ILLINOIS JOURNAL OF MATHEMATICS
Volume 25, Number 3, Fall 1981

ON THE JACOBIAN CONJECTURE

BY

DAVID WRIGHT[1]

0. Introduction

Let k be an algebraically closed field, and let $f: k^n \to k^n$ be a polynomial map. Then f is given by coordinate functions $f_1, \ldots, f_n$, where each f_i is a polynomial in n variables $X_1, \ldots, X_n$. If f has a polynomial inverse $g = (g_1, \ldots, g_n)$, then the determinant of the Jacobian matrix $\partial f_i/\partial X_j$ is a non-zero constant. This follows from the chain rule: Since $f \circ g$ is the identity, we have $X_i = g_i(f_1, \ldots, f_n)$, so

$$\delta_{ij} = \frac{\partial}{\partial X_j} g_i(f_1, \ldots, f_n) = \sum_{t=1}^{n} \frac{\partial g_i}{\partial X_t}(f_1, \ldots, f_n) \cdot \frac{\partial f_t}{\partial X_j}.$$

This says that the product

$$\left(\frac{\partial g_i}{\partial X_j}(f_1, \ldots, f_n)\right) \cdot \left(\frac{\partial f_i}{\partial X_j}\right)$$

is the identity matrix. Thus, the Jacobian determinant of f is a non-vanishing polynomial, hence a constant.

The Jacobian conjecture states, conversely, that if the characteristic of k is zero, and if $f = (f_1, \ldots, f_n)$ is a polynomial map such that the Jacobian determinant is a non-zero constant, then f has a polynomial inverse. The problem first appeared in the literature (to my knowledge) in 1939 in [11] for $k = C$. Many erroneous proofs have emerged, several of which have been published, all for $k = C$, $n = 2$.

The conjecture is trivially true for $n = 1$. For $n > 1$, the question is open. There has been a vigorous attempt by S. Abhyankar and T.-T. Moh to solve the problem for $n = 2$. In this case it is known that the Jacobian conjecture is equivalent to the assertion that whenever $f = (f_1, f_2)$ satisfies the Jacobian hypothesis, the total degree of f_1 divides that of f_2, or vice versa. Abhyankar and Moh have obtained a number of partial results by looking at the intersection of the curves f_1 and f_2 at infinite in $\mathbf{P}^2$. Moh has proved, in fact, that the conjecture is true provided the degrees of f_1 and f_2 do not exceed 100 [15].

Received August 8, 1979.

[1] Research partially supported by a National Science Foundation grant.

[2] This quite simple reduction, and some others due to E. H. Connell, will be published later in a paper now being prepared by H. Bass, Connell, and me. In that paper these reductions are used in conjunction with Abhyankar's formula for the analytic inverse of $f = (f_1, \ldots, f_n)$, i.e., those power series $g_1, \ldots, g_n$ for which $g_i(f_1, \ldots, f_n) = X_i$, $i = 1, \ldots, n$. The approach is to prove that all the high degree summands of each g_i are zero, i.e., that $g_1, \ldots, g_n$ are polynomials.

Another advance on the problem, for $n = 2$, appears in my own work [21]. I studied the group $GL_2(k[X_1, X_2])$ and proved the conjecture is true provided $(\partial f_i/\partial x_j)$ is a product of elementary matrices in $GL_2(k[X_1, X_2])$.

There is another approach to the problem which is essentially algebro-geometric, but does not appeal to anything peculiar to the case $n = 2$. This treatment appeals to the "simple connectivity" of k^n as an algebraic variety and contains quite a bit of "well-known" folklore, most of which is difficult or impossible to find in the literature. I have undertaken here to clarify these matters by including a fairly complete exposition of these methods and results, providing proofs which perhaps are novel in some cases, and always purely algebraic. I have avoided making reference to machinery much too general for the purpose at hand. I have appealed once to Zariski's Main Theorem [9, 4.4.9], and once to the Hurwitz-Zeuthen formula [10, Ch. IV, Corollary 2.4].

In Section 1, I have taken the liberty of writing a short exposé on the basic facts about separability and unramification; the reader to whom this is familiar will skip over it. Section 2 is on derivations, and culminates with a proof of the simple connectivity (no étale coverings) of affine n-space, with no appeal to transcendental methods. Section 3 contains proofs of the various partial results which I will briefly discuss in the following paragraphs.

One interesting theorem, due to S. Wang, is that the conjecture holds if each of the polynomials $f_1, \ldots, f_n$ has total degree ≤ 2. I have included a very simple proof of this which is due to S. Oda. This fact becomes especially interesting in the light of certain reductions which have been made using "stability", i.e., allowing n to increase. For example, I have proved (but not in this paper)[2] that the conjecture reduces, at the cost of increasing n, to the case where each f_i has degree ≤ 3.

The main idea in this treatment is to study the containment $A \supset B$ where $A = k[f_1, \ldots, f_n]$ and $B = k[X_1, \ldots, X_n]$. The conjecture is then equivalent to the condition $A = B$. Letting $\bar{A}$ denote the integral closure of A in B, we establish that the conjecture holds if $\bar{A} = A$ (i.e., B is birationally contained in A) or if $\bar{A} = B$ (i.e., B is integral over A). These are two well-known facts.

There is another definitive result, due to L. A. Campbell [5]. For $k = \mathbf{C}$, he proves that $f = (f_1, \ldots, f_n)$ has an inverse if f satisfies the Jacobian conditions, and if the field extension $\mathbf{C}(f_1, \ldots, f_n) \subset \mathbf{C}(X_1, \ldots, X_n)$ is a Galois extension The proof given by Campbell involves the theory of complex variables and complex manifolds. In this paper I give a purely algebraic proof of Campbell's theorem, which is valid for any field k of characteristic zero. The proof pinpoints the main obstacle to the solution of the problem, which lies in showing $\bar{A}$ is a separable A-algebra, and shows how the obstacle disappears with the assumption that $k(f_1, \ldots, f_n) \subset k(X_1, \ldots, X_n)$ is a Galois extension. It should be noted that Abhyankar has also given an algebraic proof for $n = 2$ [1].

All fields, rings, and algebras are assumed to be commutative with identity. If R is a ring, we let R^* denote its group of units. Let Q denote the rational numbers, and $\mathbf{C}$ the complex numbers. If S is an R-algebra, with structure homomorphism $f: R \to S$, given an ideal I of S, we write $I \cap R$ for $f^{-1}(I)$, even though f may not be injective.

1. Separable algebras and unramified morphisms

In order to spare the reader who is unfamiliar with these notions a greal deal of rummaging through the references, I will state the definitions and briefly prove some elementary facts, most of which are contained in at least one of these sources: [7], [3, Ch. VI], and [12].

Throughout this section, R will denote a ring and S and R-algebra. Given an S-bimodule M, we always assume $ax = xa$ for all $x \in M$, $a \in R$; and we let

$$M^S = \{x \in M \mid bx = xb \quad \text{for all} \quad b \in S\}.$$

DEFINITION. We say S is a *separable* R-algebra if the three following equivalent conditions hold.

(a) S is projective as an $S \otimes_R S$-module.

(b) The epimorphism p: $S \otimes_R S \to S$ defined by $p(a \otimes b) = ab$ splits (i.e., admits a section) as a map of $S \otimes_R S$-modules.

(c) The functor $M \mapsto M^S$ from the category of S-bimodules to the category of R-modules is exact.

