BULLETIN
BRAZILIAN
MATHEMATICAL
SOCIETY

Bull Braz Math Soc, New Series 33(2), 177-199

A perspective on algebraic geometry

Shreeram S. Abhyankar[1]

— Dedicated to IMPA on the occasion of its 50^{th} *anniversary*

Abstract. This article collects together material presented in various places during 1996-2001, namely Austria, Brazil, Canada, England, France, Germany, India, Israel, Italy, Japan, Oman, South Africa, Spain, and the United States of America, and includes all 13 talks given while visiting Brazil from June 17 to August 11, 2001 at the following institutions: Instituto de Matemática Pura e Aplicada (plenary talk at the 23^{o} Colóquio Brasileiro de Matemática), Pontifícia Universidade Católica do Rio de Janeiro, Universidade de Brasília, Universidade de São Paulo, Universidade Estadual de Campinas, Universidade Federal de Pernambuco, Universidade Federal do Amazonas, Universidade Federal do Ceará, Universidade Federal Fluminense, and the Fourth Meeting of the Brazilian group in Commutative Algebra and Algebraic Geometry. It is a pleasure to record that my visit to Brazil was organized by my very first Ph.D. student, Alberto Azevedo, and gave us a welcome opportunity to solidify our friendship.
In Section A we collect together six survey talks on algebraic geometry starting with a talk on its historical footsteps. Section B consists of four general talks. In Section C we collect together six talks discussing the Galois theory coming out of algebraic fundamental groups. Section D consists of four talks on ramification and resolution. Finally Section E collects ten talks which I gave at various special sessions in the meetings of the American Mathematical Society. Each section starts with a brief description of its content. In a concluding section I shall list some of the open problems mentioned in the various talks.

Keywords: discriminant, fundamental group, Galois group, projective polynomial, resultant, singularity, valuation.

Mathematical subject classification: 12F10, 14H30, 20D06, 20E22.

Received 7 May 2002.

[1]Abhyankar's work was partly supported by NSF Grant DMS 97-32592 and NSA grant MDA 904-99-1-0019.

A. Six Survey Talks

In the first "Footsteps" talk, I recount the march of algebraic geometry from India through Arabia to Europe and America, from 500 A.D. to the present time. I gave this talk at: the Mathematics History Conference in Northern Kentucky University on 14 October 2000; a Colloquium in Pennsylvania State University on 10 November 2000; the Mathematical Association of America Meeting in Indianapolis on 24 March 2001; a Colloquium in Warwick University on 1 June 2001; a Conference in Versailles University on 11 June 2001; the 23rd Brazilian Mathematical Colloquium in IMPA on 23 July 2001; and the Ruth Michler Memorial Conference in Annapolis on 25 October 2001. The second "What is Algebraic Geometry?" talk constitutes a birds-eye-view of algebraic geometry centered on polynomial equations; this was given in: Irvine in California on 18 November 1999; Pune in India on 31 December 1999; and TIFR in Bombay on 6 January 2000. In the third "What is Algorithmic?" talk, I stress the manipulative aspect of our subject. In the fourth talk on "Resultants and Discriminants," I touch upon Sylvester's 1840 method of solving two simultaneous equations. The fifth talk on "Resolution of Singularities" discusses that topic from characteristic zero to positive characteristic. In the sixth talk on "Galois Groups" I say a word about these important groups. Talks 3 to 6 constitute a packet of four survey talks which I gave at the National Security Agency on 25-26 January 1999. Talk 3 was repeated in the Pontifical Catholic University of Rio de Janeiro on 28 June 2001, and in the Campinas State University, Campinas, Brazil on 2 August 2001. Likewise Talk 6 was also given at the University of Kentucky on 4 December 1998.

1 In the footsteps of algebraic geometry

Algebraic geometry marched from India through England and Ireland to France, Germany, Italy, and the United States. The completing the square method of solving a quadratic equation was enunciated around 500 A.D. by the Indian Mathematician Shreedharacharya. A beautiful versified version of this was given by Bhaskarachrya in his Algebra book Beejganita in 1150 A.D., which he composed in Ujjain in Central India where he was the director of an ancient astronomical observatory. The Indian knowledge of algebra, traveling through Arabia and Italy, reached England around 1600 A.D. where it got a tremendous boost by Newton. Then algebraic geometry proper was perhaps started in Ireland by Salmon. Soon he was joined by the English algebraists Cayley and Sylvester. Salmon's books were translated into French and German, which nourished the algebraic geome-

ters Hermite and Halphen in France, and Klein and Noether in Germany. Then the Italian school of algebraic geometry was nurtured by Cremona, Veronese, Castelnuovo, Enriques and Severi. Finally the baton was brought to the United States by Zariski who was soon joined by Chevalley and Weil.

2 What is algebraic geometry?

A central theme in algebraic geometry consists of solving a finite number of polynomial equations in a finite number of variables. The solutions form an algebraic variety. Originally, the equations were over the field of complex numbers or more generally over a field of characteristic zero. Later on, applications to number theory led to the study of equations over modular fields, i.e., over fields of positive characteristic.

The degrees of freedom of a moving point on the variety is the dimension of the variety. A one dimensional variety is a curve and a two dimensional variety is a surface. A three dimensional variety may be called a solid. Most points of a variety are simple points. Singularities are special points, or points of multiplicity greater than one. Points of multiplicity two are double points, points of multiplicity three are triple points, and so on. A nodal point of a curve is a double point where the curve crosses itself, such as the alpha curve. A cusp is a double point where the curve has a beak. The vertex of a cone provides an example of a surface singularity. A reversible change of variables gives a birational transformation of a variety. Singularities of a variety may be resolved by birational transformations. The study of an algebraic variety is facilitated by resolving its singularities.

Every algebraic variety is birationally equivalent to a hypersurface, i.e., a variety defined by a single equation. A way of understanding an algebraic hypersurface is to find the Galois group of its defining equation. The said group is a certain group of permutations of the roots of the equation. It was introduced by Galois in the beginning of the last century. Galois classified groups as solvable or unsolvable, and showed that the Galois group of an equation is solvable if and only if the equation can be solved by radicals.

3 What is algorithmic algebraic geometry?

I reproduce below a slight variation of the first paragraph of the Preface to my 1990 book “Algebraic Geometry for Scientists and Engineers” published by the AMS.

What is (Algorithmic) Algebraic Geometry and what is the need for a series of lectures on it? First taking up the question as to what is Algebraic Geometry, long ago, to a major extent in my Father's time, and to a lesser extent in my own time, in high-school and college, we used to learn the two subjects of Analytic Geometry and Theory of Equations. Analytic Geometry consists of studying geometric figures by means of algebraic equations. Theory of Equations, or High School Algebra, was manipulative in nature and dealt with simplifying expressions, factoring polynomials, making substitutions, and solving equations. These two subjects were later synthesized into and started being collectively called Algebraic Geometry. Thus, Algebraic Geometry, at least in its classical form, is an amalgamation of Analytic Geometry and the Theory of Equations. This concrete and manipulative version of Algebraic Geometry is what I mean by Algorithmic Algebraic Geometry.

