# Hilbert's Thirteenth Problem

Shreeram S. ABHYANKAR*

**Abstract**
Some progress is made in Hilbert's Thirteenth problem.

**Résumé**
Un certain progrès est réalisé dans le treizième problème de Hilbert.

## 1 Introduction

Amongst the 23 problems which Hilbert formulated at the turn of the last century [Hi1], the 13th problem asks if every function of $n$ variables is composed of functions of $n-1$ variables, with the expectation that this is not so for any $n \geq 2$.

Hilbert's continued fascination with the 13th problem is clear from the fact that in his last mathematical paper [Hi2], published in 1927, where he reported on the status of his problems, Hilbert devoted 5 pages to the 13th problem and only 3 pages to the remaining 22 problems. In [Hi2], in support of the $n=2$ case of the 13th problem, Hilbert formulated his *sextic conjecture* which says that, although the solution of a general equation of degree 6 can be reduced to the situation when the coefficients depend on 2 variables, this cannot be cut down to 1 variable.

In the 1955 paper [A01] which represents the failure part of his Ph.D. Thesis, Abhyankar showed that Jung's method of resolving singularities of complex algebraic surfaces does not carry over to nonzero characteristic; he did this by constructing a 6 degree surface covering with nonsolvable local Galois group above a simple point of the branch locus. In his 1957 paper [A04], by taking a section of this surface covering, Abhyankar was led to write down several explicit families of bivariate polynomials $f(X,Y)$ giving unramified coverings of the affine line in nonzero characteristic and to suggest that their Galois groups be computed. It turned out that these Galois groups include all the alternating and symmetric groups $\mathrm{Alt}_N$ and $\mathrm{Sym}_N$ where $N>1$ is any integer, all the Mathieu groups $M_{11}$, $M_{12}$, $M_{22}$, $M_{23}$ and $M_{24}$, the linear groups $\mathrm{SL}(N,q)$ and $\mathrm{PSL}(N,q)$ where $N>1$ is any integer and $q>1$ is any

AMS 1980 *Mathematics Subject Classification* (1985 *Revision*): 12F10, 14H30, 20D06, 20E22
*Mathematics Department, Purdue University, West Lafayette, IN 47907, USA — This work was partly supported by NSF grant DMS 91–01424 and NSA grant MDA 904–92–H–3035.

prime power, the unitary groups $\mathrm{SU}(2N-1,q)$ and $\mathrm{PSU}(2N-1,q)$ where $N>1$ is any integer and $q>1$ is any prime power, the symplectic groups $\mathrm{Sp}(2N,q)$ and $\mathrm{PSp}(2N,q)$ where $N>2$ is any integer and $q>1$ is any prime power, and the orthogonal groups $\Omega^-(2N,q)$ and $\mathrm{P}\Omega^-(2N,q)$ where $N>3$ is any integer and $q>1$ is any odd prime power; see Abhyankar [A06] to [A12].

In the 1956 paper [A02] which represents the success part of his Ph.D. Thesis, Abhyankar resolved surface singularities in nonzero characteristic and observed that this completes the solution of Zariski's version of Hilbert's 14th problem in the 2 dimensional case, and shows the birational invariance of arithmetic genus for 2 dimensional varieties; later in his 1966 monograph [A05], Abhyankar resolved singularities of 3 dimensional varieties in nonzero characteristic and observed that this shows the birational invariance of arithmetic genus for 3 dimensional varieties.

Remarkably, it became apparent after 40 years that the above cited 6 degree surface covering constructed in Abhyankar's failure paper [A01] precisely solves Hilbert's sextic conjecture, and hence settles the $n=2$ case of his 13th problem, by showing that the algebraic closure $k(X,Y)^*$ of the bivariate rational function field $k(X,Y)$ over a field $k$ is strictly bigger than the compositum of the algebraic closures $k(f)^*$ of $k(f)$ with $f$ varying over all elements of the polynomial ring $k[X,Y]$. Likewise, Galois theory together with ideas from resolution of singularities of higher dimensional varieties leads to a weak form of the 13th problem for general $n$, which says that the algebraic closure $k(Z_1,\dots,Z_n)^*$ of the $n$-variable rational function field $k(Z_1,\dots,Z_n)$ is strictly bigger than the compositum of the algebraic closures $k(g)^*$ of $k(g)$ as $g$ varies over all $(n-1)$-tuples $g_1,\dots,g_{n-1}$ of elements of $k[Z_1,\dots,Z_n]$ whose linear parts are linearly independent.