The equivalence of these conditions is clear, since $M^S \cong \mathrm{Hom}_{S \otimes_R S}(S, M)$.

In a slightly different context, we say the ring homomorphism $R \to S$ is separable if it makes S a separable R-algebra.

PROPOSITION 1.1 [12, Prop. 3.3]. *If S is a separable R-algebra, and a projective R-module, then S is a finitely generated R-module.*

Proof. S is a direct summand of a free R-module, so we must have $S \oplus P$ is free with basis $\{x_i\}_{i \in I}$. Let s_i be the projection of x_i in S. Then any $a \in S$ can be written $a = \sum_{i \in I} f_i(a) s_i$ where $f_i \in \mathrm{Hom}_R(S, R)$, and $f_i(a) = 0$ for almost all $i \in I$. Then for $x \in S \otimes_R S$, we have

$$x = \sum_{i \in I} [(1_S \otimes f_i)(x)](1 \otimes s_i).$$

Now let $e \in S \otimes_R S$ be the idempotent such that $p(e) = 1$ (e exists because p splits). Then for $a \in S$, we have

$$\begin{aligned} a &= p[(1 \otimes a)e] \\ &= p\left(\left\{\sum_{i \in I} (1_S \otimes f_i)[(1 \otimes a)e]\right\}\right)(1 \otimes s_i) \\ &= \sum_{i \in I} \{(1_S \otimes f_i)[(1 \otimes a)e]\} s_i. \end{aligned}$$

Since e annihilates the kernel of p, then $(a \otimes 1 - 1 \otimes a)e = 0$, so $(1 \otimes a)e = (a \otimes 1)e$. Hence

$$(1_S \otimes f_i)[(1 \otimes a)e] = (1_S \otimes f_i)[(a \otimes 1)e] = (a \otimes 1)(1_S \otimes f_i)(e).$$

Therefore, if $(1_S \otimes f_i)(e) = 0$, then $(1_S \otimes f_i)[(1 \otimes a)e] = 0$ (independent of a), and clearly this is the case for all $i \in I$ outside of a finite subset $J \subset I$. Write $e = \sum_{t=1}^{n} x_t \otimes y_t$. Then for any $a \in S$, we have

$$\begin{aligned} a &= p[(1 \otimes a)e] \\ &= \sum_{j \in J} (1_S \otimes f_j)[(1 \otimes a)e]s_i \\ &= \sum_{j \in J} (1_S \otimes f_j)\left(\sum_{t=1}^{n} x_t \otimes a y_t\right)s_j \\ &= \sum_{j \in J} \sum_{t=1}^{n} f_j(a y_t) x_t s_j. \end{aligned}$$

This shows S is generated as an R-module by the finite set $\{x_t s_j\}_{1 \le t \le n,\, j \in J}$.

PREPOSITION 1.2. *Suppose U and V are multiplicative sets in R and S, respectively, such that the homomorphism $R \to S$ induces a homomorphism $U^{-1}R \to V^{-1}S$ of the localizations. If S is a separable R-algebra, then $V^{-1}S$ is a separable $U^{-1}R$-algebra.*

Proof. The map $V^{-1}S \otimes_{U^{-1}R} V^{-1}S \to V^{-1}S$ arises by localizing the epimorphism $S \otimes_R S \to S$ at the multiplicative set $\{(u \otimes v) \mid u, v \in V\}$. Hence, if $S \otimes S \to S$ splits, so does $V^{-1}S \otimes_{U^{-1}R} V^{-1}S \to V^{-1}S$.

Clearly the condition that S is a separable R-algebra is equivalent to the condition that the kernel J of p: $S \otimes S \to S$ is generated by an idempotent. This implies $J = J^2$, and if J is a finitely generated ideal it is equivalent: for if $J = J^2$ and J is finitely generated, then by Nakayama's Lemma there exists $e \in J$ such that $(1 - e)J = 0$, so $e = e^2$ and e generates J. Now J/J^2 is canonically isomorphic as an S-module to the module $\Omega_{S/R}$ of Kähler differentials [14, Chap. 10, Section 26]. Let (KFG) denote the following condition:

(KFG) The kernel J of p: $S \otimes S \to S$ is a finitely generated ideal.

The discussion above is then summarized by the following.

PROPOSITION 1.3. *If f is a separable R-algebra, then $\Omega_{S/D} = 0$. The converse is true provided S satisfies* (KFG).

Remark. The condition (KFG) is satisfied if S is a finitely generated R-algebra. For if S is generated by $x_1, \ldots, x_n$, then J is easily seen to be generated as an ideal by $x_i \otimes 1 - 1 \otimes x_i$, $i = 1, \ldots, n$. Also, if S satisfies (KFG), and if U and V are multiplicative sets in R and S, respectively, such that $V^{-1}S$ becomes a $U^{-1}R$-algebra, then $V^{-1}S$ satisfies (KFG) as a $U^{-1}R$-algebra, since the map $V^{-1}S \otimes_{U^{-1}R} V^{-1}S \to V^{-1}S$ is a localization of $S \otimes_R S \to S$.

PROPOSITION 1.4. *If S satisfies* (KFG), *then S being a separable R-algebra is equivalent to each of the following conditions*:

(1) *For each prime ideal $\mathscr{P}$ of S, with $\not{p} = \mathscr{P} \cap R$, $S_{\mathscr{P}}$ is a separable $R_{\not{p}}$-algebra.*

(1′) *For each maximal ideal $\mathscr{M}$ of S, with $m = \mathscr{M} \cap R$, $S_{\mathscr{M}}$ is a separable R_m-algebra.*

(2) *For each prime ideal $\not{p}$ of R, $S_{\not{p}}$ is a separable $R_{\not{p}}$-algebra.*

(2′) *For each maximal ideal m of R, S_m is a separable R_m-algebra.*

Proof. All these conditions hold if S is separable, by Proposition 1.2. Clearly (1) ⇒ (1′) and (2) ⇒ (2′). The implication (2′) ⇒ (1′) follows easily from Proposition 1.2. Assume (1′). Since S satisfies (KFG) it suffices to show $\Omega_{S/R} = 0$, by Proposition 1.3. But (1′) implies that $\Omega_{S_{\mathscr{M}}/R_m} = 0$ for all maximal ideals $\mathscr{M}$. Since $\Omega_{S_{\mathscr{M}}/R_m}$ is canonically isomorphic to $(\Omega_{S/R})_{\mathscr{M}}$, we see that $\Omega_{S/R}$ is a locally trivial S-module, hence is zero.

PROPOSITION 1.5. *Suppose R is a field. Then S is a separable R-algebra if and only if S is a finite product of fields $\prod_{i=1}^{n} F_i$ with each F_i being a finite separably algebraic extension of R.*

Proof. Assuming S is a separable R-algebra, it follows from Proposition 1.1 that S is a finite dimensional R-vector space. Therefore S is Artinian, and hence a finite product of Artinian local rings $\prod_{i=1}^{n} F_i$. To see that each F_i is a field, we will show that S is a semi-simple R-algebra, i.e., that all S-modules are projective. Given an S-module M, then for any S-module N, $\operatorname{Hom}_R(M, N)$ becomes an S-bimodule by letting $(afb)(x) = af(bx)$ for all $a, b \in S$, $f \in \operatorname{Hom}_R(M, N)$, $x \in M$. Now $\operatorname{Hom}_S(M, N) = \operatorname{Hom}_R(M, N)^S$. Since R is a field, $\operatorname{Hom}_R(M, -)$ is an exact functor, and since S is a separable R-algebra, $-^S$ is exact (see the definition of separability). Hence $\operatorname{Hom}_S(M, -)$, i.e., M is projective.