4 Resultants and discriminants

I reproduce below some lines from my 1987 paper "What is the Difference Between a Parabola and a Hyperbola" published in the Mathematical Intelligencer.

Until about thirty years ago, people used to learn in high-school and college the two subjects called Theory of Equations and Analytic Geometry. Then these two subjects gradually vanished from the syllabus. Analytic Geometry first became a chapter and then a paragraph and then finally only a footnote in books on calculus. Vis-a-vis Theory of Equations, one principal victim of this vanishing act was the resultant. At any rate, the Y-resultant Res(F,G) of two polynomials F(Y) and G(Y) is the determinant of the matrix.... This concept was introduced by Sylvester in his 1840 paper. It can be shown that F and G have a common root if and only if Res(F,G) = 0.

5 Resolution of singularities in characteristic p

I reproduce below the first paragraph of the Preface to the 1998 Edition of my book "Resolution of Singularities of Embedded Algebraic Surfaces" published by Springer. Note that a field is said to have characteristic p if in it $1+1+\cdots+1=0$ with 1 occurring p times.

The common solutions of a finite number of polynomial equations in a finite number of variables constitute an algebraic variety. The degrees of freedom of a moving point on the variety is the dimension of the variety. A one dimensional variety is a curve and a two dimensional variety is a surface. A three dimensional variety may be called a solid. Most points of a variety are simple

points. Singularities are special points, or points of multiplicity greater than one. Points of multiplicity two are double points, points of multiplicity three are triple points, and so on. A nodal point of a curve is a double point where the curve crosses itself, such as the alpha curve. A cusp is a double point where the curve has a beak. The vertex of a cone provides an example of a surface singularity. A reversible change of variables gives a birational transformation of a variety. Singularities of a variety may be resolved by birational transformations.

6 Galois groups of curves and surfaces

I reproduce below the first few lines of my 1992 paper "Galois Theory on the Line in Nonzero Characteristic" published in the Bulletin of AMS.

Originally, the equation $Y^2 + 1 = 0$ had no solution. Then the two solutions i and $-i$ were created. But there is absolutely no way to tell who is i and who is $-i$. That is Galois Theory. Thus, Galois Theory tells you how far we cannot distinguish between the roots of an equation. This is codified in the Galois Group.

B. Four General Talks

In these four general talks on algebraic geometry, I start becoming a little more technical than in the six survey talks. The seventh "Valuation" talk, given on 30 July 1999 at the Saskatoon Conference in Canada, discusses the importance of valuations for resolution of singularities. In the eighth talk on "Points at Infinity" it is shown how these points distinguish between a parabola and other other conics, and what role they play in the jacobian conjecture. This talk was given at: a Graduate Student Seminar in Purdue University on 29 March 2001; a Colloquium in Fluminense Federal University in Niteroi in Brazil on 29 June 2001; a Colloquium in University of Brasilia in Brazil on 6 July 2001; a Colloquium in Federal University of Amazon in Manaus in Brazil on 12 July 2001; a Colloquium in Federal University of Ceara in Fortaleza in Brazil on 16 July 2001; a Colloquium in Federal University of Pernambuco in Recife in Brazil on 19 July 2001; and a Colloquium in University of São Paulo in São Paulo in Brazil on 30 July 2001. In the ninth "Characteristic Sequences" talk I discuss Newton's Theorem on fractional power series expansion. This was given at: the Sultan Qaboos University in Muscat in Oman on 20 March 2000; the Angers University in France on 5 May 2000; the Paris University in France on 12 May 2000; an Affine Algebraic Geometry Conference in Oberwolfach in Germany on 17 May 2000, and the Mannheim University in Germany on 19 May 19 2000. Finally, in the tenth talk on "Jacobian," which I gave in May-June-October of 1998 at the

Universities of Paris-Cleremont-Reims in France, I discuss how the material of the fourth and fifth talks may be used in attacking the jacobian problem.

7 The role of valuation theory in resolution of singularities

The use of valuation theory in resolution of singularities was pioneered by Zariski during 1939-1944. As Zariski's pupil, I inherited this fondness for valuation theory. In my Ph.D. thesis of 1955, I heavily used valuation theory to prove resolution of singularities of algebraic surfaces over ground fields of nonzero characteristic. Later on, in 1963 and 1966, I extended the use of valuation theory to prove resolution of singularities of arithmetic surfaces and resolution of singularities of three-dimensional algebraic varieties varieties over ground field of nonzero characteristic. It is a challenge to the younger generation to extend resolution of singularities to still higher dimensions.

8 Points at infinity

The circle $X^2+Y^2=1$ has the trigonometric parametrization $X=\cos\theta$ and $Y=\sin\theta$. The substitution $\tan\frac{\theta}{2}=t$ converts this into the rational parametrization

$$X=\frac{1-t^2}{1+t^2} \quad \text{and} \quad Y=\frac{2t}{1+t^2}.$$

More generally the ellipse $\frac{X^2}{a^2}+\frac{Y^2}{b^2}=1$ has the rational parametrization

$$X=\frac{a(1-t^2)}{1+t^2} \quad \text{and} \quad Y=\frac{2bt}{1+t^2}.$$

Similarly the hyperbola $XY=1$ has the rational parametrization $X=t$ and $Y=\frac{1}{t}$. Finally the parabola $Y^2=X$ has the polynomial parametrization $X=t^2$ and $Y=t$. Thus all the conics have rational parametrizations but only the parabola has a polynomial parametrization. This is explained by the fact that the parabola has one point at infinity while the other conics have two points at infinity. Generalizing this to a higher degree plane curve $C: f(X,Y)=0$ where f is a polynomial of any degree n, it can be shown that if C has a polynomial parametrization $X=P(t)$ and $Y=Q(t)$ then C has only one point at infinity. For the converse we have to refine the idea of a point into the idea of a place and then we can say that if C has a rational parametrization and has only one place at infinity then C has a polynomial parametrization. As a corollary it can be shown that if f is a ring generator, i.e., if f and some other polynomial g

generate the polynomial ring in X and Y, then f has only one point infinity. As a related question we can ask if f is a jacobian generator, i.e., if the jacobian of f and some other polynomial g is a nonzero constant, then is it true that f has only one point at infinity? It can be shown that a positive answer to this question is equivalent to the jacobian conjecture which predicts that if the jacobian of f and g is a nonzero constant then f and g generate the polynomial ring in X and Y. It can also be shown that the jacobian conjecture is equivalent to saying that if the jacobian of f and g is a nonzero constant and m is the degree of g then either m divides n or n divides m.

9 Characteristic sequences and approximate roots

Certain exponents in Newton's fractional power series expansion lead to characteristic sequences, whose importance was recognized by Smith in 1873 and Halphen in 1884. The theory of approximate roots gives a more direct approach to similar things. A combination of both these methods provides an effective tool for studying various questions of affine algebraic geometry such as the epimorphism theorem, the automorphism theorem, and the jacobian conjecture.

