \frac{A(g)}{B(g)} = \frac{A(U,V)}{B(U,V)} \cdot V^d \tag{7}$$

is a representation of the composed function $f(g)$ as quotient of relatively prime polynomials — the factor V^d in (7) belongs to the numerator or denominator according to the sign of d.

e) *Let $f = A/B$ and $g = U/V$ be as in* d), *and assume*

$$U \notin k + kV \tag{8}$$

Then $f(g)$ is reducible in each of the following two cases:

e_1) *f is reducible*

e_2) *$\deg f > 1$, $f(\infty) = 0$ and $V \notin k$.*

f) *The condition (8) is satisfied for rational functions of the form*

f_1) $g = \sum_{i=1}^{n} g_i(X_i)$ *with* $g_i \in k(X) \setminus k$ *and* $n \geq 2$.

f_2) $g = \dfrac{g_1(X_1)g_2(X_2, \dots, X_n) + b}{g_1(X_1) + g_2(X_2, \dots, X_n)}$ *with* $g_1 \in k(X)$, $g_2 \in k(X_2, \dots, X_n)$, *both nonconstant, and $b \in k \setminus k^2$. This g is never a polynomial.*

Proof: a) If $A = a\prod_{i=1}^{d}(X - b_i)$ then $A(U,V) = a\prod_{i=1}^{d}(U - b_iV)$. This can only be a constant in the given cases.

b) follows immediately from the definition.

c) The first statement follows immediately from the definition and from $\gcd(U,V) = 1$, the second from this and the fact

$$A(X)\cdot A_1(X)+B(X)\cdot B_1(X) = 1 \Longrightarrow A(U,V)A_1(U,V)+B(U,V)B_1(U,V) = V^d$$

with $d = \deg AA_1 = \deg BB_1$, if A and B are not constant.

d) follows from c).

e) follows from d): A decomposition of $A(X)$ implies by b) a decomposition of the numerator of $f(g)$, which is nontrivial under the assumption (8) by a). This shows e_1). For e_2) one has to observe that in (7) there is now a factor V^d with $d = \operatorname{ord}_\infty f > 0$ in the numerator of $f(g)$. If A is nonconstant then $A(U,V)$ is a second nontrivial factor of the numerator; if A is constant, we have $d = \deg B = \deg f > 1$, so V^2 divides the numerator of $f(g)$.

f_1) Adjoining $X_3, \ldots, X_n$ to k and replacing g_2 by $g_2 + \sum_{i>2} g_i(X_i)$ we may assume $n = 2$, so

$$g = g_1(X_1) + g_2(X_2) = \frac{U_1(X_1)}{V_1(X_1)} + \frac{U_2(X_2)}{V_2(X_2)} = \frac{U_1V_2 + V_1U_2}{V_1V_2} = \frac{U}{V}$$

We have to show that an equation $U = aV + b$ is impossible. If we write it in the form $U_1V_2 + V_1(U_2 - aV_2) = b$, from $U_1/V_1 \notin k$ follows that the coefficients V_2 and $U_2 - aV_2$ of this linear representation of b have to be constants, so U_2 and V_2 would be constants, a contradiction to $g_2 \notin k$.

f_2) As in f_1) we may assume $n = 2$. Then

$$g_1(X_1) = \frac{U_1}{V_1} \quad , \quad g_2(X_2) = \frac{U_2}{V_2} \quad \Longrightarrow \quad g = \frac{g_1g_2 + b}{g_1 + g_2} = \frac{U_1U_2 + bV_1V_2}{U_1V_2 + V_1U_2} = \frac{U}{V}$$

An equation $U = cV + d$ with $c, d \in k$ would lead to

$$U_1(X_1)\cdot[U_2(X_2) - cV_2(X_2)] + V_1(X_1)\cdot[bV_2(X_2) - cU_2(X_2)] = d$$

As in the proof of f_1) follows from $U_1/V_1 \notin k$ that $U_2 - cV_2$ and $bV_2 - cU_2$ are constants. The determinant of these two linear forms in U_2 and V_2 is $b - c^2$, so nonzero by assumption, so U_2 and V_2 have to be constants, a contradiction to $g_2 \notin k$. The last remark, claiming the impossibility of an equation $U_1(X_1)V_2(X_2) + V_1(X_1)U_2(X_2) = \text{const.}$, is proved in the same manner. ∎

Sufficiency in Theorem B: From (5) and the additivity of L we get with $h = \sum_{i=1}^{n} h_i(X_i)$

$$\sum_{i=1}^{n} f_i(X_i) = \sum_{i=1}^{n} \left[L(h_i(X_i)) + c_i\right] = L(h) + \sum_{i=1}^{n} c_i \tag{9}$$

From assumption (6) we know that $L(X)+\sum_{i=1}^{n} c_i$ is reducible in $k[X]$. By lemma 1.e_1/f_1 with $g = h$ we conclude that $L(h)+\sum_{i=1}^{n} c_i$ is reducible in $k(X_1, \ldots, X_n)$. So from (9) we get the reducibility of $\sum_{i=1}^{n} f_i(X_i)$. ∎

Sufficiency in Theorem C: The above proof holds for the case a) of theorem C. To prove the other two cases, we have to get some equivalent of the additivity of L for the functions ℓ in the cases b) and c) of theorem C. This is done in lemma 2 for two summands, in lemma 3 for n summands.

LEMMA 2: *Let k be a field of characteristic 2.*

a) *For $b \in k$ and variables x, y over k the following holds:*

$$z = \frac{xy+b}{x+y} \implies \frac{1}{x^2+b} + \frac{1}{y^2+b} = \frac{1}{z^2+b} \tag{10}$$

$$\frac{x}{x^2+b} + \frac{y}{y^2+b} = \frac{z}{z^2+b} \tag{10'}$$

b) *The rational function*

$$\ell(X) = \frac{a_0 + \tilde{a}_0 X}{X^2+b} + \sum_{j=1}^{m} \frac{a_j}{(X^2+b)^{2^j}} \tag{11}$$

in $k(X)$ satisfies for variables x, y the addition formula

$$\ell(x) + \ell(y) = \ell(z) \qquad \text{with} \quad z = \frac{xy+b}{x+y} \tag{12}$$

Proof of a): Direct verification:

$$\frac{x}{x^2+b} + \frac{y}{y^2+b} = \frac{(x+y)(xy+b)}{(xy+b)^2 + b(x+y)^2} = \frac{z}{z^2+b}$$

gives (10'), and (10) follows from this by applying $\frac{\partial}{\partial x} + \frac{\partial}{\partial y}$. ∎

Proof of b): By iterated squaring of (10) we see from a) that each summand of $\ell(X)$ satisfies (12), therefore also the sum $\ell(X)$. ∎

LEMMA 3: *Let $n \geq 1$. The function $\ell(X)$ from (11) satisfies for variables $x_1, \ldots, x_n$ over k the addition formula*

$$\sum_{i=1}^{n} \ell(x_i) = \ell(z_n)$$

with

$$z_n = \frac{A_n(x_1, \ldots, x_n)}{B_n(x_1, \ldots, x_n)} = \frac{\sum_{i=0}^{\lfloor n/2 \rfloor} \sigma_{n-2i} b^i}{\sum_{i=0}^{\lfloor (n-1)/2 \rfloor} \sigma_{n-1-2i} b^i} = \frac{\sigma_n + b\sigma_{n-2} + \cdots}{\sigma_{n-1} + b\sigma_{n-3} + \cdots}$$

where

$$\sigma_r = \sum_{1 \leq i_1 < \cdots < i_r \leq n} x_{i_1} \cdots x_{i_r}$$

is the r^{th} elementary symmetry function of $x_1, \ldots, x_n$, so $\sigma_0 = 1$ and $\sigma_r = 0$ for $r < 0$ or $r > n$.