In Section 4 we shall prove the stronger version of the $n=2$ case of the 13th problem which says that, for any $n>1$, the integral closure $B_n$ of $A_n=k[Z_1,\dots,Z_n]$ in the algebraic closure $L_n=k(Z_1,\dots,Z_n)^*$ of the $n$-variable rational function field $K_n=k(Z_1,\dots,Z_n)$ over a field $k$ is strictly bigger than the integral closure of $A_n$ in the compositum $L_{n,1}^{(1)}$ of the algebraic closures $k(f)^*$ of $k(f)$ (in $L_n$) with $f$ varying over all elements of $A_n$. Actually, we shall prove more. Namely, let $L_{n,1}^{(2)}$ be the compositum of the algebraic closures $k(f^{(1)})^*$ of $k(f^{(1)})$ with $f^{(1)}$ varying over all elements of $L_n^{(1)}$ which are integral over $A_n$, let $L_n^{(3)}$ be the compositum of the algebraic closures $k(f^{(2)})^*$ of $k(f^{(2)})$ with $f^{(2)}$ varying over all elements of $L_n^{(2)}$ which are integral over $A_n$, and so on. Let $L_{n,1}=L_{n,1}^{(1)}\cup L_{n,1}^{(2)}\cup L_{n,1}^{(3)}\cup\dots$ and let $B_{n,1}$ be the integral closure of $A_n$ in $L_{n,1}$. Let $\widehat{A}_n=$ the formal power series ring $k^*[[Z_1,\dots,Z_n]]$ over the algebraic closure $k^*$ of $k$, let $\widehat{K}_n=$ the meromorphic series field $k^*((Z_1,\dots,Z_n))=$ the quotient field of $\widehat{A}_n$, and let $\widehat{B}_n$ be the integral closure of $\widehat{A}_n$ in the algebraic closure $\widehat{L}_n$ of $\widehat{K}_n$, where we suppose that $\widehat{L}_n$ is an overfield of $L_n$. Finally, let $\widehat{K}_n^{\mathrm{sol}}$ be the *maximal solvable* extension of $\widehat{K}_n$ (in $\widehat{L}_n$), i.e., $\widehat{K}_n^{\mathrm{sol}}$ is the maximal normal extension of $\widehat{K}_n$ (in $\widehat{L}_n$) such that the Galois groups of all the intermediate finite normal extensions are solvable (where we note that the Galois group of a finite normal extension coincides with the Galois group of the maximal separable subextension); alternatively, $\widehat{K}_n^{\mathrm{sol}}$ may be defined to be the compositum of all the finite normal extensions of $\widehat{K}_n$ with solvable Galois groups. In Section 2 we shall show that then $L_{n,1} \subset \widehat{K}_n^{\mathrm{sol}}$. In Section 3 we shall indicate how the unsolvable 6 degree surface covering of [A01] solves Hilbert's sextic conjecture. By putting together the results of Sections 2 and 3, in Section 4 we shall show that $B_n$ is strictly bigger than $B_{n,1}$; we call this the *presingleton version* of the 13th problem.

To state the corresponding version of the general case of the 13th problem, given any $n > m \geq 1$, let $L_{n,m}^{(1)}$ be the compositum of the algebraic closures $k(g)^*$ of $k(g)$ with $g$ varying over all $m$-tuples of elements of $A_n$, let $L_{n,m}^{(2)}$ be the compositum of the algebraic closures $k(g^{(1)})^*$ of $k(g^{(1)})$ with $g^{(1)}$ varying over all $m$-tuples of elements of $L_{n,m}^{(1)}$ which are integral over $A_n$, let $L_{n,m}^{(3)}$ be the compositum of the algebraic closures $k(g^{(2)})^*$ of $k(g^{(2)})$ with $g^{(2)}$ varying over all $m$-tuples of elements of $L_{n,m}^{(2)}$ which are integral over $A_n$, and so on. Let $L_{n,m} = L_{n,m}^{(1)} \cup L_{n,m}^{(2)} \cup L_{n,m}^{(3)} \cup \dots$, and let $B_{n,m}$ be the integral closure of $A_n$ in $L_{n,m}$. Then the said version conjectures that $B_n$ is strictly bigger than $B_{n,m}$; we call this the *general version* of the 13th problem. In Section 2 we shall formulate a version which is stronger than the general version and call it the *analytic version* of the 13th problem.

In Section 5 we shall settle a weak version of the general case of the 13th problem by proving that, whenever $n > m \geq 1$, $B_n$ is strictly bigger than the integral closure $B'_{n,m}$ of $A_n$ in the compositum $L'_{n,m}$ of $K_n$ and the algebraic closures $k(g)^*$ of $k(g)$ as $g$ varies over all $m$-tuples $g_1, \dots, g_m$ of elements of $A_n$ whose linear parts (i.e., terms of degree 1) are linearly independent over $k$; we call this the *prelinear version* of the 13th problem.

In Section 6 we shall prove an extremely weak version of the 13th problem which says that, for any partition $n_1 + \cdots + n_t = n$ of $n$ into positive integers $n_1, \dots, n_t$ with $t > 1$, $B_n$ is strictly bigger than the integral closure $B''_{n_1,\dots,n_t}$ of $A_n$ in the compositum $L''_{n_1,\dots,n_t}$ of $K_n$ and the algebraic closures $k(\{Z_j : n_1 + \cdots + n_{i-1} < j \leq n_1 + \cdots + n_i\})^*$ of $k(\{Z_j : n_1 + \cdots + n_{i-1} < j \leq n_1 + \cdots + n_i\})$ for $1 \leq i \leq t$; we call this the *prepartition version* of the 13th problem. It may be noted that the $n = 2$ case of this can be found in Abhyankar's 1956 paper [A03] which was written to answer a question of Igusa.