To introduce characteristic sequences, given any monic irreducible polynomial $f = f(X, Y)$ of degree n in Y with coefficients in the meromorphic series field $k((X))$ over an algebraically closed ground field k, by Newton's Theorem we can write

$$f(X^n, Y) = \prod_{1 \le i \le n} [Y - z_i(X)]$$

where

$$z_i = z_i(X) = \sum_{j \in \mathbb{Z}} z_{ij} X^j \in k((X)) \quad \text{with} \quad z_{ij} \in k.$$

Let $\mathrm{Supp}_X z_i$ be the X-support of z_i, i.e., the set of all integers j for which $z_{ij} \neq 0$, and note that this is independent of i. Let $m_0 = n$. Let $m_1 < \cdots < m_h$ be the sequence of integers augumented by $m_{h+1} = \infty$ and defined by putting $m_1 = \min(\mathrm{Supp}_X z_1)$ and

$$m_i = \min(\mathrm{Supp}_X z_1 \setminus m_0\mathbb{Z} + \cdots + m_{i-1}\mathbb{Z})$$

for $2 \le i \le h+1$. Let $d_{h+2} = \infty$ and for $0 \le i \le h+1$ let $d_i = \mathrm{GCD}(m_0, \ldots, m_{i-1})$. The sequence $m = (m_i)_{0 \le i \le h+1}$ is called the newtonian sequence of characteristic exponents of f relative to n, and the sequence $d = (d_i)_{0 \le i \le h+2}$ is called the GCD-sequence of f. For $i = 0, 1, h+1$ let $q_i = m_i$ and for $2 \le i \le h$ let $q_i = m_i - m_{i-1}$. For $i = 0, h+1$ let $r_i = s_i = q_i$ and for

$1 \le i \le h$ let $s_i = q_1 d_1 + \cdots + q_i d_i$ and $r_i = s_i/d_i$. The sequence $q = (q_i)_{0 \le i \le h+1}$ is called the difference sequence of f, the sequence $s = (s_i)_{0 \le i \le h+1}$ is called the inner product sequence of f, and the sequence $r = (r_i)_{0 \le i \le h+1}$ is called the normalized inner product sequence of f.

The approximate roots of f are defined by generalizing the completing the square method of solving quadratic equations put forth by Shreedharacharya in 500 A.D., and it at once leads to the normalized inner product sequence $r = (r_i)_{0 \le i \le h+1}$ of f which generates the semigroup of f.

10 Thoughts on the jacobian

Let $F = F(X, Y)$ and $G = G(X, Y)$ be two functions of two variables X and Y, and let $H(X, Y) = J(F, G)$, $J = J_{(X,Y)}(F, G)$ be their Jacobian with respect to X and Y, i.e., $H(X, Y) = F_X G_Y - G_X F_Y$ where subscripts denote partial derivatives. In calculus we learn the Inverse Function Theorem which says that if F and G are analytic (or continuously differentiable etc.) functions with $F(0, 0) = G(0, 0) = 0 \ne H(0, 0)$ then the equations $F = G = 0$ can be locally solved near the origin, i.e., there exist analytic function $U(F, G)$ and $V(F, G)$ with $U(0, 0) = V(0, 0) = 0$ such that $X = U(F, G)$ and $Y = V(F, G)$. Now suppose we are in precalculus high-school and the only functions we know are polynomials. Then what would happen to this Inverse Function Theorem? In other words, if F and G are polynomials in X and Y, such that their Jacobian is a nonzero constant, then can we express X and Y as polynomials in F and G? Strangely the answer to this Jacobian Problem is not known. Without assuming the Jacobian to be constant, one can relate the singularity structure of the three plane curves F, G and H. For details see my books Lectures on Expansion Techniques in Algebraic Geometry (Tata Institute of Fundamental Research, 1977) and Algebraic Geometry for Scientists and Engineers, and my papers (American Mathematical Society, 1990) On the Semigroup of a Meromorphic Curve, Part I (Proceedings of the International Symposium on Algebraic Geometry, Kyoto, 1977) and Some Remarks on the Jacobian Question (Proceedings of the Indian Academy of Sciences, vol 104, 1994).

C. Six Talks on Galois Theory

In Talk 11, I sketch the state of affairs about algebraic fundamental groups over an algebraically closed ground field of positive characteristic. This talk was given at: a Conference in Oberwolfach on 18 June 1997; a Colloquium in University of Angers on 20 May 1998; and a Colloquium in University of Brasilia on 20

June 2001. In Talk 12, given at the Field Arithmetic Conference in Tel Aviv on 7 October 1997, I start considering the case when the ground field is not algebraically closed. In Talk 13, given at TIFR in Bombay on 29 December 1998 and University of Brasilia in Brazil on 27 June 2001, I discuss Galois groups of genus zero and strong genus zero coverings. In Talk 14, I propound a descent principle by which the field of definition of a covering can be decreased from a finite field to the prime field without changing the Galois group. This talk was given at: Queen Mary Colleges of London University on 10 May 1999; Imperial College of London University on 13 May 1999; and University of Cambridge on 19 May 1999. In Talk 15, given at Pennsylvania State University on 16 November 16 2000 and Palermo University in Sicily on 17 April 17 2001, I discuss the relation of permutation polynomials and symplectic group coverings. Finally, in Talk 16, I relate the pole-polar property of a circle, and more general of a hyperquadric, first to the geometry of classical groups and thence to the construction of nice equations with various finite classical groups as Galois groups. This talk was given at: Kentucky University in March 2001; Catania University in April 2001; Cambridge University on 30 May 2001; Luminy Research Institute in June 2001; Ecole Polytechnique in in June 2001; 4th ALGA in Angra dos Reis in Brazil on 7 August 2001; and the Vicente Conference in Seville in September 2001.

11 Fundamental groups and Galois theory

Now that Harbater and Raynaud, as well as Pop, Tamagawa, and others, have thrown sufficient light on the algebraic fundamental group of an affine algebraic curve over an algebraically closed ground field, it is time to start speculating about the algebraic fundamental group in some other situations. Towards this end, I shall present some raw material and pose some conjectures. As usual, let me proceed in a historical manner.

During my Ph.D. work, my guru Zariski advised me to use Chevalley's local rings to algebracize Jung's surface desingularization of 1908 for carrying it over from the complex domain to the case of positive characteristic. In my 1955 American Journal paper, I concluded that this cannot be done because in that case the algebraic local fundamental group above a normal crossing of the branch locus need not even be solvable. In my 1957 American Journal paper, by taking a section of the unsolvable surface covering, I was led to a conjecture about the structure of the algebraic fundamental group of an affine curve. After some initial work by myself, Nori and Serre, this conjecture was settled affirmatively by Raynaud and Harbater in their 1994 papers in volumes 116 and 117 of Inventiones Mathematicae. A chatty discussion of the curve case, including references, can

be found in my 1992 paper on "Galois theory on the line in nonzero characteristic" in volume 27 of the AMS Bulletin, and also in my 1996 paper on "Factorizations over finite fields" in Number 233 of the LMS Lecture Note Series. In my 1997 paper on the "Local fundamental groups of algebraic varieties" in volume 125 of AMS Proceedings, this led me to explicitize the conjectures about higher dimensional algebraic fundamental groups which were implicit in my American Journal papers of 1955 and 1959-60. I shall now briefly comment on these conjectures.