Proof by induction: The case $n = 1$ is trivial, the case $n = 2$ is lemma 2.b. Assume the claim holds for n summands. Then we have by lemma 2.b and induction hypothesis

$$\sum_{i=1}^{n+1} \ell(x_i) = \ell(z_{n+1}) \qquad \text{with} \quad z_{n+1} = \frac{x_{n+1} z_n + b}{z_n + x_{n+1}}$$

Denoting by σ_r the elementary symmetric functions of $x_1, \ldots, x_n$ and by $\tilde{\sigma}_r$ the elementary symmetric functions of $x_1, \ldots, x_{n+1}$ we have the simple recursion formulas

$$x_{n+1} \cdot \sigma_r + \sigma_{r+1} = \tilde{\sigma}_{r+1}, \qquad r \in \mathbb{Z}$$

With these we get

$$\begin{aligned} z_{n+1} &= \frac{x_{n+1} A_n + b B_n}{A_n + x_{n+1} B_n} = \frac{\sum_i x_{n+1} \sigma_{n-2i} b^i + \sum_i \sigma_{n-1-2i} b^{i+1}}{\sum_i \sigma_{n-2i} b^i + \sum_i x_{n+1} \sigma_{n-1-2i} b^i} \\ &= \frac{\sum_i (x_{n+1} \sigma_{n-2i} + \sigma_{n+1-2i}) b^i}{\sum_i (\sigma_{n-2i} + x_{n+1} \sigma_{n-1-2i}) b^i} = \frac{\sum_i \tilde{\sigma}_{n+1-2i} b^i}{\sum_i \tilde{\sigma}_{n-2i} b^i} = \frac{A_{n+1}}{B_{n+1}} \end{aligned}$$

which ends the induction step. ∎

End of the sufficiency proof: If ℓ is one of the functions in case b) or c) of theorem C, it has the form (11). By lemma 3 we get from (5*) a formula

$$(9^*) \qquad \sum_{i=1}^{n} f_i(X_i) = \ell(h) + \sum_{i=1}^{n} c_i \qquad \text{with} \quad h = z_n\big(h_1(X_1), \ldots, h_n(X_n)\big)$$

By assumption (6*) we have to distinguish two cases: The first case is $c := \sum_{i=1}^{n} c_i \neq 0$ and $\ell(X) + c$ reducible. Because of $h = z\big(h_1, z_{n-1}(h_2, \ldots, h_n)\big)$ we can apply lemma $1.e_1/f_2$ with $g_1 = h_1$ and $g_2 = z_{n-1}(h_2, \ldots, h_n)$ to get the reducibility of $\ell(h) + c$. By (9*) the reducibility of $\sum_{i=1}^{n} f_i(X_i)$ follows in the first case. To settle the second case $c = 0$ we have by (9*) to show that $\ell(h)$ is reducible. By the assumptions in theorem C we have $\deg \ell > 1$ and $\ell(\infty) = 0$, moreover $z_{n-1}(h_2, \ldots, h_n) = z\big(h_2, z_{n-2}(h_3, \ldots, h_n)\big)$ is not a polynomial for $n > 2$, as remarked at the end of lemma 1. So the reducibility of $\ell(h)$ follows from lemma $1.e_2/f_2$ with g_1 and g_2 as in the first case. ∎

4. Composita of algebraic field extensions

Let K be a field of characteristic $p \geq 0$ with a fixed algebraic closure $\tilde{K}$. An algebraic extension K_1 of K can be embedded into $\tilde{K}$, but such an embedding $\tau : K_1 \hookrightarrow \tilde{K}$ is determined only up to applying an automorphism $\sigma \in G_K = \mathrm{Aut}(\tilde{K}|K)$, i.e. up to switching from τ to $\tau\sigma$, thereby replacing the subfield K_1^{τ} of $\tilde{K}$ by the conjugate field $K_1^{\tau\sigma}$. If K_1 is already a subfield of $\tilde{K}$, then the K-embeddings of K_1 into $\tilde{K}$ correspond to the cosets in $G_{K_1}\backslash G_K$.

Let now K_1 and K_2 be two finite algebraic extensions of K which we always suppose to be subfields of $\tilde{K}$.

Definition: A **compositum** of the fields K_1 and K_2 over K is a pair $(\sigma_1, \sigma_2) \in (G_{K_1}\backslash G_K) \times (G_{K_2}\backslash G_K)$ of K-embeddings of K_1 and K_2 into $\tilde{K}$. The pairs (σ_1, σ_2) and $(\sigma_1\sigma, \sigma_2\sigma)$ with $\sigma \in G_K$ are called **isomorphic** composita. ∎

Alternatively a pair (σ_1, σ_2) of K-embeddings $\sigma_i : K_i \hookrightarrow \tilde{K}$ induces a K-algebra homomorphism

$$\sigma_1 \otimes \sigma_2 : K_1 \otimes_K K_2 \to \tilde{K}, \qquad x_1 \otimes x_2 \mapsto x_1^{\sigma_1} \cdot x_2^{\sigma_2}$$

and conversely any such homomorphism induces a compositum of K_1 and K_2 over K. Two composita (σ_1, σ_2) and (σ_1', σ_2') are isomorphic iff the kernels of the associated maps $\sigma_1 \otimes \sigma_2$ and $\sigma_1' \otimes \sigma_2'$ coincide. These kernels are prime ideals of

$K_1 \otimes_K K_2$ and all prime ideals $\mathfrak{p} \in \operatorname{Spec}(K_1 \otimes_K K_2)$ occur as such kernels since $K_1 \otimes_K K_2$ is algebraic over K, so $(K_1 \otimes_K K_2)/\mathfrak{p}$ can be embedded into $\tilde{K}$.

Therefore the number of different composita of K_1 and K_2 over K is given by

$$\kappa(K_1, K_2 | K) := \#\operatorname{Spec}(K_1 \otimes_K K_2)$$

and this number equals the number of double cosets in $G_{K_1} \backslash G_K / G_{K_2}$, which is used in [F]. Since $K_1 \otimes_K K_2$ is a finite dimensional K-algebra, this number is finite and we have, cf. [L], p.250 or 258, a direct decomposition into local artinian rings

$$K_1 \otimes_K K_2 = \bigoplus_{i=1}^{\kappa(K_1, K_2 | K)} L_i, \qquad L_i \text{ local}$$

We will use here the following simple facts about the number $\kappa(K_1, K_2 | K)$:

(C1) Let $K_1 = K(a)$ be a simple extension and $f \in K[X]$ be the (monic) minimal polynomial of a over K, such that $K_1 \simeq K[X]/(f)$. Then by the Chinese remainder theorem one has

$$f = \prod_{i=1}^{r} f_i^{e_i} \text{ in } K_2[X] \implies K_1 \otimes_K K_2 \simeq K_2[X]/(f) \simeq \bigoplus_{i=1}^{r} K_2[X]/(f_i^{e_i})$$

where f_i are the different irreducible factors of f in $K_2[X]$ and the exponents e_i are 1 or powers of p. Therefore we have

$$\kappa(K_1, K_2 | K) = r = \#\{\text{irreducible factors of } f \text{ in } K_2[X]\}$$

and if $\kappa(K_1, K_2 | K) = 1$, then $K_1 \otimes_K K_2$ has a nontrivial radical iff $f \in K_2[X]^p$.

(C2) Let K_1^{sep} resp. K_2^{sep} be the separable parts of the field extensions $K_1|K$ resp. $K_2|K$. Because homomorphisms from rings to fields extend uniquely to purely inseparable extensions, we have

$$\kappa(K_1, K_2 | K) = \kappa(K_1^{\text{sep}}, K_2^{\text{sep}} | K)$$

(C3) If K_1 or K_2 is separable over K, then $K_1 \otimes_K K_2$ has no radical, so is a direct sum of fields. In this case

$$\begin{aligned} \kappa(K_1, K_2 | K) = 1 &\iff K_1 \otimes_K K_2 \text{ is a field} \\ &\iff K_1, K_2 \text{ linearly disjoint over } K \end{aligned}$$

(C4) If $K_1' \subseteq K_1$ is a smaller extension of K, one has

$$\kappa(K_1', K_2\,|K) \leq \kappa(K_1, K_2\,|K) \tag{13}$$

Equality holds in (13), if all residue fields of $K_1' \otimes_K K_2$ are linearly disjoint from K_1 over K_1'.

Proof: This follows from

$$K_1' \otimes_K K_2 = \bigoplus_{i=1}^{\kappa} L_i \quad \Longrightarrow \quad K_1 \otimes_K K_2 = \bigoplus_{i=1}^{\kappa} K_1 \otimes_{K_1'} L_i$$

(C5) If K_1 and K_2 are simple extensions of K with $\kappa(K_1, K_2\,|K) = 1$ and $K_1 \otimes_K K_2$ has a nontrivial radical, then each K_i contains exactly one inseparable extension L_i of degree p of K, and $L_1 \simeq_K L_2$.

Proof: Let $K_1 = K[X]/(f)$ with f monic. If $K_1 \otimes_K K_2$ is local with nontrivial radical, then (C1) implies that the coefficients of f become p^{th} powers in K_2. Let L_2 be the subfield of K_2, generated over K by the p^{th} roots of the coefficients of f. Since a subextension of a simple extension like $K_2|K$ is simple (this follows from [L], theorem VI.6.1), we see that $[L_2 : K] = p$ and L_2 is the only inseparable extension of K in K_2 of degree p. Then $K_1 \otimes_K L_2$ has a nontrivial radical, so its only residue field is K_1, therefore K_1 contains an isomorphic copy L_1 of the K-algebra L_2. ∎

For later convenience we restate (C1) and (C5) in a special case:

LEMMA 4: *Let f_1, f_2 be rational functions as in (1). Then the equations*

$$f_1(x_1) = y = f_2(x_2)$$

define two algebraic extensions $K_1 = k(x_1)$ and $K_2 = k(x_2)$ of the rational function field $K = k(y)$, and the number of irreducible factors of the numerator $N(X_1, X_2) = F_1(X_1)H_2(X_2) - H_1(X_1)F_2(X_2)$ of the rational function $f_1(X_1) - f_2(X_2)$ equals the number $\kappa(K_1, K_2\,|K)$ of composita of the two algebraic extensions of K. Moreover if $\kappa(K_1, K_2\,|K) = 1$ then $K_1 \otimes_K K_2$ has a nontrivial radical iff N is inseparable (namely a p^{th} power up to a constant) iff the fields K_i both contain $\sqrt[p]{y_\circ}$, where $y_\circ$ is some linear fraction in y.