So each F_i is a finite field extension of R. Also the F_i's are localizations of S at its maximal ideals, so by Propositions 1.4, we may assume S is a finite field extension of R, and we must show that S is a separably algebraic extension. If S is not separably algebraic, then there is a subfield L between R and S with $S = L(t)$, $t^p \in L$ (where $p = \operatorname{char} R$), and $t \notin L$. Then $S = L[T]/(T^p - t^p)L[T]$. The derivation $\partial/\partial T$ on $L[T]$ carries the ideal $(T^p - t^p)L[T]$ into itself, therefore it induces a derivation $D: S \to S$, with $D(t) = 1$ and $D(R) = 0$. By the universal property of $\Omega_{S/R}$, there is a map $h: \Omega_{S/R} \to S$ such that the diagram

$$\begin{array}{ccc} S & \xrightarrow{D} & S \\ {\scriptstyle d}\downarrow & \nearrow{\scriptstyle h} & \\ \Omega_{S/R} & & \end{array}$$

commutes. Then $h(dt) = D(t) = 1$, so $dt \neq 0$. Therefore $\Omega_{S/R} \neq 0$, which is a contradiction, according to Proposition 1.3.

Conversely, assume $S = \prod_{i=1}^{n} F_i$, with each F_i a finite, separably algebraic extension of R. By Proposition 1.4, we can reduce to the case where S itself is a finite, separably algebraic field extension, and by Proposition 1.3 it suffices to show $\Omega_{S/R} = 0$, since condition (KFG) is obviously satisfied. Let $a \in S$, and let $f(X)$ be its minimal polynomial over R. Then $\Omega_{S/R}$, $0 = d[f(a)] = f'(a)\, da$. Since $f'(a) \neq 0$, $da = 0$. So $\Omega_{S/R} = 0$ as desired.

PROPOSITION 1.6. *Suppose I is an ideal of S, and $J = I \cap R$. Let $\bar{S} = S/I$ and $\bar{R} = R/J$. If S is a separable R-algebra, $\bar{S}$ is a separable $\bar{R}$-algebra.*

Proof. The epimorphism $\bar{p}$: $\bar{S} \otimes_{\bar{R}} \bar{S} \to \bar{S}$, arises from p: $S \otimes_R S \to S$ by applying $- \otimes_S \bar{S}$ and then $\bar{S} \otimes_S -$. So if p splits, so does $\bar{p}$.

PROPOSITION 1.7. *Suppose R and S are local, with maximal ideals $\mathfrak{m}$ and $\mathcal{M}$, respectively, and residue fields $\bar{R}$ and $\bar{S}$. Assume $R \to S$ is a local homomorphism. If S is a separable R-algebra, then $\mathcal{M} = \mathfrak{m}S$ and $\bar{S}$ is a finite separable field extension of $\bar{R}$. The converse holds if S satisfies* (KFG).

Proof. It follows from Propositions 1.4 and 1.5 that $S/\mathfrak{m}S$ is a finite separable field extension of $\bar{R}$, whence the first statement. Now let us assume (KFG) holds for S, and that $\mathcal{M} = \mathfrak{m}S$, and $\bar{S}$ is a finite separable field extension of $\bar{R}$. Consider the fundamental exact sequence of $\bar{S}$-modules

$$\mathcal{M}/\mathcal{M}^2 \xrightarrow{\delta} \Omega_{S/R} \otimes_S \bar{S} \to \Omega_{\bar{S}/\bar{R}} \to 0 \quad [14, \text{Theorem 58, p. 187}].$$

Our hypothesis implies $\Omega_{\bar{S}/\bar{R}} = 0$. Furthermore, $\mathcal{M}/\mathcal{M}^2$ is generated as an $\bar{S}$-module by elements which come from $\mathfrak{m}$, since $\mathcal{M} = \mathfrak{m}S$. But if $a \in \mathfrak{m}$, $\delta(a) = da \otimes 1 = 0$. So the image of δ is zero. Therefore, $\Omega_{S/R} \otimes_S \bar{S} = 0$. Since S satisfies (KFG), $\Omega_{S/R}$ is a finitely generated S-module, and therefore $\Omega_{S/R} = 0$, by Nakayama's Lemma. Hence S is a separable R-algebra, by Proposition 1.3.

Given a prime ideal $\mathfrak{p} \subset R$, write $k(\mathfrak{p}) = R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$.

PROPOSITION 1.8. *Consider the following conditions:*

(a) *S is a separable R-algebra.*

(b) *For all prime ideals $\mathfrak{p} \subset R$, $S \otimes_R k(\mathfrak{p})$ is a separable $k(p)$-algebra.*

(b′) *For all maximal ideals $\mathfrak{m} \subset R$, $S \otimes_R k(\mathfrak{m})$ is a separable $k(\mathfrak{m})$-algebra.*

The following implications hold: (a) ⇒ (b) ⇒ (b′). *If condition* (KFG) *holds for S, then* (b) ⇒ (a). *If, in addition, all maximal ideals of S restrict to maximal ideals of R, then* (b′) ⇒ (a).

Proof. (a) ⇒ (b) follows from Propositions 1.4 and 1.6. Clearly (b) ⇒ (b′). Assume (b) holds and condition (KFG) holds for S. To show S is separable, we appeal to the criterion given in (1) of Proposition 1.4. Le $\mathcal{P}$ be a prime ideal of

S, and let $\mathfrak{p} = \mathscr{P} \cap R$. We must show the $S_{\mathscr{P}}$ is a separable $R_{\mathfrak{p}}$-algebra. Since $S_{\mathscr{P}}$ also satisfies (KFG), (as an $R_{\mathfrak{p}}$-algebra), it suffices, by Proposition 1.7, to show that $\mathscr{P}S_{\mathfrak{p}} = \mathfrak{p}S_{\mathscr{P}}$ (i.e., that $S_{\mathscr{P}}/\mathfrak{p}S_{\mathscr{P}}$ is a field), and that $S_{\mathscr{P}}/\mathfrak{p}S_{\mathscr{P}}$ is a localization of $S \otimes_R k(\mathfrak{p})$ at a prime ideal, so these conclusions follow from Proposition 1.5. The same argument can be used to prove (b′) ⇒ (a), under the additional hypothesis. For then we assume $\mathscr{P}$ is maximal, so $\mathfrak{p}$ is also, and we can make use of the hypothesis (b′), appealing to (1′) of Proposition 1.4.

Now I will restate the notion of separability in the language of algebraic geometry.

DEFINITION. Let X and Y be Noetherian schemes and $f\colon X \to Y$ a morphism of finite type. Say f is *unramified* at $x \in X$ if the local homomorphism $\mathcal{O}_{f(x)} \to \mathcal{O}_x$ is separable, i.e., (Proposition 1.7) $\mathfrak{m}_x = \mathfrak{m}_{f(x)}\mathcal{O}_x$ and $k(x)$ is a finite, separably algebraic field extension of $k[f(x)]$.

From Proposition 1.4 it is clear that such a morphism f will be separable if and only if it is given locally by separable ring homomorphisms. Note that (b′) of Proposition 8 shows that if X and Y are k-schemes of finite type (e.g. varieties), where k is some field, it suffices to check unramification at closed points of X.