So let $N^d_{k,t}$ represent a neighborhood of a simple point on a d-dimensional algebraic variety, over an algebraically closed ground field k of characteristic p, from which we have deleted a divisor having a t-fold normal crossing at the simple point. Also let $\pi^L_A(N^d_{k,t})$ be the corresponding algebraic local fundamental group, by which we mean the set of all Galois groups of finite unramified local Galois coverings of $N^d_{k,t}$. Finally let $P_t(p)$ be the set of all finite groups G such that $G/p(G)$ is an abelian group generated by t generators; here $p(G)$ denotes the subgroup of G generated by all of its p-Sylow subgroups; in case of $p = 0$ we take $p(G) = 1$. Now we may state the:

Local conjecture. For $d \geq 2$ and $t \geq 1$ we have $\pi^L_A(N^d_{k,t}) = P_t(p)$.

Algebraically speaking, let R be the formal power series ring $k[[X_1, \ldots, X_d]]$, let I be the quotient field $k((X_1, \ldots, X_d))$ of R, let $\widehat{\Omega}$ be an algebraic closure of I, and let Ω be the set of all $J \in \widehat{\Omega}$ such that $X_1R, \ldots, X_tR$ are the only height-one primes in R which are possibly ramified in J. We may now identify $\pi^L_A(N^d_{k,t})$ with the set of all Galois groups $\mathrm{Gal}(J, I)$ with J varying in Ω.

In the 1955 paper I proved the inclusion $\pi^L_A(N^d_{k,t}) \subset N^d_{k,t}$ and by examples showed that, assuming p to be nonzero, $\pi^L_A(N^d_{k,t})$ contains unsolvable groups. By refining these examples, in the 1997 paper I showed that $\pi^L_A(N^d_{k,t})$ contains $\mathrm{GL}(m, q)$ for every integer $m > 1$ and every power $q > 1$ of p. I did this by constructing the surface $F(Y) = Y^{\langle m-1\rangle} + XY + Z$ over k, where I am using the abbreviation $\langle i\rangle = 1 + q + q^2 + \cdots + q^i$. Clearly the branch locus $Z = 0$ has a simple point at the origin, and it turns out that $\mathrm{Gal}(F, k(X, Z)) = \mathrm{Gal}(F, k((X, Z))) = \mathrm{PGL}(m, q)$. This example also supports the:

Global conjecture. For $d \geq 2$ and $t \geq 0$ we have $\pi_A(L^d_{k,t}) = P_t(p)$.

Here $L^d_{k,t}$ represents the d-dimensional affine space L^d_k over k from which we have deleted t hyperplanes $H_1, \ldots, H_t$ which together with the hyperplane at infinity have only normal crossings. This can appropriately be generalized by

replacing the hyperplanes by hypersurfaces. The above example also supports the:

Local global conjecture. For $d \geq 2$ we have $\pi_A^{LG}(L_{k,1}^d) = P_1(p)$.

Here the algebraic local-global fundamental group $\pi_A^{LG}(L_{k,1}^d)$ is defined to be the set of all Galois groups of finite unramified Galois coverings V of $L_{k,1}^d$ for which there exists an affine line L in L_k^d meeting H_1 in a point P such that the inverse images of P and H_1 on V are irreducible. This local-global conjecture is obviously stronger then the $t = 1$ cases of the above local and global conjectures as well as of the so called Abhyankar conjecture for a once punctured affine line proved by Harbater.

In a recent discussion, David Harbater has raised the question whether every member of $\pi_A^L(N_{k,t}^d)$ actually belongs to $P_t'(p)$ where $P_t'(p)$ is the set of all G in $P_t(p)$ for which $p(G)$ has an abelian supplement in G, i.e., an abelian subgroup of G which together with $p(G)$ generates G. To examine Harbater's question, I asked Gernot Stroth to make me some examples of groups in $P_t(p)$ which are not in $P_t'(p)$. Here are some of the beautiful examples produced by Stroth for $t = 3$, for which I have been scanning (so far unsuccessfully) the existence or nonexistence of suitable local coverings.

The first set of Stroth groups G are for $p = 3$, and they are $G = E * \mathrm{GL}(2, 3)$, where $*$ denotes central product, and where E is either the dihedral group D_8 of order 8 or the quaternion group Q_8 of order 8. Moreover, $\mathrm{GL}(2, 3)$ can be replaced by its flat version $\mathrm{GL}^\flat(2, 3)$ by which we mean the other group which, like $\mathrm{GL}(2, 3)$, is a nonsplit central Z_2 extension of $\mathrm{PGL}(2, 3)$. Similarly, for any prime power $q \equiv 3(4)$ of any odd prime p, we get four Stroth groups by replacing $\mathrm{GL}(2, 3)$ by the unique group H (or its "flat version" $H^\flat$) such that $\mathrm{SL}(2, q) < H < \mathrm{GL}(2, q)$ with $[H : \mathrm{SL}(2, q)] = 2$. Turning to $p = 2$, we get Stroth groups $G = F * \mathrm{GL}(3, 4)$ where F is an extra-special group of order 27, i.e., F is a nonsplit central Z_3 extension of Z_3^2 with $Z(F) = Z_3$; note that there are two versions of F, depending on whether it has only elements of order 3 (quaternion type) or also elements of order 9 (dihedral type); again, instead of $\mathrm{GL}(3, 4)$ we can take its flat version $\mathrm{GL}^\flat(3, 4)$.

12 Arithmetic monodromy versus geometric monodromy

Influenced by Mike Fried's frequent comments, I have been calculating the Galois groups of my previous nice equations over prime fields as opposed to my earlier calculations which were over algebraically closed fields. That is, in Fried's

language, I have been calculating the arithmetic monodromy groups in addition to the geometric monodromy groups. To my surprise, frequently the two groups turn out to be different.

13 Calculating Galois groups

Many old results tell us about the Galois groups of Galois extensions $k(y)/k(x)$ of pure transcendental extensions, i.e., the Galois groups of Galois coverings of the projective line by the projective line. For characteristic zero, these go back to Hurwitz and Klein in the last century. For positive characteristic, they are due to Balwant Singh and Stichtenoth-Henn around 1970. But suppose we do not require $k(y)/k(x)$ to be Galois, but look at the Galois group of the Galois closure of $k(y)/k(x)$. Then what do we get? In other words, let x be a rational function of y, i.e., let $x = g(y)/h(y)$ where $g(y)$ and $h(y)$ are coprime polynomials, and let $f(x, y) = g(y) - xh(y)$. Then how to find the Galois group $\mathrm{Gal}(f, k(x))$? Let us call such a Galois group a genus zero group, or the Galois group of a rational function. Moreover, if x is a polynomial in y, i.e., if $h(y) = 1$, then let us call $\mathrm{Gal}(f, k(x))$ a strong genus zero group or the Galois group of a polynomial. Now which finite groups are of genus zero? Amongst them which are of strong genus zero? Over a ground field k of characteristic zero? Over a ground field k of positive characteristic? Thus this is a very rich area of investigation and it is full of juicy Ph.D. problems. It gives an opportunity to learn and use basic algebraic geometry. It also gives an opportunity to learn and use the powerful tools of the modern theory of finite simple groups. In particular one learns the connection between permutation polynomials and symplectic groups.