Proof: Since $F_2(X_2) - YH_2(X_2)$ is irreducible in $K_2[X_2, Y]$, the minimal polynomial f of x_2 over K is $F_2(X_2) - yH_2(X_2)$ up to a factor. Over K_1 this polynomial

becomes essentially $N(X_1, X_2)$, and the lemma follows from (C1). The last statement follows from (C5) and its proof, since the coefficients of f are linear fractions $(ay+b)/(cy+d)$ with $a, b, c, d \in k$. ∎

The following essential result about counting composita we take from [F], but replace the geometric language there by a pure field theoretic formulation (which seems to be more appropriate) and remove group theory from the proof (which shortens the proof):

LEMMA 5: *If K_1 and K_2 are finite algebraic extensions of K, then there are separable subextensions K_1' and K_2', which have the same Galois hull over K and the same number of composita over K as the given fields K_1 and K_2, in formulas:*

$$K \subseteq K_i' \subseteq K_i, \qquad K_i'|K \text{ separable}, \qquad i = 1, 2$$
$$\widehat{K_1'} = \widehat{K_2'}, \qquad \kappa(K_1, K_2|K) = \kappa(K_1', K_2'|K)$$

where the normal hull $\widehat{K'}$ of an algebraic extension $K'|K$ is the smallest normal extension of K, containing K'.

Proof: By (C2) we may assume that the extensions $K_i|K$ are separable for $i = 1, 2$. If $\widehat{K_1} = \widehat{K_2}$, we are done. Otherwise we may assume $K_1 \not\subseteq \widehat{K_2}$. Take $L_1 = K_1 \cap \widehat{K_2} < K_1$. Since $\widehat{K_2}|K$ is Galois, the fields K_1 and $\widehat{K_2}$ are linearly disjoint over L_1, so all residue fields of $L_1 \otimes_K K_2$, being subfields of $\widehat{K_2}$ and containing L_1, are linearly disjoint from K_1 over L_1. From (C4) we get

$$\kappa(K_1, K_2|K) = \kappa(L_1, K_2|K)$$

with $L_1 < K_1$. Continuing this procedure we come to the conclusion of the lemma. ∎

5. Other ingredients

In this paragraph we state some auxiliary facts. Lemma 7 is only used in the proof of lemma 8 which takes its motivation from the key lemma 9, whose proof uses Gordan's theorem.

THEOREM OF LÜROTH/GORDAN (1876/1887, see [S2, p.6/9]): *Let $L|K$ be a field extension of transcendence degree 1 which is contained in a rational function field, i.e. in a purely transcendental extension $K(X_1, X_2, \ldots, X_n)|K$. Then $L = K(t)$ is itself a rational function field.*

LEMMA 6: *The symbol $f(\xi;\pi)$ for the zeroth coefficient of the expansion of a rational function $f \in k(X)$ at a place ξ with respect to a uniformizing element π, as defined in 1.4, has the following properties:*

a) *It is linear in f : For $f_1, f_2 \in k(X)$ and $\lambda_1, \lambda_2 \in k$ holds*

$$(\lambda_1 f_1 + \lambda_2 f_2)(\xi;\pi) = \lambda_1 f_1(\xi;\pi) + \lambda_2 f_2(\xi;\pi)$$

b) *If $\operatorname{char} k = p$ then $f(\xi;\pi)^p = f^p(\xi;\pi)$. [But otherwise it does not behave well under multiplication, and therefore not under composition of rational functions.]*

c) *From* a) *and* b) *follows that an additive polynomial $L \in k[X]$ satisfies*

$$L\big(f(\xi;\pi)\big) = (L \circ f)(\xi;\pi), \qquad f \in k(X)$$

Proof: Immediate computation. ∎

LEMMA 7 (MULTINOMIAL COEFFICIENTS): *For $i = 1, \ldots, r$ let $n_i \geq 0$ be natural numbers with sum n. Then the coefficient of $X_1^{n_1} X_2^{n_2} \cdots X_r^{n_r}$ in the polynomial $(X_1 + X_2 + \cdots + X_r)^n$ is the natural number*

$$\binom{n}{n_1\ n_2\ \cdots\ n_r} = \frac{n!}{n_1!\, n_2! \cdots n_r!}$$

It is not divisible by the prime p, iff no carry over occurs in the summation $n_1 + n_2 + \cdots + n_r$, done in the p-adic representation of the integers n_i. This condition means that the p-adic digits of the sum are the sum of the p-adic digits of the summands. A trivial example for this case is

$$n = 0 + \cdots + 0 + n + 0 + \cdots + 0$$

and exactly if n is a power of p these are the only examples for a sum n without carry over.

Proof: If ord_p denotes the p-adic valuation on rational numbers, i.e. the exponent of p occurring in the prime factorization, one has the well known formula, cf. e.g. [H], p.263,

$$\operatorname{ord}_p(n!) = \frac{n - s_p(n)}{p-1} \tag{14}$$

where $s_p(n)$ is the sum of the digits in the p-adic representation of n. In the case $n = \sum_{i=1}^{r} n_i$ we have

$$0 \leq \operatorname{ord}_p \binom{n}{n_1\ n_2\ \dots\ n_r} = \operatorname{ord}_p(n!) - \sum_{i=1}^{r} \operatorname{ord}_p(n_i!)$$

and from (14) follows

$$s_p(n) \leq \sum_{i=1}^{r} s_p(n_i)$$

with equality iff the multinomial coefficient is not divisible by p:

$$\binom{n}{n_1\ n_2\ \dots\ n_r} \not\equiv 0 \bmod p \iff s_p(n) = \sum_{i=1}^{r} s_p(n_i)$$

The right hand side is an equivalent of saying that no carry over occurs in the p-adic summation of the n_i. This shows lemma 7 and the following corollary. ∎

COROLLARY: *If* $\binom{n}{n_1\ n_2\ \dots\ n_r} \not\equiv 0 \bmod p$, *then* $\binom{n}{m\ m'\ 0\ \dots\ 0} \not\equiv 0 \bmod p$ *with*

$$m = \sum_{i=1}^{s} n_i, \qquad m' = \sum_{i=s+1}^{r} n_i, \qquad 0 \leq s \leq r$$

LEMMA 8: *If* $G \in k[T] \setminus k$ *is a polynomial and* $f_i \in k(X) \setminus k$ *are rational functions for* $i = 1, \dots, m$ *with* $m > 1$ *and* $h \in k(X_1, \dots, X_m)$ *such that*

$$G\big(h(X_1, \dots, X_m)\big) = \sum_{i=1}^{m} f_i(X_i) \tag{15}$$

then we have a decomposition

$$h(X_1, \dots, X_m) = \sum_{i=1}^{m} h_i(X_i) \tag{16}$$

with $h_i \in k(X)$ *for* $i = 1, \dots, m$ *and* $G - G(0)$ *is an additive polynomial.*

Proof: Since the decomposition (16) is unique, if it exists, up to additive constants, we may assume the field k to be algebraically closed. From (15) follows that every pole of the rational function h is a pole of one of the rational functions $f_i(X_i)$. Therefore h is of the form

$$h(X_1, \dots, X_m) = \frac{A(X_1, \dots, X_m)}{B_1(X_1) \cdots B_m(X_m)}$$

with polynomials A and B_i. Since k is algebraically closed there are substitutions $X_i := X_i - \xi_i$, $h := h - \tau$ and $G(t) := G(t + \tau)$ such that

$$f_i(0) = 0 \quad , \quad \text{so} \quad B_i(0) \neq 0 \qquad \text{and} \qquad h(0, \ldots, 0) = 0$$

Thus $G(0) = 0$ and we can write h as a power series in $X_1, \ldots, X_m$. Putting $h_i(X_i) := h(0, \ldots, X_i, \ldots, 0)$, we get $f_i = G(h_i)$. Let

$$r(X_1, \ldots, X_m) := h(X_1, \ldots, X_n) - \sum_{i=1}^{m} h_i(X_i)$$

Then r is a rational function whose denominator divides that of h and which satisfies $r(0, \ldots, X_i, \ldots, 0) = 0$. Hence each monomial in the numerator of r is divisible by at least two variables, so that we may write (the fraction need not be reduced)

$$(17) \qquad r = \frac{C(X_1, \ldots, X_m)}{B_1(X_1) \cdots B_m(X_m)} \qquad \text{with} \quad C = \sum_{i<j} P_{ij} X_i X_j$$

