ON FUNCTION COMPOSITIONS THAT ARE POLYNOMIALS

ERHARD AICHINGER

ABSTRACT. For a polynomial map \( f : k^n \to k^m \) (\( k \) a field), we investigate those polynomials \( g \in k[t_1, \ldots, t_n] \) that can be written as a composition \( g = h \circ f \), where \( h : k^m \to k \) is an arbitrary function. In the case that \( k \) is algebraically closed of characteristic 0 and \( f \) is surjective, we will show that \( g = h \circ f \) implies that \( h \) is a polynomial.

1. Introduction. In the present note, we investigate the situation where the value of a polynomial depends only on the value of certain given polynomials. To be precise, let \( k \) be a field, \( m, n \in \mathbb{N} \), and let \( g, f_1, \ldots, f_m \in k[t_1, \ldots, t_n] \). We say that \( g \) is determined by \( f = (f_1, \ldots, f_m) \) if, for all \( a, b \in k^n \) with \( f_1(a) = f_1(b), \ldots, f_m(a) = f_m(b) \), we have \( g(a) = g(b) \). In other words, \( g \) is determined by \( f \) if and only if there is a function \( h : k^m \to k \) such that

\[
g(a) = h(f_1(a), \ldots, f_m(a)) \quad \text{for all } a \in k^n.
\]

For given \( f_1, \ldots, f_m \in k[t_1, \ldots, t_n] \), the set of all elements of \( k[t_1, \ldots, t_n] \) that are determined by \( (f_1, \ldots, f_m) \) is a \( k \)-subalgebra of \( k[t_1, \ldots, t_n] \); we will denote this \( k \)-subalgebra by \( k\langle f_1, \ldots, f_m \rangle \) or \( k\langle f \rangle \); in this algebra, we find exactly those polynomials that can be written as \( p(f_1, \ldots, f_m) \) with \( p \in k[x_1, \ldots, x_m] \). Clearly,

---

Keywords and phrases. Polynomial composition, polynomial maps.
Supported by the Austrian Science Fund (FWF): P24077.
Received by the editors on June 19, 2013.
DOI:10.1216/JCA-2015-7-3-303 Copyright ©2015 Rocky Mountain Mathematics Consortium
$k[f] \subseteq k\langle f \rangle$. The other inclusion need not hold in general: on any field $k$, let $f_1 = t_1, f_2 = t_1t_2$. Then $f_2^2/f_1 = t_1t_2^2$ is $(f_1, f_2)$-determined, but $t_1t_2^2 \notin k[f_1, f_2]$.

The second set with which we will compare $k\langle f \rangle$ is the set of all polynomials that can be written as rational functions in $f_1, \ldots, f_m$. We denote the quotient field of $k[t_1, \ldots, t_n]$ by $k(t_1, \ldots, t_n)$. For $r_1, \ldots, r_m \in k(t_1, \ldots, t_n)$, the subfield of $k(t_1, \ldots, t_n)$ that is generated by $k \cup \{r_1, \ldots, r_m\}$ is denoted $k(r_1, \ldots, r_m)$. We first observe that there are polynomials that can be written as rational functions in $f$, but fail to be $f$-determined. As an example, we see that $t_2 \in k\langle t_1, t_1t_2 \rangle$, but since $(0, 0 \cdot 0) = (0, 0 \cdot 1)$ and $0 \neq 1$, the polynomial $t_2$ is not $(t_1, t_1t_2)$-determined. As for the converse inclusion, we take a field $k$ of positive characteristic $\chi$. Then $t_1$ is $(t_1^\chi)$-determined, but $t_1 \notin k(t_1^\chi)$.

On the positive side, it is known that $k[ f_1, \ldots, f_m ] = k\langle f_1, \ldots, f_m \rangle$ holds in the following cases (cf., [1, Theorem 3.1]):

- $k$ is algebraically closed, $m = n = 1$, and the derivative $f'$ of $f$ is not the zero polynomial, and, more generally,
- $k$ is algebraically closed, $m = n$, and there are univariate polynomials $g_1, \ldots, g_m \in k[t]$ with $g'_1 \neq 0, \ldots, g'_m \neq 0$, $f_1 = g_1(t_1), \ldots, f_m = g_m(t_m)$.

Let us now briefly outline the results obtained in the present note. Let $k$ be an algebraically closed field of characteristic 0, and let $f_1, \ldots, f_m \in k[t_1, \ldots, t_n]$ be algebraically independent over $k$. Then we have $k\langle f \rangle \subseteq k\langle f \rangle$ (Theorem 3.3). The equality $k[f] = k\langle f \rangle$ holds if and only if $f$ induces a map from $k^n$ to $k^m$ that is almost surjective (see Definition 2.1). This equality is stated in Theorem 3.4. Similar results are given for the case of positive characteristic.

The last equality has a consequence on the functional decomposition of polynomials. If $f$ induces a surjective mapping from $k^n$ to $k^m$, $(k$ an algebraically closed of characteristic 0), and if $h : k^m \rightarrow k$ is an arbitrary function such that $h \circ f$ is a polynomial function, then $h$ is a polynomial function. In an algebraically closed field of positive characteristic $\chi$, we will conclude that $h$ is a composition of taking $\chi$th roots and a polynomial function (Corollary 4.2).