In Sections 4, 5 and 6 we shall actually prove the analytic, and hence stronger, forms of the presingleton, prelinear and prepartition versions and we shall respectively call these the *singleton, linear* and *partition versions.*

In his discussion of the 13th problem, Hilbert did not make it clear what kind of functions he had in mind. We have interpreted them as integral functions. In their

1976 reformulation, Arnold-Shimura [ArS] took them to be algebraic functions. In their 1963 articles, Arnold [Ar] and Kolmogorov [Kol] thought of them as continuous functions.

It is a pleasure to thank Jim Madden for stimulating conversations concerning the Hilbert 13th problem.

## 2 Analytic version and solvability

Given any field $k$ and integers $n > m \geq 1$, let $A_n, B_n, K_n, L_n, k^*, \widehat{A}_n, \widehat{B}_n, \widehat{K}_n, \widehat{L}_n, \widehat{K}_n^{\mathrm{sol}}$ and $L_{n,m}^{(1)}, L_{n,m}^{(2)}, L_{n,m}^{(3)}, \ldots, L_{n,m}, B_{n,m}$ be as in Section 1. Let $\widetilde{L}_{n,m}^{(1)}$ be the compositum of the algebraic closures $k^*(g)^*$ of $k^*(g)$ with $g$ varying over all $m$-tuples of elements of $\widehat{A}_n$. Let $\widetilde{L}_{n,m}^{(2)}$ be the compositum of the algebraic closures $k^*(g^{(1)})^*$ of $k^*(g^{(1)})$ with $g^{(1)}$ varying over all $m$-tuples of elements of $\widetilde{L}_{n,m}^{(1)} \cap \widehat{B}_n$, let $\widetilde{L}_{n,m}^{(3)}$ be the compositum of the algebraic closures $k^*(g^{(2)})^*$ of $k^*(g^{(2)})$ with $g^{(2)}$ varying over all $m$-tuples of elements of $\widetilde{L}_{n,m}^{(2)} \cap \widehat{B}_n$, and so on. Let $\widetilde{L}_{n,m} = \widetilde{L}_{n,m}^{(1)} \cup \widetilde{L}_{n,m}^{(2)} \cup \widetilde{L}_{n,m}^{(3)} \cup \ldots$, and let $\widetilde{B}_{n,m}$ be the integral closure of $\widehat{A}_n$ in $\widetilde{L}_{n,m}$. Now obviously:

*Remark 2.1.* $L_{n,m} \subset \widetilde{L}_{n,m}$ and hence $B_{n,m} \subset \widetilde{B}_{n,m}$.

Therefore if we conjecture that $B_n \not\subset \widetilde{B}_{n,m}$ and call this the *preanalytic version* of the 13th problem, then clearly:

*Remark 2.2.* The preanalytic version for $k, n, m$ implies the general version for $k, n, m$.

For any finite sequence $r = (r_1, \ldots, r_u)$ of elements in $\widehat{B}_n$, by basic properties of complete local rings, as given in Chapter VIII of [ZS2], we see that $\widehat{A}_n[r]$ is an $n$-dimensional complete local domain and $k^*$ is a coefficient field of $\widehat{A}_n[r]$, i.e., $k^*$ is mapped bijectively onto the residue field $\widehat{A}_n[r]/M(\widehat{A}_n[r])$ by the residue class epimorphism $\mu_r : \widehat{A}_n[r] \mapsto \widehat{A}_n[r]/M(\widehat{A}_n[r])$ where $M(\widehat{A}_n[r])$ is the maximal ideal in $\widehat{A}_n[r]$. Given any finite sequence of elements $s = (s_1, \ldots, s_v)$ in $\widehat{A}_n[r]$, we put $\bar{s} = (\bar{s}_1, \ldots, \bar{s}_v) = (s_1 - \tilde{s}_1, \ldots, s_v - \tilde{s}_v)$, where $\tilde{s}_1, \ldots, \tilde{s}_v$ are the unique elements in $k^*$ such that $\mu_r(s_1) = \mu_r(\tilde{s}_1), \ldots, \mu_r(s_v) = \mu_r(\tilde{s}_v)$, and by $k^*[[s]]$ we denote the closure of $k^*[\bar{s}]$ in $\widehat{A}_n[r]$ with respect to its Krull topology. Note that then $k^*[[s]]$ is a complete local domain of dimension at most $v$ and $k^*$ is a coefficient field of $k^*[[s]]$; by $k^*((s))$ we denote the quotient field of $k^*[[s]]$; likewise by $k^*((s))^*$ we denote the algebraic closure of $k^*((s))$ (in $\widehat{L}_n$). If $r' = (r'_1, \ldots, r'_{u'})$ is any other finite sequence in $\widehat{B}_n$ such that the elements $s_1, \ldots, s_v$ belong to $\widehat{A}_n[r']$ then by passing to $\widehat{A}_n[r, r']$ we see that (for any finite sequence $s$ in $\widehat{B}_n$) the above definitions of $\bar{s}$, $k^*[[s]]$, $k^*((s))$ and $k^*((s))^*$ are independent of $r$ (for instance we can take $r = s$). Note that if $s$ is a singleton, i.e., if $v = 1$, then either $k^*[[s]] = k^*$ or $k^*[[s]]$ is a complete discrete valuation ring, and hence in both the cases (by generalized Newton's Theorem) $k^*((s))^*$ is a *solvable extension* of $k^*((s))$, i.e., $k^*((s))^*$ is a normal extension of

$k^*((s))$ such that the Galois groups of all the finite normal intermediate extensions are solvable. [The said generalized Newton's Theorem says that the Galois group of a finite Galois extension of a field which is complete with respect to a discrete valuation with algebraically closed residue field is always solvable; in view of Hensel's Lemma (see Chapter VIII of [ZS2]), this follows from the fact that the inertia group of a discrete valuation is always solvable (see Chapter V of [ZS1])].