We have to show that $r = 0$. Otherwise some variable occurs in r, say X_1, and r, as a rational function in X_1, has a pole which may be a zero ξ of B_1 or ∞. By a transformation $X_1 := \xi + X_1^{-1}$ in the first case we may assume $X_1 = \infty$ to be a pole of r. From (17) we get power series expansions in $R((X_1^{-1}))$ with $R = k[[X_2, \ldots, X_m]]$:

$$(18) \qquad r = c_0 X_1^{e_0} + d_0 X_1^{e_0 - 1} + \cdots, \qquad h_1 = c_1 X_1^{e_1} + d_1 X_1^{e_1 - 1} + \cdots$$

with descending exponents, $e_0 > 0$, $e_1 \in \mathbb{Z}$, $c_1 \in k^\times$ and $c_0 \in \mathfrak{p} \setminus \{0\}$ where $\mathfrak{p} = (X_2, \ldots, X_m)$ is the maximal ideal of R. We develop the polynomial G as

$$(19) \qquad G(Y_0 + Y_1 + \cdots + Y_m) = \sum_{(i_0 i_1 \ldots i_m) \in J} a_{i_0 i_1 \ldots i_m} Y_0^{i_0} \cdots Y_m^{i_m}$$

where the finite index set $J \subseteq \mathbb{N}_0^{m+1}$ with $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$ contains only the indices (i) with $a_{(i)} \neq 0$. Then J is symmetric, contains $(d\,0 \ldots 0)$ with $d = \deg G$ and satisfies the condition

$$(20) \qquad (i_0 i_1 \ldots i_m) \in J \implies (j i_1 0 \ldots 0) \in J$$

with $j = i_0 + i_2 + \cdots + i_m$ by the corollary of lemma 7. We substitute $Y_i := h_i$ and $Y_0 := r$ in (19) to get

$$G\big(h(X_1, \ldots, X_m)\big) = \sum_{(i)\in J} a_{(i)} r^{i_0} h_1^{i_1} \cdots h_m^{i_m} \tag{21}$$

Substituting the expansions (18) into equation (21) we get a representation of $G(h)$ as power series in $R(\!(X_1^{-1})\!)$. By (20) the highest powers of X_1 in $G(h)$ come from elements of type $(i_0 i_1 0 \ldots 0) \in J$, i.e. from

$$r^{i_0} h_1^{i_1} = c_0^{i_0} c_1^{i_1} X_1^{i_0 e_0 + i_1 e_1} + \cdots$$

The elements $c_0^a X_1^b$ in the leading terms are linearly independent over k since $0 \neq c_0 \in \mathfrak{p}$. Choose $(i_0, i_1) \in \mathbb{N}_0^2$ such that

$$i_0 > 0 \qquad (i_0 i_1 0 \ldots 0) \in J \qquad i_0 e_0 + i_1 e_1 = e \ \text{ maximal}$$

From $(d0 \ldots 0) \in J$ follows $e > 0$. The leading term $L = c c_0^{i_0} X_1^e$ of $a_{(i_0 i_1 0 \ldots 0)} r^{i_0} h_1^{i_1}$ with $c \in k^\times$ cannot cancel against any other term in (21): First no other term in (21) starts with a higher power of X_1 — except possibly the summands $h_1^{i_1}$, however they are in $k(\!(X_1^{-1})\!)$, so cannot cancel against L. Secondly we have already seen that the leading term L is linearly independent from other leading terms $c_0^a X_1^e$ with $a \neq i_0$ and the same exponent e in (21). Since L does not cancel, in $G(h)$ occurs a term $c c_0^{i_0} X_1^e$ with $i_0 > 0$ and $e > 0$. This contradicts equation (15), by which $G(h) \in k(\!(X_1^{-1})\!) + k(X_2, \ldots, X_m)$, since $c_0 \in \mathfrak{p} \setminus \{0\}$. This contradiction shows $r = 0$ and gives the equation (16).

To show that $G - G(0)$ is additive we first remark that (15) and (16), putting $X_j = 0$ for $j \neq i$, together with $f_j(0) = 0$ implies $G(h_i) = f_i(X_i)$. Now look at equation (21) with $r = 0$. All the summands $h_1^{i_1} h_2^{i_2} \cdots h_m^{i_m}$ are linearly independent over k, since the $h_i(X_i)$ are algebraically independent over k. Therefore the equation (15), i.e.

$$\sum_{(i)\in J} a_{(i)} h_1^{i_1} \cdots h_m^{i_m} = \sum_{i=1}^{m} G(h_i)$$

can only hold, if all elements in J have at most one non zero entry. By lemma 7 this implies that all positive exponents occurring in the polynomial G are powers of p. This gives the additivity of $G - G(0)$. ∎

6. The Key Lemma

We now take the first step to draw conclusions from the reducibility of the numerator F of $\sum_{i=1}^{n} f_i(X_i)$ with $n \geq 3$. We distinguish two cases: If F has two different prime factors, we speak of the first case. The second case is an F which is up to a constant a nontrivial power of an irreducible polynomial. The following key step in the proof of the theorems shows that the reducibility of F implies a functional decomposition of the sum of all but one of the $f_i(X_i)$.

KEY LEMMA 9: *Let F be the polynomial of (3).*

1. CASE: *If F has more than one prime factor, then there is a separable rational function $g \in k(X)$ of degree ≥ 2 and a rational function $h \in k(X_2, \ldots, X_n)$ such that*

$$g\big(h(X_2, \ldots, X_n)\big) = \sum_{i=2}^{n} f_i(X_i) \tag{22}$$

and

$$g(Z) + f_1(X_1) \quad \text{is reducible} \tag{23}$$

2. CASE: *If F is up to a constant factor a nontrivial power of an irreducible polynomial, the above assertions (22) and (23) are true with $g(X) = l(X^p)$ for some linear fractional function $l(t) = (at + b)/(ct + d)$ with $a, b, c, d \in k$ and $ad \neq bc$. In this case the reducibility claim (23) can be formulated as: There is an $h_1 \in k(X)$ such that $f_1(X) = -g\big(h_1(X)\big)$.*

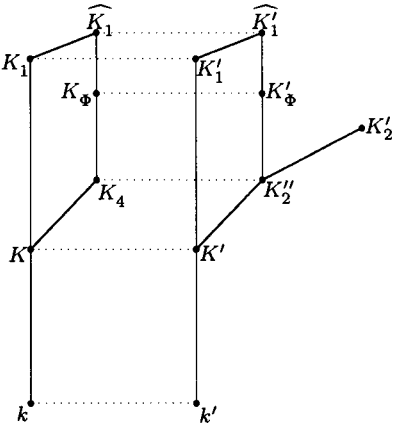
Proof of 1. case: F has more than one prime factor. Let $k' = k(X_3, \ldots, X_n)$ and apply lemma 4 to the two rational functions $-f_1(X)$ and $f_2(X) + \sum_{i=3}^{n} f_i(X_i)$ in $k'(X)$: The equations

$$f_2(x_2) + \sum_{i=3}^{n} f_i(X_i) = y = -f_1(x_1)$$

define two algebraic extensions $K_1' = k'(x_1)$ and $K_2' = k'(x_2)$ of $K' = k'(y)$, and the irreducible factors of the numerator F of $f = f_1(X_1) + \cdots + f_n(X_n)$ correspond to the composita of K_1' and K_2' over K'. From the assumption of the first case follows that there are at least two different composita of K_1' and K_2' over K'. By lemma 5 we can replace K_i' by separable subfields $K_i'' \supset K$ with

$$\widehat{K_1''} = \widehat{K_2''} \qquad \text{and} \qquad \kappa(K_1'', K_2'' \,|K') > 1 \tag{24}$$

From $K_2'' = K'$ we get $\kappa(K_1'', K_2''|K') = 1$ by (C1); therefore $[K_2'' : K'] > 1$. Now the Galois hull $\widehat{K_1''}$ of $K_1''|K'$ is contained in the separable part K'_Φ of the splitting field $\widehat{K_1'}$ of the minimal polynomial $\Phi = F_1 + yH_1$ for x_1 over K'. Since Φ has coefficients in $K = k(y)$, the Galois extension $K'_\Phi|K'$ is a constant field extension of the Galois extension $K_\Phi|K$, where K_Φ is the separable part of the splitting field $\widehat{K_1}$ of Φ over K. Since $K' = K(X_3, \ldots, X_n)|K$ is purely transcendental, the extensions K_Φ and K' are linearly disjoint over K, so we have



$$\mathrm{Gal}(K_\Phi|K) = \mathrm{Gal}(K'_\Phi|K')$$

and the intermediate fields of these extensions correspond bijectively. By the equation in (24) we have $K_2'' \subseteq \widehat{K_2''} = \widehat{K_1''} \subseteq K'_\Phi$, so the field K_2'' has the form $K_2'' = K_4(X_3, \ldots, X_n)$ with some separable extension $K_4|K$. Since $K_4|k$ is a function field of one variable, contained in the rational function field $K_2' = k(x_2, X_3, \ldots, X_n)|k$, by Gordan's theorem it is itself rational over k. So we have $K_4 = k(z) \supseteq k(y)$, which gives an equation $y = g(z)$ with a separable rational function $g \in k(X)$ of degree $[K_4 : K] = [K_2'' : K'] > 1$. From $z \in K_2'$ we get a rational function $h \in k(X_2, \ldots, X_n)$ such that $z = h(x_2, X_3, \ldots, X_n)$. Together we get

$$f_2(x_2) + \sum_{i=3}^{n} f_i(X_i) = y = g(z) = g\big(h(x_2, X_3, \ldots, X_n)\big)$$

so equation (22). Since $K_1' = k'(x_1)$ and $K_2'' = k'(z)$ have by (24) more than one compositum, by lemma 4 the numerator of $g(Z) + f_1(X_1)$ is reducible over k' and so over k. Now all claims are proved in the first case.