2. Preliminaries about polynomials. For the notions from algebraic geometry used in this note, we refer to [2]; deviating from their
FUNCTION COMPOSITIONS THAT ARE POLYNOMIALS

305

definitions, we call the set of solutions of a system of polynomial equations an algebraic set (instead of affine variety). For an algebraically closed field \( k \) and \( A \subseteq k^m \), we let \( I_m(A) \) (or simply \( I(A) \)) be the set of polynomials vanishing on every point in \( A \), and for \( P \subseteq k[t_1, \ldots, t_m] \), we let \( V_m(P) \) (or simply \( V(P) \)) be the set of common zeroes of \( P \) in \( k^m \). The Zariski-closure \( V(I(A)) \) of a set \( A \subseteq k^m \) will be abbreviated by \( \overline{A} \). The dimension of an algebraic set \( A \) is the maximal \( d \in \{0, \ldots, m \} \) such that there are \( i_1 < i_2 < \cdots < i_d \in \{1, \ldots, m \} \) with \( I(A) \cap k[x_{i_1}, \ldots, x_{i_d}] = \{0\} \). We abbreviate the dimension of \( A \) by \( \dim(A) \) and set \( \dim(\emptyset) := -1 \). For \( f_1, \ldots, f_m, g \in k[t_1, \ldots, t_n] \), and \( D := \{(f_1(a), \ldots, f_m(a), g(a)) | a \in k^n\} \), its Zariski-closure \( \overline{D} \) is an irreducible algebraic set, and its dimension is the maximal number of algebraically independent elements in \( \{f_1, \ldots, f_m, g\} \). The closure theorem [2, page 258] tells that there exists an algebraic set \( W \subseteq k^{m+1} \) with \( \dim(W) < \dim(\overline{D}) \) such that \( \overline{D} = \overline{D} \cup W \). If \( \dim(\overline{D}) = m \), then there exists an irreducible polynomial \( p \in k[x_1, \ldots, x_{m+1}] \) such that \( \overline{D} = V(p) \). We will denote this \( p \) by \( \text{Irr}(\overline{D}) \); \( \text{Irr}(\overline{D}) \) is then defined up to a multiplication with a nonzero element from \( k \).

Above this, we recall that a set is constructible if and only if it can be generated from algebraic sets by a finite application of the set-theoretic operations of forming the union of two sets, the intersection of two sets, and the complement of a set, and that the range of a polynomial map from \( k^n \) to \( k^m \) and its complement are constructible. This is of course a consequence of the theorem of Chevalley-Tarski [4, Exercise II.3.19], but since we are only concerned with the image of \( k^n \), it also follows from [2, page 262, Corollary 2].

**Definition 2.1.** Let \( k \) be an algebraically closed field, \( m, n \in \mathbb{N} \), and let \( f = (f_1, \ldots, f_m) \in (k[t_1, \ldots, t_n])^m \). By \( \text{range}(f) \), we denote the image of the mapping \( \hat{f} : k^n \to k^m \) that is induced by \( f \). We say that \( f \) is almost surjective on \( k \) if the dimension of the Zariski-closure of \( k^m \setminus \text{range}(f) \) is at most \( m - 2 \).

**Proposition 2.2.** Let \( k \) be an algebraically closed field, and let \( (f_1, \ldots, f_m) \in k[t_1, \ldots, t_n]^m \) be almost surjective on \( k \). Then the sequence \( (f_1, \ldots, f_m) \) is algebraically independent over \( k \).

**Proof.** Seeking a contradiction, we suppose that there is \( u \in
\[ k[x_1, \ldots, x_m] \text{ with } u \neq 0 \text{ and } u(f_1, \ldots, f_m) = 0. \text{ Then } \text{range}(f) \subseteq V(u); \text{ hence, } \dim(\text{range}(f)) \leq m - 1. \text{ Since } f \text{ is almost surjective, } k^m \text{ is then the union of two algebraic sets of dimension } \leq m - 1, \text{ a contradiction.} \]

We will use the following easy consequence of the description of constructible sets:

**Proposition 2.3.** Let \( k \) be an algebraically closed field, and let \( B \) be a constructible subset of \( k^m \) with \( \dim(B) \geq m - 1 \). Then there exist algebraic sets \( W, X \) such that \( W \) is irreducible, \( \dim(W) = m - 1 \), \( \dim(X) \leq m - 2 \), and \( W \setminus X \subseteq B \).

**Proof.** Since \( B \) is constructible, there are irreducible algebraic sets \( V_1, \ldots, V_p \) and algebraic sets \( W_1, \ldots, W_p \) with \( W_i \subsetneq V_i \) and \( B = \bigcup_{i=1}^p (V_i \setminus W_i) \) (cf., [2, page 262]). We assume that the \( V_i \)'s are ordered with nonincreasing dimension. If \( \dim(V_1) = m \), then \( k^m \setminus W_1 \subseteq B \). Let \( U \) be an irreducible algebraic set of dimension \( m - 1 \) with \( U \nsubseteq W_1 \). Then \( U \cap (k^m \setminus W_1) = U \setminus (W_1 \cap U) \). Since \( W_1 \cap U \neq U \), setting \( W := U, X := W_1 \cap U \) yields the required sets.