Let $\widehat{L}^{(1)}_{n,m}$ be the compositum of the fields $k^*((g))^*$ with $g$ varying over all $m$-tuples of elements of $\widehat{A}_n$. Let $\widehat{L}^{(2)}_{n,m}$ be the compositum of the fields $k^*((g^{(1)}))^*$ with $g^{(1)}$ varying over all $m$-tuples of elements of $\widehat{L}^{(1)}_{n,m} \cap \widehat{B}_n$, let $\widehat{L}^{(3)}_{n,m}$ be the compositum of the fields $k^*((g^{(2)}))^*$ with $g^{(2)}$ varying over all $m$-tuples of elements of $\widehat{L}^{(2)}_{n,m} \cap \widehat{B}_n$, and so on. Let $\widehat{L}_{n,m} = \widehat{L}^{(1)}_{n,m} \cup \widehat{L}^{(2)}_{n,m} \cup \widehat{L}^{(3)}_{n,m} \cup \dots$, and let $\widehat{B}_{n,m}$ be the integral closure of $\widehat{A}_n$ in $\widehat{L}_{n,m}$. Now obviously:

*Remark 2.3.* $\widetilde{L}_{n,m} \subset \widehat{L}_{n,m}$ and hence $\widetilde{B}_{n,m} \subset \widehat{B}_{n,m}$.

Therefore if we conjecture that $B_n \not\subset \widehat{B}_{n,m}$ and call this the *analytic version* of the 13th problem, then clearly:

*Remark 2.4.* The analytic version for $k, n, m$ implies the preanalytic version for $k, n, m$.

By induction on $i$ we shall show that $\widehat{L}^{(i)}_{n,1} \subset \widehat{K}^{\mathrm{sol}}_n$ for all $i \geq 0$ where $\widehat{L}^{(0)}_{n,1} = \widehat{K}_n$. Obviously $\widehat{L}^{(0)}_{n,1} \subset \widehat{K}^{\mathrm{sol}}_n$. So let $i > 0$ and assume that $\widehat{L}^{(i-1)}_{n,1} \subset \widehat{K}^{\mathrm{sol}}_n$. Given any $h \in \widehat{L}^{(i)}_{n,1}$, we can find a finite sequence $r = (r_1, \dots, r_u)$ of elements in $\widehat{L}^{(i-1)}_{n,1} \cap \widehat{B}_n$ such that $h$ is algebraic over the compositum $D$ of $k^*((r_1)), \dots, k^*((r_u))$. Clearly $D$ is the quotient field of the compositum $C$ of $k^*[[r_1]], \dots, k^*[[r_u]]$, and we have $C \subset \widehat{A}_n[r]$. By the induction hypothesis $\widehat{A}_n[r] \subset \widehat{K}^{\mathrm{sol}}_n$ and hence $D \subset \widehat{K}^{\mathrm{sol}}_n$. As noted above, $k^*((r_j))^*$ is a solvable extension of $k^*((r_j))$. This being so for every $j$ we see that $D(k^*((r_1))^*, \dots, k^*((r_u))^*)$ is a solvable extension of $D$. Therefore $D(k^*((r_1))^*, \dots, k^*((r_u))^*) \subset \widehat{K}^{\mathrm{sol}}_n$ and hence $h \in \widehat{K}^{\mathrm{sol}}_n$. Consequently $\widehat{L}^{(i)}_{n,1} \subset \widehat{K}^{\mathrm{sol}}_n$. This completes the induction. Thus, in view of 2.1 and 2.3, we have proved that:

***Theorem 2.5* —** *$\widehat{L}_{n,1} \subset \widehat{K}^{sol}_n$ and hence in particular $L_{n,1} \subset \widehat{K}^{sol}_n$.*

# 3 Unsolvable coverings

Given any field $k$ and integer $n > 1$, let $A_n, B_n, K_n, L_n, k^*, \widehat{A}_n, \widehat{B}_n, \widehat{K}_n, \widehat{L}_n, \widehat{K}^{\mathrm{sol}}_n$ be as in Section 1. Let

$$F = F(Y) = Y^Q + Z_2^R Y + Z_1^S \in A_n[Y] \subset \widehat{A}_n[Y]$$

where $R$ and $S$ are positive integers and $Q > 1$ is an integer with $\mathrm{GCD}(Q-1, R) = 1$. By the calculation of the $Y$-discriminant $\mathrm{Disc}_Y(F)$ of $F$ on page 105 of [A06] we see that $\mathrm{Disc}_Y(F) \neq 0$ and hence we can talk about the Galois group $\mathrm{Gal}(F, \widehat{K}_n)$ of $F$ over $\widehat{K}_n$ as a subgroup of $\mathrm{Sym}_Q$. Let $G = \mathrm{Gal}(F, \widehat{K}_n)$.