14 Descent principle in modular Galois theory

We propound a Descent Principle by which equations over $\mathrm{GF}(q^n)(X)$ may be deformed to have incarnations over $\mathrm{GF}(q)$ without changing their Galois groups. Currently this is achieved by starting with a vectorial (= additive) q-polynomial of q-degree m with Galois group $\mathrm{GL}(m, q)$ and then, under suitable conditions, enlarging its Galois group to $\mathrm{GL}(m, q^n)$ by forming its generalized iterate relative to an auxiliary irreducible polynomial of degree n. So, alternatively, we may regard this as an Ascent Principle. In some cases the proof is based on CT (= the Classification Theorem of Finite Simple Groups) in its incarnation of CPT (= Classification of all Projectively Transitive subgroups of GL, i.e., all subgroups of GL acting transitively on nonzero vectors); this incarnation was initiated by Hering and refined by Liebeck. In some other cases the proof is based on the

the Cameron-Kantor Classification of Two-Transitive Subgroups of PGL. In yet other cases the proof uses Kantor's Theorem on groups containing a Singer cycle.

15 Symplectic groups and permutation polynomials

The linear group trinomial provides a mnemonic device for the recently discovered permutation polynomials of Müller-Cohen-Matthews, whereas the symplectic group equation generalizes them, thereby giving rise to strong genus zero coverings for characteristic two.

16 Nice equations for nice groups

Consider the following two homework problems, and show how they give rise to three ways of measuring distances and angles, and eventually to the construction of nice equations with various finite classical groups as Galois groups. The raising of a polynomial to a polynomial power may lead to bringing down the ground fields of these equations from finite fields to prime fields.

Homework problem. Draw the two tangent lines to a circle C from a point P, and let L be the line joining the two points of contact. Call L the polar of P, and P the pole of L. Show that if the polar of P passes thru a point Q then the polar of Q passes thru P.

Another homework problem. Show that in the above problem, the circle may be replaced by any conic such as an ellipse or parabola or hyperbola, or even by a quadric or a hyperquadric.

D. Four talks on ramification and resolution

These talks which I gave in Japan in February 1998 are centered around the four topics as exemplified by the titles of the talks. Talk 17 was also given at the Obergurgal Conference in Austria in September 1997. Likewise Talk 20 was also given at: Halle in Germany on 28 October 1997; Urbana in Illinois on 6 November 1997; and Paris-Marseilles-Grenoble-Angers in France on 14-19-22-30 October 1998.

17 Analytic desingularization

As witnessed by the famous works of Zariski and Hironaka, desingularization proofs tend to be very long and difficult. Recently I have found a very short

and simple proof of analytic desingularization in characteristic zero for any dimension. It is hoped that this will remove the fear of desingularization from young minds and embolden them to study it further. The said proof is extracted from my previous work on good points. It was inspired by discussions with the Control Theorist Hector Sussmann, the Subanalytic Geometer Adam Parusiński, and the Algebraic Geometer Wolfgang Seiler. Once again this illustrates the fundamental unity of all Mathematics from Control Theory to Complex Analysis to Algebra and Algebraic Geometry. Actually, this proof is a variation of the good point proof for surfaces which I gave in the Purdue Seminar of 1966, and which was expanded in my 1988 paper in the Advances In Mathematics. The conversion of the surface proof into the higher dimensional proof is based on a new avatar of an algorithmic trick employed in Item (10.24) of my 1966 book on "Resolution of Singularities of Embedded Algebraic Surfaces" published by Academic Press. The details of this new higher dimensional version of the proof can be found in the Appendix of the 1998 Second Edition of that book published by Springer-Verlag as part of their series on Monographs in Mathematics.

18 Lazy Weierstrass and lazy Newton

Weierstrass Preparation Theorem and Newton's Theorem on Fractional Power Series Expansion are two very versatile theorems linking Polynomials and Power Series. However, Newton does not work in nonzero characteristic, and Weierstrass does not work in the arithmetic case. Also it does take some refined work to prove them. So I propose their lazy versions. Being lazy, these versions work in the more general multivariate arithmetical setting. They also facilitates the cleaning up of polynomials required in extending desingularization from the characteristic zero case to the nonzero characteristic case and the arithmetic case of mixed characteristic. All this can be formalized by the concepts of polyform, characteristic data, and supermultiplicity. I shall present a philosophical discussion how these concepts might lead to an algorithmic proof of desingularization in all dimensions and all characteristics including the arithmetic case. An informal version of such a discussion, together with a large list of references, can be found in my 1990 book on "Algebraic Geometry for Scientists and Engineers" published by the American Mathematical Society as Number 35 in their Series of Mathematical Surveys and Monographs.

19 Polynomial expansion

The idea of the initial form of an element in a regular local ring can be refined by introducing the concept of its polyform. The existence of polyforms will be proved relative to any finite sequence in any (commutative unitary nonnull) ring satisfying some mild separation conditions. For uniqueness, the sequence is assumed to be regular. The concept of polyforms is expected to simplify desingularization proofs and related matters. In effect, many desingularization processes amount to finding a regular system of parameters relative to which the polyform of a given element in a regular local ring has a tight shape. One can illustrate this by revisiting desingularization of plane curves in any characteristic including mixed characteristic. What one can reprove is that given any curve on any nonsingular algebraic or arithmetic surface, by applying a finite sequence of quadratic transformations to the surface it can be achieved that the total transform of the curve has only normal crossings. This will be a simplified version of the canonical desingularization of curves described in my 1983 paper on Desingularization of Plane Curves in vol 40 of the Proceedings of Symposia in Pure Mathematics. In the future, it is hoped to use polyforms to give simplified versions of the higher dimensional canonical desingularization processes discussed in in my 1983 Springer Lecture Notes on Weighted Expansion for Canonical Desingularization and in my 1988 Advances in Mathematics paper on Good Points of a Hypersurface, and to extend them to any characteristic including mixed characteristic.