If \( \dim(V_1) = m - 1 \), then \( W := V_1 \) and \( X := W_1 \) are the required sets.

The case \( \dim(V_1) \leq m - 2 \) cannot occur because then \( \overline{B} \subseteq V_1 \cup \ldots \cup V_p \) has dimension at most \( m - 2 \). \( \Box \)

Let \( k \) be a field, and let \( p, q, f \in k[t] \) be such that \( \deg(f) > 0 \). It is known that \( p(f) \) divides \( q(f) \) if and only if \( p \) divides \( q \) [3, Lemmas 2.1 and 2.2]. The following Lemma yields a multivariate version of this result.

**Lemma 2.4.** Let \( k \) be an algebraically closed field, \( m, n \in \mathbb{N} \), and let \( f = (f_1, \ldots, f_m) \in (k[t_1, \ldots, t_n])^m \). Then the following are equivalent:

(i) \( f \) is almost surjective on \( k \).

(ii) \( k(f_1, \ldots, f_m) \cap k[t_1, \ldots, t_n] = k[f_1, \ldots, f_m] \) and \( (f_1, \ldots, f_m) \) is algebraically independent over \( k \).

(iii) For all \( p, q \in k[x_1, \ldots, x_m] \) with \( p(f_1, \ldots, f_m) \mid q(f_1, \ldots, f_m) \), we have \( p \mid q \).
Proof. (i) ⇒ (ii). (This proof uses some ideas from the proof of Theorem 4.2.1 in [5, page 82].) Let \( g \in k(f_1, \ldots, f_m) \cap k[t_1, \ldots, t_n] \).

Then there are \( r, s \in k[x_1, \ldots, x_m] \) with \( \gcd(r, s) = 1 \) and \( g = r(f_1, \ldots, f_m)/s(f_1, \ldots, f_m) \), and thus

\[
(2.1) \quad g(t_1, \ldots, t_n) \cdot s(f_1, \ldots, f_m) = r(f_1, \ldots, f_m).
\]

Suppose \( s \notin k \). Then \( V(s) \) has dimension \( m - 1 \). We have \( V(s) = (V(s) \cap \text{range}(f)) \cup (V(s) \cap (k^m \setminus \text{range}(f))) \subseteq V(s) \cap \text{range}(f) \cup V(s) \cap (k^m \setminus \text{range}(f)) \).

Since \( f \) is almost surjective, \( V(s) \cap \text{range}(f) \) is then of dimension \( m - 1 \). Hence, it contains an irreducible component of dimension \( m - 1 \), and thus there is an irreducible \( p \in k[x_1, \ldots, x_m] \) such that \( V(p) \subseteq V(s) \cap \text{range}(f) \).

Since then \( V(p) \subseteq V(s) \), the Nullstellensatz yields \( n_1 \in \mathbb{N} \) with \( p \mid s^{n_1} \), and thus by the irreducibility of \( p, p \mid s \). Now we show that, for all \( a \in V(s) \cap \text{range}(f) \), we have \( r(a) = 0 \). To this end, let \( b \in k^n \) with \( f(b) = a \). Setting \( t := b \) in (2.1), we obtain \( r(a) = 0 \). Thus, \( V(s) \cap \text{range}(f) \subseteq V(r) \), and therefore \( V(s) \cap \text{range}(f) \subseteq V(r) \), which implies \( V(p) \subseteq V(r) \).

By the Nullstellensatz, we have an \( n_2 \in \mathbb{N} \) with \( p \mid r^{n_2} \) and thus, by the irreducibility of \( p, p \mid r \). Now \( p \mid r \) and \( p \mid s \), contradicting \( \gcd(r, s) = 1 \). Hence, \( s \in k \), and thus \( g \in k[f_1, \ldots, f_m] \). The algebraic independence of \( (f_1, \ldots, f_m) \) follows from Proposition 2.2.

(ii) ⇒ (iii). Let \( p, q \in k[x_1, \ldots, x_m] \) be such that \( p(f_1, \ldots, f_m) \mid q(f_1, \ldots, f_m) \). If \( p(f_1, \ldots, f_m) = 0 \), then \( q(f_1, \ldots, f_m) = 0 \), and thus, by the algebraic independence of \( (f_1, \ldots, f_m) \), we have \( q = 0 \) and thus \( p \mid q \). Now assume \( p(f_1, \ldots, f_m) \neq 0 \). We have \( a(t_1, \ldots, t_n) \in k[t_1, \ldots, t_n] \) such that

\[
(2.2) \quad q(f_1, \ldots, f_m) = a(t_1, \ldots, t_n) \cdot p(f_1, \ldots, f_m),
\]

and thus \( a(t_1, \ldots, t_n) \in k(f_1, \ldots, f_m) \cap k[t_1, \ldots, t_n] \). Thus, there exists \( b \in k[x_1, \ldots, x_m] \) such that \( a(t_1, \ldots, t_n) = b(f_1, \ldots, f_m) \). Now (2.2) yields

\[
q(f_1, \ldots, f_m) = b(f_1, \ldots, f_m) \cdot p(f_1, \ldots, f_m).
\]

Using the algebraic independence of \( (f_1, \ldots, f_m) \), we obtain \( q(x_1, \ldots, x_m) = b(x_1, \ldots, x_m) \cdot p(x_1, \ldots, x_m) \), and thus \( p \mid q \).