In Example 5 of [A01] we have concluded that if char $k$ (= characteristic of $k$) is a prime number $p$, $n = 2$, $Q = p + 1$, $R = p - 1$ and $S = p + 1$, then $G$ is a large complicated subgroup of $\mathrm{Sym}_{p+1}$ because its order is divisible by $p(p + 1)$. By using the MTR (= Method of Throwing away Roots) technique of [A06] and by paraphrasing a proof given there we shall show that if $p \neq 7$ and the integers $R$ and $S$ have suitable divisibility properties then actually $G = \mathrm{PSL}(2, p)$.

Moreover we shall show that, without the above assumptions of the said Example 5, most of the time (especially when char $k$ is zero) $G$ is unsolvable.

More precisely we shall prove 3.1 to 3.5:

***Lemma 3.1*** — *$G$ is doubly transitive.*

***Lemma 3.2*** — *If char $k = p > 0$ and $Q = q + 1$ where $q > 1$ is a power of p, and in case of $p = 2$ we have $GCD(q - 1, S) = 1$ whereas in case of $p > 2$ we have $GCD(q - 1, S) = 2$, then $G = PSL(2, q)$ except that in case of $q = p = 7$ we may have $G = PSL(2, 7)$ or $A\Gamma L(1, 8)$.*

***Lemma 3.3*** — *If $Q$ is not a prime power then $G$ is unsolvable.*

***Theorem 3.4 (A form of the sextic conjecture)*** — *If $Q = 6$ then $G$ is unsolvable.*

***Corollary 3.5*** — $B_n \not\subset \widehat{K}_n^{sol}$.

To prove 3.1 we first note that obviously $F$ is an irreducible monic distinguished polynomial in $Z_1$ over $k^*[[Y, Z_2, \ldots, Z_n]]$ and hence by a Gauss Lemma type argument using the Weierstrass Preparation Theorem we see that $F$ is irreducible as a polynomial in $Y$ over $\widehat{K}_n$. Therefore $G$ is transitive. Let $V$ be the real discrete valuation of $\widehat{K}_n$ whose valuation ring is the localization of $\widehat{A}_n$ at the principal prime ideal generated by $Z_1$. Now the coefficients of $F$ have nonnegative $V$-value and by reducing them modulo the maximal ideal of the valuation ring of $V$ we get the polynomial $H = Y^Q + Z_2^R Y$. Clearly $H$ factors as $H = Y(Y^{Q-1} + Z_2^R)$ into two coprime irreducible factors over the residue field $k^*((Z_2, \ldots, Z_n))$ of $V$. Therefore by Hensel's Lemma, $F$ factors into two coprime monic irreducible polynomials of degrees 1 and $Q - 1$ in $Y$ over the $V$-completion $k^*((Z_2, \ldots, Z_n))((Z_1))$ of $\widehat{K}_n$, and hence upon letting $\beta$ to be a root of $F(Y)$ we see that $V$ has exactly two extensions $W$ and $W'$ to $\widehat{K}_n(\beta)$ and after labelling them suitably we have $W(\beta) > 0 = W'(\beta)$ and then the ramification exponents of $W$ and $W'$ are both 1 whereas their residue degrees are 1 and $Q - 1$ respectively. From this it follows that $G$ is doubly transitive, which proves 3.1.

By Burnside's Theorem (see page 89 of [A06] including footnotes 37 to 40), a doubly transitive permutation group contains a unique minimal normal subgroup, and the said subgroup is either elementary abelian or nonabelian simple; moreover, the first case occurs if and only if the unique minimal normal subgroup is regular as a permutation group; hence in the first case the degree of the group = the degree of the said subgroup = the order of the said subgroup = a prime power. Therefore 3.1 implies 3.3.

Noting that 6 is (the smallest integer which is) not a prime power, 3.3 implies 3.4. Now $\beta \in B_n$ and, taking $Q = 6$, by 3.4 we get $\beta \notin \widehat{K}_n^{\text{sol}}$, which proves 3.5.