Proof of 2. case: In this case we have $\kappa(K_1', K_2'|K') = 1$ in the notation of the proof of the first case, so by the last part of lemma 4 the polynomial F is up to a constant factor a p^{th} power. We modify the proof of the first case as follows: Lemma 4 shows that K_1' and K_2' both contain a unique subfield K_2'', inseparable of degree p over K'. Since the algebraic extension $K_1'|K'$ comes from the simple extension $K_1 = K(x_1)|K$, given by $\Phi(x_1) = 0$, by a purely transcendental base

extension $K'|K$, the lattices of intermediate fields of $K_1'|K'$ and $K_1|K$ correspond bijectively to each other, preserving inclusions, degree, separability: Intermediate fields $K_\circ$ of $K_1|K$ correspond to the monic divisors $\Phi_\circ$ of Φ in $K_1[X]$, having the zero x_1 and being irreducible in the field $K_\circ$ generated over K by its coefficients; over K' the same polynomials $\Phi_\circ$ occur, which proves the claim. So the field K_2'' comes from a unique subfield $K_4 \subseteq K_1$, inseparable of degree p over K. As above we get $K_4 = k(z)$ and $y = g(z)$ with g inseparable of degree p, so $g(z) = l(z^p)$ with a linear fractional function l. As above we come to equation (22). From $z \in K_1$ we get some $h_1 \in k(X)$ with $z = h_1(x_1)$, so $f_1(x_1) = -y = -g(z) = -g(h_1(x_1))$. This implies (23). ∎

7. Proof of theorem B (Necessity)

We take the common assumptions of theorems B and C: There are at least three non constant rational functions $f_i \in k(X)$, represented elements $c_i \in k$ and the sum $\sum_{i=1}^n f_i(X_i)$ is reducible. We start from the key lemma to get an equation (22) which we will exploit now. Differentiating equation (22) we get for $i = 2, \dots, n$

$$(25)\quad g'\big(h(X_2,\dots,X_n)\big)\cdot h^{(i)}(X_2,\dots,X_n) = f_i'(X_i) \qquad \text{with} \quad h^{(i)} = \frac{\partial h}{\partial X_i}$$

with $g' \neq 0$ in the first case and $g' = 0$ in the second case.

In lemma 10 and propositions 11 and 14, which belong to the first case of the key lemma, we will assume that

$$f_i'(X_i) \neq 0, \qquad 2 \leq i \leq n$$

Namely $f_i' = 0$ implies by (25) that $h^{(i)} = 0$, so f_i and h are functions in X_i^p. By an iterated change of variables of type $X_i^p := X_i$ in (22), which does not change g, we come to the above assumption.

In the following lemma and its proof we use the notion of degree of a rational function as defined in (2).

LEMMA 10: *A separable rational function g satisfying equation (22) satisfies*

$$\deg g' \leq 2$$

Proof: Taking the partial derivative of

$$h(X_2,\dots,X_n) = \frac{A(X_2,\dots,X_n)}{B(X_2,\dots,X_n)} \qquad \gcd(A,B) = 1$$

with respect to X_2 we get, writing $h^{(2)}$ for $\partial h/\partial X_2$,

$$h^{(2)} = \frac{A^{(2)}}{B} - \frac{AB^{(2)}}{B^2}$$

Hence

$$\deg_{X_3} h^{(2)} \leq 2 \cdot \deg_{X_3} h \tag{26}$$

The equation in (25) with $i = 2$ has a right hand side f_2' free from X_3 (remember that we can assume $f_2' \neq 0$), therefore we have

$$\deg_{X_3} g'(h) = \deg_{X_3} h^{(2)}$$

Together with (26) we get

$$\deg g' \cdot \deg_{X_3} h = \deg_{X_3} g'(h) = \deg_{X_3} h^{(2)} \leq 2 \cdot \deg_{X_3} h$$

Dividing through $\deg_{X_3} h$ gives the lemma. ∎

PROPOSITION 11: *Let k be a field and let k be perfect if $\operatorname{char} k = 2$. Then a separable rational function $g(t)$ satisfying (22) has after a linear fractional transformation in t the derivative*

$$g'(t) = 1$$

Proof: A linear fractional transformation

$$l(t) = \frac{at+b}{ct+d} = \frac{U}{V} \qquad a, b, c, d \in k,\ ad - bc = \Delta \neq 0$$

transforms equation (22) into an equation of the same shape via $g \circ h = g_l \circ h_l$ with $g_l = g \circ l$ and $h_l = l^{-1} \circ h$. By lemma 10 we have $\deg g_l' \leq 2$. Moreover, with $g' = A/B$ we have by the chain rule and (7)

$$g_l'(t) = g'(l(t)) \cdot \frac{\Delta}{(ct+d)^2} = \Delta \cdot \frac{A(U,V)}{B(U,V)} \cdot V^{\deg B - \deg A - 2} \tag{27}$$

We first show that the numerator A of g' has to be a constant. Otherwise choose a transformation l such that $c \neq 0$ and $B(a/c) \neq 0$, perhaps enlarging the base field k if $k = \mathbb{F}_2$. From

$$B(X) = \sum_{i=0}^{m} a_i X^i \quad \Longrightarrow \quad B(U,V) = \sum_{i=0}^{m} a_i (at+b)^i (ct+d)^{m-i} = B(a/c)c^m t^m + \cdots$$

follows that $\deg B = \deg B(U,V)$. But a nonconstant A leads in (27) to g_l' having a denominator $B(U,V) \cdot V^{2+\deg A - \deg B}$ of degree $2 + \deg A > 2$, contradicting $\deg g_l'(t) \leq 2$.

Moreover as a derivative of a rational function g' cannot have a simple rational pole, so by lemma 10, i.e. by $\deg B \leq 2$, either $g'(t) = a \neq 0$ is constant or g' is of the shape

$$g'(t) = \frac{b}{(t+c)^2}\,, \qquad 0 \neq b, c \in k$$

[here we use that k is not imperfect of characteristic 2, because in this case also the possibility $g' = a(t^2+b)^{-1}$ with $b \notin k^2$ has to be considered.] The linear fractional transformation $l(t) = a^{-1}t$ or $l(t) = -c + bt^{-1}$ then gives $g_l' = 1$. ∎

COROLLARY 12: *If k has characteristic zero, then equation (22) with $\deg g \geq 2$ is impossible, so theorem A is true.*

Proof: If $\operatorname{char} k = 0$, from proposition 11 follows that g is a linear polynomial. This contradicts the assumption $\deg g > 1$ in the key lemma. So equation (22) is impossible which means that F is always irreducible. ∎

Convention: In the following we have $\operatorname{char} k = p > 0$. ∎

COROLLARY 13: *The equation (25) has in the case of proposition 11 the form*

$$(25^*) \qquad h^{(i)}(X_2, \ldots, X_n) = f_i'(X_i) \qquad \text{with} \quad h^{(i)} = \frac{\partial h}{\partial X_i}$$

PROPOSITION 14: *The rational function g of proposition 11 is a polynomial.*

Proof: Otherwise g has a finite pole, we may take this pole to be $t = 0$, assuming k to be algebraically closed. From $h = A/B$ we see that any irreducible factor A_1 of A gives a pole $A_1 = 0$ of $g(h) = \sum f_i(X_i)$. Then A_1 has to be a divisor of the denominator $H_i(X_i)$ of some f_i, and therefore $A_1 = A_1(X_i)$ is a polynomial of one variable. So $A = \prod_{i=2}^n P_i(X_i)$ is a polynomial with multiplicatively separated variables, so $h^{(i)}$ is divisible by P_j for $j \neq i$. From equations (25*) we see that the numerator of $f_i'(X_i)$ is divisible by $P_j(X_j)$ for all $j \neq i$, which is only possible if A is a constant. But $h = 1/B$ gives $h^{(i)} = -B^{(i)}/B^2$. Now h and so B depends on all variables X_j. This dependence cannot vanish in the quotient $B^{(i)}/B^2$, since $\deg_{X_j} B^{(i)} \leq \deg_{X_j} B < \deg_{X_j} B^2$. For $i \neq j$ this dependence contradicts (25*). ∎

PROPOSITION 15: *Let k be a field and let k be perfect if $\operatorname{char} k = 2$. Then in the second case of the key lemma the rational function g can be taken as polynomial $g(X) = aX^p + c$.*