(iii) ⇒ (i). Seeking a contradiction, we suppose that \( f \) is not almost surjective. Let \( B := k^m \setminus \text{range}(f) \). Then \( \dim(B) \geq m - 1 \). Since \( B \) is constructible, Proposition 2.3 yields \( W, X \) with \( W \) irreducible,
Seeking a contradiction, we suppose that \( \dim(V) = m \) for all \( k \in \mathbb{N} \). If \( m = 0 \), then \( \dim(V) = 0 \). Hence, \( V \) is algebraically independent, \( \pi \), and hence \( \dim(V) = m \). Thus, \( \dim(V) = m \).\( \square \)

3. \( f \)-determined polynomials. We will first show that often all \( f \)-determined polynomials are rational functions of \( f \). Special care, however, is needed in the case of positive characteristic. In an algebraically closed field of characteristic \( \chi > 0 \), the unary polynomial \( t_1 \) is \((t_1^*)\)-determined, but \( t_1 \) is neither a polynomial nor a rational function of \( t_1^* \).

**Definition 3.1.** Let \( k \) be a field of characteristic \( \chi > 0 \), let \( n \in \mathbb{N} \), and let \( P \) be a subset of \( k[t_1, \ldots, t_n] \). We define the set \( \text{rad}_\chi(P) \) by

\[
\text{rad}_\chi(P) := \{ f \in k[t_1, \ldots, t_n] \mid \text{there is } \nu \in \mathbb{N}_0 \text{ such that } f^\nu \in P \}.
\]

**Lemma 3.2.** Let \( k \) be an algebraically closed field, let \( m, n \in \mathbb{N} \), let \( f_1, \ldots, f_m \) be algebraically independent polynomials in \( k[t_1, \ldots, t_n] \), let \( g \in k(f_1, \ldots, f_m) \), and let \( D := \{(f_1(a), \ldots, f_m(a), g(a)) \mid a \in k^n\} \). Then \( \dim(D) = m \).

**Proof.** By the closure theorem [2, page 258], there is an algebraic set \( W \) such that \( \overline{D} = D \cup W \) and \( \dim(W) < \dim(D) \). Let \( \pi : k^{m+1} \to k^m, (y_1, \ldots, y_{m+1}) \mapsto (y_1, \ldots, y_m) \) be the projection of \( k^{m+1} \) onto the first \( m \) coordinates, and let \( \overline{\pi(W)} \) be the Zariski-closure of \( \pi(W) \). We will now examine the projection of \( D \). Since \( f_1, \ldots, f_m \) is algebraically independent, \( \pi(D) \) is Zariski-dense in \( k^m \), and hence \( \dim(\overline{\pi(D)}) = m \). Since \( \dim(V) \geq \dim(\overline{\pi(V)}) \) holds for every algebraic set \( V \), we then obtain \( \dim(D) \geq \dim(\overline{\pi(D)}) = m \). Seeking a contradiction, we suppose that \( \dim(D) = m + 1 \).
In the case \( \dim(\pi(W)) = m \), we use [2, page 193, Theorem 3], which tells \( \pi(W) = V_m(I(W) \cap k[x_1, \ldots, x_m]) \), and we obtain that \( k^m = V_m(I(W) \cap k[x_1, \ldots, x_m]) \), and therefore \( I(W) \cap k[x_1, \ldots, x_m] = \{0\} \). Hence, \( x_1 + I(W), \ldots, x_m + I(W) \) are algebraically independent in \( k[x_1, \ldots, x_{m+1}]/I(W) \). Since \( \dim(W) \leq m \), we observe that the sequence \( (x_1 + I(W), \ldots, x_{m+1} + I(W)) \) is algebraically dependent over \( k \), and therefore, there is a polynomial \( q(x_1, \ldots, x_{m+1}) \in I(W) \) with \( \deg_{x_{m+1}}(q) > 0 \). Let \( r \) be the leading coefficient of \( q \) with respect to \( x_{m+1} \), and let \( (y_1, \ldots, y_m) \in k^m \) be such that \( r(y_1, \ldots, y_m) \neq 0 \). Then there are only finitely many \( z \in k \) with \( (y_1, \ldots, y_m, z) \in W \). Since \( D = k^{m+1} \), there are then infinitely many \( z \in k \) with \( (y_1, \ldots, y_m, z) \in D \), a contradiction to the fact that \( g \) is \( f \)-determined.

In the case \( \dim(\pi(W)) \leq m - 1 \), we take \( (y_1, \ldots, y_m) \in k^m \setminus \pi(W) \). For all \( z \in k \), we have \( (y_1, \ldots, y_m, z) \in \overline{D} \) and \( (y_1, \ldots, y_m, z) \notin W \), and therefore all \( (y_1, \ldots, y_m, z) \) are elements of \( D \), a contradiction to the fact that \( g \) is \( f \)-determined.