20 Higher dimensional algebraic fundamental groups

During my Ph.D. work, my guru Zariski advised me to use Chevalley's local rings to algebracize Jung's surface desingularization of 1908 for carrying it over from the complex domain to the case of positive characteristic. In my 1955 American Journal paper, I concluded that this cannot be done because in that case the algebraic local fundamental group above a normal crossing of the branch locus need not even be solvable. In my 1957 American Journal paper, by taking a section of the unsolvable surface covering, I was led to a conjecture about the structure of the algebraic fundamental group of an affine curve. After some initial work by myself, Nori and Serre, this conjecture was settled affirmatively by Raynaud and Harbater in their 1994 papers in volumes 116 and 117 of Inventiones Mathematicae. A chatty discussion of the curve case, including references, can be found in my 1992 paper on "Galois theory on the line in nonzero characteristic" in volume 27 of the AMS Bulletin, and also in my 1996 paper on "Factorizations

over finite fields" in Number 233 of the LMS Lecture Note Series. In my 1997 paper on the "Local fundamental groups of algebraic varieties" in volume 125 of AMS Proceedings, this led me to explicitize the conjectures about higher dimensional algebraic fundamental groups which were implicit in my American Journal papers of 1955 and 1959-60. Currently there is work being done on these higher dimensional conjectures.

E. Ten talks in special sessions of AMS meetings

The places and dates of the AMS Meetings where I gave these ten talks are as follows. Talk 21: Lawrenceville, Kansas, October 96. Talk 22: Chatanooga, Tennessee, October 96. Talk 23: Columbia, Missouri, November 96. Talk 24: Pretoria, South Africa, June 97. Talk 25: Louiville, Kentucky, March 98. Talk 26: San Antonio, Texas, January 99. Talk 27: Gainsville, Florida, March 99. Talk 28: Urbana, Illinois, March 99. Talk 29: Washington, DC, January 2000. Talk 30: Irvine, California, November 2001. Moreover, Talk 29 was also given at: MSRI in California in October 1999; Columbia in Missouri in October 1999; and University of Brasilia on 4 July 2001.

21 Hilbert's thirteenth problem and genus zero coverings

Hilbert's 13th problem, stated in 1900, asks if every function of n variables is composed of functions of $n-1$ variables, with expected negative answer for every $n \geq 2$. In 1927, for $n = 2$, Hilbert formulated his sextic conjecture saying 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 1955, to show that Jung's complex surface desingularization of 1908 does not carry over to nonzero characteristic, I constructed a 6 degree surface covering with nonsolvable local Galois group above a simple point of the branch locus. This surface covering solves Hilbert's sextic conjecture, and hence settles the $n = 2$ case of his 13th problem by showing that, for a field k, the algebraic closure $k(X, Y)^*$ of $k(X, Y)$ is strictly bigger than the compositum of $k(f)^*$ with f varying over all elements of $k[X, Y]$. Likewise, Galois theory and higher dimensional desingularization lead to a weak form of the 13th problem for general n, which says that $k(Z_1, \ldots, Z_n)^*$ is strictly bigger than the compositum of $k(g)^*$ as g varies over all $(n-1)$-tuples $(g_1, \ldots, g_{n-1})$ of elements of $k[Z_1, \ldots, Z_n]$ with linearly independent linear parts. In 1957, by taking a section of the said surface covering, I wrote down several families of polynomials $f(X, Y)$ giving unramified genus zero coverings of the punctured affine X-axis. As f varies over

these families, the Galois group $\mathrm{Gal}(f, k(X))$ varies over all the alternating and symmetric groups A_m and S_m where $m > 1$ is any integer, all the Mathieu groups M_{11}, M_{12}, M_{23}, M_{22} and M_{24}, and all the linear and symplectic groups $\mathrm{GL}(m, q)$, $\mathrm{SL}(m, q)$, $\mathrm{PGL}(m, q)$, $\mathrm{PSL}(m, q)$, $\mathrm{Sp}(2m, q)$ and $\mathrm{PSp}(2m, q)$, where $q > 1$ is any prime power.

22 Local fundamental groups of algebraic varieties

Now that Harbater and Raynaud have settled the Abhyankar Conjecture about the algebraic fundamental groups of algebraic curves, made in my 1957 paper, it seems worthwhile to explicitize the Local Conjecture about the local algebraic fundamental group $\pi_A^L(N_{k,t}^d)$ at a t-fold normal crossing in a d-dimensional algebraic variety V with $d \geq 2$ over an algebraically closed ground field k of characteristic $p > 0$, which was implicit in my 1955 paper. Likewise it is worthwhile to explicitize the Global Conjecture about the algebraic fundamental group $\pi_A(V - W)$ of the complement of a $(d-1)$-dimensional subvariety W of V. Assuming W to have a t-normal crossing at a simple point P of V, $\pi_A^L(N_{k,t}^d)$ is defined to be the set of all inertia groups above P in finite Galois coverings of V with branch locus at P contained in W, and the Local Conjecture predicts that if $t > 0$ then $\pi_A^L(N_{k,t}^d) = P_t(p)$ where $P_t(p)$ is the set of all (p, t)-groups, i.e., all finite groups G for which $G/p(G)$ is an abelian group generated by t generators where $p(G)$ is the subgroup of G generated by all of its p-Sylow subgroups. Likewise, $\pi_A(V - W)$ is defined to be the set of all Galois groups of finite Galois coverings of V with branch locus contained in W, and the Global Conjecture predicts that if V is the projective space and W has only normal crossings and has $t+1$ irreducible components, with $t \geq 0$, of degrees $e(1), \ldots, e(t+1)$, then $\pi_A^L(V - W) = P_t^*(p)$ where $P_t^*(p)$ is the set of all finite groups G for which $G/p(G)$ is an abelian group generated by $t+1$ generators $a_1, \ldots, a_{t+1}$ with the relation $a_1^{e(1)} \ldots a_{t+1}^{e(t+1)} = 1$; note that if $e(t+1) = 1$ then $P_t^*(p) = P_t(p)$. I have provided some evidence for these two conjectures and also for a third Local-Global Conjecture linking them.

23 Factorizations over finite fields

Partitions of roots of unity lead to factorizations of univariate polynomials over finite fields which in turn lead to certain multivariate factorizations of Generalized Artin Schreier polynomials. These and some other multivariate factorizations of Generalized Artin Schreier polynomials give rise to coverings whose Galois groups are symplectic, orthogonal and unitary groups over finite fields. They

also give rise to various PPs = Permutation Polynomials and EPs = Exceptional Polynomials. In particular, this applies to the MCM polynomials, which are the PPs and EPs in characteristic 2, recently (1993-94) discovered by Müller, Cohen and Matthews in response to the seminal paper (1993) of Fried, Guralnick and Saxl on the Carlitz Conjecture. It also applies to the LZ polynomials, which are the PPs and EPs in characteristic 3, more recently (1995) discovered by Lenstra and Zieve, again in response to the Fried-Guralnick-Saxl paper. The said factorization method rediscovers the MCM and LZ polynomials and weaves them into a common family of orthogonal group coverings which is valid in every positive characteristic. The seeds of all these factorizations can be codified into a Mantra.

Conclusion. Amazingly, most Lie Type Finite Simple Groups, as well as many PPs and EPs, are born out of polynomial solutions of Artin Schreier Type Equations.

Happy thought. Once again High-School Algebra triumphs.