Suppose S is a finitely generated R-algebra, i.e., $S = R[X_1, \dots, X_n]/I$. Then there is the exact sequence

$$I/I^2 \xrightarrow{\delta} \Omega_{R[X_1, \dots, X_n]/R} \otimes_R S \to \Omega_{S/R} \to 0.$$

Now $\Omega_{R[X_1, \dots, X_n]/R}$ is free on the generators $dX_1, \dots, dX_n$. Assume in addition that S is finitely presented, so that I is generated by a finite collection $f_1, \dots, f_m$. Then I/I^2 is generated by the images $\bar{f}_1, \dots, \bar{f}_m$, and

$$\delta(\bar{f}_i) = \sum_{j=1}^{n} \overline{\left(\frac{\partial f_i}{\partial X_j}\right)}\, \overline{dX_j}.$$

(The overbar denotes the image after tensoring with S.). Thus the exact sequence shows that $\Omega_{S/R} = 0$, i.e., δ is an epimorphism, if and only if $\delta(\bar{f}_i)$, $i = 1, \dots, m$, generate

$$\Omega_{R[X_1, \dots, X_n]/R} \otimes_R S = S\,\overline{dX_1} \oplus \cdots \oplus S\,\overline{dX_n}.$$

This holds if and only if the $m \times n$ matrix $(\overline{\partial f_i/\partial X_j})$ (with entries in S) has a left inverse. The condition (KFG) holds for S, so the next proposition follows.

PROPOSITION 1.9 [20]. *Let $S = R[X_1, \dots, X_n]/(f_1, \dots, f_m)R[X_1, \dots, X_n]$. Then S is a separable R-algebra if and only if $(\overline{\partial f_i/\partial X_j})$ has a left inverse ($\overline{\partial f_i/\partial X_j}$ denotes the image of $\partial f_i/\partial X_j$ in S.)*

Now let k be a field, and let $S = k[X_1, \dots, X_n]$. Suppose $f_1, \dots, f_n \in S$ satisfy the Jacobian condition $\det(\partial f_i/\partial X_j) \in k^*$. It follows easily from this condition that $f_1, \ldots, f_n$ are algebraically independent. (Just consider the linear homogeneous terms.) Let $R = k[f_1, \ldots, f_n]$. We have a map of R-algebras ϕ: $R[Y_1, \ldots, Y_n] \to S$ sending Y_i to X_i. Clearly the polynomials $g_i(X, Y) = f_i(X) - f_i(Y)$ lie in the kernel of ϕ. (I simply write X for $X_1, \ldots, X_n$ and Y for $Y_1, \ldots, Y_n$.) Viewing

$$R[Y] = k[f_1(X), \ldots, f_n(X), Y_1, \ldots, Y_n]$$

as a polynomial ring in $2n$ variables over k, it is clear that $g_i(X, Y)$, $i = 1, \ldots, n$, are part of a system of variables for it. Specifically,

$$R[Y] = k[g_1(X, Y), \ldots, g_n(X, Y), Y_1, \ldots, Y_n].$$

Therefore, $R[Y]/[g_1(X, Y), \ldots, g_n(X, Y)]R[Y]$ is a polynomial ring in n variables over k. It follows that $g_1(X, Y), \ldots, g_n(X, Y)$ generate the kernel of ϕ. Also,

$$\det \left| \frac{\partial}{\partial Y_j} g_i(X, Y) = \frac{\partial}{\partial Y_j} f_i(Y) \right| \in k^*.$$

Therefore, by Proposition 1.9, S is a separable R-algebra. This proves the following.

PROPOSITION 1.10. *Let k be a field, $S = k[X_1, \ldots, X_n]$, $f_1, \ldots, f_n \in S$ with $\det(\partial f_i/\partial X_j) \in k^*$. Then, letting $R = k[f_1, \ldots, f_n]$, S is a separable R-algebra.*

Note. In fact, the above is true where k is any ring.

PROPOSITION 1.11 [19, proof of Theorem 2.2]. *Suppose $R = k[t]$, where k is an algebraically closed field, and t is algebraically independent over k. Suppose S is the integral closure of R in a finite field extension L of $F = k(t)$. If S is a separable R-algebra, then $S = R$.*

Proof. The containment $F \subset L$ corresponds to a morphism f: $C \to \mathbf{P}^1_k$ where C is the non-singular curve whose function field is L. Since S is a separable R-algebra, it follows from Propositions 1.4 and 1.7 that L is a separably algebraic field extension of F, and that no ramification occurs above any of the points of spec R in $\mathbf{P}^1_k$. According to the Hurwitz-Zeuthen formula [10, Chap. IV. Cor. 2.4], we have

$$2G - 2 - n(2g - 2) = \sum_{x \in C} [e(x) - 1]$$

where G is the genus of L, g is the genus of F, $n = [L: F]$, and $e(x)$ is the ramification index of f: $C \to \mathbf{P}^1_k$ at x. Since S is a separable R-algebra, $e(x) > 1$ can occur only for points of C lying above the point y at infinity in $\mathbf{P}^1_k$. We also know $n = \sum_{x \in C, f(x) = y} e(p)$, from local field theory [18, Chap. I, Proposition 10]. Since $g = 0$, we have $2(G + n - 1) < n$, which can only happen if $n = 1$, i.e., $L = F$. Since $R = k[t]$ is integrally closed, this implies $S = R$.

2. Derivations on Q-algebras and the simple connectivity of $A^n(k)$

Let R be a ring containing Q, and $D: R \to R$ a derivation. The kernel of D is a subring of R and is called the ring of constants with respect to D. If T is a multiplicative subset of R, D extends uniquely to a derivation on $T^{-1}R$ by letting

$$D\left(\frac{a}{b}\right) = \frac{bDa - aDb}{b^2}.$$

If I is an ideal of R such that $D(I) \subset I$, then D induces a derivation on R/I. We say D is locally nilpotent on R if for any $a \in R$, there exists an integer $n > 0$ such that $D^n(a) = 0$. Suppose S is an R-algebra and D is a derivation on S which is R-linear (i.e., the image of R in S consists of constants). Then given an R-algebra R', D induces an R' linear derivation on $S' = S \otimes_R R'$.

If D is a derivation on R, then the map $\phi: R \to R[[T]]$ defined by

$$\phi(a) = \sum_{n=0}^{\infty} \frac{D^n(a)}{n!} T^n$$

is a ring homomorphism, and

$$\phi \circ D = \frac{d}{dT} \circ \phi.$$

If D is locally finite, ϕ is a homomorphism into $R[T]$.