Proof: If k is perfect, then by the key lemma g has the shape $g = l(X)^p$ with a linear fractional function l, so in equation (22) we can replace g by X^p and h by $l(h)$. Now let k be imperfect, especially infinite. Translating the X_i, the f_i and g by additive constants, we may assume that $h(0,\dots,0)$ is defined and $f_i(0) = 0$. If g is not a polynomial it can be written as $g(X) = \frac{a}{X^p+b} + c$. If $b = b_0^p$ we get $g(X^{-1} - b_0) = aX^p + c$, which gives the claim. Now assume $b \notin k^p$. From (22) follows

$$f_i(X_i) = g\big(h_i(X_i)\big) \qquad \text{with} \quad h_i = h(0,\dots,X_i,\dots,0)$$

With $h_i(X_i) = A_i(X_i)/B_i(X_i)$ and $\gcd(A_i, B_i) = 1$ we get

$$f_2(X_2) + f_3(X_3) = \frac{aB_2^p(X_2)}{A_2^p(X_2) + bB_2^p(X_2)} + \frac{aB_3^p(X_3)}{A_3^p(X_3) + bB_3^p(X_3)} + 2c \tag{28}$$

The denominator of the right hand side is, up to a multiplicative constant,

$$(A_2^p + bB_2^p)(A_3^p + bB_3^p) = C^p + bD^p + b^2E^p \tag{29}$$

with $C = A_2A_3$, $D = A_2B_3 + B_2A_3$ and $E = B_2B_3$ being linearly independent over k. This can be seen as follows:

$$\lambda C + \mu D + \nu E = 0 \implies A_2(X_2)\cdot(\lambda A_3 + \mu B_3) = B_2(X_2)\cdot(\mu A_3 + \nu B_3)$$

Since $A_2/B_2 \notin k$ this implies $\lambda A_3 + \mu B_3 = 0 = \mu A_3 + \nu B_3$. From $A_3/B_3 \notin k$ follows $\lambda = \mu = \nu = 0$, which ends the proof of the linear independence of C, D, E. If $p > 2$ the powers $1, b, b^2$ are linearly independent over $k(X_2, X_3)^p$. Therefore the denominator (29) of (28) can never be a constant multiple of some $F^p + bG^p$. But from (22) follows

$$f_2(X_2) + f_3(X_3) = \frac{a}{h(X_2, X_3, 0, \dots, 0)^p + b} + c$$

Thus $b \notin k^p$ and $p > 2$ leads to a contradiction. ∎

PROPOSITION 16: *Let k be a field and let k be perfect if char $k = 2$. After a linear fractional transformation of the variable of g we get for the rational functions g and h in (22) that*

$$h(X_2, \ldots, X_n) = \sum_{i=2}^{n} h_i(X_i) \tag{30}$$

and $G(X) = g(X) - g(0)$ is an additive polynomial.

Proof: Propositions 14 and 15 assert that g becomes a polynomial after a linear fractional transformation. An application of lemma 8 to the equation (22) gives (30) and the additivity of G. ∎

End of the Proof of Theorem B: We have to find an additive polynomial L and rational functions h_i with (5) and (6). By proposition 16 the equation (22) has now the form

$$\sum_{i=2}^{n} G(h_i(X_i)) = G\Big(\sum_{i=2}^{n} h_i(X_i)\Big) = \sum_{i=2}^{n} f_i(X_i) - g(0) \tag{22*}$$

Therefore there are constants $d_i \in k$ such that

$$G(h_i(X_i)) = f_i(X_i) + d_i \ , \qquad 2 \le i \le n$$

By assumption there exists a rational place ξ of $k(X)$ and a uniformizing parameter π such that $c_i = f_i(\xi; \pi)$. By lemma 6.c we get with $u_i = h_i(\xi; \pi) \in k$

$$G(u_i) = c_i + d_i \ , \qquad 2 \le i \le n$$

Subtracting the last two equations and replacing $h_i := h_i + u_i$ we get

$$G(h_i(X_i)) = f_i(X_i) - c_i \qquad \text{for } \ 2 \le i \le n \tag{31}$$

which is (5) up to the index $i = 1$. By (23) in the key lemma 9 with $Z := X_2 + X_3$ the numerator of $\tilde{f}(X_2, X_3, X_1) = g(X_2) + G(X_3) + f_1(X_1)$ is reducible. Applying the key lemma to $\tilde{f}$ and proceeding as above, the equivalent of (31) shows that G and $f_1 - c_1$ are composed by an additive polynomial L of degree > 1

$$G = L(g_1), \qquad f_1 = L(h_1) + c_1 \tag{32}$$

(in the inseparable case is $L = G$). Substituting $h_i =: g_1 \circ h_i$ for $i > 1$ we get from (31) and (32) the equations (5).

To finish the proof of theorem B we have to show (6). The application of the key lemma to $\tilde{f}$ above gives by (23) that the polynomial $P(Z, X_2) = L(Z) + c_1 + G(X_2) + g(0)$ is reducible. By (22*) and lemma 6.c we have $\sum_{i=2}^{n} c_i - g(0) = G(u)$ with $u = \sum_{i=2}^{n} u_i$. So $P(X, u) = L(X) + \sum_{i=1}^{n} c_i$ is reducible. ∎

Remark: One can avoid the change from G to L in (32) if one chooses in the key lemma 9, i.e. in equation (22), a rational function g of minimal degree (of course ≥ 2). ∎

8. Proof of Theorem C (Necessity)

Let k be an imperfect field of characteristic 2 and let $n \geq 3$. As in §7 we start with nonconstant rational functions $f_i \in k(X)$, represented elements c_i, assume that $\sum_{i=1}^{n} f_i(X_i)$ is reducible and apply the key lemma 9, getting functions g and h. We have to find functions $\ell, h_i \in k(X)$ which satisfy (5*) and (6*) where ℓ has one of the forms a), b) or c) in theorem C. If the proof in §7 goes through, then (5*) and (6*) hold with ℓ being an additive polynomial of degree > 1, i.e. case a) of theorem C. It remains to check those points of the proof in §7 where the argument fails for an imperfect field of characteristic 2. In these cases we will come to cases b) and c) of theorem C.

Using the remark at the end of §7 we choose g in lemma 9 of minimal degree ≥ 2. Moreover we set $c := \sum_{i=1}^{n} c_i$ and distinguish the cases $g' \neq 0$ and $g' = 0$.

First Case $g' \neq 0$: The exception in proposition 11 is the case

$$g'(t) = \frac{a}{t^2 + b} \qquad 0 \neq a, b \in k, \quad b \notin k^2$$

In the larger field $k_1 = k(\beta)$ with $\beta^2 = b$ the proof of proposition 11 (and then the whole proof of theorem C for this case) goes through, together with proposition 14 we get: The linear fractional transformation $l(t) = at^{-1} + \beta$ gives a polynomial $g_1(t) = g(at^{-1} + \beta) \in k_1[X]$ with $g_1'(t) = 1$. By lemma 8 the separable polynomial $G(t) = g_1(at) + g_1(0) = g(t^{-1} + \beta) + g(\infty) \in k_1[X]$ is additive, so

$$G(t) = \sum_{j=0}^{m} (a_j + \beta b_j) t^{2^j}, \qquad a_j, b_j \in k$$

with

$$G\Big(\frac{1}{t+\beta}\Big) = g(t) + g(\infty) \ \in k(t) \tag{33}$$

To see the effect of (33) for the coefficients of G we write

$$\begin{aligned} G\Big(\frac{1}{t+\beta}\Big) &= \sum_{j=0}^{m} \frac{a_j + \beta b_j}{(t+\beta)^{2j}} = \frac{a_0 + \beta b_0}{t+\beta} + \frac{a_1 + \beta b_1}{t^2+b} + \sum_{j=1}^{m-1} \frac{a_{j+1} + \beta b_{j+1}}{(t^2+b)^{2j}} \\ &= \frac{(a_0 + \beta b_0)t + a_1 + b b_0 + \beta(a_0 + b_1)}{t^2+b} + \sum_{j=1}^{m-1} \frac{a_{j+1} + \beta b_{j+1}}{(t^2+b)^{2j}} \end{aligned}$$

This sum is in $k(t)$ iff

$$a_0 = b_1, \qquad b_0 = b_2 = \cdots = b_m = 0$$

and the separability means $a_0 \neq 0$. After an affine substitution $t := a_0 t + a_1/a_0$ we see that the transformed g satisfies

$$g(t) = \ell(t) + g(\infty) \qquad \text{with} \qquad \ell(t) = \frac{t}{t^2 + b_\circ} + \sum_{j=1}^{m} \frac{\tilde{a}_j}{(t^2+b_\circ)^{2j}}$$

where $\tilde{a}_j \in k$, $b_\circ \in k \setminus k^2$, so ℓ is a function of case b) of theorem C. Over k_1, i.e. by case a) of theorem C, we have for $1 \leq i \leq n$ representations

$$f_i - c_i = G(\tilde{h}_i) \qquad \text{with } \tilde{h}_i \in k_1(t)$$

They induce with a linear fractional transformation h_i of $\tilde{h}_i$ representations

$$f_i - c_i = \ell(h_i) = \frac{h_i}{h_i^2 + b_\circ} + \sum_{j=1}^{m} \frac{\tilde{a}_j}{(h_i^2 + b_\circ)^{2j}} \qquad \text{with } h_i \in k_1(t)$$

Since the left hand side is in $k(t)$ and $h_i^2 \in k(t)$, we see from the first summand of the right hand side that $h_i \in k(t)$ holds. This gives (5*).