24 Semilinear transformations

In previous papers, nice trinomial equations were given for unramified coverings of the once punctured affine line in nonzero characteristic p with the projective general group $\mathrm{PGL}(m, q)$ and the general linear group $\mathrm{GL}(m, q)$ as Galois groups where $m > 1$ is any integer and $q > 1$ is any power of p. These Galois groups were calculated over an algebraically closed ground field. If we calculate over the prime field, as Galois groups we get the projective general semilinear group $\mathrm{P\Gamma L}(m, q)$ and the general semilinear group $\mathrm{\Gamma L}(m, q)$. We also obtain the semilinear versions of the local coverings considered previously.

25 Analytic desingularization in characteristic zero

Recently I have found a very short and simple proof of analytic desingularization in characteristic zero for any dimension. This proof is a variation of the good point proof for surfaces which I gave in the Purdue Seminar of 1966. The conversion of the surface proof into the higher dimensional proof is based on a new avatar of an algorithmic trick employed in Item (10.24) of my 1966 book on "Resolution of Singularities of Embedded Algebraic Surfaces" published by Academic Press. The details of this new higher dimensional version of the proof

can be found in the Appendix of the 1998 Second Edition of that book published by Springer-Verlag as part of their series on Monographs in Mathematics.

26 Resolution of singularities and its history

In the last century, singularities of a plane curve $f(x, y) = 0$ were resolved by Riemann (1865), Noether (1873), and Dedekind (1882), by the methods of analysis, geometry, and algebra, respectively. In case of characteristic zero, after the pioneering work of Levi (1897), Jung (1908), Albanese (1924), and Walker (1934), singularities of a surface $g(x, y, z) = 0$ and a solid $h(x, y, z, w) = 0$ were resolved by Zariski in 1939 and 1944 respectively, and then for a higher dimensional variety by Hironaka (1964). For nonzero characteristic, I resolved surface singularities in 1955 and solid singularities in 1966. In 1963 I extended my surface proof to include arithmetical surfaces, and in 1968 I extended it further to two-dimensional excellent schemes. Seeing that not much progress in desingularization has been done in the last 30 years, Springer-Verlag has just put out a new edition of my resolution book first published in 1966. In this new edition, I have added an appendix giving a very short proof of analytic desingularization in characteristic zero for any dimension.

27 Higher dimensional algebraic fundamental groups

Let $\pi_A^L(N_{k,t}^d)$ be the algebraic local fundamental group above a t-fold normal crossing of the branch locus at a simple point of a d-dimensional algebraic variety over an algebraically closed field k of characteristic p, with $t \geq 1$ and $d \geq 2$. Implicitly in Amer Jour of 1955 and explicitly in Proc AMS of 1997, I conjectured that $\pi_A^L(N_{k,t}^d) = P_t(p)$, where $P_t(p)$ is the set of all finite groups G for which $G/p(G)$ is abelian on t generators. Harbater has asked if $\pi_A^L(N_{k,t}^d) \subset P_t'(p)$, where $P_t'(p)$ is the set of those G in $P_t(p)$ for which $p(G)$ has an abelian supplement. For $t = 3$, Stroth has constructed groups S in $P_t(p) \setminus P_t'(p)$, and I have been scanning whether they belong to $\pi_A^L(N_{k,t}^d)$. For any prime power $q \equiv 3(4)$ of any odd prime p we get four Stroth groups $S = E * L =$ the central product of E and L, where $E = D_8$ (dihedral) or Q_8 (quaternion), and $L = H$ with $\mathrm{SL}(2, q) < H < \mathrm{GL}(2, q)$ with $[H : \mathrm{SL}(2, q)] = 2$ or $L = H^\flat =$ the other nonsplit central Z_2 extension of $H/Z(H)$; note that if $q = 3$ then $H = \mathrm{GL}(2, 3)$. For $q = p = 2$ take $E =$ extra-special group of order 27 (two choices), and $L = \mathrm{GL}(3, 4)$ or $\mathrm{GL}^\flat(3, 4)$.

28 Galois embedding for linear groups

A GEP (= Galois Embedding Problem) is a (finite) Galois extension M/K together with an epimorphism $u : G \to H$ of finite groups and an isomorphism $r : H \to \mathrm{Gal}(M, K)$. A solution of this GEP is a Galois extension L/K together with an isomorphism $v : G \to \mathrm{Gal}(L, K)$ such that L is an overfield of M and $ru = vs$ where $s : \mathrm{Gal}(L, K) \to \mathrm{Gal}(M, K)$ is the Galois theoretic epimorphism. Let $m > 0$ be an integer, let $q > 1$ be a power of a prime p, let K be any overfield of $\mathrm{GF}(q)$, and for every integer $i \geq -1$ let $\langle i \rangle = 1+q+q^2+\cdots+q^i$. A separable monic projective q-polynomial of q-prodegree m over K is a polynomial of the form $f(Y) = Y^{\langle m \rangle} + \sum_{i=1}^{m} a_i Y^{\langle m-1-i \rangle}$ with $a_i \in K$ and $a_m \neq 0$. Assume that m is divisible by $q-1$, and consider the GEP given by a Galois extension M/K together with the canonical epimorphism $u : \mathrm{GL}(m, q) \to \mathrm{PGL}(m, q)$ and an isomorphism $r : \mathrm{PGL}(m, q) \to \mathrm{Gal}(M, K)$. Recently I have proved the Embedding Criterion which says that: this GEP has a solution if and only if M/K is the splitting field of a separable monic projective q-polynomial of q-prodegree m over K.

29 Desingularization and modular Galois descent

In my 1955 Ph.D. Thesis, following my Guru Zariski's advice, I used Chevalley's Local Rings to analyze Jung's 1908 method of desingularization, which led me to study the local algebraic fundamental group at a normal crossing. For algebraically closed ground fields, I have discussed this in AMS Abstract Nos 915-14-26 and 940-14-28 in vol 17 (1996) p 536 and vol 20 (1999) p 253. Now the case of finite ground fields leads me to calculate the Galois group $\mathrm{Gal}(E^{[s]}, K)$ of the generalized s-th iterate $E^{[s]}$ of the generic vectorial q-polynomial

$$E = Y^{q^m} + \sum_{1 \leq i \leq m} X_i Y^{q^{m-i}} \quad \text{over} \quad K = k(X_1, \ldots, X_m)$$

with indeterminates $X_1, \ldots, X_m$ over field $k \supset \mathrm{GF}(q)$, where $q = p^u$ with positive integers m, n, u, and

$$s = \sum_{0 \leq i \leq n} s_i T^i \quad \text{with} \quad s_i \in \mathrm{GF}(q) \quad \text{and} \quad s_n \neq 0$$

is irreducible in $\mathrm{GF}(q)[T]$. By definition $E^{[s]}(Y) = \sum_{0 \leq i \leq n} s_i E^{[[i]]}(Y)$ where