PROPOSITION 2.1. *Let S be a ring containing Q, and D a locally nilpotent derivation on S. Suppose $t \in S$ with $D(t) = 1$. Then $S = R[t]$, where R is the ring of constants and t is algebraically independent over R. Furthermore, $D = d/dt$.*

Proof. Let $\bar{S} = S/tS$, and let $\rho: S \to \bar{S}[T]$ be the composite of the homomorphism $\phi: S \to S[T]$ described above followed by the projection $S[T] \to \bar{S}[T]$. I claim ρ is an isomorphism. If so, then since

$$\rho \circ D = \frac{d}{dT} \circ \rho,$$

we have $R = \rho^{-1}(\bar{S})$; also $T = \rho(t)$, so the proposition will follow from this claim. To prove that ρ is surjective, it suffices to show its image contains $\bar{S}$. Given $a \in S$, let $\bar{a}$ denote its image in $\bar{S}$. We wish to see that $a \in \bar{S}[T]$ is in the image of ρ. Now

$$\rho(a) = \bar{a} + \overline{D(a)}\, T + \cdots + \frac{1}{n!} \overline{D^n(a)}\, T^n$$

and

$$\overline{D^k(a)} = 0 \quad \text{for } k > n.$$

Therefore, if $n > 0$, we can replace a by

$$a - \frac{1}{n!} D^n(a)t^n.$$

This lowers n and preserves $\bar{a}$, so we can conclude that ρ is surjective. Furthermore, if $a \in S$ is in the kernel of ρ, then $D^n(a) \in tS$ for $n \geq 0$. In particular $a = a_1 t$, and since $\rho(t) = T$, then $\rho(a_1) = 0$, and so $a_1 = a_2 t$, so $a = a_2 t^2$. We can continue this to prove that $t^n \mid a$ for all $n > 0$. I will show this is impossible unless $a = 0$. Consider the homomorphism $\phi: S \to S[T]$. $\phi(t) = t + T$, so if $t^n \mid a$, then $(t + T)^n$ divides $\phi(a)$, therefore the degree of $\phi(a)$ is no less than n, if $\phi(a) \neq 0$. Since $(t + T)^n$ divides $\phi(a)$ for all $n > 0$, $\phi(a) = 0$. Therefore, $a = 0$. This concludes the proof.

PROPOSITION 2.2. *Let S be a ring containing q, and let $D_1, \ldots, D_n$ be a family of commuting, locally nilpotent derivations on S.* Suppose there exists $t_1, \ldots, t_n \in S$ *such that $D_i(t_j) = \delta_{ij}$. Then $S = R[t_1, \ldots, t_n]$, where R is the ring of elements which are constants with respect to each of $D_1, \ldots, D_n$; $t_1, \ldots, t_n$ are algebraically independent over R; and $D_i = \partial/\partial t_i$.*

Proof. By Proposition 2.1, $S = R_1[t_1]$, where R_1 is the ring of constants with respect to D_1, t_1 is algebraically independent over R_1, and $D_1 = d/dt_1$. It follows easily from the fact that D_1 commutes with D_i, $i = 2, \ldots, n$, that $D_i(R_1) \subset R_1$. By induction, we have $R_1 = R[t_2, \ldots, t_n]$, and the proposition follows.

PROPOSITION 2.3 (Seidenberg [17]). *Let R be an integral domain containing Q, and let S be its complete integral closure. Suppose D is a derivation on K, the field of fractions of R. If $D(R) \subset R$, then $D(S) \subset S$.*

Proof. By hypothesis, the homomorphism $\phi: K \to K[[t]]$ induced by D carries R into $R[[t]]$. Suppose $a \in S$. Then a is "almost integral" over R, i.e., there exists $b \in R$ such that $ba^n \in R$ for $n \geq 1$. Applying ϕ, we have $\phi(b) \cdot \phi(a)^n \in R[[t]]$, and hence $b\phi(b)[\phi(a) - a]^n \in R[[t]]$. Since

$$\phi(a) - a = D(a)t + \frac{D^2(a)}{2} t^2 + \cdots,$$

it follows that $b^2 D(a)^n \in R$ for $n = 0, 1, 2, \ldots$, i.e., $D(a) \in S$.

The following proposition is an easy special case of some more general facts proved in [19], (see Propositions 1.2, 1.3 and 1.5).

PROPOSITION 2.4. *Let R be a discrete valuation ring containing q, D a derivation on R, and $x \in R$ such that $D(x) \in R^*$. Then x is a uniformizing parameter for R.*

Proof. Let t be a parameter, so that $x = ut^n$ with $u \in R^*$, $n \geq 0$. Then $D(x) = nut^{n-1} + D(u)t^n$. So t^{n-1} divides $D(x)$. Therefore, $n = 1$, since $D(x) \in R^*$.

The following proposition is one of the main results of [19]. I will essentially reproduce Vasconcelos' proof.

PROPOSITION 2.5 (Vasconcelos [19, Theorem 2.2]). *Suppose R is an integral domain containing Q, and suppose S is a domain containing R and integral over R. Suppose D is a derivation on S which restricts to a derivation on R which is locally nilpotent on R. Then D is locally nilpotent on S.*

Proof. One easily verifies that if $D|_R = 0$, then $D = 0$. So we may assume $D|_R \neq 0$. Let T denote the set of non-zero elements of R which are constants with respect to D. There exists $a \in R$ such that $D(a) \in T$, since $D|_R$ is locally nilpotent. The hypotheses of the proposition are preserved if we replace R and S by $T^{-1}R$ and $T^{-1}S$, and D by $T^{-1}D$. Letting $t = a/D(a)$, we have $D(t) = 1$, and so $R = K[t]$, and $D = d/dt$, by Proposition 2.1. Furthermore, K is a field. The algebraic closure of K in S consists of constants, so by enlarging R, we may assume K is algebraically closed in S. Then replacing R and S by $R \otimes_K \bar{K}$ and $S \otimes_K \bar{K}$, where $\bar{K}$ is the algebraic closure of K, and D by $D \otimes \mathrm{id}_{\bar{K}}$, the situation is preserved, so we may assume K is algebraically closed. Having made these reductions, I will show $S = R$.

Let $a \in S$, $\neq 0$, and let $a^n + b_{n-1}a^{n-1} + \cdots + b_0 = 0$ be an expression of integral dependence of a over R of minimal degree. Applying D, and solving for $D(a)$, we get

$$D(a) = -\frac{D(b_{n-1})a^{n-1} + \cdots + D(b_0)}{na^{n-1} + (n-1)b_{n-2}a^{n-2} + \cdots + b_1}$$

(the denominator being non-zero because of the minimality of n). Thus we see that $D(a)$ lies in the field $K(t, a)$. It follows that D carries $K(t, a) \cap S$ into itself, so for our purposes, we may replace S by its integral closure (Proposition 2.3), and thereby assume S is the integral closure of $K[t]$ in $K[t, a]$. It follows from Proposition 2.4 applied after localization that the map spec $S \to$ spec R is an unramified morphism of curves, and therefore, by Propositions 1.4 and 1.7, S is a separable R-algebra. Therefore $S = R$, by Proposition 1.11.

PROPOSITION 2.6. *Let A be a Noetherian regular local ring with maximal ideal m, and let $F = A/m$. Suppose A contains a field k and suppose $s_1, \ldots, s_r \in A$ such that the residues $\bar{s}_1, \ldots, \bar{s}_r \in F$ form a separating transcendence basis of F over k. Let $t_1, \ldots, t_n$ be a regular system of parameters for A. Then $\Omega_{A/k}$ is free and $dt_1, \ldots, dt_n, ds_2, \ldots, ds_n$ form a basis.*