To prove 3.2, assume that char $k = p > 0$ and $Q = q + 1$ where $q > 1$ is a power of $p$. Let $F'(Y) \in \widehat{K}_n(\beta)[Y]$ be obtained by throwing away the root $\beta$ of $F(Y)$. Then $F'(Y) = (1/Y)[F(Y + \beta) - F(\beta)] = Y^q + \beta Y^{q-1} - (Z_1^S/\beta)$. Let $\widetilde{F}(Y)$ be obtained from $F'(Y)$ by reciprocation. Then $\widetilde{F}(Y) = (-\beta/Z_1^S)Y^q F'(1/Y) = Y^q - (\beta^2/Z_1^S)Y - (\beta/Z_1^S)$. Let $\widetilde{F}'(Y) \in \widehat{K}_n(\beta,\gamma)[Y]$ be obtained by throwing away a root $\gamma$ of $\widetilde{F}(Y)$. Then $\widetilde{F}'(Y) = (1/Y)[\widetilde{F}(Y+\gamma) - \widetilde{F}(\gamma)] = Y^{q-1} - (\beta^2/Z_1^S)$. Hence if $p > 2$ and $S \equiv 0 \pmod 2$ then $\widetilde{F}'(Y) = [Y^{(q-1)/2} + (\beta/Z_1^{S/2})][Y^{(q-1)/2} - (\beta/Z_1^{S/2})]$. In view of the relations $F(\beta) = 0$ and $W(\beta) > 0$ we have $\beta = Z_1^S\tilde{\beta}$ with $W(\tilde{\beta}) = 0$. Now in view of the equation $F(\beta) = 0$ we see that $W(\tilde{\beta} + Z_2^{-R}) > 0$. Consequently in view of the equation $\widetilde{F}(\gamma) = 0$ we see that $W$ has a unique extension $U$ to $\widetilde{K}_n(\beta,\gamma)$ and for this extension the ramification exponent is 1 and the residue degree is $q$. It follows that if $p = 2$ and $\mathrm{GCD}(q-1, S) = 1$ then the polynomial $\widetilde{F}'(Y)$ is irreducible over $\widetilde{K}_n(\beta,\gamma)$, whereas if $p > 2$ and $\mathrm{GCD}(q-1, S) = 2$ then the polynomials $Y^{(q-1)/2} + (\beta/Z_1^{S/2})$ and $Y^{(q-1)/2} - (\beta/Z_1^{S/2})$ are irreducible over $\widetilde{K}_n(\beta,\gamma)$. Therefore as on page 114 of [A06], as a consequence of the Zassenhaus-Feit-Suzuki Theorem, we get 3.2.

# 4 Singleton version

Given any field $k$ and integer $n > 1$, let $A_n, B_n, K_n, L_n, k^*, \widehat{A}_n, \widehat{B}_n, \widehat{K}_n, \widehat{L}_n, \widehat{K}_n^{\text{sol}}$ and $B_{n,1}, L_{n,1}, \widehat{B}_{n,1}, \widehat{L}_{n,1}$ be as in Section 1. Let us call the assertion $B_n \not\subset \widehat{B}_{n,1}$ the *singleton version* of the 13th problem. Then by 2.5 and 3.5 we get the following:

***Theorem 4.1*** — *The singleton version is true, i.e.,* $B_n \not\subset \widehat{B}_{n,1}$. *In particular, the presingleton version is true, i.e.,* $B_n \not\subset B_{n,1}$.

# 5 Linear version

Given any field $k$ and integers $n > m \geq 1$, let $A_n, B_n, K_n, L_n, k^*, \widehat{A}_n, \widehat{B}_n, \widehat{K}_n, \widehat{L}_n$ and $B'_{n,m}, L'_{n,m}$ be as in Section 1. Let $\widehat{L}'_{n,m}$ be the compositum of $\widehat{K}_n$ and the algebraic closures $k^*((g))^*$ of $k^*((g))$ with $g$ varying over all $m$-tuples of elements of $\widehat{A}_n$ whose constant terms are zero and whose linear parts are linearly independent over $k^*$. Let $\widehat{B}'_{n,m}$ be the integral closure of $\widehat{A}_n$ in $\widehat{L}'_{n,m}$. Now obviously:

*Remark 5.1.* $L'_{n,m} \subset \widehat{L}'_{n,m}$ and hence $B'_{n,m} \subset \widehat{B}'_{n,m}$.

Therefore if we assert that $B_n \not\subset \widehat{B}'_{n,m}$ and call this the *linear version* of the 13th problem, then clearly:

*Remark 5.2.* The linear version for $k, n, m$ implies the prelinear version for $k, n, m$.

We shall now prove the following:

***Lemma 5.3*** — *Let $\Delta$ be a nonzero homogeneous polynomial of degree $e > 1$ in $Z_1, \ldots, Z_n$ with coefficients in $k^*$ such that $(0, \ldots, 0)$ is the only point in $k^{*n}$ at which $\Delta = 0 = \Delta_i$ for $1 \le i \le n$ where $\Delta_i$ is the partial derivative of $\Delta$ relative to $Z_i$. Then (I) for every set of linearly independent homogeneous linear polynomials $z_1, \ldots, z_n$ in $Z_1, \ldots, Z_n$ with coefficients in $k^*$ we have $\Delta \notin k^*[z_1, \ldots, z_{n-1}]$ (thus, in the sense of Hironaka's desingularization paper [Hir], for the singularity of the hypersurface $\Delta = 0$ at the origin we have $\nu = e$ and $\tau = n$).*

*Moreover (II) if $n > 2$ then $\Delta$ is irreducible in $k^*[Z_1, \ldots, Z_n]$. Now let $\Theta \in \widehat{A}_n$ be such that $\Theta - \Delta \in M(\widehat{A}_n)^{e+1}$ where $M(\widehat{A}_n)$ is the maximal ideal in $\widehat{A}_n$, let $d > 1$ be an integer which is nondivisible by char $k$, and let $\Theta^{1/d}$ be a dth root of $\Theta$ in $\widehat{L}_n$, i.e., an element of $\widehat{L}_n$ whose dth power is $\Theta$.*

*Then (III) assuming $n > 2$ we have $\Theta^{1/d} \notin \widehat{B}'_{n,m}$ (in particular, by taking $\Theta = \Delta = Z_1^e + \cdots + Z_n^e$ where $e > 1$ is an integer nondivisible by char $k$, we get a concrete element $\Theta \in A_n$ which has the desired properties and hence for which we have $\Theta^{1/d} \in B_n$ but $\Theta^{1/d} \notin \widehat{B}'_{n,m}$).*

In view of the last parenthetical observation, 5.3 implies the linear version for $n > 2$; for $n = 2$, the linear version follows from the singleton version proved in 4.1.