Hence, we have \( \dim(D) = m \). \( \square \)

**Theorem 3.3.** Let \( k \) be an algebraically closed field, let \( \chi \) be its characteristic, let \( m, n \in \mathbb{N} \), and let \( (f_1, \ldots, f_m) \) be a sequence of polynomials in \( k[t_1, \ldots, t_n] \) that is algebraically independent over \( k \). Then we have:

(i) If \( \chi = 0 \), then \( k\langle f_1, \ldots, f_m \rangle \subseteq k(f_1, \ldots, f_m) \cap k[t_1, \ldots, t_n] \).

(ii) If \( \chi > 0 \), then \( k\langle f_1, \ldots, f_m \rangle \subseteq \text{rad}_k(k(f_1, \ldots, f_m) \cap k[t_1, \ldots, t_n]) \).

**Proof.** Let \( g \in k\langle f_1, \ldots, f_m \rangle \). We define

\[
D := \{(f_1(a), \ldots, f_m(a), g(a)) \mid a \in k^n\},
\]

we let \( \overline{D} \) be its Zariski-closure in \( k^{m+1} \), and we let \( W \) be an algebraic set with \( \dim(W) < \dim(\overline{D}) \) and \( \overline{D} = D \cup W \). By Lemma 3.2, we have \( \dim(D) = m \). Now, we distinguish cases according to the characteristic of \( k \). Let us first suppose \( \chi = 0 \). Let \( q := \text{Irr}(\overline{D}) \) be an irreducible polynomial with \( \overline{D} = V(q) \), and let \( d := \deg_{x_{m+1}}(q) \). Since \( f_1, \ldots, f_m \) are algebraically independent over \( k \), we have \( d \geq 1 \). We will now prove \( d = 1 \). Suppose \( d > 1 \). We write \( q = \sum_{i=0}^d q_i(x_1, \ldots, x_m) x_{m+1}^i \). We recall that, for a field \( K \), and \( f, g \in K[t] \) of positive degree, the resultant \( \text{res}_t(f, g) \) is 0 if and only if \( \deg(\gcd_{K[t]}(f, g)) \geq 1 \).
page 156, Proposition 8]. Let \( r := \text{res}_{x_{m+1}}(q, (\partial/\partial x_{m+1})q) \) be the resultant of \( q \) and its derivative when seen as elements of the ring \( k[x_1, \ldots, x_m][x_{m+1}] \). If \( r = 0 \), then \( q \) and \( (\partial/\partial x_{m+1})q \) have a common divisor in \( k[x_1, \ldots, x_m][x_{m+1}] \) with \( 1 \leq \deg_{x_{m+1}}(q) \leq d - 1 \) in \( k[x_1, \ldots, x_m][x_{m+1}] \). Using a standard argument involving Gauss’s lemma, we find a divisor \( a \) of \( q \) in \( k[x_1, \ldots, x_{m+1}] \) such that \( 1 \leq \deg_{x_{m+1}}(a) \leq d - 1 \). This contradicts the irreducibility of \( q \). Hence, \( r \neq 0 \). Since \( \dim(\pi(W)) \leq m - 1 \), \( r \neq 0 \), and \( q_d \neq 0 \), we have \( V(r) \cup V(q_d) \cup \pi(W) \neq k^m \). Thus, we can choose \( a \in k^m \) such that \( r(a) \neq 0 \), \( q_d(a) \neq 0 \), and \( a \not\in \pi(W) \). Let \( \tilde{q}(t) := q(a, t) \). Since \( \text{res}_t(\tilde{q}(t), \tilde{q}'(i)) = r(a) \neq 0 \), \( \tilde{q} \) has \( d \) different roots in \( k \), and thus \( q(a, x) = 0 \) has \( d \) distinct solutions for \( x \), say \( b_1, \ldots, b_d \). We will now show \( \{(a, b_i) \mid 1 \leq i \leq d\} \subseteq D \). Let \( i \in \{1, \ldots, d\} \), and suppose that \( (a, b_i) \not\in D \). Then \( (a, b_i) \in W \), and thus \( a \in \pi(W) \), a contradiction. Thus, all the elements \( (a, b_1), \ldots, (a, b_d) \) lie in \( D \). Since \( d > 1 \), this implies that \( g \) is not \((f_1, \ldots, f_m)\)-determined. Therefore, we have \( d = 1 \). Since \( (f_1, \ldots, f_m) \) is algebraically independent, the polynomial \( q \) witnesses that \( g \) is algebraic of degree 1 over \( k(f_1, \ldots, f_m) \), and thus lies in \( k(f_1, \ldots, f_m) \). This concludes the case \( \chi = 0 \).

Now we assume \( \chi > 0 \). It follows from Lemma 3.2 that, for every \( h \in k[t_1, \ldots, t_n] \), the Zariski-closure of

\[
D(h) := \{(f_1(a), \ldots, f_m(a), h(a)) \mid a \in k^n\}
\]

is an irreducible variety of dimension \( m \) in \( k^{m+1} \). This implies that there is an irreducible polynomial \( \text{Irr}(D(h)) \subset k[x_1, \ldots, x_m] \) such that \( D(h) = V(\text{Irr}(D(h))) \). Furthermore, by the closure theorem [2], there is an algebraic set \( W(h) \subset k^m \) such that \( \dim(W(h)) \leq m - 1 \) and \( D(h) \cup W(h) = \overline{D(h)} \). We will now prove the following statement by induction on \( \deg_{x_{m+1}}(\text{Irr}(D(h))) \).