Proof. The differentials $d\bar{s}_1, \ldots, d\bar{s}_r$ for a basis for $\Omega_{F/k}$ [14, Theorem 59, p. 191]. Considering the exact sequence

$$m/m^2 \to \Omega_{A/k} \otimes_A F \to \Omega_{F/k} \to 0$$

we see that the images of $dt_1, \ldots, dt_n, ds_1, \ldots, ds_r$ generate $\Omega_{A/k} \otimes_A F$, and therefore, by Nakayama's Lemma, these differentials generate $\Omega_{A/k}$. We must show they are linearly independent. Let $\hat{A}$ be the completion of A. Then $A \subset \hat{A}$, and $\hat{A} \cong F[[t_1, \ldots, t_d]]$ [14, Cor. 2, p. 206]. Let $D_i = \partial/\partial t_i$, $i = 1, \ldots, n$, which we will consider as a derivation from A to $F[[t_1, \ldots, t_n]]$. Since F is a separably algebraic field extension of $k(\bar{s}_1, \ldots, \bar{s}_r)$, the derivation $\partial/\partial \bar{s}_j$ extends (uniquely) to F [22, Cor. 2′, p. 125], and so it induces a derivation E_j on $F[[t_1, \ldots, t_n]]$, such that $E_j(t_i) = 0$ for $j = 1, \ldots, r$ and $i = 1, \ldots, n$. Again, we view E_j as a derivation from A to $F[[t_1, \ldots, t_n]]$. Now suppose there is a relation

$$\sum_{i=1}^{n} a_i\, dt_i + \sum_{j=1}^{r} b_j\, ds_j = 0$$

in $\Omega_{A/k}$. The derivations E_q, $1 \leq q \leq r$, induce a homomorphism

$$\Omega_{A/k} \to F[[t_1, \ldots, t_n]]$$

sending dx to $E_q(x)$ for any $x \in A$. Since $E_q(t_i) = 0$, we have

$$\sum_{j=1}^{r} b_j E_q(s_j) = 0.$$

Note that the order of $E_q(s_j)$ is zero if $j = q$, and positive if $j \neq q$. (Here the order of an element of $\hat{A}$ is the largest power of the maximal ideal which contains it.) If not all the b_j's are zero, then we choose q so that the order of b_q is minimal, and the equation $\sum_{j=1}^{r} b_j E_q(s_j) = 0$ becomes an impossibility. Hence, $b_1 = \cdots = b_r = 0$, and so $\sum_{i=1}^{n} a_i\, dt_i = 0$ in $\Omega_{A/k}$. The derivations D_p, $1 \leq p \leq n$, also induce homomorphisms

$$\Omega_{A/k} \to F[[t_1, \ldots, t_n]],$$

and since $D_p(t_i) = \delta_{ip}$, we must have $a_1 = \cdots = a_n = 0$. Therefore, $dt_1, \ldots, dt_n$, $ds_1, \ldots, ds_r$ for a basis.

PROPOSITION 2.7. *Let k be a field of characteristic zero, and let R and S be integral domains which are finitely generated k-algebras, with $R \subset S$ and S integral over R. Assume one of the following conditions.*

(a) *R is regular and S is a separable R-algebra.*

(b) *R and S are normal, and for all height one prime ideal $\mathscr{P} \subset S$, $S_{\mathfrak{p}}$ is separable over $R_{\mathfrak{p}}$, where $\mathfrak{p} = \mathscr{P} \cap R$.*

Then any k-derivation on R extends uniquely to a k-derivation on S. If (a) *holds, then S is also regular, and a flat R-module.*

Proof. In case R (and hence S) is a field, any derivation extends uniquely, by the well known facts of separable field extensions [22, Cor. 2′, p. 125]. For the general case, let D be a k-derivation on R. Let K and L be the fields of fractions of R and S, respectively. Then D extends to a unique derivation on K, and hence to L (by the above); we will denote this derivation by D. We must show $D(S) \subset S$. To do so, we will show $D(S_{\mathscr{P}}) \subset S_{\mathscr{P}}$ for all prime ideals $\mathscr{P} \subset S$. Under condition (b) S is normal, so it suffices to prove $D(S_{\mathscr{P}}) \subset S_{\mathscr{P}}$ for height one primes $\mathscr{P}$, since S is the intersection of its localizations at height one primes. So under either assumption, we have $R_{\not{p}}$ is regular, where $\not{p} = \mathscr{P} \cap R$. Set $A = R_{\not{p}}$, $B = S_{\mathscr{P}}$. Let $t_1, \ldots, t_n$ be a regular system of parameters for A. Then by Proposition 1.7, $t_1, \ldots, t_n$ also generate the maximal ideal of B. Since $\dim B = \dim A$, B is regular and the t's form a regular system of parameters for B also. This proves, under the assumption (a), that S is regular. Let $s_1, \ldots, s_r \in A$ be elements whose residues form a transcendence basis of the residue field of A over k. Then $s_1, \ldots, s_r$ do the same for B. By Proposition 2.6, the differentials $dt_1, \ldots, dt_n, ds_1, \ldots, ds_r$ form a basis for $\Omega_{A/k}$, and also for $\Omega_{B/k}$. Therefore the map

$$\Omega_{A/k} \otimes_A B \to \Omega_{B/k}$$

is an isomorphism, so for every B-module M,

$$\operatorname{Hom}_A (\Omega_{A/k}, M) = \operatorname{Hom}_B (\Omega_{B/k}, M).$$

Taking $M = B$ we see that every k-derivation $A \to B$ extends uniquely to a k-derivation on B. In particular, $D|_A$ has an extension D' to B, which also extends to L. But then $D' = D$, so $D(B) \subset B$.

With regard to the flatness of S, in case (a), we note that $S_{\not{p}}$ is a finitely generated module over $A = R_{\not{p}}$ and A is a regular local ring. Hence

$$\text{proj dim}_A S_{\not{p}} + \text{depth}_A S_{\not{p}} = \dim A \quad [14, \text{Chap. } 6].$$

But a regular system of parameters for A is also a regular sequence for $S_{\not{p}}$. Therefore $\text{depth}_A S_{\not{p}} = \dim A$, so $\text{proj dim}_A S_{\not{p}} = 0$.

PROPOSITION 2.8. *Let k. R, and S be as in Proposition 2.7, with k of characteristic zero. Assume that either* (a) *or* (b) *(of 2.7) holds. Assume that R is a polynomial ring $A[t_1, \ldots, t_n]$. Then there exists a subring B of S containing A such that $S = B[t_1, \ldots, t_n]$ and the containment $A \subset B$ is finite and satisfies which ever of the conditions* (a) *and* (b) *that $R \subseteq S$ satisfies.*

Proof. It clearly suffices to treat the case $n = 1$. The derivation d/dt on R extends to a derivation D on S by Proposition 2.7. According to Proposition 2.5, D is locally nilpotent on S. It follows from Proposition 2.1 that $S = B[t]$ with $B \supset A$. From this it is easy to prove that A and B satisfy the right conditions.

Note that it $A = k$ in Proposition 2.8, then B is a finite field extension of k. Thus we have proved the following:

THEOREM 2.9. *Let k be an algebraically closed field of characteristic zero. If $f\colon V \to A_k^n$ is an unramified, finite morphism of varieties, then f is an isomorphism. If V is normal, it suffices to check non-ramification at points of V corresponding to height one primes. (V is necessarily affine in this case because f, being finite, is an affine morphism.)*

Recall that a scheme W is called *simply connected* if every étale covering of W is trivial. An étale covering is a finite, flat, unramified morphism $f\colon V \to W$; it is called trivial if V is the disjoint union of finitely many copies of W, and f restricted to each copy is the identity. In the case where W is a nonsingular variety, such a morphism is automatically flat if it is finite and unramified (Proposition 2.7). Whence the above theorem can be restated as follows.

