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 Alt_N and 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 $L_{n,m} = L_{n,m}^{(1)} \cup L_{n,m}^{(2)} \cup L_{n,m}^{(3)} \cup \ldots$, 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 $g_1, \ldots, g_m$ 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 $n_1, \ldots, n_t$ with $t > 1$, B_n is strictly bigger than the integral closure $B''_{n_1,\ldots,n_t}$ of A_n in the compositum $L''_{n_1,\ldots,n_t}$ 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 $A_n, B_n, K_n, L_n, k^*, \widehat{A}_n, \widehat{B}_n, \widehat{K}_n, \widehat{L}_n, \widehat{K}_n^{\rm sol}$ 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 $\widehat{L}_{n,m} = \widehat{L}^{(1)}_{n,m} \cup \widehat{L}^{(2)}_{n,m} \cup \widehat{L}^{(3)}_{n,m} \cup \ldots$, 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 $r = (r_1, \ldots, r_u)$ of elements in $\widehat{L}^{(i-1)}_{n,1} \cap \widehat{B}_n$ such that h is algebraic over the compositum D of $k^*((r_1)), \ldots, k^*((r_u))$. Clearly D is the quotient field of the compositum C of $k^*[[r_1]], \ldots, k^*[[r_u]]$, 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 $D(k^*((r_1))^*, \ldots, k^*((r_u))^*)$ is a solvable extension of D. Therefore $D(k^*((r_1))^*, \ldots, k^*((r_u))^*) \subset \widehat{K}^{\mathrm{sol}}_n$ 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