Every \( f \)-determined polynomial \( h \in k[t_1, \ldots, t_n] \) is an element of \( \text{rad}_\chi(k(f_1, \ldots, f_m) \cap k[t_1, \ldots, t_n]) \).

Let \( d := \deg_{x_{m+1}}(\text{Irr}(D(h))) \).

If \( d = 0 \), then \( f_1, \ldots, f_m \) are algebraically dependent, a contradiction. If \( d = 1 \), then since \( f_1, \ldots, f_m \) are algebraically independent, \( h \) is algebraic of degree 1 over \( k(f_1, \ldots, f_m) \) and thus lies in \( k(f_1, \ldots, f_m) \cap k[t_1, \ldots, t_n] \).
$k[t_1, \ldots, t_n]$. Let us now consider the case $d > 1$. We set

$$e := \deg_{x_{m+1}} \left( \partial \frac{\partial}{\partial x_{m+1}} \text{Irr}(\overline{D(h)}) \right).$$

If $\partial / (\partial x_{m+1}) \text{Irr}(\overline{D(h)}) = 0$, then there is a polynomial $p \in k[x_1, \ldots, x_{m+1}]$ such that $\text{Irr}(\overline{D(h)}) = p(x_1, \ldots, x_m, x_{m+1})$. We know that $h^x$ is $f$-determined; hence, by Lemma 3.2, $\overline{D(h^x)}$ is of dimension $m$. Since

$$p(f_1, \ldots, f_m, h^x) = \text{Irr}(\overline{D(h)}) (f_1, \ldots, f_m, h) = 0,$$

we have $p \in I(D(h^x))$. Thus, $\overline{D(h^x)} \subseteq V(p)$. Therefore, the irreducible polynomial $\text{Irr}(\overline{D(h^x)})$ divides $p$, and thus

$$\deg_{x_{m+1}} (\text{Irr}(\overline{D(h^x)})) \leq \deg_{x_{m+1}} (p) < \deg_{x_{m+1}} (\text{Irr}(\overline{D(h)})).$$

By the induction hypothesis, we obtain that $h^x$ is an element of $\text{rad}_x (k(f_1, \ldots, f_m) \cap k[t_1, \ldots, t_n])$. Therefore, $h \in \text{rad}_x (k(f_1, \ldots, f_m) \cap k[t_1, \ldots, t_n])$. This concludes the case that $(\partial / \partial x_{m+1}) (\text{Irr}(\overline{D(h)})) = 0$.

If $e = 0$, we choose $a = (a_1, \ldots, a_m) \in k^m$ such that

$$\frac{\partial}{\partial x_{m+1}} \text{Irr}(\overline{D(h)}) \ (a_1, \ldots, a_m, 0) \neq 0,$$

such that the leading coefficient of $\text{Irr}(\overline{D(h)})$ with respect to $x_{m+1}$ does not vanish at $a$, and such that $a \notin \pi(W(h))$. Then $\text{Irr}(\overline{D(h)})(a, x) = 0$ has $d$ different solutions for $x$, say $b_1, \ldots, b_d$. Since $\{(a, b_i) \mid i \in \{1, \ldots, d\} \} \cap W(h) = \emptyset$ because $a \notin \pi(W(h))$, we have $\{(a, b_i) \mid i \in \{1, \ldots, d\} \} \subseteq D(h)$. Since $h$ is $f$-determined, $d = 1$, contradicting the case assumption.

If $e > 0$, then we compute the resultant $r := \text{res}_{x_{m+1}}^{(d,e)} (\text{Irr}(\overline{D(h)}), (\partial / \partial x_{m+1}) \text{Irr}(\overline{D(h)}))$, seen as polynomials of degrees $d$ and $e$ over the field $k(x_1, \ldots, x_m)$ in the variable $x_{m+1}$. As in the case $\chi = 0$, the irreducibility of $\text{Irr}(\overline{D(h)})$ yields $r \neq 0$. Now we let $a \in k^m$ be such that $r(a) \neq 0$, the leading coefficient $(\text{Irr}(\overline{D(h)}))_d$ of $\text{Irr}(\overline{D(h)})$ with respect to $x_{m+1}$ does not vanish at $a$, and $a \notin \pi(W(h))$. Setting $\tilde{q}(t) := \text{Irr}(\overline{D(h)})(a, t)$, we see that $\text{res}_{t}^{(d,e)} (\tilde{q}(t), \tilde{q}'(t)) \neq 0$. Thus, $\tilde{q}$ has $d$ distinct zeroes $b_1, \ldots, b_d$, and then $\{(a, b_i) \mid i \in \{1, \ldots, d\} \} \subseteq D(h)$. Since $d > 1$, this contradicts the fact that $h$ is $f$-determined. \qed
Theorem 3.4. Let $k$ be an algebraically closed field of characteristic 0, let $m, n \in \mathbb{N}$, and let $f = (f_1, \ldots, f_m)$ be a sequence of algebraically independent polynomials in $k[t_1, \ldots, t_n]$. Then the following are equivalent:

(i) $k\langle f_1, \ldots, f_m \rangle = k[f_1, \ldots, f_m]$.