REFORMULATION OF THEOREM 2.9. *If k is an algebraically closed field of characteristic zero, then A_k^n is simply connected.*

3. Special cases

The following notation will be fixed throughout this section. Let

$$B = k[X_1, \ldots, X_n]$$

where k is a field of characteristic zero, and let $f_1, \ldots, f_n \in B$ be such that $\det(\partial f_i/\partial X_j) \in k^*$. Let $A = k[f_1, \ldots, f_n]$, and let $\bar{A}$ denote the integral closure of A in B. Let $T = \operatorname{spec} A$, $V = \operatorname{spec} \bar{A}$, and $W = \operatorname{spec} B$.

$$\begin{array}{cc} B & W \\ \cup & \downarrow \\ \bar{A} & V \\ \cup & \downarrow \\ A & T \end{array}$$

We know from Theorem 1.10 that B is a separable A-algebra, i.e., the morphism $W \to T$ is unramified.

PROPOSITION 3.1. *The map $W \to V$ is an open immersion, and if $V \neq W$, the complement $V - W$ has pure codimension one.*

Proof. Since B is a separable A-algebra, it is an easy consequence (Propositions 1.4 and 1.7) that B is separable over any subring containing A; in particular, B is separable over $\bar{A}$. Therefore, each fiber of the birational morphism $W \to V$ is finite (Proposition 1.5). Since V is normal, we may apply Zariski's Main Theorem [9, 4.4.9], which says that $W \to V$ is an open immersion. It is a well-known fact that the complement of an affine open subvariety in a normal variety, if non-empty, has pure codimension one. For the benefit of the reader, I will prove this for the case at hand. Since V is normal, if $\operatorname{codim}(V - W) > 1$ then every section over W extends to a section over V, i.e., $\bar{A} = B$, i.e., $V = W$. Hence if $V \neq W$, then $\operatorname{codim}(V - W) = 1$. To see that the codimension is pure, choose $g \in \Gamma(V) = \bar{A}$ such that g vanishes along those irreducible components of $V - W$ which are of codimension one, but does not vanish along the other components. Let $V_g = \operatorname{spec}(\bar{A}_g)$, $W_g = \operatorname{spec}(B_g)$. Then W_g is an open subvariety of V_g and the same argument as above shows that if $W_g \neq V_g$, then $\operatorname{codim}(V_g - W_g) = 1$. But $\operatorname{codim}(V_g - W_g) > 1$ by the choice of g, so $V_g = W_g$. But V_g intersects the components of $V - W$ which are of higher codimension and $W_g \subset W$. Hence there are no such components.

THEOREM 3.2. *If the containment $A \subset B$ is birational, then $A = B$.*

Proof. In this case $\bar{A} = A$. By Proposition 3.1 $W \to T$ is an open immersion, and if $A \neq B$, then $T - W$ has codimension one. Since A is factorial, there exists an irreducible $g \in A$ such that $V(g) \cap W = \varnothing$. Therefore, $g^{-1} \in B$, a contradiction, since $k^* = A^* = B^*$.

THEOREM 3.3. *If $B = \bar{A}$, then $A = B$.*

Proof. It follows from Propositions 1.4 and 1.5 that $K \subset L$ is a finite field extension, i.e., that $f_1, \ldots, f_n$ are algebraically independent over k (a fact which is easy to prove directly from the Jacobian condition). In the case $B = \bar{A}$ it follows from Proposition 2.8 that $B = k'[f_1, \ldots, f_n]$, where k' is a finite field extension of k. But since k is algebraically closed in B we have $k' = k$, hence $A = B$.

THEOREM 3.4. *If k is algebraically closed and the morphism $W \to T$ is injective on closed points, then it is an isomorphism, i.e. $A = B$.*

Proof. Since $f_1, \ldots, f_n$ are algebraically independent, B is algebraic over A and for some non-constant $g \in A$, $B[1/g]$ is integral over $A[1/g]$. Choose a closed point $x \in T$ in the image of W which does not vanish at g. Then x corresponds to a maximal ideal $\mathfrak{m}$ of A, and $B_{\mathfrak{m}}$ is separable and integral over $A_{\mathfrak{m}}$. The injectivity implies, moreover, that $B_{\mathfrak{m}}$ is a local ring. Since k is algebraically closed, the residue fields of both local rings are equal to k. Let $\mathscr{M}$ be the maximal ideal of $B_{\mathfrak{m}}$. Then $\mathscr{M} = \mathfrak{m}B_{\mathfrak{m}}$ (Proposition 1.7), and $B_{\mathfrak{m}} = k \oplus \mathscr{M} = k \oplus \mathfrak{m}B_{\mathfrak{m}} = A_{\mathfrak{m}} + \mathfrak{m}B_{\mathfrak{m}}$. Since $B_{\mathfrak{m}}$ is a finite $A_{\mathfrak{m}}$-module, Nakayama's Lemma implies $A_{\mathfrak{m}} = B_{\mathfrak{m}}$. Thus the containment $A \subset B$ is birational, and, by Theorem 3.2, we are done.

LEMMA 3.5 (S. Oda). *Assume k is algebraically closed and each f_i is of the form $X_i + h_i$ where h_i is a homogeneous polynomial, all of the same degree. Then the morphism $W \to T$ is injective along any straight line through the origin in W (with respect to the coordinate functions $X_1, \ldots, X_n$).*

Remark. It has been shown that one can reduce the conjecture to the case $f_i = X_i + h_i$ with h_i homogeneous of degree d, where $d \leq 3$. This will appear in the paper by Bass, Connell, and Wright mentioned in the footnote in Section 0'.

Proof. If $d = \deg h_i$ is 0 or 1, the conclusion is easily obtained. Assume the lemma is false, so that $d > 1$. Let $(\alpha_1, t, \ldots, \alpha_n t)$ parameterize a line over which injectivity fails. Let

$$F_i(t) = f_i(\alpha_1 t, \ldots, \alpha_n t) = \alpha_i t + h_i(\alpha_1 t, \ldots, \alpha_n t)$$
$$= \alpha_i t + \beta_i t^d \quad \text{where } \beta_i \in k.$$

Our assumption says there exist $a, b \in k$, $a \neq b$, such that $F_i(a) = F_i(b)$, for $i = 1, \ldots, n$. Then $\alpha_i a + \beta_i a^d = \alpha_i b + B_i b^d$, i.e., $\alpha_i(a - b) = \beta_i(b^d - a^d)$. It follows that each $f_i(t)$ is a scalar multiple of a polynomial $F(t) = t^d + \alpha t$. Since $d > 1$ and k is algebraically closed, there is a root c of $F'(t) = dt^{d-1} + \alpha$, and hence $F_i'(c) = 0$ for $i = 1, \ldots, n$. But

$$F_i'(t) = \sum_{j=1}^{n} \alpha_j \frac{\partial f_i}{\partial X_j} (\alpha_1 t, \ldots, \alpha_n t)$$

by the chain rule and so

$$0 = \sum_{j=1}^{n} \alpha_j \frac{\partial f_i}{\partial X_j} (\alpha_1 c, \ldots, \alpha_n c).$$

This contradicts the fact that

$$\det \left| \frac{\partial f_i}{\partial X_j} (\alpha_1 c, \ldots, \alpha_n c) \right| = 1.$$

THEOREM 3.6 (S. Wang [20]). *If the total degree in $X_1, \ldots, X_n$ of each $f_i, i = 1, \ldots, n$, is ≤ 2, then $A = B$.*

Proof. Tensoring with the algebraic closure of k, we may assume k is algebraically closed. It suffices, by Theorem 3.4, to show that $W \to T$ is injective on closed points. Suppose not. Then we can make a linear change of variables to arrange that the origin and one other point go to the same point, which may be assumed to be the origin in T. We now have $f_i = g_i + h_i$ where g_i and h_i are homogeneous of degrees one and two, respectively, and we can now make a homogeneous linear change of variables to arrange that $g_i = X_i$. This is a contradiction with Lemma 3.5, and so the theorem is proved.