To prove (I), let $\delta$ be the expression of $\Delta$ as a polynomial in $z_1, \ldots, z_n$ with coefficients in $k^*$, and let $\delta_i$ be the partial derivative of $\delta$ with respect to $z_i$. Now the condition that $(0, \ldots, 0)$ is the only point of $k^{*n}$ at which $\Delta = 0 = \Delta_i$ for $1 \le i \le n$ is equivalent to the condition that $(0, \ldots, 0)$ is the only point of $k^{*n}$ at which $\delta = 0 = \delta_i$ for $1 \le i \le n$. If $\Delta \in k^*[z_1, \ldots, z_{n-1}]$ then we would have $\delta = 0 = \delta_i$ for $1 \le i \le n$ at $(0, \ldots, a_n)$ for every $a_n \in k^*$ which would be a contradiction. Therefore we must have $\Delta \notin k^*[z_1, \ldots, z_{n-1}]$. This proves (I).

If $\Delta = \Delta'\Delta''$ with nonconstant polynomials $\Delta'$ and $\Delta''$ then $\Delta'$ and $\Delta''$ must be homogeneous, $\Delta' = 0 = \Delta''$ for an $(n-2)$-dimensional algebraic set in $k^{*n}$, and every point of $\Delta' = 0 = \Delta''$ is singular for $\Delta = 0$. This proves (II).

To prove (III) assume that $\Theta^{1/c} \in \widehat{B}'_{n,m}$ where $c$ is a positive integer nondivisible by char $k$. Then $\Theta^{1/c}$ is separable over $\widehat{K}_n$. Therefore we can find a finite number of triples $(g^{(j)}, h^{(j)}, P^{(j)})_{1 \le j \le u}$ such that, for $1 \le j \le u$, $g^{(j)}$ is an $m$-tuple of elements of $\widehat{A}_n$ whose constant terms are zero and whose linear parts are linearly independent over $k^*$, $h^{(j)} \in k^*((g^{(j)}))^*$, and $P^{(j)} = P^{(j)}(Y)$ is a univariate monic polynomial over $k^*[[g^{(j)}]]$ whose $Y$-discriminant $\mathrm{Disc}_Y(P^{(j)})$ is a nonzero element of $k^*[[g^{(j)}]]$ and for which $P^{(j)}(h^{(j)}) = 0$, and such that $\Theta^{1/d} \in \widehat{K}_n(h^{(1)}, \dots, h^{(u)})$. Now assume that $n > 2$. Then by (II) we see that $\Theta$ is irreducible in $\widehat{A}_n$, and hence we get a real discrete valuation $\Omega$ of $\widehat{K}_n$ whose valuation ring is the localization of $\widehat{A}_n$ at the principal prime ideal generated by $\Theta$. For any $j$, by (I) we see that $\mathrm{Disc}_Y(P^{(j)})$ is nondivisible by $\Theta$ in $\widehat{A}_n$ and hence $\Omega$ is unramified in $\widehat{K}_n(h^{(j)})$. This being so for $1 \le j \le u$, we conclude that $\Omega$ is unramified in $\widehat{K}_n(h^{(1)}, \dots, h^{(u)})$. Since $\Theta^{1/d} \in \widehat{K}_n(h^{(1)}, \dots, h^{(u)})$, we must have $c = 1$. This proves (III).

As said above, as a consequence of 4.1, 5.2 and 5.3 we get:

***Theorem 5.4* —** *The linear version is true, i.e.,* $B_n \not\subset \widehat{B}'_{n,m}$. *In particular, the prelinear version is true, i.e.,* $B_n \not\subset B'_{n,m}$.

# 6 Partition version

Given any field $k$ and integers $n_1 + \cdots + n_t = n$ with $n_1 > 0, \dots, n_t > 0, t > 1$ let $A_n, B_n, K_n, L_n, k^*, \widehat{A}_n, \widehat{B}_n, \widehat{K}_n, \widehat{L}_n$ and $B''_{n_1,\dots,n_t}, L''_{n_1,\dots,n_t}$ be as in Section 1. Let $L''_{n_1,\dots,n_t}$ be the compositum of $\widehat{K}_n$ and the algebraic closures $k^*((\{Z_j : n_1+\cdots+n_{i-1} < j \le n_1+\cdots+n_i\}))^*$ of $k^*((\{Z_j : n_1+\cdots+n_{i-1} < j \le n_1+\cdots+n_i\}))$ for $1 \le i \le t$. Let $B''_{n_1,\dots,n_t}$ be the integral closure of $\widehat{A}_n$ in $L''_{n_1,\dots,n_t}$. Now obviously:

*Remark 6.1.* $L''_{n_1,\dots,n_t} \subset \widehat{L}''_{n_1,\dots,n_t}$ and hence $B''_{n_1,\dots,n_t} \subset \widehat{B}''_{n_1,\dots,n_t}$.