(ii) $f$ is almost surjective.

Proof. (i) $\Rightarrow$ (ii). Suppose that $f$ is not almost surjective. Then, by Lemma 2.4, there are $p, q \in k[x_1, \ldots, x_m]$ such that $p(f_1, \ldots, f_m) \mid q(f_1, \ldots, f_m)$ and $p \mid q$. Let $d := \gcd(p, q)$, $p_1 := p/d$, $q_1 := q/d$. Let $a(t_1, \ldots, t_n) \in k[t_1, \ldots, t_n]$ be such that

$$p_1(f_1, \ldots, f_m) \cdot a(t_1, \ldots, t_n) = q_1(f_1, \ldots, f_m).$$

We claim that $b(t_1, \ldots, t_n) := q_1(f_1, \ldots, f_m) \cdot a(t_1, \ldots, t_n)$ is $f$-determined and is not an element of $k[f_1, \ldots, f_m]$. In order to show that $b$ is $f$-determined, we let $c, d \in k^n$ be such that $f(c) = f(d)$. If $p_1(f(c)) \neq 0$, we have $b(c) = q_1(f(c)) \cdot a(c) = q_1(f(c)) \cdot (q_1(f(c))/p_1(f(c))) \cdot (q_1(f(d))/p_1(f(d))) = q_1(f(d)) \cdot a(d) = b(d)$. If $p_1(f(c)) = 0$, we have $b(c) = q_1(f(c)) \cdot a(c)$. By (3.1), we have $q_1(f(c)) = 0$, and thus $b(c) = 0$. Similarly, $b(d) = 0$. This concludes the proof that $b$ is $f$-determined.

Let us now show that $b \notin k[f_1, \ldots, f_m]$. We have

$$b(t_1, \ldots, t_n) = \frac{q_1(f_1, \ldots, f_m)^2}{p_1(f_1, \ldots, f_m)}.$$

If $b \in k[f_1, \ldots, f_m]$, there is $r \in k[x_1, \ldots, x_m]$ with $r(f_1, \ldots, f_m) = b(t_1, \ldots, t_n)$. Then $r(f_1, \ldots, f_m) \cdot p_1(f_1, \ldots, f_m) = q_1(f_1, \ldots, f_m)^2$. From the algebraic independence of $(f_1, \ldots, f_m)$, we obtain $r(x_1, \ldots, x_m) \cdot p_1(x_1, \ldots, x_m) = q_1(x_1, \ldots, x_m)^2$; hence, $p_1(x_1, \ldots, x_m) \mid q_1(x_1, \ldots, x_m)^2$. Since $p_1, q_1$ are relatively prime, we then have $p_1(x_1, \ldots, x_m) \mid q_1(x_1, \ldots, x_m)$, contradicting the choice of $p$ and $q$. Hence, $f$ is almost surjective.

(ii) $\Rightarrow$ (i). From Theorem 3.3, we obtain $k(f) \subseteq k(f) \cap k[t_1, \ldots, t_n]$. Since $f$ is almost surjective, Lemma 2.4 yields $k(f) \cap k[t_1, \ldots, t_n] = k[f]$, and thus $k(f) \subseteq k[f]$. The other inclusion is obvious. \qed
Theorem 3.5. Let $k$ be an algebraically closed field of characteristic $\chi > 0$, let $m, n \in \mathbb{N}$, and let $f = (f_1, \ldots, f_m)$ be a sequence of algebraically independent polynomials in $k[t_1, \ldots, t_n]$. Then the following are equivalent:

(i) $k(f_1, \ldots, f_m) = \text{rad}_\chi(k[f_1, \ldots, f_m])$.

(ii) $f$ is almost surjective.

Proof. (i) $\implies$ (ii). As in the proof of Theorem 3.4, we produce an $f$-determined polynomial $b$ and relatively prime $p_1, q_1 \in k[x_1, \ldots, x_m]$ with $p_1 \nmid q_1$ and

$$b(t_1, \ldots, t_n) = \frac{q_1(f_1, \ldots, f_m)^2}{p_1(f_1, \ldots, f_m)}.$$ 

Now suppose that there is a $\nu \in \mathbb{N}_0$ with $b^{\nu} \in k[f_1, \ldots, f_m]$. Then $p_1(f_1, \ldots, f_m)\chi^{\nu}$ divides $q_1(f_1, \ldots, f_m)^{2\chi^{\nu}}$ in $k[f_1, \ldots, f_m]$, and thus $p_1(x_1, \ldots, x_m)$ divides $q_1(x_1, \ldots, x_m)^{2\chi^{\nu}}$ in $k[x_1, \ldots, x_m]$. Since $p_1$ and $q_1$ are relatively prime, we obtain $p_1 \mid q_1$, contradicting the choice of $p_1$ and $q_1$.