The proof of (6*) in the case $c \neq 0$ runs parallel to the corresponding proof of (6) at the end of §7. From the key lemma 9 we have

$$\ell\big(h(X_2, \ldots, X_n)\big) = \sum_{i=2}^{n} f_i(X_i) + g(\infty)$$

This shows that the f_i have no k-rational pole since ℓ has none, so the represented elements c_i are values of f_i. Therefore there is some $d \in k \cup \{\infty\}$ with

$$\ell(d) = \sum_{i=2}^{n} c_i + g(\infty)$$

Moreover (23) in the key lemma gives the reducibility of

$$\ell(Z) + g(\infty) + f_1(X_1) = \ell(Z) + \ell(d) + \ell(h_1(X_1)) + c \tag{34}$$

In the right hand side of (34) we substitute for X_1 a constant in k, which preserves the Z-degree of the numerator, and use the addition formula (12) for ℓ to get the reducibility of

$$\ell(Z) + \ell(e) + c = \frac{A(Z)}{B(Z)} \tag{35}$$

for some $e \in k$. By (12) we have $\ell(Z) + \ell(e) = \ell(X)$ with $X = (eZ + b)/(Z + e)$. To get (6*), i.e. the reducibility of $\ell(X) + c$, we only have to check that the linear fractional involution $X = U/V$ with $U = eZ + b = eV + e^2 + b$ preserves the reducibility of A/B. From $c \neq 0$ follows $A(e) \neq 0$ by (35). So we see from lemma 1.a that for a nonconstant factor A_1 of A also $A_1(U, V)$ is nonconstant, since $U - bV$ is only constant for $b = e$ and this b is not a zero of A_1. From lemma 1.b follows now that a nontrivial factorization of A implies a nontrivial factorization of $A(U, V)$. This gives (6*). ∎

Second Case $g' = 0$: The exception in proposition 15 is the case

$$g(t) = \frac{a}{t^2 + b} + e =: \ell(t) + e, \qquad 0 \neq a, b, e \in k,\ b \notin k^2$$

From the key lemma 9 we have

$$\ell\big(h(X_2, \ldots, X_n)\big) = \sum_{i=2}^{n} f_i(X_i) + e, \qquad \ell(h_1(X)) = f_1(X) + e \tag{22**}$$

As in the first case this shows that the represented elements c_i are values of f_i, say $c_i = f_i(0)$ by translation of the X_i's. Adding the two equations in (22**) and substituting 0 for all X_i we see by the addition formula (10) that $\sum_{i=1}^{n} c_i$ is a value of ℓ, which gives (6*). Substituting $f_i := f_i - c_i$, we get $f_i(0) = 0$ and $e = \ell(h_1(0))$. So by a linear fractional transformation of h and h_1, using (10), we may assume $e = 0$. Then (22**) gives $f_i = \ell(h_i)$ with $h_i = h(0, \ldots, X_i, \ldots, 0)$ for $2 \leq i \leq n$, so (5*). This finishes the proof of theorem C. ∎

9. Rational functions with an addition law

Let $\ell \in k(x)$ be a rational function of one variable. A rational function $z \in k(x,y)$ in two variables is said to be an **addition law** for ℓ, if

$$\ell(x) + \ell(y) = \ell(z) \tag{36}$$

The addition law need not be unique. For example, an additive polynomial ℓ has the addition law $z = x + y$, and also the addition law $\tilde{z} = x + y + \alpha$ for each zero α of ℓ. Similarly, in characteristic 2, both $z = (xy + b)/(x + y)$ and $\tilde{z} = b(x + y)/(xy + b)$ are addition laws for $\ell(x) = \frac{x}{x^2+b}$, see (10′).

Obviously equation (36) is a special case of equation (22) with $n = 3$, $g = f_2 = f_3 = \ell$ and $h = z$. Therefore the case of characteristic zero is trivial: By corollary 12 we have $\deg \ell = 1$ or $\ell = 0$, and by (A4) below all linear fractional functions ℓ have an addition law. For prime characteristic theorems B and C can be used to determine all rational functions having an addition law. Indeed all such functions have essentially already occurred.

First let us mention four simple properties of rational functions with an addition law:

(A1) The functions ℓ, satisfying (36) with a fixed law z, form a vector space over the ground field k. The only constant function with (36) is the zero function.

(A2) If $\operatorname{char} k = p > 0$ then with ℓ also ℓ^p has the addition law z. Therefore, if L is an additive polynomial, then with ℓ also $L \circ \ell$ has the addition law z.

(A3) Conversely, if L is an additive polynomial and if $L \circ f$ has an addition law, then there is a zero $d \in k$ of L such that $f(x) - d$ has the same addition law.

Proof: $L(f(x)) + L(f(y)) = L(f(z))$ implies $L(f(x) + f(y) - f(z)) = 0$, so $f(x) + f(y) - f(z) = d \in k(x,y) \cap \tilde{k} = k$ and $L(d) = 0$. ∎

(A4) If $l(x) = (ax + b)/(cx + d)$ with $a, b, c, d \in k$ and $ad \neq cd$ is a Moebius transformation, i.e. an automorphism of $k(x)|k$, and if ℓ has the addition law z then $\tilde{\ell} = \ell \circ l$ has the addition law $\tilde{z}(x,y) = l^{-1}\big(z(l(x), l(y))\big)$.

We met already two examples of such functions:

(E1) In the first example in §1 we saw that the additive polynomials (4) have the most simple addition law $z = x + y$. They form a vector space over k, closed under taking p^{th} powers. Among their Moebius transforms they are characterized by the following two properties: Their only pole is ∞, and all vanish for $x = 0$.

(E2) In lemma 2 we found other classes of examples: If k is a field of characteristic 2, then

$$\ell(x) = \frac{a_0 + \tilde{a}_0 x}{x^2 + b} + \sum_{i=1}^{n} \frac{a_i}{(x^2+b)^{2^i}} \tag{11}$$

with $b, \tilde{a}_0, a_i \in k$ has by (12) the addition law $z = \dfrac{xy+b}{x+y}$. If $b \notin k^2$ these functions are not Moebius transforms of additive polynomials since they have no rational pole but a single pole with the inseparable quadratic residue field $k_1 = k(\sqrt{b})$. For a fixed $b \in k \setminus k^2$ the functions (11) again form a vector space over k, closed under taking squares as one sees from

$$\left[\frac{x}{x^2+b}\right]^2 = \frac{1}{x^2+b} + \frac{b}{(x^2+b)^2}$$

Among their Moebius transforms they are characterized by the following two properties: Their only pole corresponds to the fixed prime polynomial x^2+b (i.e. a generator, namely $\sqrt{b}$, of the residue field $k_1|k$ is chosen), and all vanish for $x = \infty$.

LEMMA 17: *Let ℓ be a rational function of degree > 1 with an addition formula (36). Then the addition law z is a quotient of two polynomials of the type $axy + bx + cy + d$, but z is not of the type $a + b/V(x,y)$. The function ℓ has a zero in $\mathbb{P}_1(k) = k \cup \{\infty\}$ and has in the algebraic closure $\tilde{k}$ of k exactly one pole $\xi \in \mathbb{P}_1(\tilde{k})$, which is the unique solution of the equation $z(\xi, y) = \xi$, so is either rational or inseparable quadratic over k (with $p = 2$). The sum $\sum_{i=1}^{n} \ell(x_i)$ is reducible for $n \geq 2$.*

Proof: Taking degrees in (36) and using $\deg(f(g)) = \deg(f) \cdot \deg(g)$ for rational functions f, g in one variable, we see that the law z is of degree 1 in each of its variables, so has the claimed shape. If one would have $z = a + b/V$, then $z(\infty, y) = a$ is a constant, so from (36) one sees that ∞ and a would be poles of ℓ. In the third step of this proof we will see that this is impossible.

By iteration of (36) we get rational functions $z_n = z_n(x_1, \cdots, x_n)$ such that $\sum_{i=1}^{n} \ell(x_i) = \ell(z_n)$. Taking $n = p$ and $x_1 = \cdots = x_p$ we see that ℓ takes the value zero on $\mathbb{P}_1(k)$.