Therefore if we assert that $B_n \not\subset \widehat{B}''_{n_1,\dots,n_t}$ and call this the *partition version* of the 13th problem, then clearly:

*Remark 6.2.* The partition version for $k, n_1, \dots, n_t$ implies the prepartition version for $k, n_1, \dots, n_t$.

Also clearly:

*Remark 6.3.* The partition version obviously follows from the linear version 5.4.

Alternatively:

*Remark 6.4.* Upon letting $\lambda = k^*((Z_2, \dots, Z_{n-1}))^*$ and $\Lambda =$ the integral closure of $\lambda[[Z_1, Z_n]]$ in the compositum of $\lambda((Z_1))^*$, $\lambda((Z_n))^*$ and $\lambda((Z_1, Z_n))$, by the two proofs sketched in [A03] we see that for any $g(Z_1) \in \lambda[[Z_1]]$ and $h(Z_n) \in \lambda[[Z_n]]$ with $g(0) = 0 \ne g(Z_1)$ and $h(0) = 0 \ne h(Z_n)$ and any integer $E > 1$ nondivisible by char $k$ we have $[g(Z_1) + h(Z_n)]^{1/E} \notin \Lambda$. Clearly $\widehat{B}''_{n_1,\dots,n_t} \subset \Lambda$. By taking $g(Z_1) \in k[Z_1]$ and $h(Z_n) \in k[Z_n]$ (for instance $g(Z_1) = Z_1$ and $h(Z_n) = Z_n$)) we also get $[g(Z_1) + h(Z_n)]^{1/E} \in B_n$. Thus the partition version also follows from [A03].

In view of 6.2, by 6.3 or 6.4 we get:

***Theorem 6.5* —** *The partition version is true, i.e.,* $B_n \not\subset \widehat{B}''_{n_1,\dots,n_t}$. *In particular, the prepartition version is true, i.e.,* $B_n \not\subset B''_{n_1,\dots,n_t}$.

## References


[A01] S. S. Abhyankar, *On the ramification of algebraic functions*, American Journal of Mathematics, 77, 1955, 572-592

[A02] ———, *Local uniformization on algebraic surfaces over ground fields of characteristic $p \neq 0$*, Annals of Mathematics, 63, 1956, 491-526

[A03] ———, *On the compositums of algebraically closed subfields*, Proceedings of the American Mathematical Society, 7, 1956, 905-907

[A04] ———, *Coverings of algebraic curves*, American Journal of Mathematics, 79, 1957, 825-856

[A05] ———, *Resolution of Singularities of Embedded Algebraic Surfaces*, Academic Press, New York, 1966

[A06] ———, *Galois theory on the line in nonzero characteristic*, Bulletin of the American Mathematical Society, 27, 1992, 68-133

[A07] ———, *Fundamental group of the affine line in positive characteristic*, Proceedings of the 1992 Bombay International Colloquium on Geometry and Analysis held at the Tata Institute of Fundamental Research, (To Appear)

[A08] ———, *Nice equations for nice groups*, Israel Journal of Mathematics, 88, 1994, 1-24

[A09] ———, *Mathieu group coverings and linear group coverings*, Proceedings of the July 1993 AMS Conference in Seattle on "Recent Developments in the Inverse Galois Problem", (To Appear)

[A10] ———, *Again Nice equations for nice groups*, Proceedings of the American Mathematical Society, (To Appear)

[A11] ———, *More Nice equations for nice groups*, Proceedings of the American Mathematical Society, (To Appear)

[A12] ———, *Further Nice equations for nice groups*, Transactions of the American Mathematical Society, (To Appear)

[Ar] V. I. Arnold, *English Translation of Dokl. Akad. Nauk SSSR Article*, AMS Translations, 28, 1963, 51-54, 61-147

[ArS] V. I. Arnold and G. Shimura, *Superposition of algebraic functions*, Mathematical Developments Arising From Hilbert's Problems, AMS Proceedings of Symposia in Pure and Applied Mathematics, XXVIII, 1976, 45-46

[Hi1] D. Hilbert, *Mathematische Probleme*, Archiv für Mathematik und Physik, 1, 1901, 44-63 and 213-237

[Hi2] ———, *Über die Gleichung neunten Grades*, Mathematische Annalen, 97, 1927, 243-250

[Hir] H. Hironaka, *Resolution of singularities of an algebraic variety over a ground field of characteristic zero*, Annals of Mathematics, 79, 1964, 109-326

[Kol] A. N. Kolmogorov, *English Translation of Dokl. Akad. Nauk SSSR Article*, AMS Translations, 28, 1963, 55-59

[ZS1] O. Zariski and P. Samuel, *Commutative Algebra, Vol I*, Van Nostrand, Princeton, 1958

[ZS2] ————, *Commutative Algebra, Vol II*, Van Nostrand, Princeton, 1960