(i) $\implies$ (ii). From Theorem 3.3, we obtain $k(f) \subseteq \text{rad}_\chi(k(f) \cap k[t_1, \ldots, t_n])$. Since $f$ is almost surjective, Lemma 2.4 yields $k(f) \cap k[t_1, \ldots, t_n] = k[f]$, and thus $k(f) \subseteq \text{rad}_\chi(k[f])$. The other inclusion follows from the fact that the map $\varphi : k \to k$, $\varphi(y) := y^\chi$ is injective. $\Box$

4. Function compositions that are polynomials. For a field $k$, let $f = (f_1, \ldots, f_m) \in (k[t_1, \ldots, t_n])^m$, and let $h : k^m \to k$ be an arbitrary function. Then we write $h \circ f$ for the function defined by $(h \circ f)(a) = h(f_1(a), \ldots, f_m(a))$ for all $a \in k^n$. For an algebraically closed field $K$ of characteristic $\chi > 0$, $y \in K$ and $\nu \in \mathbb{N}_0$, we let $s^{(\nu)}(y)$ be the element in $K$ with $(s^{(\nu)}(y))^{\chi^{\nu}} = y$; so $s^{(\nu)}$ takes the $\chi^{\nu}$th root.

Theorem 4.1. Let $k$ be a field, let $K$ be its algebraic closure, let $m, n \in \mathbb{N}$, let $g, f_1, \ldots, f_m \in k[t_1, \ldots, t_n]$, and let $h : K^m \to K$ be an arbitrary function. Let $R := f(K^n)$ be the range of the function from $K^n$ to $K^m$ that $f = (f_1, \ldots, f_m)$ induces on $K$. We assume that $\dim(K^m \setminus R) \leq m - 2$, and that $h \circ f = g$ on $K$, which means that

$$h(f(a)) = g(a) \text{ for all } a \in K^n.$$
Then we have:

(i) If $k$ is of characteristic $0$, then there is a $p \in k[x_1, \ldots, x_m]$ such that $h(b) = p(b)$ for all $b \in R$.

(ii) If $k$ is of characteristic $\chi > 0$, then there are $p \in k[x_1, \ldots, x_m]$ and $\nu \in \mathbb{N}_0$ such that $h(b) = s^{(\chi^\nu)}(p(b))$ for all $b \in R$.

Proof. Let us first assume that $k$ is of characteristic $0$. We observe that as a polynomial in $K[t_1, \ldots, t_n]$, $g$ is $f$-determined. Hence, by Theorem 3.4, there is a $q \in K[x_1, \ldots, x_m]$ such that $q(f_1, \ldots, f_m) = g$. Writing

$$q = \sum_{(i_1, \ldots, i_m) \in I} \alpha_{i_1, \ldots, i_m} x_1^{i_1} \cdots x_m^{i_m},$$

we obtain $g = \sum_{(i_1, \ldots, i_m) \in I} \alpha_{i_1, \ldots, i_m} f_1^{i_1} \cdots f_m^{i_m}$. Expanding the right hand side and comparing coefficients, we see that $(\alpha_{i_1, \ldots, i_m})_{(i_1, \ldots, i_m) \in I}$ is a solution of a linear system with coefficients in $k$. Since this system has a solution over $K$, it also has a solution over $k$. The solution over $k$ provides the coefficients of a polynomial $p \in k[x_1, \ldots, x_m]$ such that $p(f_1, \ldots, f_m) = g$. From this, we obtain that $p(f_1(a), \ldots, f_m(a)) = g(a)$ for all $a \in K^n$, and thus $p(b) = h(b)$ for all $b \in R$. This completes the proof of item (i).

In the case that $k$ is of characteristic $\chi > 0$, Theorem 3.5 yields a polynomial $q \in K[x_1, \ldots, x_m]$ and $\nu \in \mathbb{N}_0$ such that $q(f_1, \ldots, f_m) = g^{\chi^\nu}$. As in the previous case, we obtain $p \in k[x_1, \ldots, x_m]$ such that $p(f_1, \ldots, f_m) = g^{\chi^\nu}$. Let $b \in R$, and let $a$ be such that $f(a) = b$. Then $s^{(\chi^\nu)}(p(b)) = s^{(\chi^\nu)}(p(f(a))) = g(a) = h(f(a)) = h(b)$, which completes the proof of (ii).

We will now state the special case that $k$ is algebraically closed and $f$ is surjective in the following corollary. By a polynomial function, we will simply mean a function induced by a polynomial with all its coefficients in $k$.

**Corollary 4.2.** Let $k$ be an algebraically closed field, let $f = (f_1, \ldots, f_m) \in (k[t_1, \ldots, t_n])^m$, and let $h : k^m \to k$ be an arbitrary function. We assume that $f$ induces a surjective mapping from $k^n$ to $k^m$ and that $h \circ f$ is a polynomial function. Then we have:

(i) If $k$ is of characteristic $0$, then $h$ is a polynomial function.
(ii) If $k$ is of characteristic $\chi > 0$, then there is a $\nu \in N_0$ such that $h^{\chi^\nu} : (y_1, \ldots, y_m) \mapsto h(y_1, \ldots, y_m)^{\chi^\nu}$ is a polynomial function.

REFERENCES


Erhard Aichinger, Institut für Algebra, Johannes Kepler Universität Linz, 4040 Linz, Austria

Email address: erhard@algebra.uni-linz.ac.at