We now prove the claim about the poles of ℓ. Since ℓ is nonconstant the set

$$P := \{\xi \in \mathbb{P}_1(\tilde{k});\ \ell(\xi) = \infty\}$$

of geometric poles of ℓ is nonempty. If $\xi \in P$, equation (36) shows that $z(\xi, y)$ is a constant in $\mathbb{P}_1$, which is again a pole of ℓ, so

$$\xi \in P \implies z(\xi, y) \in P \tag{37}$$

Consider $z(x, y)$ as linear fractional function in x over $k(y)$. If ℓ would have three geometric poles ξ_i for $i = 1, 2, 3$, then the function z is determined by the three values $z(\xi_i, y) \in P \subseteq \mathbb{P}_1(\tilde{k})$, so would not depend on y, a contradiction. If ℓ would have two poles, by (A4) we can assume, possibly after an algebraic extension of k, they are 0 and ∞. Then for $x \in \{0, \infty\}$ we have $z(x, y) \in \{0, \infty\}$ by (37). By symmetry the same holds for y. Hence z has the form $ax^\delta y^\varepsilon$ with $\delta, \varepsilon = \pm 1$. But ℓ, having only poles at 0 and ∞, is of the form $\ell(x) = \sum_{i=-m}^{n} a_i x^i$ with $m, n > 0$, so (36) becomes an equation

$$\sum_{i=-m}^{n} a_i(x^i + y^i) = \sum_{i=-m}^{n} a_i a^i x^{i\delta} y^{i\varepsilon}$$

which is absurd. This shows the uniqueness of the pole ξ of ℓ. From (37) we see that this pole must be a solution of $z(\xi, y) = \xi$, the converse is true by (36), so this at most quadratic equation in ξ has only one root in $\mathbb{P}_1$.

Finally we show the reducibility of

$$\sum_{i=1}^{n} \ell(x_i) = \ell\big(z_n(x_1, \ldots, x_n)\big), \qquad n > 1$$

If z is a polynomial, then $z(\infty, y) = \infty$, so ∞ is the pole of ℓ, so ℓ is a polynomial. Having a rational zero, ℓ is reducible, so $\ell(z_n)$ is reducible.

Now let $z = U/V$ with $V \notin k$ and $\ell = A/B$. From $z \neq a + b/V$ we see that $U \notin k + kV$. If ℓ is reducible, we can apply lemma $1.e_1$, to get the reducibility of $\ell(z_n)$. In the remaining case ℓ is irreducible. Since ℓ has a rational zero in $\mathbb{P}_1(k)$, either $\ell(\infty) = 0$ or $\deg A = 1$. In the second case also $\ell(\infty) = 0$ holds, because $\deg \ell > 1$. Now apply lemma $1.e_2$ to see that $\ell(z_n)$ is reducible. ∎

THEOREM D: *Let $\ell \in k(x)$ be a rational function with an addition law. If ℓ is a polynomial, it is after a translation $x := x - d$ additive, i.e. of form (4). In general, modulo a Moebius transformation of the variable, ℓ has one of the following forms:*

a) $\operatorname{char} k = 0$: $\ell(x) = x$ *or* $\ell = 0$.

b) $\operatorname{char} k = p$ *and* $k = k^2$ *in case* $p = 2$: ℓ *is an additive polynomial.*

c) $\operatorname{char} k = 2$ *and* $k \neq k^2$: *Then* ℓ *is an additive polynomial or has the shape (11) with* $b \in k \setminus k^2$ *and* $\tilde{a}_0, a_j \in k$ *for* $0 \leq j \leq m$.

Proof: If $\ell \neq 0$ is a polynomial, from lemma 8 with $m = 2$, $G = f_1 = f_2 = \ell$ and $h = z$ follows that $\ell(x) = L(x) + c$ with L as in (4). So equation (36) has the form $L(x) + L(y) + c = L(z)$, which implies $z - x - y = d \in k$ with $c = L(d)$. Hence $\ell(x) = L(x + d)$ and therefore $\ell(x - d) = L(x)$ is additive.

Now let $\ell \neq 0$ be arbitrary. The case a) of characteristic zero was already done before (A1). So let $\operatorname{char} k = p > 0$. If ℓ is of degree 1, we get the result of case a). So let ℓ have a degree > 1. By lemma 17 the sum $\ell(x_1) + \ell(x_2) + \ell(x_3)$ is reducible and ℓ represents 0. So by theorem B, resp. C, with $f_i = \ell$ and $c_i = 0$, we get a decomposition

$$\ell = \ell_\circ(h) \qquad \text{with} \quad h \in k(x) \tag{38}$$

of ℓ with a special function $\ell_\circ$ of type (E1) or (E2).

Proof of b) (Application of theorem B): Here $\ell_\circ$ is an additive polynomial. By (A3) we can change h by adding a rational zero of $\ell_\circ$ such that (38) holds and h has the same addition law. Since $\deg h < \deg \ell$, by induction on the degree of ℓ we can assume h being the Moebius transform of some additive polynomial. So after a Moebius transformation as in (A4) we may assume h to be additive. Then also ℓ is an additive polynomial.

Proof of c) (Application of theorem C): Let k be a field of characteristic 2 with $k \neq k^2$. If $\ell_\circ$ is an additive polynomial, we can conclude as in the proof of b), since both examples (E1) and (E2) are closed under composition with an additive polynomial. Otherwise $\ell_\circ$ is of type (11) which combines cases b) and c) of theorem C. We write $\ell_\circ(x) = A/B$ with $A \in k[x]$ and $B = (x^2 + b)^{2^m}$, and $h = U/V$ with $U, V \in k[x]$ relatively prime. Since $\ell_\circ$ has no rational pole we have $\operatorname{ord}_\infty \ell_\circ \geq 0$. From (7) and (38) follows a reduced representation

$$\ell(x) = \frac{N}{(U^2 + bV^2)^{2^m}} \qquad \text{with} \quad N \in k[x] \tag{38*}$$

with $m \geq 1$. From part b) we know already that in some purely inseparable extension k_1 of k we have $\ell(x) = L(l(x))$ where $L \in k_1[x]$ is additive, say of degree $2^{m'}$, and $l(x) = (\alpha x + \beta)/(\gamma x + \delta)$ is a linear fractional function in $k_1(x)$.

Since ℓ is no polynomial, l is no polynomial and we put $\gamma = 1$. Comparing the denominator of (38*) and the denominator $(x+\delta)^{2^{m'}}$ of $L \circ l$ we get with $r := m' - m > 0$ the equation

$$U^2 + bV^2 = \varepsilon(x+\delta)^{2^r} = \varepsilon x^{2^r} + \varepsilon\delta^{2^r}, \qquad \varepsilon \in k_1^\times$$

Since $b \notin k^2$, it follows from this that U and V are linear combinations of 1 and x^q with $q = 2^{r-1}$, so we have

$$h(x) = l_1(x^q) \qquad \text{with} \quad l_1(x) = \frac{a_0 x + a_1}{a_2 x + a_3} \in k(x) \setminus k$$

Now the finite poles ξ of ℓ in (38*) are given by the equation $U(\xi)^2 + bV(\xi)^2 = 0$, so

$$h(\xi)^2 = b \tag{39}$$

Denoting by $l_2(x) := l_1(\sqrt{x})^2$ the fractional linear function with the coefficients a_i^2, and defining $b_2 \in k \setminus k^2$ by $b = l_2(b_2)$, equation (39) is equivalent to

$$l_2(\xi^{2q}) = b \qquad \text{i.e.} \qquad \xi^{2q} = b_2$$

By lemma 17 the rational function ℓ has a single pole which is at most quadratic over k. So we get $q = 1$. Therefore $h = l_1$ is of degree 1 and $\ell(X) = \ell_0(l_1(X))$ is a Moebius transform of some function of type (11). ∎

Remark: The classification, modulo Moebius transforms, of rational functions with an addition law, done in theorem D, does not single out unique representatives modulo Moebius transforms: On the space of additive polynomials still operates the one dimensional group $\{x \mapsto ax;\ a \in k\}$ of Moebius transformations. In contrast, in the space of the functions in (11) with fixed $b \in k \setminus k^2$ to any element there are only finitely many Moebius equivalent ones. ∎

References

[E] A. Ehrenfeucht, *Kryterium absolutnej nierozkładalności wielomianów*, Prace Matematyczne Warszawa **2** (1956), 167–169.

[F] M. Fried, *Irreducibility results for separated variables equations*, Journal of Pure and Applied Algebra **48** (1987), 9–22.

[H] H. Hasse, *Number Theory (Die Grundlehren der mathematischen Wissenschaften, Band 229)*, Springer-Verlag, 1980.

[HJ] D. Haran and M. Jarden, *The absolute Galois group of a pseudo p-adically closed field*, Journal für die reine und angewandte Mathematik **383** (1988), 147–206.

[L] S. Lang, *Algebra (second edition)*, Addison-Wesley, 1984.

[S1] A. Schinzel, *Some unsolved problems on polynomials*, in: Neki nerešeni problemi u matematici, Matematička Biblioteka Beograd **25** (1963), 63–70.

[S2] A. Schinzel, *Selected Topics on Polynomials*, The University of Michigan Press, 1982.

[S3] A. Schinzel, *Reducibility of polynomials in several variables II*, Pacific Journal of Mathematics **118** (1985), 531–563.

[T1] H. Tverberg, *A remark on Ehrenfeucht's criterion for irreducibility of polynomials*, Prace Matematyczne Warszawa **8** (1964), 117–118.

[T2] H. Tverberg, *On the irreducibility of polynomials* $f(x) + g(y) + h(z)$, Quarterly Journal of Mathematics Oxford, Second Series **17** (1966), 364–366.