THEOREM 3.7 (Campbell [5] for $k = \mathbf{C}$). *Let K and L be the fields of fractions of A and B, respectively. If L is a Galois extension of K, then $A = B$.*

(*Note.* This theorem includes Theorem 3.2.)

Proof. It will be shown that for all height one prime ideals $\mathscr{P} \subset \bar{A}$, $\bar{A}_{\not p}$ is a separable $A_{\not p}$-algebra, where $\not p = \mathscr{P} \cap A$. Once this is established then it follows from Proposition 2.8 (criterion (b)) that $\bar{A} = k']f_1, \ldots, f_n]$ where k' is a finite field extension of k. But since k is algebraically closed in B, $k' = k$, so $\bar{A} = A$. Therefore, the containment $A \subset B$ is birational, so $A = B$ by Proposition 3.2.

So let $\mathscr{P} \subset \bar{A}$ be a height one prime ideal, and let $\not p = \mathscr{P} \cap A$. Since A is factorial, $\not p = cA$, for some irreducible $c \in A$. Since $B^* = A^*$, $c \notin B^*$, so there is a height one prime ideal $\mathscr{L}$ of B containing c. Since B is a separable A-algebra, $B_{\mathscr{L}}/\mathscr{L}B_{\mathscr{L}}$ is a finite field extension of A_{q}/qA_{q}, where $q = \mathscr{L} \cap A$ (Propositions 1.4 and 1.7), so both fields have the same transcendence degree over k. Therefore, the height of q is also one, and since $q \subset \not p$, we must have $q = \not p$. Let

$\mathscr{P}' = \mathscr{L} \cap \bar{A}$. Then $\mathscr{P}' \cap A = \not{p}$ and since, by Proposition 3.1, spec $B \to$ spec $\bar{A}$ is an open immersion, $\bar{A}_{\not{p}'} = B_{\mathscr{L}}$. Therefore, $\bar{A}_{\not{p}'}$ is separable over $A_{\not{p}}$. Since $K \subset L$ is a Galois extension, there exists an element $\sigma \in \text{Gal}\,(L/K)$ such that $\sigma(\mathscr{P}) = \mathscr{P}'$ [13, Chap. IX, Prop. 11]. Then $\sigma(\bar{A}_{\not{p}}) = \bar{A}_{\not{p}'}$. Therefore, $\bar{A}_{\not{p}}$ is a separable $A_{\not{p}}$-algebra. This proves the theorem.

The following theorem summarizes the results of this section.

THEOREM. *Let k be a field of characteristic zero, and let*

$$f_1, \ldots, f_n \in k[X_1, \ldots, X_n]$$

be such that det $(\partial f_i/\partial X_j)$ *is a non-zero constant. Then*

$$f = (f_1, \ldots, f_n)\colon k^n \to k^n$$

has a polynomial inverse provided any one of the following conditions holds.

(1) *$k[X_1, \ldots, X_n]$ is integral over $k[f_1, \ldots, f_n]$.*

(2) *$k(X_1, \ldots, X_n)$ is a Galois field extension of $k(f_1, \ldots, f_n)$ (e.g. $k(X_1, \ldots, X_n) = k(f_1, \ldots, f_n)$).*

(3) *The polynomial map $\bar{k}^n \to \bar{k}^n$ given by f, where $\bar{k}$ is the algebraic closure of k, is injective.*

(4) *The total degree of each polynomial $f_1, \ldots, f_n$* is ≤ 2.

BIBLIOGRAPHY

1. S. S. ABHYANKAR, *Expansion techniques in algebraic geometry*. Lectures on Mathematics and Physics, No. 57, Tata Institute of Fundamental Research, Bombay, 1977.
2. S. S. ABHYANKAR and T.-T. MOH, *Embeddings of the line in the plane*, J. Reine Angew. Math., vol. 276 (1976), pp. 148–166.
3. A. ALTMAN and S. KLEIMAN, *Introduction to Grothendieck duality theory*, Lectures Notes in Mathematics, vol. 146, Springer-Verlag, New York, 1970.
4. H. BASS, E. H. CONNELL and D. L. WRIGHT, *Locally polynomial algebras are symmetric algebras*, Inventiones Math., vol. 38 (1977), pp. 279–299.
5. L. A. CAMPBELL, *A condition for a polynomial map to be invertible*, Math. Ann., vol. 205 (1973), pp. 243–248.
6. I. CANALS and E. LLUIS, *Acerca de un resultado de Segre*, An. Inst. Mat. Nac. Autónoma México, vol. 10 (1970), pp. 1–15.
7. F. DEMYER and E. INGRAM, *Separable algebras over commutative rings*, Lecture Notes in Mathematics, vol. 181, Springer-Verlag, New York, 1971.
8. W. ENGEL, *Ein Satz über ganze Cremona-Transformationen der Ebene*, Math. Ann., vol. 130 (1955), pp. 11–19.
9. A. GROTHENDIECK and J. DIEUDONNÉ, *Eléments de Géométrie Algebrique, Étude Cohomologique des Faisceaux Cohérents (Premier Partie)*, Publications Mathématiques, No. 11, Institut des Hautes Études Scientifiques, Paris, 1961.
10. R. HARTSHORNE, *Algebraic geometry*, Springer-Verlag, New York, 1977.
11. O. H. KELLER, *Ganze Cremona-Transformationen*, Monatshefte für Mathematik und Physik, vol. 47, pp. 299–306 (1939).
12. M. A. KNUS and M. OJANGUREN, *Théorie de la Déscente et Algèbres d'Azumaya*, Lecture Notes in Mathematics, vol. 389, Springer-Verlag, New York, 1974.
13. S. LANG, *Algebra*, Addison-Wesley, Reading, Mass., 1965.
14. H. MATSUMURA, *Commutative algebra*, W. A. Benjamin, New York, 1970.

15. T.-T. Moh, *On the global Jacobian conjecture for polynomials of degree less than* 100, to appear.
16. B. Segre, *Corrispondenze di Möbius e transformazioni creminiane intere*, Atti Accad. Sci. Torino Cl. Sci. Fis. Mat. Natur., vol. 91 (1956–1957), pp. 3–19.
17. A. Seidenberg, *Derivations and integral closure*, Pacific J. Math., vol. 16 (1996), pp. 167–173.
18. J.-P. Serre, *Corps Locaux*, Publications de l'Institut de Mathématique de l'Université de Nancago VIII, Actualités Scientifiques et Industrielles 1296, Hermann, Paris, 1962.
19. V. Vasconcelos, Derivations on commutative Noetherian Rings, Math. Zeitschr., vol. 112 (1969), pp. 229–233.
20. S. Wang, *A Jacobian criterion for separability*, J. Algebra,
21. D. Wright, *The amalgamated free product structure of* $GL_2(k[X_1, \ldots, X_n])$ *and the weak Jacobian theorem for two variables*, J. Pure Appl. Algebra, vol. 12 (1978), pp. 235–251.
22. O. Zariski and P. Samuel, *Commutative algebra*, Van Nostrand, Princeton, N.J., 1958.

Washington University
St. Louis, Missouri