$$E^{[[i]]}(Y) = E(E^{[[i-1]]}(Y)) \quad \text{with} \quad E^{[[0]]}(Y) = Y.$$

I conjecture that then $\mathrm{Gal}(E^{[s]}, K) = \mathrm{GL}(m, q^n)$. For $m = 1$ this was proved by Carlitz in 1938. In March 1999, by using CT = Classification Theorem of finite simple groups, jointly with Sundaram, I proved this when m is square-free with $\mathrm{GCD}(m, n) = 1$ and $\mathrm{GCD}(mnu, 2p) = 1$. Now I can prove it when the last hypothesis is replaced by the weaker hypothesis that $\mathrm{GCD}(mnu, p) = 1$. I can also prove the conjecture for the easy case when $m = n = 2$. By putting $X_1 = \cdots = X_{m-2} = 0$ in E we get the trinomial $E^\dagger = Y^{q^m} + XY^q + ZY$ over $K^\dagger = k(X, Z)$ where $(X, Z) = (X_{m-1}, X_m)$ with $m > 1$. The above conjecture can be strengthened by asking if for the s-th iterate $E^{\dagger[s]}$ of the trinomial $E^\dagger$ we still have $\mathrm{Gal}(E^{\dagger[s]}, K^\dagger) = \mathrm{GL}(m, q^n)$. I can prove this stronger version to be true when m is prime with $\mathrm{GCD}(m, n) = 1$ and $\mathrm{GCD}(mnu, p) = 1$. Previously I had shown that for the said trinomial we have $\mathrm{Gal}(E^\dagger, K^\dagger) = \mathrm{GL}(m, q)$ when we continue to assume $k \supset \mathrm{GF}(q)$, but over the prime field we have $\mathrm{Gal}(E^\dagger, \mathrm{GF}(p)(X, Z)) = \Gamma\mathrm{L}(m, q)$; see PAMS vol 125 (1997) p 1643 and PAMS vol 127 (1999) p 2511. The descent via generalized iteration mitigates this bloating towards semilinearity. Alternatively we may think of this as ascent from $\mathrm{GL}(m, q)$ to $\mathrm{GL}(m, q^n)$. It is hoped that similar descent or ascent should work for other Lie Type finite groups. A better understanding of modular Galois Theory should be quite useful for analyzing singularities.

30 Sufficiency of projective polynomials

Let $m > 1$ be an integer, let $q > 1$ be a power of a prime p, and let K be an overfield of $\mathrm{GF}(q)$. By a monic separable vectorial q-polynomial of q-degree m over K we mean a polynomial of the form

$$E(Y) = Y^{q^m} + \sum_{1 \le i \le m} a_i Y^{q^{m-i}} \quad \text{with} \quad a_i \in K \quad \text{and} \quad a_m \neq 0.$$

By a monic separable projective q-polynomial of q-prodegree m over K we mean a polynomial of the form

$$F(Y) = Y^{\langle m-1 \rangle} + \sum_{1 \le i \le m} b_i Y^{\langle m-1-i \rangle} \quad \text{with} \quad b_i \in K \quad \text{and} \quad b_m \neq 0,$$

where $\langle i \rangle = 1 + q + \cdots + q^i$. It is well known that in a natural manner $\mathrm{Gal}(E, K)$ and $\mathrm{Gal}(F, K)$ are subgroups of $\mathrm{GL}(m, q)$ and $\mathrm{PGL}(m, q)$ respectively. In Trans AMS, 352 (2000), 3881-3912, I proved the converse of the first statement by showing that if L/K is a Galois extension whose Galois group is abstractly isomorphic to a subgroup of $\mathrm{GL}(m, q)$ then L is the splitting field of some

monic separable vectorial q-polynomial of q-degree m over K. Now from this I deduce a partial converse of the second statement by showing that if k is an algebraically closed field of characteristic p and $M/k(X)$ is a Galois extension whose Galois group is abstractly isomorphic to a subgroup of $\mathrm{PGL}(m, q)$ then M is the splitting field of some monic separable vectorial q-polynomial of q-degree m over $k(X)$. This deduction follows from a result which was recently proved by Harbater, Haran, Jarden, Pop, and Voelklein, and which says that every embedding problem over $k(X)$ can be solved. Actually I do not need this full embedding result, which is paraphrased by saying that $k(X)$ is omega-free, but only the projectivity of the absolute Galois group of $k(x)$ which comes out of standard material from Galois cohomology.

Some Open Problems

Let us pull together some of the open problems scattered throughout the paper.

Resolution of singularities. An algebraic variety consists of the common solutions of a finite number of polynomial equations in a finite number of variables. A correspondence between two varieties is birational means the defining equations are rational both ways. The resolution problem asks if a variety can be birationally transformed into a variety having no singular points. This has been done for dimension up to three and any characteristic, and also for any dimension and zero characteristic. The problem is to do it for any dimension and any characteristic. By letting the coefficients of the equations to be integers we get arithmetical varieties and their resolution problem. This has been done only for dimensions one and two.

Jacobian conjecture. Given a finite number of polynomial functions in the same number of variables, whose jacobian is a nonzero constant, the Jacobian Conjecture asks if the inverse functions are necessarily polynomials. In spite of hundreds of papers written on this subject, we do not know the answer even for two polynomials in two variables. Here the coefficient field is assumed to be of characteristic zero.

Explicit Galois theory. We want to show that any nice finite group can be realized as the Galois group of a nice equation. For instance, for any integer $m > 1$ and any power $q > 1$ of any prime p, the nice trinomial $Y^{1+q+\cdots+q^{m-1}} + XY + Z$ has the projective linear group $\mathrm{PGL}(m, q)$ as its Galois group over $\mathrm{GF}(q)(X, Z)$.

Similar things have been done for several other groups. However many other groups remain. There is also the question of the ground field. For example, when calculated over $\mathrm{GF}(p)(X, Z)$, the Galois group of the above trinomial gets enlarged to the projective semilinear group $\mathrm{P\Gamma L}(m, q)$. This can sometimes be mitigated by using generalized iterates which are formed by taking suitable linear combinations of usual iterates. The validity of the generalized iteration method needs to be extended to wider ranging situations. To state a specific open problem in this direction, let E be the vectoral version of the above trinomial, i.e., $E = Y^{q^m} + XY^q + ZY$. Also let

$$s = \sum_{0 \le i \le n} s_i T^i \quad \text{with} \quad s_i \in \mathrm{GF}(q) \quad \text{and} \quad s_n \neq 0$$

be irreducible in $\mathrm{GF}(q)[T]$ where n is any positive integer. Consider the generalized s-th iterate

$$E^{[s]} = \sum_{0 \le i \le n} s_i E^{[[i]]}$$

where the ordinary i-th iterate $E^{[[i]]}$ is defined by $E^{[[0]]} = Y$ and $E^{[[i]]} = E(E^{[[i-1]]})$. Then for what values of m and n (may be all?) is the Galois group of $E^{[s]}$ over $\mathrm{GF}(q)(X, Z)$ isomorphic to $\mathrm{GL}(m, q^n)$?

Shreeram S. Abhyankar
Mathematics Department
Purdue University
West Lafayette, IN 47907
USA

E-mail: ram@cs.purdue.edu